UNIVERZITET U NOVOM SADU
INSTITUT ZA MATEMATIKU


**Milan Z. Grulović**

# OSNOVI TEORIJE GRUPA

**Novi Sad 1997.**

UNIVERZITET U NOVOM SADU
INSTITUT ZA MATEMATIKU

Milan Z. Grulović

# OSNOVI TEORIJE GRUPA

1997

*Autor:* Dr Milan Z. Grulović, vanredni profesor Prirodno-matematičkog fakulteta u Novom Sadu

*Recenzenti:* Dr Stojan Bogdanović, redovni profesor Ekonomskog fakulteta u Nišu
Dr Žarko Mijajlović, redovni profesor Matematičkog fakulteta u Beogradu

*Izdavač:* Institut za matematiku u Novom Sadu

*Štampanje ove publikacije finansijski je pomoglo:*
Ministarstvo za nauku i tehnologiju Republike Srbije

ŠTAMPA:

felton, d.o.o.
Novi Sad, Trg Dositeja Obradovića 6
Tel./Faks: 021/54-245

CIP – Каталогизација у публикацији
Библиотека Матице српске, Нови Сад

512.54(075.8)

GRULOVIĆ, Milan Z.
Osnovi teorije grupa / Milan Z. Grulović. - Novi Sad : Institut za matematiku, 1997 (Novi Sad : Feljton). - VIII, 670 str. ; 24 sm. - Institut za matematiku

Bibliografija: str. 639-649. - Registar

a) Teorija grupa

0



# Predgovor

Teorija grupa je, može se slobodno reći, najstarija grana moderne algebre. Ponikla iz teorije o rešavanju algebarskih jednačina pomoću radikala njene korene nalazimo u radovima Josepha Louis Lagrangea (1736 - 1813), Augustin Louis Cauchya (1789 - 1857), Paulo Ruffinija (1765 - 1822), Henrika Abela (1802 - 1829) i, posebno, Evariste Galois (1811 - 1832), koji je i uveo termine *grupa, prosta grupa, potpuno invarijantna podgrupa* i u okviru svoje čuvene teorije prvi došao do konačnih polja. S obzirom na to svoje poreklo (u pitanju su bile grupe permutacija promenljivih ili nula polinoma), kroz gotovo celi devetnaesti vek prvenstveno su se razmatrale konačne grupe permutacija (što je ostavilo traga i na leksiku, danas već arhaičnu i pomalo zaboravljenu; videti npr. [22]). No, brzo se došlo do spoznaje da su esencijalni problemi koji su bili razmatrani unutar ovih grupa nezavisni od prirode elemenata, drugim rečima, težište je trebalo staviti na svojstva algebarske operacije. Otuda i poznata formulacija Arthura Cayleya (1821 - 1895), u čijim se radovima po prvi put prepoznaju postulati teorije grupa: *A group is defined by means of the laws of combinations of its symbols.* Ovo je rezultiralo postavljanjem teorije grupa na prave osnove i olakšalo i ubrzalo njen napredak. Uzgred rečeno, do Cayleyevog uvodjenja koncepta abstraktne grupe (1854), teorija grupa se zvala "teorija supstitucija". Ovaj koncept je, svejedno, široko prihvaćen tek pošto je Walther von Dyck (1856 - 1934) uveo prezentaciju grupa.

Kraj devetnaestog i prve decenije dvadesetog veka su bili zlatno doba teorije konačnih grupa zahvaljujući u prvom redu radovima Ludwiga Sylowa (1832 - 1918), Georgea Frobeniusa (1849 - 1917), Williama Burnsidea (1852 - 1927), Otto Ludwiga Höldera (1859 - 1937), Issai Schura (1875 - 1914). U knjizi o grupama Camillea Jordana (1838 - 1922) (koji je, inače, definisao *faktor grupe* i *izomorfnost grupa*): *Traité des substitutions et des équations algebraiques*, Paris, 1870., već se nazire problematika beskonačnih grupa i prezentacija grupa. Ujedno, ona je bila i spomenik besmrtnom delu E. Galois, nastradalog u dvoboju pre nego što je napunio dvadesetprvu godinu. Razvoj teorije beskonačnih grupa u prvi mah su inicirali zahtevi geometrije i topologije. Od posebnog uticaja su u tom smislu bili radovi Sophusa Liea (1842 - 1899), tvorca teorije neprekidnih grupa, Felixa Kleina (1849 - 1925), Henrica Poincaréa (1854 - 1912), Nielsa Nielsena (1865 - 1931), Maxa Dehna (1878 - 1952) i Heinricha Tietzea (1880 - 1964). Rečenica iz pristupne besede (*de facto* vrste ispita) za profesora na Univerzitetu u Erlangenu (poznatoj kao Erlanger Programm) F. Kleina, kojom se želi obuhvatiti sva raznovrsnost geometrije, pa time i ukazati na njene dalje moguće puteve, glasi: *Data je jedna mnogostrukost i jedna grupa transformacija te mnogostrukosti; razviti teoriju*

*invarijanata koja se odnosi na tu grupu* (citat je preuzet iz knjige Erika Templa Bella: *Matematika, kraljica i ropkinja nauke*, "Vuk Karadžić", Beograd, 1967). Prvi pregled elemenata teorije grupa bez uslovljavanja konačnosti redova dat je u knjizi: *Абстрактная теория групп*, Москва, 1916., Отто Юльевича Шмидта (1891 - 1956), utemeljivača sovjetske teoretsko-grupovne škole, po mnogo čemu rodonačelnika teorije beskonačnih grupa i jednog od njenih glavnih predvodnika sve do pojave "grupističke" škole Александра Геннадиевича Куроша (1908 - 1971). Brzom i svestranom razvoju teorije grupa u dvadesetom veku vidan doprinos su dali (uz već pomenute) brojni matematičari: Heinz Prüfer (1896 - 1934), Otto Schreier (1901 - 1929), Петр Сергеевич Новиков (1901 - 1975), Richard Dagobert Brauer (1901 - 1977), Reinhold Baer (1902 - 1979), Philip Hall (1904 - 1982), Leo Zippin (1905 - ), Wilhelm Magnus (1907 - 1990), Лев Семенович Понтрягин (1908 - 1988), Анатолий Иванович Мальцев (1909 - 1967), Helmut Wielandt (1910 - 1984), Marshall Hall, Jr. (1910 - 1990), Сергей Николаевич Черников (1912 - 1987), Hans Julius Zassenhaus (1912 - 1991), Bernhard H. Neumann, Hanna Neumann (1914 - 1971), Tibor Szele (1918 - 1955), H. Ulm, Л. Куликов, László Fuchs (1924 - ), Jean-Pierre Serre (1926 - ), Михаил Иванович Каргаполов (1928 - 1976), Walter Feit (1930 - ), Сергей Иванович Адян (1931 - ), Griggs John Thompson (1932 - ) i mnogi, mnogi drugi.

Teorija grupa je danas toliko raznovrsna i isprepletena sa brojnim drugim algebarskim, i ne samo algebarskim, disciplinama da je i nemoguće dati iole obuhvatniji pregled svih njenih dostignuća ili problematike. Mnogi problemi na čijim rešenjima su radile plejade matematičara kroz mnoge godine pa i decenije, definitivno su rešeni: ustanovljeno je da su sve grupe neparnog reda rešive ([46]); izvršena je klasifikacija raznih familija grupa, pominjem samo, svih konačnih prostih grupa – videti [7], [55]; negativan odgovor su dobili čuveni Burnsideovi problemi s početka veka, tzv. opšti i ograničeni: klasa lokalno konačnih grupa je prava podklasa klase periodičnih grupa ([54]), grupa konačnog eksponenta i konačno generisana nije nužno konačna ([127]), dok je treći problem (na tu temu) – oslabljeni, rešen delimično i to sa afirmativnim odgovorom: konačnih grupa sa konačnim fiksnim brojem generatora i fiksnim eksponentom koji je prost broj ima konačno mnogo ([84]); jednim (kontra)primerom А. Ю. Ольшанск-ог ([128]) negativno je odgovoreno na Шмидт-ov problem, "problem maksimalnosti" (R. Baer) i "problem minimalnosti" (С. Н. Черников), i opet prva dva problema Burnsidea: Prüferove grupe nisu jedine beskonačne grupe čije su sve prave podgrupe konačne (Prüferove grupe ostaju jedine takve u klasi lokalno konačnih grupa – [77]), grupa koja ispunjava uslov maksimalnosti podgrupa nije nužno ekstenzija policiklične grupe konačnom grupom, grupa koja ispunjava uslov minimalnosti podgrupa nije nužno grupa Черникова (ali jeste ako je i lokalno konačna – [159]); rešen je (negativno) problem reči: postoje grupe sa konačnom prezentacijom i neodlučivim problemom reči i konjugovanosti, itd. itd.).



Neki problemi su, opet, tek parcijalno načeti i još uvek čekaju na potpun odgovor, a u međuvremenu iskrsavaju sve novi i novi, interesantni bilo sami po sebi bilo zbog njihove povezanosti i značaja za druge teorije. Rešenja su vrlo često dobijena ili se pak moraju tražiti van same teorije grupa, dakle u multidisciplinarnim oblastima. Na kraju, ne treba zaboraviti ni na veliki uzajamni uticaj teorije grupa i mnogih nematematičkih teorija: kristalografije, spektroskopije, kvantne mehanike, kvantne teorije polja. Sve ovo je čini izuzetno atraktivnom disciplinom, što i rezultira "upošljavanjem" brojnih matematičkih poslenika širom sveta u "njenu firmu".

Ova knjiga je pisana za studente matematike redovnih i prvih godina poslediplomskih studija, ali je napisana tako da je mogu koristiti, u meri i obimu u kojim ih već interesuje teorija grupa, i studenti tehničkih fakulteta i đaci matematičkih gimnazija. Ovim pre svega želim reći da se nisam koristio jezikom i rezultatima teorije kategorija i univerzalne algebre. Time su, naravno, mnogi rezultati izgubili od svoje opštosti i mnogi dokazi u eleganciji, a sam tekst u savremenosti, ali je ujedno predznanje potrebno za njegovo čitanje svedeno na minimum. Zapravo, potrebno je znanje elemenata (linearne) algebre i teorije skupova (matematičke logike) koje se stiče na uvodnim kursevima, s tim što sam i sâm zbog čitaočevog komfora tu i tamo ponovio neke osnovne stvari iz tih predmeta. Kad su skupovi u pitanju, u osnovi su prvih par rezultata kardinalne aritmetike, Zornova lema i transfinitna indukcija. Koristio sam von Neumannovu definiciju ordinala; dakle, ordinal je tranzitivan skup dobro uređen relacijom pripadanja (iz čega proizilazi da je svaki ordinal skup ordinala manjih od njega – tako je nula, najmanji ordinal, prazan skup, $10 = \{0, 1, \ldots, 9\}$, skup prirodnih brojeva $\omega = \{0, 1, \ldots, n, \ldots\}$), a kardinali su ordinali koji se ne mogu injektivno preslikati na neki svoj početni segment; videti, recimo, [86], [163].

Knjiga je podeljena u četiri poglavlja i šezdeset paragrafa. Gledano sa aspekta nastave predviđena je za dvosemestarski kurs, s tim što bi se u prvom delu obradila prva i po izboru neka od preostale tri glave. Umesto predgovora svakoj glavi ovde ću u par reči izneti njihov sadržaj.

Prva je, kao što joj i samo ime kaže, opšteg karaktera i najvećim svojim delom je predsprema za druga poglavlja. U njoj se, pored upoznavanja sa osnovnim pojmovima, daju rezultati koji važe za klasu svih grupa (npr. teoreme o izomorfizmu, neki rezultati o mrežama podgrupa), opisuju pojedine klase grupa ili podgrupa (ciklične grupe, grupe permutacija, grupe Hamiltona, neke familije prostih grupa, izvodne podgrupe, podgrupe Sylowa) kao i konstrukcije kojima se od datih familija grupa dobijaju nove grupe ili koje objašnjavaju strukturne veze grupe i njenih podgrupa. Poseban paragraf je posvećen Курош-evoj teoremi o uslovu za egzistenciju centralno izomorfnih produženja ma koje dve dekompozicije grupe.

Preostala tri poglavlja su u velikoj meri međusobno nezavisna i kao takva

mogu se čitati proizvoljnim redom.

Druga glava se odnosi na kombinatornu teoriju grupa (kombinatornu u smislu da su joj kombinatorne metode jedno od osnovnih oruđa, no postoji i tesna sprega teorije grupa sa pojedinim oblastima diskretne matematike, u prvom redu teorijom grafova – videti, recimo, [29]; o tome ovde neće biti reči). Pored elemenata prezentacije grupa i Tietzeovih transformacija i osnovnih osobina slobodnih i generalno slobodnih proizvoda, kao i slobodnih grupa (koje su samo specijalan slučaj slobodnih proizvoda), date su i dve najvažnije, kada su u pitanju slobodni proizvodi, teoreme: teorema Kuroša o podgrupama slobodnih proizvoda i Грушко-Neumannova teorema o tzv. minimalnim sistemima konačno generisanih slobodnih proizvoda. Tu se mogu naći i prvi rezultati koji se tiču varijeteta i utapanja grupa, pa s time u vezi i prve informacije o nekim posebnim grupama (deljivim, $\aleph_\alpha$-univezalnim, algebarski zatvorenim), odnosno o kardinalnosti nekih familija (neizomorfnih) grupa.

U trećoj glavi su "na delu" Abelove grupe. Prezentirani su klasifikacije i fundamentalna svojstva pojedinih familija Abelovih grupa (konačno generisanih, deljivih, Arhimedovih linearno uređenih, lokalno cikličnih, konačno kogenerisanih), potrebni i dovoljni uslovi da bi (Abelova) grupa bila direktna suma cikličnih grupa (kriterijum Куликова, teoreme Prüfera), kao i osnovne osobine potpunih (izolovanih) podgrupa, algebarski kompaktnih grupa, bazičnih podgrupa $p$-grupa, $p$-grupa bez elemenata beskonačne visine, kompletno razloživih i mešovitih grupa. Teorema H. Ulma za prebrojive reducirane $p$-grupe, koja u kombinaciji sa teoremama H. Prüfera i L. Zippina omogućuje potpunu klasifikaciju prebrojivih reduciranih $p$-grupa, obično se navodi kao jedan od prvih "netrivijalnijih" primera *algebarskih strukturnih teorema* (koje su, u osnovi, "dobre" karakterizacije datih klasa algebri), rezultata koji su sastavni deo tzv. *stability theory*, danas izuzetno atraktivne discipline teorije modela.

U četvrtoj glavi se ispituju familije grupa sa posebnim sistemima podgrupa. U prvom planu su klase nilpotentnih i rešivih grupa i oko njih se manje-više sve vrti. Ostale su (koje pominjemo) ili ekstenzije ovih klasa (generalno nilpotentne i generalno rešive grupe, lokalno nilpotentne i lokalno rešive grupe) ili podklase neke od njih ($N$-grupe, superrešive, policikличne) ili pak klase koje imaju "dodirnih tačaka" sa nilpotentnim i rešivim grupama ($M$-grupe) ili, konačno, one koje su na "suprotnom kraju" od rešivih grupa (konačne poluproste grupe). Paragraf "Lokalne teoreme" je baziran na radovima Мальцева [104] i [107]. Prvi je, citiramo knjigu [78], *ubacio "i" u frazu "lokalne teoreme algebre i logike"* i ujedno je polazna tačka teorije modela, a drugi je razradio detalje i "zaokružio priču".

I nekoliko opštih napomena. Priloženi materijal je lični izbor, moje viđenje onoga što bi trebalo da sadrže prvi kursevi iz teorije grupa, dok se ne krene



u specijalizaciju ili ne ovlada dovoljno i drugim oblastima algebre, neophodnim za dalji rad u teoriji grupa (tu sam vidljivo pod uticajem monografije [92]). Tekst je uglavnom baziran na sledećim knjigama (monografijama i udžbenicima): [67], [78], [96], [97], [101], [141], [142], [146], [149] i, posebno, [50], [92] i [140]. Spisak literarure ukazuje na izvore koje sam koristio, citirao ili koje jednostavno preporučujem za dalje čitanje (bilo kao dopunu ovog gradiva bilo radi upoznavanja sa temama koje ili uopšte nisu obrađivane ili su tek uzgred spomenute). Nastojao sam da tekst bude koherentan, te da dokazi tvrđenja ne izlaze van okvira knjige, tj. da se zasnivaju samo na raspoloživim argumentima. Svi su rezultati, sem nekoliko izuzetaka, u potpunosti obrazloženi, s tim što u nekim slučajevima, upravo zbog navedenog zahteva, nisu predočena i druga, kraća i elegantnija rešenja koja bi, međutim, zahtevala ili dosta dodatnog "materijala" ili prihvatanje nekih činjenica "zdravo za gotovo". Sigurno će biti čitalaca koji će smatrati da su pojedini (ili mnogi) dokazi dati s više detalja nego što je možda potrebno ili pak s odviše formalizma. Kao opravdanje navodim činjenicu da veliki deo ovog gradiva ne stiže do studenata kroz redovnu nastavu, pa ovakvo pisanje treba, po mom mišljenju, da im olakša rad. Primeri imaju ulogu vežbi, iako su i oni dati sa dokazima. Ali oni nisu tu samo da ilustruju; često se na njih oslanja kasnija građa i stoga ih ne treba "preskakati" u čitanju.

Notacija je manje-više uobičajena, no kako ona zna da varira od knjige do knjige, treba konsultovati spisak sa kraja, ukoliko se tekst ne čita od početka ili ne redom. U mnogim slučajevima sam naveo više oznaka za isti pojam, da bih se onda opredelio za jednu od njih. Opet, nisam imao uvek na raspolaganju sve standardne oznake, recimo za spletene (venačne) proizvode. Funkcije sam pisao zdesna, jer smatram da takav zapis ima svojih prednosti (barem više od mana); doduše, ređe se koristi, ali ga imamo i u, recimo, [67], [140]. Krajevi dokaza (poslednjih tačaka) teorema, s jedne strane, i lema, korolara, primera i stavova, s druge, obeleženi su, respektivno, sa ■ i □. Upotrebljavam različite oznake za teoreme i leme (stavove), jer se koji put u okviru dokaza teoreme javljaju leme (stavovi) sa svojim dokazima. Sva tvrđenja i definicije su numerisani sa dva broja; prvi ukazuje na paragraf u kome se tvrđenje ili definicija nalaze, drugi na njegovo ili njeno mesto u paragrafu. Inače, brojanje u paragrafu ide redom, a ne posebno po teoremama, lemama itd.

Poseban problem je sa prevodom matematičkih termina. Naime, dosta njih se po prvi put javlja u našoj matematičkoj literaturi, pa sam često uz prvo pojavljivanje takvih termina naznačavao i njihova "strana imena", obično engleska. S druge strane, zadržao sam, recimo, neprevedeno *koset* (eng. *coset*, što, pretpostavljam, po analogiji sa nemačkom, francuskom i ruskom verzijom, dolazi od *co*mpanion *set*), dok se kod nas koristi *suskup*, odnosno *razred* ili *klasa* ([16], [90], [155]). Imena stranih matematičara koja se pišu latinično zadržana su kroz ceo tekst u originalu; jer, dok se izgovor nekih može (relativno dobro) "registrovati" (npr. Cayley – Kejli, Schreier – Šrajer, Sylow – Silov

itd.) ili pak postoji pravopisni dogovor oko zapisa (Galois – Galoa), u dosta slučajeva nemamo adekvatan zapis (Burnside, Hölder, Prüfer). Imena ruskih matematičara su data u originalu samo u predgovoru i bibliografiji.

Kao student sticao sam znanja iz teorije grupa kod izvanrednih profesora, akademikâ široke matematičke i opšte kulture i značajnih postignuća, dr Mirka Stojakovića, na redovnim, i dr Đure Kurepe, na poslediplomskim studijama. Doprinos ovom tekstu su takođe dali, bilo kroz predavanja bilo kroz razgovore o algebri i logici, i profesori dr Svetozar Milić, dr Slaviša Prešić, dr Janez Ušan i dr Zoran Stojaković.

Zahvaljujem se recenzentima, profesorima dr Stojanu Bogdanoviću i dr Žarku Mijajloviću, na uloženom trudu oko čitanja rukopisa i korisnim sugestijama, kao i Radošu Bakiću koji je ispravio mnoge štamparske greške i ukazao mi na nejasnoće i nekorektnosti u nekoliko dokaza.

Tekst sam sâm otkucao. Bio je to ujedno moj prvi susret sa "svetom kompjutera". U "upoznavanju" su s mnogo dobre volje učestvovali dr Dušanka Perišić, dr Zoran Budimac, mr Nenad Đapić i mr Dragan Mašulović, na čemu im i ovom prilikom zahvaljujem. Svejedno, susret je ispao prilično neprijatan. Ponajviše, cenim, zbog toga što se moj kompjuter (SX-386), koji inače ni po jednoj zvaničnoj proceni ne spada u misleće mašine, ponašao ne samo kao intiligentno nego po pravilu i kao vrlo zločesto biće. Istine radi moram reći da *oni* iz računskog centra nude i jedno drugo tumačenje ovog fenomena koje je više vezano za moju ličnost. Bilo kako bilo smatrao sam fer ponudom da podelimo greške, ali je kompjuter to sa indignacijom odbio.

Ako se nađe koja dobra reč za knjigu, odgovornost za to će biti na mom ocu. Po struci pravnik, po duši matematičar, bio mi je najbolji učitelj. Sestra me je učila postojanosti u teškim trenucima. Teoretski sam to lako usvajao, ali sam u praksi teško sledio njen primer; jedan od razloga da se ova knjiga javlja sa prilično zakašnjenjem. Majka je tu uvek bila sa svojom podrškom. Konačno, bez njenih crnih kafa i povremeno zabrinutog: "hoće li to *ikad* biti gotovo?", ova knjiga ne bi ni bila moguća.

Primiću sa zahvalnošću primedbe, kritike, korekcije i sugestije koje bi uticale na poboljšanje eventualno ponovljenog izdanja.

Novi Sad
septembar 1997

Autor

# Glava 1

# Opšti deo

## 1 Algebarske operacije, algebre

Za skupove $A$ i $B$ sa $A^B$ označavamo skup svih preslikavanja skupa $B$ u skup $A$ ($A^B = \{f \mid f : B \longrightarrow A\}$). Kada je $n$ konačni ordinal veći od nule a $A$ neprazan skup, često se neformalno, i mi ćemo tako i činiti, identifikuje funkcija $f \in A^n$ sa uređenom n-torkom $((0)f, \ldots, (n-1)f)$. Tako će za nas $A^n$ biti $\{(a_0, \ldots, a_{n-1}) \mid a_i \in A, 0 \leq i < n\}$. Posebno, ako je $n = 0$, imamo $A^0 = \{0\}$ (0 je oznaka za prazan skup – koristimo von Neumanovu definiciju ordinala).

Primetimo uzgred da je $0^B = 0$ ako je $B \neq 0$.

**Definicija 1.1** *$n$-arna operacija (operacija dužine $n$) nad nepraznim skupom $A$ je preslikavanja skupa $A^n$ u $A$. U slučaju $n = 0$ funkciju poistovećujemo sa slikom elementa 0. Operacije dužine nula zovemo konstantama, dužine jedan unarnim, dužine dva binarnim, dužine tri ternarnim operacijama.*

*Operacije dužine $n$ ($n \in \omega$) zovemo uopšte konačnim. Prema tome, skup svih konačnih operacija nad nepraznim skupom $A$ je*

$$\bigcup_{n\in\omega}\{f \mid f : A^n \longrightarrow A\}.$$

Ako je $\cdot$ binarna operacija nad $A$, umesto $((a,b),c) \in \cdot$ ili, manje formalnog, $\cdot(a,b) = c$, koristimo uobičajeno $a \cdot b = c$.

**Definicija 1.2** *(Univerzalna) algebra* **A** *je uređen par $\langle A, F\rangle$, gde je $A$ neprazan skup i $F$ neprazan podskup skupa konačnih operacija nad $A$ koji sadrži bar jednu operaciju dužine veće od ili jednake 1 (izbegavamo trivijalni slučaj kada su nam na raspolaganju samo konstante).*

**Napomena.** Ukoliko je skup $F$ konačan, npr. $F = \{f_1, \ldots, f_k\}$, pisaćemo $\langle A, f_1, \ldots, f_k\rangle$ umesto, formalno, $\langle A, \{f_1, \ldots, f_k\}\rangle$. Skup $A$ zovemo *domenom* ili *nosačem* algebre **A**.

Algebre (algebarske strukture) označavaćemo sa **A**, **B**, **C**,..., a njihove domene odgovarajućim velikim "običnim" slovima $A, B, C, \ldots$.

**Definicija 1.3** *Binarna operacija $\cdot$ nad skupom $A$ je asocijativna akko važi:*

$$\forall a, b, c \in A \;\; a \cdot (b \cdot c) = (a \cdot b) \cdot c;$$

*komutativna akko važi:* $\forall a, b \in A \;\; a \cdot b = b \cdot a$.

*Za operaciju $\cdot$ važi zakon leve kancelacije (skraćivanja) akko je ispunjeno:*

$$\forall a, b, c \in A \;\; a \cdot b = a \cdot c \implies b = c;$$

*analogno se definiše zakon desne kancelacije. Zakon kancelacije važi akko važe zakoni leve i desne kancelacije.*

**Definicija 1.4** *Algebra sa samo jednom i to binarnom operacijom zove se grupoid.*

*Asocijativni grupoid (odnosno grupoid čija je operacija asocijativna) je polugrupa (ili semigrupa).*

**Lema 1.5** *U polugrupi je "proizvod" elemenata, uzetih nekim fiksnim redom, nezavisan od toga kako su zagrade raspoređene.*

**Dokaz**. Jasno, interesantno je da imamo bar tri elementa. Neka je, dakle, $n$ veće od 2 i neka su $a_1, \ldots, a_n$ elementi polugrupe $\mathbf{G} = \langle G, \cdot \rangle$. Indukcijom po $n$ (koja počinje sa trojkom) dokazujemo da su rezultati "množenja" tih elemenata, uzetih po datom redu, isti za sve distribucije zagrada.

Sama definicija asocijativnosti operacije nam rešava slučaj $n = 3$. Pretpostavimo stoga da je tvrđenje tačno za proizvode sa $k$ faktora, za svako $k$ manje od $n$, gde je $n$ veće od 3. Za bilo koje dve raspodele zagrada u množenju datih $n$ elemenata, dobićemo, s obzirom na induktivnu pretpostavku, proizvode oblika $(a_1 \cdot \ldots \cdot a_i) \cdot (a_{i+1} \cdot \ldots \cdot a_n)$, $(a_1 \cdot \ldots a_j) \cdot (a_{j+1} \cdot \ldots \cdot a_n)$. Recimo da je $i$ manje od $j$. Očigledno, dovoljno je da pokažemo: $(a_1 \cdot \ldots \cdot a_i) \cdot (a_{i+1} \cdot \ldots \cdot a_n) = (a_1 \cdot \ldots \cdot a_{i+1}) \cdot (a_{i+2} \cdot \ldots \cdot a_n)$ (jer onda smo u stanju da sukcevnim "pomeranjem za po jedno mesto" prvi proizvod svedemo na drugi). No očigledno je, zbog asocijativnosti operacije i induktivne hipoteze:

$$(a_1 \cdot \ldots \cdot a_i) \cdot (a_{i+1} \cdot \ldots \cdot a_n) = (a_1 \cdot \ldots \cdot a_i) \cdot (a_{i+1} \cdot (a_{i+2} \cdot \ldots \cdot a_n)) =$$

$$((a_1 \cdot \ldots \cdot a_i) \cdot a_{i+1}) \cdot (a_{i+2} \cdot \ldots \cdot a_n) = (a_1 \cdot \ldots \cdot a_{i+1}) \cdot (a_{i+2} \cdot \ldots \cdot a_n). \square$$

Prethodna lema nas, kada je reč o množenju u polugrupama, oslobađa brige oko raspodele zagrada. Najčešće ćemo ih jednostavno izostavljati; stavljaćemo ih kada smatramo da to olakšava čitanje formule ili praćenje dokaza.



U prezentaciji (najčešće konačnih) grupoida (grupoida čiji su domeni konačni) služićemo se koji put i tzv. Cayleyevim tablicama. Tako npr. grupoidu $\langle \{a, b\}, \cdot \rangle$, gde je $a \cdot a = a$, $a \cdot b = a$, $b \cdot a = b$ i $b \cdot b = a$, ogovara Cayleyeva tablica

| $\cdot$ | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $a$ |
| $b$ | $b$ | $a$ |

**Definicija 1.6** *Element $e$ grupoida $\mathbf{G}$ je levi (desni) jedinični ili neutralni element akko $\forall a (\in G)$ $e \cdot a = a$ $(a \cdot e = a)$.*

*Element $e$ je jedinični akko je i levi i desni jedinični.*

*Ako je $e$ (levi, desni) jedinični element grupoida $\mathbf{G}$, $b$ je levi (desni) inverzni element elementa $a$, s obzirom na $e$, akko je $b \cdot a = e$ $(a \cdot b = e)$.*

Ubuduće ćemo, kad god to kontekst dozvoli, pisati jednostavno $\forall a$, $\exists a$ umesto $\forall a \in G$, $\exists a \in G$.

**Lema 1.7** $(a)$ *Grupoid može imati najviše jedan jedinični element:*

$(b)$ *Ako grupoid ima i levi i desni jedinični element, onda su oni jednaki i to je jedinični element grupoida;*

$(c)$ *Ako su u polugrupi sa jediničnim elementom $(e)$ $b$ levi i $c$ desni inverzni element elementa $a$, onda je $b = c$.*

**Dokaz**. $(b)$ Neka je $e_l$ levi jedinični, a $e_d$ desni jedinični element grupoida $\mathbf{G}$. Tada je: $e_l = e_l e_d = e_d$.

$(c)$ $b = be = b(ac) = (ba)c = ec = c$.$\square$

**Definicija 1.8** *Kvazigrupa je grupoid sa svojstvom da su za sve elemente $a, b$ jednačine $a \cdot x = b$ i $x \cdot a = b$ jednoznačno rešive.*

**Lema 1.9** *U kvazigrupi važi zakon skraćivanja.*

**Lema 1.10** *Grupoid je komutativan akko je njegova Cayleyeva tablica simetrična u odnosu na glavnu dijagonalu.*

Provera asocijativnosti u osnovi je teži (što ne znači i težak) zadatak. Zainteresovane upućujemo na [14], paragraf 1.1 ili [80], paragraf 1.2.

# 2 Grupe, homomorfizmi grupa

Presek klasa polugrupa i kvazigrupa je klasa grupa. Imamo, naime:

**Definicija 2.1** *Grupa je asocijativna kvazigrupa.*

*Grupa je Abelova (komutativna) akko je njena operacija komutativna.*

Sledeće definicije (2.2 i 2.3) su ekvivalentne sa 2.1

**Definicija 2.2** *Grupa je polugrupa sa jediničnim elementom* $(e)$ *u kojoj je svaki element inverzibilan (invertibilan) (tj. u kojoj važi:* $\forall a\, \exists b\ a \cdot b = b \cdot a = e$*).*

Jedinstveni inverzni element elementa $a$ (videti 1.7$(c)$) nadalje ćemo obeležavati sa $a^{-1}$ ili, kada je u pitanju aditivna notacija (koja se obično koristi za Abelove grupe), sa $-a$. S obzirom na već rečeno odmah sledi $(a^{-1})^{-1} = a$. Takođe važi $(a_1 \cdot \ldots \cdot a_n)^{-1} = a_n^{-1} \cdot \ldots \cdot a_1^{-1}$.

Uopšte u polugrupi sa jediničnim elementom $e$ za element $a$ koji ima inverzni usvajamo sledeću definiciju ($z$ je ceo broj):

$$a^z = \begin{cases} \underbrace{a \cdot \ldots \cdot a}_{z-puta} & z > 0 \\ e & z = 0 \\ \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{(-z)-puta} & z < 0. \end{cases}$$

**Definicija 2.3** *Grupa je polugrupa sa bar jednim levim (desnim) jediničnim elementom za koji svaki element ima levi (desni) inverzni.*

Proverimo samo da definicija 2.3 implicira 2.2 (ostale implikacije su još trivijalnije). Neka je $e$ levi jedinični element polugrupe $\mathbf{G} = \langle G, \cdot \rangle$ za koji svaki element ima levi inverzni. Neka je $b$ levi inverzni element elementa $a$ i neka je $c$ levi inverzni element elementa $b$ . No tada je $ab = e(ab) = (cb)(ab) = c(ba)b = ceb = cb = e$, te je $b$ i desni inverzni element elementa $a$, stoga i jedinstveni inverzni element elementa $a$, s obzirom na $e$. Ali, $e$ je i desni jedinični, znači (jedinstveni) jedinični; zaista: $ae = a(ba) = (ab)a = ea = a$.

**Napomena**. U definiciji 2.3 treba paziti da se ne "pobrkaju strane". Tako npr. u polugrupi $\mathbf{G} = \langle G, \cdot \rangle$, gde je $|G| \geq 2$ i $\forall a, b\ a \cdot b = b$, svaki element je levi jedinični i za svaki levi jedinični svaki element ima desni inverzni ali, jasno, $\mathbf{G}$ nije grupa.

Ubuduće ćemo gotovo redovito koristiti, sem u slučaju konkretnih primera, znak $\cdot$ (odnosno $+$) za operacije u grupi (Abelovoj grupi). $e$ $(0)$ će biti jedinični (neutralni) element ili, eventualno, $e_G$ $(0_G)$ kada želimo da naglasimo da je u pitanju jedinični (neutralni) element grupe $\mathbf{G}$. Često ćemo jednostavno pisati, kada je mogućnost zabune isključena, $ab$ umesto $a \cdot b$.

**Primer 2.4** $(a)$ *Grupe koje su svakom srednjoškolcu svakako poznate su:* $\mathbf{Z} = \langle Z, + \rangle$, $\mathbf{Ra} = \langle Ra, + \rangle$, $\mathbf{Re} = \langle Re, + \rangle$, $\langle Ra \setminus \{0\}, \cdot \rangle$, $\langle Re \setminus \{0\}, \cdot \rangle$ *(aditivne grupe celih, racionalnih i realnih brojeva i multiplikativne grupe nenula racionalnih i realnih brojeva; naravno, u poslednja dva slučaja nulu smo morali izbaciti – to je jedini element polugrupa* $\langle Ra, \cdot \rangle$, $\langle Re, \cdot \rangle$ *bez inverznog elementa.*



*Oznake za date aditivne grupe zadržaćemo kroz ceo tekst.*

$(b)$ $\langle Z, +_n \rangle$, *gde je* $n$ *pozitivan prirodan broj i*

$$a +_n b \stackrel{\text{def}}{=} a + b - [\frac{a+b}{n}]n \quad (\text{"}\textit{sabiranje po modulu } n\text{"}),$$

*komutativna je polugrupa bez jediničnog elementa* ([ ] *je funkcija najveće celo, dakle, za realni broj* $x$, $[x] \stackrel{\text{def}}{=}$ *najveći ceo broj manji od ili jednak* $x$).

*Za pozitivan prirodan broj* $n$ *je* $\mathbf{Z}_n = \langle \{0, \ldots, n-1\}, +_n \rangle$, *Abelova grupa.*

**Dokaz**. Dokazaćemo samo drugi deo primera uz napomenu da su dokazi asocijativnosti operacija $+_n$ nad skupom Z i nad skupom $n = \{0, \ldots, n-1\}$ u osnovi isti.

Lako se proverava da je $+_n$ preslikavanje skupa $n^2$ u $n$. Ta operacija je i asocijativna, jer:

$$(a +_n b) +_n c = (a + b - [\frac{a+b}{n}]n) + c - [\frac{(a + b - [\frac{a+b}{n}]n) + c}{n}]n =$$

$$a + b + c - [\frac{a+b}{n}]n + [\frac{a+b}{n}]n - [\frac{a+b+c}{n}]n = a + b + c - [\frac{a+b+c}{n}]n;$$

(koristili smo sledeće svojstvo funkcije [ ]: za ceo broj $x$ je $[x + y] = x + [y]$). Isto tako je i $a +_n (b +_n c) = a + b + c - [\frac{a+b+c}{n}]n$. Konačno, 0 je jedinični (neutralni) element, inverzni element nenula elementa $a$ je $n - a$.

$(c)$ *Za pozitivan prirodan broj* $n$ *je* $\langle Z, \cdot_n \rangle$, *gde je*

$$a \cdot_n b \stackrel{\text{def}}{=} ab - [\frac{ab}{n}]n \quad (\text{"}\textit{množenje po modulu } n\text{"}),$$

*komutativna polugrupa bez jediničnog elementa.*

*Ako je* $n$ *prirodan broj veći od* 1, *tada je* $\langle n, \cdot_n \rangle$ *komutativna polugrupa sa jediničnim elementom* (1) *u kojoj element* $a$ *ima inverzni akko je* $(a, n) = 1$, *tj. akko su* $a$ *i* $n$ *uzajamno prosti brojevi* ( $(a, b) \stackrel{\text{def}}{=}$ *najveći zajednički delilac brojeva* $a$ *i* $b$).

**Dokaz**. Proverićemo samo poslednji deo tvrđenja. Naravno, slučaj $n = 2$ nije interesantan. Uzmimo stoga da je $n$ veće od 2.

Neka $a$ ima inverzni element $b$. Onda je $a \cdot_n b = 1$, tj. $ab - [\frac{ab}{n}]n = 1$, pa je prema poznatoj Euklidovoj teoremi $(a, n) = 1$. S druge strane, ako je $(a, n) = 1$, onda je, opet prema Euklidovoj teoremi, $au + nv = 1$ za neke cele brojeve $u$ i $v$. Neka je $u = kn + b$, gde je $1 \leq b < n$, $k \in Z$. Sledi, na osnovu već rečenog o funkciji [ ], $a \cdot_n b = 1$.

U vezi tačaka $(b)$ i $(c)$ zabeležimo još: ako je $a \in \omega$ i $b \in Z$, tada je:

$$\underbrace{b +_n \cdots +_n b}_{a-puta} = \underbrace{(b + \cdots + b)}_{a-puta} - [\frac{\overbrace{b + \cdots + b}^{a-puta}}{n}]n = ab - [\frac{ab}{n}]n = a \cdot_n b.$$

Konstatujmo takođe da je operacija $\cdot_n$ distributivna u odnosu na $+_n$. Jer,

$$(a+_n b)\cdot_n c = (a+b-[\frac{a+b}{n}]n)\cdot_n c = (a+b)c-[\frac{a+b}{n}]cn-[\frac{(a+b)c-[\frac{a+b}{n}]cn}{n}]n =$$

$$(a+b)c-[\frac{a+b}{n}]cn-[\frac{(a+b)c}{n}]n+[\frac{a+b}{n}]cn = (a+b)c-[\frac{(a+b)c}{n}]n,$$

a i

$$a \cdot_n c +_n b \cdot_n c = (ac - [\frac{ac}{n}]n) +_n (bc - [\frac{bc}{n}]n) =$$

$$ac - [\frac{ac}{n}]n + bc - [\frac{bc}{n}]n - [\frac{ac - [\frac{ac}{n}]n + bc - [\frac{bc}{n}]n}{n}]n =$$

$$(a+b)c - [\frac{(a+b)c}{n}]n.$$

**Napomena**. *U grupi* $\mathbf{Z}_n$ *je, prema navedenom, za* $0 < k \in n$ *i* $z \in Z$:

$$\underbrace{k +_n \cdots +_n k}_{z-puta} = \begin{cases} z \cdot_n k & z > 0 \\ 0 & z = 0 \\ (-z) \cdot_n (n-k) & z < 0. \end{cases}$$

$(d)$ $\mathbf{GL}_n(\mathbf{Re}) = \langle GL_n(\mathbf{Re}), \cdot \rangle$, *gde je* $GL_n(\mathbf{Re})$ *skup realnih regularnih matrica formata* $n \times n$ *i* $\cdot$ *matrično množenje, nekomutativna je grupa za* $n$ *veće od* 1 *(u vezi sa ovim primerom i njegovom notacijom videti paragraf* 19*).*

$(e)$ *Neka je* $A$ *neprazan skup,* $S_A \stackrel{\text{def}}{=} \{f \mid f$ *je bijektivno preslikavanje skupa* $A$ *na sebe* $\}$ *i* $\circ$ *kompozicija preslikavanja:* $(a)(f \circ g) \stackrel{\text{def}}{=} ((a)f)g)$. *Tada je* $\mathbf{S}_A = \langle S_A, \circ \rangle$ *grupa, tzv. simetrična grupa skupa* $A$. *Za* $n$ *veće od* 2 *ova grupa je neabelova.*

$(f)$ *Kleinova grupa je Abelova grupa sa četiri elementa, recimo* $e, a, b, c$, *u kojoj je, ako je* $e$ *jedinični element:* $a^2 = b^2 = c^2 = e$, $ab = c$, $ca = b$ *i* $bc = a$.

$(g)$ $\langle P(A), \triangle \rangle$, *gde je* $P(A)$ *partitivni skup (ma kakvog skupa)* $A$ *i* $\triangle$ *tzv. simetrična razlika (za podskupove* $B, C$ *skupa* $A$ *je:* $B \triangle C \stackrel{\text{def}}{=} (B \setminus C) \cup (C \setminus B)$*) Abelova je grupa.*

**Dokaz**. Provera asocijativnost se svodi na proveru da je formula propozicionalnog računa, adekvatna skupovnoj, tautologija (postoje, jasno, i drugi načini, ali ovaj smatramo najlakšim); neutralni element je prazan skup a svaki element je sam sebi inverzan.□



**Definicija 2.5** $(a)$ *Red grupe* $\mathbf{G}$ *je kardinalnost njenog domena, u oznaci* $|G|$. *Grupa* $\mathbf{G}$ *je konačna ako je* $|G|$ *(pozitivan) prirodan broj, inače je beskonačna.*

$(b)$ *Red elementa* $a$ *grupe* $\mathbf{G}$ *je najmanji pozitivan prirodan broj* $n$ *za koji je* $a^n = \underbrace{a \cdot \ldots \cdot a}_{n-puta} = e$, *ukoliko takav postoji. Ako je* $a^n \neq e$ *za svaki pozitivan prirodan broj* $n$, *onda kažemo da je element* $a$ *beskonačnog reda.*

*Za prost broj* $p$ *je grupa* $\mathbf{G}$ *primarna s obzirom na* $p$, $p$*-primarna ili jednostavno* $p$*-grupa akko je red svakog njenog elementa stepen broja* $p$ *(naravno, podrazumevamo da različiti elementi mogu imati različite redove, tj. biti različiti stepeni broja* $p$*; posebno, red jediničnog elementa je nulti stepen broja* $p$*).*

Jasno, ako je red elementa $a$ pozitivan prirodan broj $n$, tada je $a^{-1} = a^{n-1}$ i $a^j \neq a^k$ za $0 \leq j < k < n$.

Lako je proveriti i da je, generalno, $a^k \cdot a^m = a^{k+m}$ za sve cele brojeve $k, m$.

U konačnim grupama su, naravno, svi elementi konačnog reda. U beskonačnim grupama moguće su sve kombinacije: svi elementi su konačnog reda, imamo elemenata i konačnog (tu ne računamo jedinični element) i beskonačnog reda, i svi elementi (sem jediničnog) su beskonačnog reda. U zavisnosti koja od ovih kombinacija važi grupe delimo na *periodične* ili *torzione*, *mešovite* i *torziono slobodne*. U 2.4$(a)$ aditivne grupe su torziono slobodne dok su multiplikativne mešovite. $\mathbf{GL}_n(\mathbf{Re})$ je mešovita grupa a takva je i $\mathbf{S}_A$ za $|A| \geq \aleph_0$. Grupa $\langle P(A), \triangle \rangle$ (tačka $(g)$) je, za beskonačan skup $A$, beskonačna (reda $2^{|A|}$) periodična grupa: svi su elementi, sem jediničnog, reda 2 (stoga je ova grupa i Abelova – videti narednu lemu).

**Definicija 2.6** *Za elemente* $a$ *i* $b$ *grupe* $\mathbf{G}$ *kažemo da su konjugovani akko postoji element* $g$ $(\in G)$ *takav da je* $b = g^{-1} \cdot a \cdot g$.

*Element sa konačno mnogo konjugata zove se* $FC$*-element. Grupa čiji svi elementi imaju konačno mnogo konjugata zove se* $FC$*-grupa.*

Primetimo: relacija konjugovanosti je relacija ekvivalencije na skupu $G$; i dodajmo: o karakterizaciji $FC$-grupa će biti reči u 15.7.

**Lema 2.7** *U (svakoj) grupi* $\mathbf{G}$ *važi (za bilo koje njene elemente* $a, a_1, \ldots, a_n$*):*

$(a)$ $a$ *i* $a^{-1}$ *su istog reda;*

$(b)$ *konjugovani elementi su istog reda;* $a_1 \cdot a_2$ *i* $a_2 \cdot a_1$ *su istog reda;*

$(c)$ *ako je* $a^n = e$, *onda red elementa* $a$ *deli* $n$*;*

$(d)$ *ako su* $a_1, \ldots, a_n$ *međusobno permutabilni elementi konačnih redova, respektivno,* $k_1, \ldots, k_n$, *onda red elementa* $a_1 \cdot \ldots \cdot a_n$ *deli* $NZS(k_1, \ldots, k_n)$, *gde je* $NZS$ *funkcija najmanji zajednički sadržalac.*

($e$) *ako je* $\mathbf{G}$ *parnog reda, onda sadrži element reda* 2;

($f$) *ako su svi nejedinični elementi reda* 2, $\mathbf{G}$ *je Abelova grupa.*

**Dokaz.** ($a$) Neka je, za $n > 1$ i $a \neq e$, $a^n = e$. Onda je $a^n \cdot (a^{-1})^n = (a^{-1})^n$, tj. $e = (a^{-1})^n$. Analogno, iz $(a^{-1})^k = e$ sledi $a^k = e$. Prema tome, ili su i $a$ i $a^{-1}$ beskonačnog reda ili su oba elementa konačnog i to istog reda.

($b$) Treba samo iskoristiti:

$$(g^{-1}ag)^n = \underbrace{g^{-1}ag \cdot g^{-1}ag \cdot \ldots \cdot g^{-1}ag}_{n \text{ puta}} = g^{-1}a^n g.$$

Elementi $a_1 \cdot a_2$ i $a_2 \cdot a_1$ su konjugovani – $a_1 \cdot a_2 = a_2^{-1} \cdot (a_2 \cdot a_1) \cdot a_2$.

($e$) Jasno, nejedinični element $g$ je reda 2 akko je $g = g^{-1}$. Stoga je $G = \{e\} \cup \bigcup\{\{g, g^{-1}\} \mid g\ (\in G)$ je reda većeg od $2\} \cup \{g \mid g\ (\in G)$ je reda $2\}$ pa ako je $|G|$ paran broj, postoji bar jedan element reda 2; možemo zapravo konstatovati da je takvih elemenata uvek neparan broj.

($f$) Ako su svi nejedinični elementi reda 2, onda $(ab)^2 = abab = e$ implicira: $a^2bab^2 = ab$, odnosno, $ba = ab$.□

**Napomena.** U vezi sa tačkom ($d$) prethodne leme recimo: proizvod nepermutabilnih elemenata konačnog reda ne mora biti konačnog reda; npr. u grupi $\mathbf{GL_2(Re)}$ elementi $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ i $B = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$ su reda 2 ali je $AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ (a onda i $BA = (AB)^{-1}$) element beskonačnog reda; indukcijom se lako provera da je $(AB)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.

**Definicija 2.8** *Neka su* $\mathbf{G} = \langle G, \cdot \rangle$ *i* $\mathbf{H} = \langle H, * \rangle$ *dve grupe. Preslikavanje* $\varphi : G \longrightarrow H$ *je homomorfno preslikavanje grupe* $\mathbf{G}$ *u grupu* $\mathbf{H}$ *akko važi:* $\forall a, b \in G \quad (a \cdot b)\varphi = (a)\varphi * (b)\varphi$ *(obično se taj zahtev sažeto formuliše sa: slika proizvoda jednaka je proizvodu slika).*

*Homomorfizam (– homomorfno preslikavanje) koji je ujedno i bijektivno preslikavanje zovemo izomorfizam. Ako postoji izomorfno preslikavanje grupe* $\mathbf{G}$ *na grupu* $\mathbf{H}$, *tada kažemo da su grupe* $\mathbf{G}$ *i* $\mathbf{H}$ *izomorfne, u notaciji* $\mathbf{G} \cong \mathbf{H}$.

*Ako je* $\mathbf{H}$ *baš* $\mathbf{G}$, *onda govorimo o endomorfizmu tj. automorfizmu (= bijektivni endomorfizam) grupe* $\mathbf{G}$.

*Skup svih homomorfnih (izomorfnih) preslikavanja grupe* $\mathbf{G}$ *u grupu* $\mathbf{H}$ *obeležavaćemo sa* $Hom(\mathbf{G}, \mathbf{H})$ $(Is(\mathbf{G}, \mathbf{H}))$. *Posebno, za* $Hom(\mathbf{G}, \mathbf{G})$, $Is(\mathbf{G}, \mathbf{G})$ *koristićemo* $End(\mathbf{G})$, *tj.* $Aut(\mathbf{G})$.



Primetimo da je $Hom(\mathbf{G}, \mathbf{H})$ neprazan skup za bilo koje dve grupe $\mathbf{G}$ i $\mathbf{H}$; jer, uvek imamo tzv. trivijalni homomorfizam koji sve elemente grupe $\mathbf{G}$ preslikava u jedinični element grupe $\mathbf{H}$.

**Lema 2.9** ($a$) *Ako je* $\varphi \in Hom(\mathbf{G}, \mathbf{H})$ *i* $a \in G$, *tada je* $(a^k)\varphi = ((a)\varphi)^k$ *za svaki ceo broj* $k$; *posebno* ($k = 0$), $(e_G)\varphi = e_H$;

($b$) *Ako je* $\varphi \in Hom(\mathbf{G}, \mathbf{H})$ $(\varphi \in Is(\mathbf{G}, \mathbf{H}))$ *i* $\psi \in Hom(\mathbf{H}, \mathbf{K})$ $(\psi \in Is(\mathbf{H}, \mathbf{K}))$, *onda je* $\varphi \circ \psi \in Hom(\mathbf{G}, \mathbf{K})$ $(\varphi \circ \psi \in Is(\mathbf{G}, \mathbf{K}))$;

($c$) *Ako je* $\varphi \in Is(\mathbf{G}, \mathbf{H})$, $\varphi$ *preslikava klasu konjugovanih elemenata u klasu konjugovanih elemenata; konkretno*

$$\{(g^{-1}ag)\varphi \mid g \in G\} = \{h^{-1}(a)\varphi\, h \mid h \in H\}.$$

($d$) *Ako je* $\varphi \in Is(\mathbf{G}, \mathbf{H})$, *tada je* $\varphi^{-1} \in Is(\mathbf{H}, \mathbf{G})$ *(preslikavanje* $\varphi^{-1} : H \longrightarrow G$ *je, jasno, definisano sa:* $(h)\varphi^{-1} = g$ *akko* $(g)\varphi = h$);

($e$) $\mathbf{End(G)} = \langle End(\mathbf{G}), \circ \rangle$ *je polugrupa sa jediničnim elementom (*$\circ$ *je, podrazumevamo, kompozicija preslikavanja);*

$\mathbf{Aut(G)} = \langle Aut(\mathbf{G}), \circ \rangle$ *je grupa tzv. grupa automorfizama grupe* $\mathbf{G}$.

($f$) $\cong$ *je relacija ekvivalencije u klasi svih grupa.*

**Dokaz.** ($d$) Neka je $\mathbf{G} = \langle G, \cdot \rangle$, $\mathbf{H} = \langle H, \star \rangle$ i $\varphi \in Is(\mathbf{G}, \mathbf{H})$. Pokažimo samo da $\varphi^{-1}$ ima svojstvo homomorfnosti (bijektivnost je vrlo očigledna); za $h_1, h_2$ iz $H$ je:

$$(h_1 \star h_2)\varphi^{-1} = (((h_1)\varphi^{-1})\varphi \star ((h_2)\varphi^{-1})\varphi)\varphi^{-1} = (((h_1)\varphi^{-1} \cdot (h_2)\varphi^{-1})\varphi)\varphi^{-1} =$$

$$((h_1)\varphi^{-1} \cdot (h_2)\varphi^{-1})\imath_G = (h_1)\varphi^{-1} \cdot (h_2)\varphi^{-1}.$$

($e$) Ako su $\varphi, \psi$ endomorfizmi grupe $\mathbf{G}$, onda je to i $\varphi \circ \psi$, jer je:

$$(a \cdot b)(\varphi \circ \psi) = ((a \cdot b)\varphi)\psi = ((a)\varphi \cdot (b)\varphi)\psi = ((a)\varphi)\psi \cdot ((b)\varphi)\psi =$$

$$(a)(\varphi \circ \psi) \cdot (b)(\varphi \circ \psi).\square$$

**Napomena.** U algebri se, gotovo po pravilu, identifikuju izomorfne algebarske strukture; jer za algebru su daleko interesantniji algebarski zakoni i svojstva koji važe u njenim strukturama (to je uostalom i osnovni cilj njenog izučavanja) od prirode elemenata i operacija tih struktura. Tako se u kasnijem tekstu kada se kaže npr. "postoje samo dve grupe sa svojstvom ...", podrazumeva u stvari: "postoje, do na izomorfizam, dve grupe sa svojstvom ...", tj. particija klase svih grupa sa datim svojstvom koju vrši relacija $\cong$ sadrži (samo) dve podklase; obično se u takvom slučaju u tvrđenju navedu izabrani "predstavnici" podklasa.

**Primer 2.10** (*a*) *Preslikavanje $\varphi$ skupa $GL_n(\mathbf{Re})$ (videti 2.4(d)) u $Re \setminus \{0\}$ dato sa $(A)\varphi = det(A)$ surjektivno je homomorfno preslikavanje grupe $\mathbf{GL}_n(\mathbf{Re})$ u grupu $\langle Re \setminus \{0\}, \cdot\rangle$ (ali ne i injektivno ako je $n$ veće od 1).*

(*b*) *Neka je za (ma koju) grupu $\mathbf{G}$ preslikavanje $\psi : G \longrightarrow Aut(\mathbf{G})$ dato sa $(a)\psi = u_a$ i $(g)u_a \stackrel{\text{def}}{=} a^{-1} \cdot g \cdot a$. Onda je $\psi$ homomorfno preslikavanje grupe $\mathbf{G}$ u grupu $\mathbf{Aut}(\mathbf{G})$ (ne nužno ni "jedan-jedan" ni "na").*

**Dokaz.** Zaista, $(g)(u_a \circ u_b) = b^{-1} \cdot (a^{-1} \cdot g \cdot a) \cdot b = (a \cdot b)^{-1} \cdot g \cdot (a \cdot b) = (g)u_{a \cdot b}$ pa je $(a \cdot b)\psi = (a)\psi \circ (b)\psi$.

$u_a$ zovemo *unutrašnjim automorfizmom.* Skup svih unutrašnjih automorfizama grupe $\mathbf{G}$ označićemo sa $Inn(\mathbf{G})$, a grupu $\mathbf{Inn}(\mathbf{G})$ (videti 2.15) zvati *grupom unutrašnjih automorfizama*; oznaka dolazi od engleske reči *inner* = unutrašnji.

(*c*) *Prirodni logaritam (ln) je izomorfno preslikavanje multiplikativne grupe pozitivnih realnih brojeva, $\langle Re^+, \cdot\rangle$, na aditivnu grupu realnih brojeva.*

(*d*) *Ako su skupovi $A$ i $B$ iste kardinalnosti, onda je $\mathbf{S}_A \cong \mathbf{S}_B$.*

**Dokaz.** Neka je $f : A \longrightarrow B$ bijektivno preslikavanje. Tada je preslikavanje $F : S_A \longrightarrow S_B$ definisano sa $(\alpha)F = f^{-1} \circ \alpha \circ f$ $(\alpha \in S_A)$ izomorfizam grupa $\mathbf{S}_A$ i $\mathbf{S}_B$.

(*e*) *Ako su grupe $\mathbf{G}$ i $\mathbf{H}$ izomorfne, onda su izomorfne i njihove grupe automorfizama i $|Aut(\mathbf{G})| = |Is(\mathbf{G}, \mathbf{H})|$.*

**Dokaz.** Prvi deo se dokazuje kao i u prethodnom primeru samo što sada, naravno, koristimo izomorfno preslikavanje grupe $\mathbf{G}$ na grupu $\mathbf{H}$. Drugi deo se jednako lako proverava.

(*f*) $\mathbf{End}(\mathbf{Ra}) \cong \langle Ra, \cdot\rangle$; $\mathbf{Aut}(\mathbf{Ra}) \cong \langle Ra \setminus \{0\}, \cdot\rangle$.

**Dokaz.** Za nenula racionalni broj $r$ je preslikavanje $\varphi : a \longrightarrow a \cdot r$, očigledno, automorfizam grupe $\mathbf{Ra}$. ($\varphi$ je bijekcija i $(a+b)\varphi = (a+b) \cdot r = a \cdot r + b \cdot r = (a)\varphi + (b)\varphi$). $\varphi_0$ je trivijalni endomorfizam. Opet, ako je $\varphi \in End(\mathbf{Ra})$ i $(1)\varphi = r$, onda je, za svaki pozitivan prirodan broj $n$, $(n)\varphi = (\underbrace{1 + \cdots + 1}_{n-puta})\varphi = n \cdot (1)\varphi = n \cdot r$ i odatle $(-n)\varphi = -(n)\varphi = (-n) \cdot r$. Dalje, ako je $q$ pozitivan prirodan broj i $p$ ceo broj, iz $p \cdot r = (p)\varphi = (q \cdot \frac{p}{q})\varphi = q \cdot (\frac{p}{q})\varphi$ sledi $(\frac{p}{q})\varphi = \frac{p}{q} \cdot r$, pa je $\varphi = \varphi_r$. Prema tome, svaki endomorfizam je određen slikom jedinice i $\{\varphi_r \mid r \in Ra\}$ je skup svih endomorfizama a $\{\varphi_r \mid r \in Ra \setminus \{0\}\}$ skup svih automorfizama grupe $\mathbf{Ra}$. Preostaje još da se proveri: $\varphi_r \circ \varphi_s = \varphi_{r \cdot s}$. No, $(1)(\varphi_r \circ \varphi_s) = (r)\varphi_s = r \cdot s = (1)\varphi_{r \cdot s}$.

(*g*) *Grupe $\mathbf{Aut}(\langle Ra^+, \cdot\rangle)$ i $\mathbf{Aut}(\langle Ra \setminus \{0\}, \cdot\rangle)$ su kardinalnosti c (kontinuum).*

**Dokaz.** Jasno je da su kardinalnosti ovih grupa manje ili jednake kontinuum.



Posmatrajmo ovom prilikom grupu $\langle Ra^+, \cdot\rangle$. Svako bijektivno preslikavanje $\varphi$ skupa prostih brojeva ($P$) na sebe, a takvih ima $2^{\aleph_0} = c$, određuje jedinstven automorfizam $\phi$ naše grupe, takav da je $\phi|_P = \varphi$ (preciznije rečeno, $\varphi$ se može proširiti na jedinstven način do automorfizma grupe). U osnovi ovog tvrđenja je poznata činjenica da se svaki pozitivan racionalan broj može na jedinstven način predstaviti kao proizvod elemenata iz skupa $P \bigcup P^{-1}$ ($(P^{-1}$ je, podsećamo, $\{p^{-1} \mid p \in P\}$). Ako je $a = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$, $\alpha_i \in Z \setminus \{0\}$ (indeks $i$ ovde ne znači da je $p_i$ $i$-ti po redu prost broj), stavimo jednostavno $(a)\phi = ((p_1)\varphi)^{\alpha_1} \cdot \ldots \cdot ((p_n)\varphi)^{\alpha_n}$; lako se proverava da je $\phi$ jedinstven automorfizam saglasan sa $\varphi$ na skupu $P$.

Naravno, ovim nisu obuhvaćeni svi automorfizmi grupe, npr. i svaka bijekcija $\varphi : P \longrightarrow P^{-1}$ ( jedna od njih je $p \longrightarrow p^{-1}$) može se proširiti do automorfizma, kao i svako bijektivno preslikavanje $\varphi$ skupa $P \bigcup P^{-1}$ na sebe, koja ispunjava uslov $(p^{-1})\varphi = ((p)\varphi)^{-1}$.

Analogno razmatranje vredi i za grupu $\langle Ra \setminus \{0\}, \cdot\rangle$, s tim što sada umesto skupa $P$ imamo u vidu skup $P \bigcup -P$ ($-P \stackrel{\text{def}}{=} \{-p \mid p \in P\}$). Jasno, bijektivno preslikavanje $\varphi$ skupa $P \bigcup -P$ na sebe mora ispunjavati uslov $(-p)\varphi = -(p)\varphi$ da bi se moglo proširiti do automorfizma; jer svaki automorfizam ove grupe preslikava $-1$ u $-1$ budući da je to jedini element reda 2.

Iz (*e*), (*f*) i (*g*) proizilazi da grupa $\mathbf{Ra}$ nije izomorfna ni sa jednom od grupa $\langle Ra^+, \cdot\rangle$, $\langle Ra \setminus \{0\}, \cdot\rangle$ (a ni ove dve nisu međusobno izomorfne – grupa $\langle Ra^+, \cdot\rangle$ nema element reda 2). No to se može vrlo jednostavno i direktno pokazati. Naime, iz $\varphi \in Is(\mathbf{Ra}, \langle Ra^+, \cdot\rangle)$ i $(a)\varphi = 2$ sledilo bi: $(a)\varphi = (\frac{a}{2} + \frac{a}{2})\varphi = ((\frac{a}{2})\varphi)^2 = 2$, pa bi, po tome, $\sqrt{2}$ bio racionalan broj. Ovo tvrđenje je, inače, samo poseban slučaj opšteg stava (videti dokaz leme 19.16):

*Ni za jedno polje $\mathbf{F} = \langle F, +, \cdot\rangle$, grupe $\langle F, +\rangle$ (aditivna grupa polja $\mathbf{F}$) i $\langle F \setminus \{0\}, \cdot\rangle$ (multiplikativna grupa polja $\mathbf{F}$) nisu izomorfne.*

Pretpostavljeni izomorfizam $\varphi \in Is(\langle F \setminus \{0\}, \cdot\rangle, \langle F, +\rangle)$ bi dao:

$$(1)\varphi = ((-1)^2)\varphi = (-1)\varphi + (-1)\varphi = 0,$$

pa bi karakteristika polja bila 2. Polje, naravno, ne može biti konačno, a pošto bi važilo: $\forall a \in F \setminus \{0\}$ $(a^2)\varphi = 0$, injektivnost preslikavanja $\varphi$ bi dala $a^2 = 1$ za svaki nenula element $a$. To bi opet značilo da jednačina $x^2 = 1$ ima u polju $\mathbf{F}$ beskonačno mnogo rešenja, kontradikcija.□

Kad smo već spomenuli polja dajemo i definicije prstena, polja i vektorskih struktura, premda ćemo se na ove strukture samo iznimno pozivati.

**Definicija 2.11** *Prsten $\mathbf{R} = \langle R, +, \cdot\rangle$ je algebra sa dve binarne operacije ($+$ i $\cdot$) takva da je $\langle R, +\rangle$ Abelova grupa i $\langle R, \cdot\rangle$ polugrupa, dok je operacija $\cdot$ distributivna u odnosu na $+$:*

$$\forall x, y, z \;\; z \cdot (x + y) = z \cdot x + z \cdot y, \;\; (x + y) \cdot z = x \cdot z + y \cdot z.$$

*Prsten* $\mathbf{R}$ *je komutativan akko je polugrupa* $\langle R, \cdot \rangle$ *komutativna; prsten* $\mathbf{R}$ *sa bar dva elementa je sa jedinicom akko polugrupa* $\langle R, \cdot \rangle$ *ima jedinični element; nenula element* $a$ *prstena* $\mathbf{R}$ *(element različit od neutralnog elementa grupe* $\langle R, + \rangle$ *- 0) je levi delitelj nule akko postoji nenula element* $b (\in R)$ *takav da je* $a \cdot b = 0$*; analogno se definiše desni delitelj nule ; element prstena je delitelj nule akko je i levi i desni delitelj nule.*

*Komutativan prsten* $\mathbf{R}$ *sa jedinicom i bez delitelja nule zove se integralni domen.*

*Polje je integralni domen,* $\langle R, +, \cdot \rangle$*, za koji još važi da je* $\langle R \setminus \{0\}, \cdot \rangle$ *grupa.*

*Abelova grupa* $\mathbf{V} = \langle V, + \rangle$ *je vektorski prostor nad poljem* $\mathbf{F} = \langle F, +, \cdot \rangle$ *(u cilju razlikovanja operacija grupe i polja praksa je da se elementi grupe* $\mathbf{V}$*, tj. vektori, označavaju malim latiničnim, a elementi polja, tj. skalari, malim grčkim slovima) ako je dato preslikavanje* $F \times V \longrightarrow V$ *(sliku elementa* $(\alpha, a)$ *označavaćemo sa* $\alpha a$*) za koje važi (za svako* $a, b \in V$ *i svako* $\alpha, \beta \in F$*):*

(1) $\alpha(a + b) = \alpha a + \alpha b$;

(2) $(\alpha + \beta)a = \alpha a + \beta a$;

(3) $\alpha(\beta a) = (\alpha \cdot \beta)a$

*i*

(4) $1a = a$ (1 *je jedinični element grupe* $\langle F \setminus \{0\}, \cdot \rangle$ *- multiplikativne grupe polja* $\mathbf{F}$*).*

Navedimo samo (nešto više o prstenima i poljima biće u paragrafu 19)

**Lema 2.12** *U svakom prstenu* $\mathbf{R} = \langle R, +, \cdot \rangle$ *važi (za svako* $a, b \in R$*):*

(1) $a \cdot 0 = 0 \cdot a = 0$;

(2) $a \cdot (-b) = (-a) \cdot b = -(ab)$ ($-a$ *je, jasno, inverzni element elementa* $a$ *u grupi* $\langle R, + \rangle$);

(3) $(-a) \cdot (-b) = ab$.

**Dokaz**. Direktna posledica distributivnosti operacije $\cdot$ u odnosu na $+$ i svojstva kancelacije. Na primer:

(1) $0 + a \cdot 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ i odatle $0 = a \cdot 0$. Analogno, $0 \cdot a = 0$.

U dokazu tačke (2) treba koristiti tačku (1), u dokazu tačke (3) tačku (2) i jedinstvenost inverznog elementa (dakle, $-(-a) = a$).□

**Lema 2.13** *Algebra* $\langle Z_n, +_n, \cdot_n \rangle$ *je komutativan prsten sa jedinicom za* $n > 1$*, a polje akko je* $n$ *prost broj.*

**Dokaz**. Direktna posledica tačaka $(b)$ i $(c)$ primera 2.4.□

Konstatujmo ovom prilikom još i sledeće



**Lema 2.14** *Neka je* $\mathbf{G}$ *grupoid i* $\mathbf{H}$ *njegova homomorfna slika. Ako je grupoid* $\mathbf{G}$ *komutativan (asocijativan, sa (levim, desnim) jediničnim elementom), onda je i grupoid* $\mathbf{H}$ *komutativan (asocijativan, sa (levim, desnim) jediničnim elementom).*

**Korolar 2.15** *Ako je* $\mathbf{G}$ *grupa i* $\mathbf{H}$ *njena homomorfna slika, onda je i* $\mathbf{H}$ *grupa.*

**Dokaz**. Koristiti prethodnu lemu i definiciju 2.3.□

Ništa od navedenog u 2.14 ne važi u obrnutom smeru. Kontraprimeri se lako dobijaju uzimanjem za $\mathbf{H}$ jednoelementne grupe i izborom adekvatnog (nekomutativnog, neasocijativnog,...) grupoida $\mathbf{G}$.

**Lema 2.16** *Grupa je Abelova akko je preslikavanje* $x \longrightarrow x^{-1}$ *automorfizam akko je preslikavanje* $x \longrightarrow x^2$ *endomorfizam.*

# 3 Podgrupe

Ispitivanje grupe se u osnovi svodi na traženje njenih podgrupa (posebno nekih, iz raznih razloga specifičnih), kao i relacija koja među tim podgrupama postoje.

**Definicija 3.1** *Neka je* $\mathbf{G} = \langle G, \cdot \rangle$ *grupa,* $H$ *neprazan podskup njenog domena i neka je* $\mathbf{H} = \langle H, \cdot|_{H^2} \rangle$ *takođe grupa* ($\cdot|_{H^2}$ *je restrikcija funkcije* $\cdot$ *na skup* $H^2$ *- naravno, nadalje ćemo pisati jednostavno* $\langle H, \cdot \rangle$*). Grupa* $\mathbf{H}$ *je onda podgrupe grupe* $\mathbf{G}$*; pišemo* $\mathbf{H} \leq \mathbf{G}$.

$\mathbf{H}$ *je prava podgrupa grupe* $\mathbf{G}$ *(pišemo* $\mathbf{H} < \mathbf{G}$*) akko je* $H$ *pravi podskup skupa* $G$ *(kad je u pitanju pravi podskup koristićemo notaciju* $H \subset G$*).*

Ako je $|G| \geq 2$ uvek imamo bar dve (tzv. trivijalne) podgrupe: samu grupu $\mathbf{G}$ i tzv. jediničnu podgrupu $\mathbf{E} = \langle \{e\}, \cdot \rangle$.

**Lema 3.2** *Neka je* $\mathbf{G} = \langle G, \cdot \rangle$ *grupa i neka je* $H$ *neprazan podskup skupa* $G$*.* $H$ *je domen podgrupe akko* $\forall a, b \in H \ a \cdot b^{-1} \in H$ *akko* $(i)$ $\forall a, b \in H \ a \cdot b \in H$ *i* $(ii)$ *ako* $a \in H$*, onda i* $a^{-1} \in H$*.*

**Dokaz**. Proverimo samo "pravac" ($\Longleftarrow$) prvog "akko" (drugi pravac je trivijalan). Neka $a \in H$. Onda i $a \cdot a^{-1} = e \in H$ pa odatle $e \cdot a^{-1} = a^{-1} \in H$. Zatvorenost takođe važi, jer ako $a, b \in H$, onda i $a \cdot b = a \cdot (b^{-1})^{-1} \in H$.□

**Napomena**. Ako je, za neprazne poskupove $H$ i $K$ domena grupe $\mathbf{G}$, $H^{-1} \stackrel{\text{def}}{=} \{h^{-1} \mid h \in H\}$ i $HK \stackrel{\text{def}}{=} \{hk \mid h \in H, k \in K\}$ (tzv. *proizvod* skupova $H$ i $K$ - notaciju ćemo zadržati kroz celi tekst), tada, prema prethodnoj lemi, očigledno važi:

*neprazan podskup* $H$ *domena grupe* $\mathbf{G}$ *je domen podgrupe akko* $(i)$ $HH \subseteq H$ *i* $(ii)$ $H = H^{-1}$.

**Korolar 3.3** *(a) Konačna polugrupa* $\mathbf{H}$ *u kojoj važi zakon kancelacije je grupa;*

*(b) Neka je* $H$ *neprazan, konačan podskup domena* $G$ *grupe* $\mathbf{G}$. $H$ *je domen podgrupe akko važi:* $\forall a, b \in H \;\; a \cdot b \in H$;

*(c) Neka je* $\varphi$ *homomorfno preslikavanje grupe* $\mathbf{G}$ *u grupu* $\mathbf{H}$ *i neka je* $\mathbf{B}$ *podgrupa grupe* $\mathbf{H}$. *Tada je* $(B)\varphi^{-1} \stackrel{\text{def}}{=} \{g \in G \mid (g)\varphi \in B\}$ *domen podgrupe grupe* $\mathbf{G}$, *koju ćemo (pomalo proizvoljno) označiti sa* $(\mathbf{B})\varphi^{-1}$.

**Dokaz.** *(a)* Neka je $a$ ma koji element polugrupe $\mathbf{H}$. Zbog konačnosti polugrupe i zakona kancelacije koji u njoj važi dobijamo $aH \stackrel{\text{def}}{=} \{ah \mid h \in H\} = H$ kao i $Ha = H$ (naravno, $Ha \stackrel{\text{def}}{=} \{ha \mid h \in H\}$). Stoga je $ae = a$ za neko $e$ iz $H$. Element $e$ je desni jedinični element polugrupe; jer, ako je $b$ ma koji element i $ca = b$ (sada koristimo $Ha = H$), onda je: $be = (ca)e = c(ae) = ca = b$. Trivijalno pak sledi da za ovaj desni jedinični element svaki element polugrupe ima desni inverzni, pa je $\mathbf{H}$ grupa (2.3).

*(b)* Neposredna posledica prethodne tačke no dajemo i direktan dokaz. Od interesa je, jasno, samo pravac ($\Longleftarrow$). Svaki element iz $H$ je konačnog reda, pošto su svi njegovi stepeni u $H$ a skup $H$ je konačan; to opet znači da ako je $a$ u $H$, onda je i $a^{-1}$ u $H$.

Primetimo još da se uslov konačnosti podskupa $H$ ne može isključiti. Tako je npr. skup prirodnih brojeba zatvoren za sabiranje, ali $\langle \omega, + \rangle$ nije podgrupa grupe $\mathbf{Z}$.

*(c)* Primetimo samo da je $(B)\varphi^{-1}$ neprazan skup jer sadrži barem $e_G$ ($(e_G\varphi = e_H \in B)$; ostalo je još očiglednije.□

**Primer 3.4** *(a) Neka je* $\mathbf{G}$ *grupa.* $Z(\mathbf{G}) \stackrel{\text{def}}{=} \{a \in G \mid \forall g \in G \;\; a \cdot g = g \cdot a\}$ *je domen podgrupe koju zovemo centrom grupe* $\mathbf{G}$ *i obeležavamo sa* $\mathbf{Z}(\mathbf{G})$ *(ili koji put, kao u četvrtoj glavi, sa* $\zeta_1\mathbf{G}$ – 46.23*). Ako je* $\mathbf{Z}(\mathbf{G}) = \mathbf{E}$, *kažemo i da je grupa* $\mathbf{G}$ *bez centra. Jasno,* $\mathbf{G} = \mathbf{Z}(\mathbf{G})$ *akko je* $\mathbf{G}$ *Abelova grupa.*

*(b) Neka je* $a$ *element grupe* $\mathbf{G}$. *Skup* $C(a) \stackrel{\text{def}}{=} \{g \in G \mid g \cdot a = a \cdot g\}$ *je takozvani centralizator elementa* $a$. *Opet je* $\mathbf{C}(a) = \langle C(a), \cdot \rangle$ *podgrupa grupe* $\mathbf{G}$. *Očigledno:* $\mathbf{C}(a) = \mathbf{G}$ *akko* $a \in Z(\mathbf{G})$.

*Analogno definišemo centralizator ma kog nepraznog podskupa* $X$ *(ili podgrupe* $\mathbf{H}$*) skupa* $G$ *(grupe* $\mathbf{G}$*):* $C(X) \stackrel{\text{def}}{=} \{g \in G \mid \forall x \in X \; x \cdot g = g \cdot x\}$. *Lako se proverava da je i to domen podgrupe (*$\mathbf{C}(X)$*). Centralizator podgrupe* $\mathbf{H}$ *označavaćemo sa* $\mathbf{C}(\mathbf{H})$).

*(c) Svaki od sledećih podskupova je nosač podgrupe grupe* $\mathbf{GL}_n(\mathbf{Re})$:
*(i)* $\{A \in GL_n(\mathbf{Re}) \mid det(A) > 0\}$;
*(ii)* $\{A \in GL_n(\mathbf{Re}) \mid det(A) = 1\}$;



*(iii)* $\{A \in GL_n(\mathbf{Re}) \mid A$ *je gornja trougaona matrica, tj.* $a_{ij} = 0$ *za* $j < i\}$; $\{A \in GL_n(\mathbf{Re}) \mid A$ *je donja trougaona matrica, tj.* $a_{ij} = 0$ *za* $j > i\}$;
*(iv)* $\{A \in GL_n(\mathbf{Re}) \mid A$ *je dijagonalna matrica* $\}$.

*(d) Skupovi (i)* $\{f \in S_A \mid f|_X = \imath_X\}$, *gde je* $\emptyset \neq X \subseteq A$, *i* $\imath_X$ *identično preslikavanje skupa* $X$ *i (ii)* $\{f \in S_A \mid f$ *"premešta" samo konačno mnogo elemenata* $\}$ *su domeni podgrupa grupe* $\mathbf{S}_A$.

*(e) Skup* $I^p \stackrel{\text{def}}{=} \{f \in S_{Re} \mid \forall a, b \; |a - b| = |(a)f - (b)f|\}$ *je domen podgrupe grupe* $\mathbf{S}_{Re}$, *tzv. grupe izometrija prave (elementi skupa* $I^p$ *su, dakle, bijektivna preslikavanja realne ose koja očuvavaju rastojanje).*

**Dokaz.** $I^p \neq \emptyset$ jer (identično preslikavanje) $\imath \in I^p$, a ako je $f, g \in I^p$, onda je $|(a)(f \circ g^{-1}) - (b)(f \circ g^{-1})| = |((a)(f \circ g^{-1}))g - ((b)(f \circ g^{-1})g| = |(a)f - (b)f| = |a - b|$, pa je i $f \circ g^{-1} \in I^p$.

*Grupa izometrija ravni se definiše analogno. Njen domen* $(I^r)$ *je, znači, skup svih funkcija* $f \in S_{Re \times Re}$ *takvih da je za svako* $(a, c), (b, d) \in Re \times Re$:

$$\sqrt{(a-b)^2 + (c-d)^2} = \sqrt{(a_1 - b_1)^2 + (c_1 - d_1)^2},$$

*gde je* $(a, c)f = (a_1, c_1)$ *i* $(b, d)f = (b_1, d_1)$; *geometrijski gledano, njeni elementi su biunivoka preslikavanja ravni koja očuvavaju rastojanja.*

**Dokaz** Provera da se zaista radi o grupi slična je prethodnom slučaju. Iskoristićemo ovaj primer da dobijemo jednu interesantnu familiju grupa (dijedarske grupe) koja će nas pratiti kroz celu knjigu.

Za tipične predstavnike izometrija uzimamo:
*translacije* $\tau_{a,b}$, $a, b \in Re$ : $(x, y)\tau_{a,b} = (x + a, y + b)$;
*rotacije* $\rho_\alpha$ oko koordinatnog početka za ugao $\alpha$ u tzv. pozitivnom smeru tj. u smeru suprotnom kretanju kazaljke na satu ako je $\alpha > 0$: $(x, y)\rho_\alpha = (x\cos\alpha - y\sin\alpha, x\sin\alpha + y\cos\alpha)$;
*simetrično preslikavanje u odnosu na* $y-$*osu,* $\sigma_y$: $(x, y)\sigma_y = (-x, y)$.

Primetimo: $\tau_{0,0} = \rho_0 = \imath$ (identično preslikavanje), $(\tau_{a,b})^{-1} = \tau_{-a,-b}$, $(\rho_\alpha)^{-1} = \rho_{-\alpha}$, $(\sigma_y)^{-1} = \sigma_y$, $\tau_{a,c} \circ \tau_{b,d} = \tau_{a+b,c+d}$, $\rho_\alpha \circ \rho_\beta = \rho_{\alpha+\beta}$.

Važi (što i obrazlaže naš izbor tipičnih izometrija)

**Stav 1** (1) *Svaki element grupe izometrija ravni određen je slikom triju nekolinearnih tačaka;*

(2) *Svaka izometrija je proizvod tipičnih izometrija.*

**Dokaz.** (1) Neka su $A$, $B$ i $C$ tri nekolinearne tačke (umesto sa uređenim parovima realnih brojeva nadalje ćemo raditi sa tačkama ravni čije su koordinate tim parovima određene) i neka je, za $f, g \in I^r$, $(A)f = (A)g = A_1, (B)f = (B)g = B_1$ i $(C)f = (C)g = C_1$. Neka je, dalje, $D$ proizvoljna tačka ravni (različita od $A$, $B$ i $C$) pa pokažimo da je $(D)f = (D)g$. Ako je

$d(A,D) = a$, $d(B,D) = b$ i $d(C,D) = c$, tada je $d(A_1,(D)f) = d(A_1,(D)g) = a$, $d(B_1,(D)f) = d(B_1,(D)g) = b$ i $d(C_1,(D)f) = d(C_1,(D)g) = c$ ($d(A,B)$ je rastojanje tačaka $A$ i $B$). Prema tome tačke $(D)f$ i $(D)g$ leže u preseku kružnica $O_1, O_2$ i $O_3$, sa centrima u, respektivno, $A_1, B_1, C_1$ i poluprečnicima $a$, $b$ i $c$. No onda je $(D)f = (D)g$; u suprotnom bi kružnice $O_1$, $O_2$ i $O_3$ imale dve zajedničke tačke, pa bi njihovi centri bili kolinearni, ali trougao $\Delta ABC$ podudaran je trouglu $\Delta A_1B_1C_1$ (radi se o trouglovima sa jednakim stranama), kontradikcija.

(2) Neka je data izometrija $f$. Uočimo tačke $O(0,0)$, $A(1,0)$ i $B(0,1)$, i pretpostavimo da je $(O)f = (a,b)$. Tada je $((O)f)\tau_{-a,-b} = O$, a tačka $((B)f)\tau_{-a,-b}$ mora ležati na kružnici sa centrom u koordinatnom početku poluprečnika 1, jer je $1 = d(O,B) = d((O)(f \circ \tau_{-a,-b}), (B)(f \circ \tau_{-a,-b}))$. Stoga $(B)(f \circ \tau_{-a,-b})$ ima koordinate $(cos\alpha, sin\alpha)$, za neki ugao $\alpha$, te je $(B)(f \circ \tau_{-a,-b} \circ \rho_{\frac{\pi}{2}-\alpha}) = B$ i, naravno, $(O)(f \circ \tau_{-a,-b} \circ \rho_{\frac{\pi}{2}-\alpha}) = O$. Proizilazi: $d((A)(f \circ \tau_{-a,-b} \circ \rho_{\frac{\pi}{2}-\alpha}), O) = 1$ i $d((A)(f \circ \tau_{-a,-b} \circ \rho_{\frac{\pi}{2}-\alpha}), B) = \sqrt{2}$, pa je $(A)(f \circ \tau_{-a,-b} \circ \rho_{\frac{\pi}{2}-\alpha})$ ili tačka $A$ ili tačka $(-1,0)$. U prvom slučaju $f \circ \tau_{-a,-b} \circ \rho_{\frac{\pi}{2}-\alpha}$ ostavlja fiksnim tri nekolinearne tačke $O$, $A$ i $B$, dakle, prema (1), $f \circ \tau_{-a,-b} \circ \rho_{\frac{\pi}{2}-\alpha} = \imath$, tj. $f = \rho_{\alpha-\frac{\pi}{2}} \circ \tau_{a,b}$. U drugom slučaju je $f \circ \tau_{-a,-b} \circ \rho_{\frac{\pi}{2}-\alpha} \circ \sigma_y = \imath$ i $f = \sigma_y \circ \rho_{\alpha-\frac{\pi}{2}} \circ \tau_{a,b}$.

Očigledno, umesto simetrije u odnosu na $y-$osu mogli smo koristiti i simetriju u odnosu na $x$-osu ($\sigma_x = \sigma_y \circ \rho_\pi$).□

Čitaocu prepuštamo da dokaže sledeće:

**Stav 2.** *Svaki element grupe* $\mathbf{I}^p$ *određen je slikom dveju (različitih) tačaka; za tipične izometrije, u smislu gornjeg tvrđenja, možemo uzeti translacije:*

$$\tau_a : \ (x)\tau_a = x + a$$

*i simetriju u odnosu na koordinatni početak*

$$\sigma : \ (x)\sigma = -x.$$

Vratimo se ponovo grupi izometrije ravni $\mathbf{I}^r$. Neka je $S$ neprazan podskup ravni i neka je $D_S = \{f \in I^r \mid \forall A \in Re \times Re \ \ A \in S$ akko $(A)f \in S\}$. $D_S$ je domen podgrupe grupe $\mathbf{I}^r$ (dakle i grupe $\mathbf{S}_{Re\times Re}$). Jasno, $D_S \neq \emptyset$ (uvek $\imath \in D_S$); ako $f, g \in D_S$, očigledno $f \circ g \in D_S$, a zbog $A = ((A)f^{-1})f \in S$ akko $(A)f^{-1} \in S$, i $f^{-1} \in D_S$. Grupu $\mathbf{D}_S$ zovemo grupom simetrije skupa $S$. Posebno, grupa simetrija pravilnog $n-$tougla zove se dijedarska grupa stepena $n$ i obično se označava sa $\mathbf{D}_n$. Uočimo sledeće:

**Stav 3.** *Neka je $S$ pravilan $n-$tougao. Tada svako $f$ iz $D_n$ ostavlja fiksnim centar kruga opisanog oko $S$, a temena preslikava u temena. Takođe važi:* $|D_n| = 2n$.

**Dokaz.** Neka je $A$ centar a $R$ poluprečnik kružnice opisane oko $S$. $A$ je jedinstvena tačka ravni sa svojstvom: $\forall B \in S \ \ d(A,B) \leq R$. Kako je $(S)f = S$ i kako $f$ očuvava rastojanje, to je $(A)f = A$, pa se i temena preslikavaju u temena.



U daljem, pretpostavićemo da je centar opisane kružnice koordinatni početak i da je (bar) jedno teme, recimo $A_1$, na $y$-osi (da li će još jedno teme biti na $y$-osi zavisi, naravno, od parnosti broja $n$, u svakom slučaju $y$-osa je jedna osa simetrije našeg $n$-tougla; isto tako učinjeni izbor ne utiče na opštost razmatranja – ovim jednostavno želimo da iskoristimo već uvedenu notaciju). Očigledno su

$$\imath, \rho_{\frac{2\pi}{n}}, \rho_{2\frac{2\pi}{n}} = (\rho_{\frac{2\pi}{n}})^2, \ldots, \rho_{(n-1)\frac{2\pi}{n}} = (\rho_{\frac{2\pi}{n}})^{n-1}, \sigma_y, \sigma_y \circ \rho_{\frac{2\pi}{n}}, \ldots, \sigma_y \circ \rho_{(n-1)\frac{2\pi}{n}}$$

različiti elementi grupe $\mathbf{D}_n$. No više od $2n$ elemenata i ne može biti u $D_S$. Jer, slika temena $A_1$ mora, upravo smo videli, opet biti teme; za njen izbor imamo, dakle, na raspolaganju $n$ temena. Kako je slika temena $A_2$ teme susedno slici temena $A_1$, nakon učinjenog izbora za sliku temena $A_1$, preostaju nam dve mogućnosti za izbor slike temena $A_2$, a jednom odabrane slike ova dva temena određuju slike ostalih temena.

Na kraju ovog primera dajemo i Cayleyevu tablicu dijedarske grupe stepena 4 tj. grupe simetrije kvadrata. U cilju pojednostavljenja notacije a time i preglednosti tablice, umesto $\sigma_y$ i $\rho_{\frac{2\pi}{4}} = \rho_{\frac{\pi}{2}}$ pisaćemo samo, respektivno, $\sigma$, $\rho$, pa će $\rho_{2\frac{2\pi}{4}} = \rho_\pi$ i $\rho_{3\frac{2\pi}{4}} = \rho_{\frac{3\pi}{2}}$ biti $\rho^2$, tj. $\rho^3$. Tablica se lako dobija koristeći se relacijama $\rho \circ \sigma = \sigma \circ \rho^3$ i $\rho^4 = \sigma^2 = \imath$. U tabeli ćemo takođe izostavljati znak operacije $\circ$.

| $\circ$ | $\imath$ | $\rho$ | $\rho^2$ | $\rho^3$ | $\sigma$ | $\sigma\rho$ | $\sigma\rho^2$ | $\sigma\rho^3$ |
|---|---|---|---|---|---|---|---|---|
| $\imath$ | $\imath$ | $\rho$ | $\rho^2$ | $\rho^3$ | $\sigma$ | $\sigma\rho$ | $\sigma\rho^2$ | $\sigma\rho^3$ |
| $\rho$ | $\rho$ | $\rho^2$ | $\rho^3$ | $\imath$ | $\sigma\rho^3$ | $\sigma$ | $\sigma\rho$ | $\sigma\rho^2$ |
| $\rho^2$ | $\rho^2$ | $\rho^3$ | $\imath$ | $\rho$ | $\sigma\rho^2$ | $\sigma\rho^3$ | $\sigma$ | $\sigma\rho$ |
| $\rho^3$ | $\rho^3$ | $\imath$ | $\rho$ | $\rho^2$ | $\sigma\rho$ | $\sigma\rho^2$ | $\sigma\rho^3$ | $\sigma$ |
| $\sigma$ | $\sigma$ | $\sigma\rho$ | $\sigma\rho^2$ | $\sigma\rho^3$ | $\imath$ | $\rho$ | $\rho^2$ | $\rho^3$ |
| $\sigma\rho$ | $\sigma\rho$ | $\sigma\rho^2$ | $\sigma\rho^3$ | $\sigma$ | $\rho^3$ | $\imath$ | $\rho$ | $\rho^2$ |
| $\sigma\rho^2$ | $\sigma\rho^2$ | $\sigma\rho^3$ | $\sigma$ | $\sigma\rho$ | $\rho^2$ | $\rho^3$ | $\imath$ | $\rho$ |
| $\sigma\rho^3$ | $\sigma\rho^3$ | $\sigma$ | $\sigma\rho$ | $\sigma\rho^2$ | $\rho$ | $\rho^2$ | $\rho^3$ | $\imath$ . |

Primetimo još: generalno, za bilo koje $n$ veće od 2, u dijedarskoj grupi $\mathbf{D}_n$ važi:

$$\rho_{\frac{2\pi}{n}} \circ \sigma_y = \sigma_y \circ \rho_{\frac{2\pi}{n}}^{n-1}, \ \rho_{\frac{2\pi}{n}}^n = \sigma_y^2 = \imath.$$

Lako se proverava da je ovim relacijama potpuno određena "tablica množenja" date dijedarske grupe.□

*(f) Za prost broj $p$ Prüferova ili kvaziciklična $p$-grupa, u oznaci $\mathbf{p}^\infty$, podgrupa je multiplikativne grupe nenula kompleksnih brojeva, $\langle C \setminus \{0\}, \cdot\rangle$, sa domenom $\{z \in C \mid z^{p^n} = 1, n \in \omega\}$.*

*(g) U polugrupi sa jediničnim elementom skup inverzibilnih (invertibilnih) elemenata domen je njene podpolugrupe koja je ujedno i grupa.*

**Napomena.** Prema poslednjoj tački prethodnog primera i 2.4(*c*), za prirodan broj $n$ veći od 1 je $\langle\{a \in n \mid (a,n) = 1\}, \cdot_n\rangle$ grupa reda $\varphi(n)$. Eulerova funkcija $\varphi(n) \stackrel{\text{def}}{=} |\{a \mid 1 \leq a < n, (a,n) = 1\}|$ (Leonhard Euler, 1707-1783), podsećamo, za $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, gde su $p_i$, $1 \leq i \leq k$, (različiti) prosti brojevi i $\alpha_i \geq 1$, ima vrednost $n \cdot \prod_{i=1}^{k}(1 - \frac{1}{p_i})$.

**Definicija 3.5** *Neka je* $\mathbf{H}$ *podgrupa i* $a$ *element grupe* $\mathbf{G}$. *Skup* $aH$ *već definisan u dokazu tačke* (*a*) *leme* 3.3 *(svejedno, podsećamo:* $aH \stackrel{\text{def}}{=} \{ah \mid h \in H\}$*)* $(Ha)$ *zovemo levim (desnim) kosetom (suskupom, razredom, kompleksom) podgrupe* $\mathbf{H}$ *određen elementom* $a$.

**Lema 3.6** *Neka je* $\mathbf{H}$ *podgrupa grupe* $\mathbf{G}$. *Tada važi:*

(*a*) $\forall a, b \in G \ \ |aH| = |Hb| = |H|$;

(*b*) $b \in aH \ \ (b \in Ha)$ *akko* $aH = bH \ \ (Ha = Hb)$;

(*c*) *Relacija* $\rho_H$, *definisana na skupu* $G$ *sa:* $a\rho_H b$ *akko* $b \in aH \ \ (b \in Ha)$, *relacija je ekvivalencije;*

(*d*) $|\{aH \mid a \in G\}| = |\{Hb \mid b \in G\}|$.

**Dokaz.** (*a*) i (*b*) je trivijalno, (*c*) je direktna posledica tačke (*b*).

(*d*) Funkcija $F : aH \longrightarrow Ha^{-1}$ bijektivno je preslikavanje skupa levih koseta $\{aH \mid a \in G\}$ u skup desnih koseta $\{Hb \mid b \in G\}$.□

**Definicija 3.7** *Kardinalni broj skupa levih (desnih) koseta podgrupe* $\mathbf{H}$ *zovemo indeksom podgrupe* $\mathbf{H}$ *i označavamo ga sa* $[\mathbf{G} : \mathbf{H}]$. *Ako je* $[\mathbf{G} : \mathbf{H}]$ *prirodan broj kažemo da je podgrupa* $\mathbf{H}$ *konačnog indeksa.*

Primetimo da važi:

**Lema 3.8** *Ako je* $\mathbf{H}$ *podgrupa indeksa* $n$ *konačne grupe* $\mathbf{G}$, *postoje elementi* $g_1, \ldots, g_n$ *takvi da su* $\{g_i H \mid 1 \leq i \leq n\}$ *i* $\{Hg_i \mid 1 \leq i \leq n\}$, *respektivno, skupovi (svih) levih odnosno desnih koseta.*

**Dokaz.** Tvrđenje je direktna posledica sledeće teoreme diskretne matematike:

*Među familijama nepraznih podskupova* $\{A_1, \ldots, A_n\}$ *i* $\{B_1, \ldots, B_n\}$ *konačnog skupa* $G$ *postoji uzajamno jednoznačna korespondencija takva da korespondentni skupovi imaju neprazan presek akko za svaka dva podskupa* $I, J$ *skupa* $\{1, \ldots, n\}$ *važi:*

$$|\bigcup_{i \in I} A_i \cap \bigcup_{j \in J} B_j| \geq |I| + |J| - n.$$



Očigledno, uslovi teoreme su ispunjeni za bilo koji izbor skupova levih i desnih koseta, a koset je, već smo videli, određen bilo kojim svojim elementom.□

Prethodni rezultat nije moguće uopštiti. Tako u grupi

$$\mathbf{G} = \langle\{\begin{bmatrix} 2^k & p(x) \\ 0 & 1 \end{bmatrix} \mid p(x) \in Ra[x],\ k \in Z\}, \cdot\rangle$$

($\cdot$ je matrično množenje) levi koset podgrupe

$$\mathbf{H} = \langle\{\begin{bmatrix} 1 & q(x) \\ 0 & 1 \end{bmatrix} \mid q(x) \in Z[x]\}\rangle$$

određen elementom $\begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{bmatrix}$ sadrži beskonačno mnogo desnih koseta iste podgrupe, npr. sve one određene elementima $A_n = \begin{bmatrix} \frac{1}{2} & \frac{1}{2}x^n \\ 0 & 1 \end{bmatrix}$, $n \in \omega$, te ne postoji skup elemenata $\{B_k \mid k \in \omega\}$ takav da su $\{B_k H \mid k \in \omega\}$ i $\{HB_k \mid k \in \omega\}$ skupovi (svih) levih tj. desnih koseta podgrupe $\mathbf{H}$ (imamo u vidu 3.6(*b*) i činjenicu da levi i desni koset istog elementa imaju neprazan presek).

**Korolar 3.9** *Neka je* $\mathbf{H}$ *podgrupa grupe* $\mathbf{G}$. *Tada važi:*

(*a*) $|G| = |H| \cdot [\mathbf{G} : \mathbf{H}]$;

(*b*) *Ako je* $\mathbf{G}$ *konačna grupa,* $|H|$ *i* $[\mathbf{G} : \mathbf{H}]$ *su delioci reda grupe.*

**Dokaz.** (*a*) Relacija $\rho_H$ vrši particiju skupa $G$ i klase ekvivalencije su baš levi (desni) koseti podgrupe $\mathbf{H}$. Preostaje još samo da se iskoristi sledeća činjenica: ako su $A_i$, $i \in I$, neprazni disjunktni skupovi iste kardinalnosti $\lambda$, onda su skupovi $\bigcup_{i \in I} A_i$ i $\lambda \times I$ iste kardinalnosti.□

**Korolar 3.10** *Ako je* $\mathbf{H} \leq \mathbf{G}$, $|G| \geq \aleph_0$ *i* $|H| < |G|$, *tada je* $[\mathbf{G} : \mathbf{H}] = |G|$.

**Primer 3.11** (*a*) *Za pozitivan prirodan broj* $n$ *je* $n\mathbf{Z} \stackrel{\text{def}}{=} \langle\{nz \mid z \in Z\}, +\rangle$ *podgrupa grupe* $\mathbf{Z}$ *indeksa* $n$;

$[\mathbf{Ra} : \mathbf{Z}] = \aleph_0$;

$[\mathbf{C} : \mathbf{Re}] = c$ (= *kontinuum*).

**Dokaz.** Koseti podgrupe $n\mathbf{Z}$ (grupe $\mathbf{Z}$) su (koristimo aditivnu notaciju): $Z$, $1 + Z$, ..., $(n-1) + Z$.

Ako su $p$ i $q$ različiti prosti brojevi, onda su $\frac{1}{p} + Z$ i $\frac{1}{q} + Z$ različiti koseti podgrupe $\mathbf{Z}$ grupe $\mathbf{Ra}$.

Dva kompleksna broja određuju isti koset podgrupe $\mathbf{Re}$ grupe $\mathbf{C}$ akko imaju iste imaginarne delove.

(*b*) *Podgrupa grupe* $\mathbf{GL}_n(\mathbf{Re})$, $n \geq 2$, *iz tačke* (*i*) *primera* 3.4(*c*) *indeksa je* 2, *dok su ostale (iz istog primera) indeksa c (kontinuum).*

**Dokaz.** Razmotrimo samo slučaj podgrupe regularnih gornjih trougaonih matrica (obeležimo je sa $\mathbf{H}$). Neka je $A_a$ matrica

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a & 0 & \dots & 1 \end{bmatrix}.$$

Lako se proverava da su levi koseti $A_aH$ i $A_bH$ različiti za različite brojeve $a$ i $b$. Stoga je $[\mathbf{GL}_n(\mathbf{Re}) : \mathbf{H}] \geq c$ pa je, naravno, $[\mathbf{GL}_n(\mathbf{Re}) : \mathbf{H}] = c$.

Čitaocu prepuštamo direktan dokaz - pretpostavka da je indeks podgrupe $\mathbf{H}$ manji od kardinalnosti $c$ vodi u kontradikciju.

(*c*) *Ako je* $|A| \geq \aleph_0$ *i* $|A| > |A \setminus X|$, *tada su podgrupe grupe* $\mathbf{S}_A$ *iz* 3.4(*d*) *reda, respektivno,* $2^{|A\setminus X|}$ *i* $2^{|A|}$, *dakle, obe su indeksa* $2^{|A|}$ *(zbog prve pogrupe pretpostavljamo da naša metateorija uključuje GCH).*

(*d*) *Grupa izometrija ravni* $\mathbf{I}^r$ *je kardinalnosti kontinuum.*

Pokazali smo da je svaka izometrija proizvod tipičnih, a takvih je kontinuum mnogo. Odatle $[\mathbf{S}_{Re\times Re} : \mathbf{I}^r] = 2^c$.

(*e*) *Grupa je periodična ako ima (pravu) periodičnu podgrupu konačnog indeksa.*

**Dokaz.** Neka je $\mathbf{H}$ periodična podgrupa konačnog indeksa grupe $\mathbf{G}$ i neka je $g \in G \setminus H$. Među kosetima $g^nH$, $n \in \omega$, mora biti jednakih, dakle, za neki prirodan broj $k$ veći od 1 je $g^kH = H$, tj. $g^k \in H$. Sledi da je element $g$ konačnog reda.

Primetimo da obrat gornjeg tvrđenja ne važi u opštem (tj. ako tražimo da je podgrupa prava). Jedan kontraprimer su, recimo, Prüferove grupe – videti napomenu uz 7.10.□

**Lema 3.12** *Ako je* $\mathbf{H}$ *podgrupa grupe* $\mathbf{K}$ *a* $\mathbf{K}$ *podgrupa grupe* $\mathbf{G}$, *tada je*

$$[\mathbf{G} : \mathbf{H}] = [\mathbf{G} : \mathbf{K}] \cdot [\mathbf{K} : \mathbf{H}].$$

**Dokaz.** Neka je $\{g_i \mid i \in I\}$ skup reprezenata levih koseta podgrupe $\mathbf{K}$, tzv. *leva transverzala* – iz svakog levog koseta izabrali smo po jednog "delegata" (čitalac već pogađa da je *desna tansverzala* skup reprezenata desnih koseta).

Korespondencija $\phi : (g_i, kH) \longrightarrow g_ikH$ je biunivoko preslikavanje skupa $\{g_i \mid i \in I\} \times \{kH \mid k \in K\}$ u skup $\{gH \mid g \in G\}$. Pokažimo samo da je "na". Neka je $g \in g_iK$. Tada je, za neko $k \in K$, $g = g_ik$, pa je $gH = g_ikH = (g_i, kH)\phi$.



Imamo prema tome $|\{g_i \mid i \in I\} \times \{kH \mid k \in K\}| = |\{gH \mid g \in G\}|$, tj. $|\{g_i \mid i \in I\}| \cdot |\{kH \mid k \in K\}| = |\{gH \mid g \in G\}|$, odnosno, $[\mathbf{G} : \mathbf{K}] \cdot [\mathbf{K} : \mathbf{H}] = [\mathbf{G} : \mathbf{H}]$.

Za $|G|$ konačno (dakle, kad nam je na raspolaganju i deljenje) možemo dati i ovakav dokaz:

prema 3.8 je $\frac{|K|}{|H|} = [\mathbf{K} : \mathbf{H}]$, odatle sledi redom

$$\frac{[\mathbf{G} : \mathbf{K}] \cdot |K|}{|H|} = [\mathbf{G} : \mathbf{K}] \cdot [\mathbf{K} : \mathbf{H}],$$

$$\frac{|G|}{|H|} = [\mathbf{G} : \mathbf{K}] \cdot [\mathbf{K} : \mathbf{H}],$$

$$[\mathbf{G} : \mathbf{H}] = [\mathbf{G} : \mathbf{K}] \cdot [\mathbf{K} : \mathbf{H}].\square$$

**Korolar 3.13** *Ako su* $\mathbf{H}$ *i* $\mathbf{K}$ *podgrupe grupe* $\mathbf{G}$ *i ako je* $\mathbf{H} \leq \mathbf{K}$, *tada je*

$$[\mathbf{G} : \mathbf{K}] \leq [\mathbf{G} : \mathbf{H}].$$

**Lema 3.14** *Ako su* $\mathbf{H}$ *i* $\mathbf{K}$ *podgrupe grupe* $\mathbf{G}$ *i ako je* $\mathbf{H} \leq \mathbf{K}$, *T leva (desna) transverzala podgrupe* $\mathbf{K}$ *u* $\mathbf{G}$ *i S leva (desna) transverzala podgrupe* $\mathbf{H}$ *u* $\mathbf{K}$, *onda je TS (ST) leva (desna) transverzala podgrupe* $\mathbf{H}$ *u* $\mathbf{G}$.

**Dokaz.** Videti (i analizirati) dokaz prethodne leme.□

**Lema 3.15** (*a*) *Podskup T domena grupe* $\mathbf{G}$ *je leva (desna) transverzala podgrupe* $\mathbf{H}$ *akko je, za svaki element g iz G, gT (Tg) leva (desna) transverzala podgrupe* $\mathbf{H}$;

(*b*) *Neka je T leva (desna) transvezala podgrupe* $\mathbf{H}$ *u* $\mathbf{G}$. *Ako je T domen (pod)polugrupe grupe* $\mathbf{G}$, *onda je i domen podgrupe.*

**Dokaz.** (*a*) Neka je $T$ leva transverzala podgrupe $\mathbf{H}$ u $\mathbf{G}$. Jasno, za različite elemente $a$ i $b$ iz $T$ je, zbog $aH \cap bH = \emptyset$, $gaH \cap gbH = \emptyset$. Dalje, ako je element $g^{-1}x$ u kosetu $aH$, onda je $x = g(g^{-1}x)$ element koseta $gaH$; dakle, $G = \bigcup_{a\in T} gaH$.

Analogno sledi: ako je $gT$ leva transverzala podgrupe $\mathbf{H}$, tada je to i $T$.

(*b*) Pretpostavimo da je leva transverzala, $T$, podgrupe $\mathbf{H}$ domen polugrupe i neka je $\mathbf{H}$ indeksa većeg od 1 (izbegavamo trivijalni slučaj). Pokazaćemo prvo da predstavnik koseta $H$ mora biti baš jedinični element; zaista, ako bi to bio nejedinični element $h$ iz $H$ i ako bi element $a$ iz $T$ bio predstavnik nekog drugog koseta ($aH \neq H$), imali bismo s jedne strane $a \neq ah \in T$, a s druge $aH = (ah)H$, kontradikcija. Slično, ako za nejedinični element $b$ iz $T$ ne bi bilo i $b^{-1}$ u $T$, onda bi za neko $c$ iz $T$ različito od $b^{-1}$ bilo $b^{-1} \in cH$, dakle i, za neki nejedinični element $h_1$ iz $H$, $b^{-1} = ch_1$, tj. $c = b^{-1}h_1^{-1}$ i $bc = b(b^{-1}h_1^{-1}) = h_1^{-1} \in T$, protivno prethodnom.□

**Lema 3.16** *Neka je $T$ leva transverzala podgrupe $\mathbf{H}$ grupe $\mathbf{G}$ i neka je, za $g$ iz $G$, $g = (g)\tau \cdot (g)\eta$, gde je $(g)\tau \in T$, $(g)\eta \in H$ (jasno, $(g)\tau$ i $(g)\eta$ su jednoznačno određeni). Za $\tau : G \longrightarrow T$ (reprezentativno preslikavanje domena $G$ na $T$) i $\eta : G \longrightarrow H$ (projekciju domena $G$ na $H$) važi, za svako $g \in G$ i svako $h \in H$:*

$$(gh)\tau = (g)\tau, \quad (gh)\eta = (g)\eta \cdot h.$$

**Dokaz.** Jasno, $g$ i $gh$ su elementi istog levog koseta podgrupe $\mathbf{H}$ te je $(gh)\tau = (g)\tau$. Stoga je i: $gh = (g)\tau \cdot (g)\eta \cdot h = (gh)\tau \cdot (gh)\eta = (g)\tau \cdot (gh)\eta$, a odatle je $(gh)\eta = (g)\eta \cdot h$.

Naravno, analogna tvrđenja važe i za desne transverzale.□

Primetimo, pre nego što pređemo na naredno tvrđenje, da je presek familija podgrupa opet podgrupa (podgrupu $\langle \bigcap_{i\in I} H_i, \cdot \rangle$, gde je $\mathbf{H}_i \leq \mathbf{G}$, označavaćemo jednostavno sa $\bigcap_{i\in I} \mathbf{H}_i$). Opet, unija dve podgrupe je podgrupa akko je unija jednaka jednoj od njih. U opštem, unija lanca podgrupa (skup podgrupa linearno uređen s obzirom na inkluziju) je podgrupa. S druge strane, ako je dat lanac grupa $\{\mathbf{G}_\alpha \mid \alpha < \lambda\}$, gde je $\mathbf{G}_\alpha \leq \mathbf{G}_\beta$ za $\alpha < \beta\ (< \lambda)$, onda se može na jedinstven (i prirodan) način definisati operacija $\cdot$ na skupu $\bigcup_{\alpha<\lambda} G_\alpha$ tako da $\langle \bigcup_{\alpha<\lambda} G_\alpha, \cdot \rangle$ bude grupa – unija grupa $\mathbf{G}_\alpha, \alpha < \lambda$, u oznaci $\bigcup_{\alpha<\lambda} \mathbf{G}_\alpha$, kao i da je, za svako $\alpha < \lambda$, $\mathbf{G}_\alpha$ njena podgrupa. Naravno, gledano skupovno, $\cdot = \bigcup_{\alpha<\lambda} \cdot_\alpha$, gde je $\cdot_\alpha$ operacija grupe $\mathbf{G}_\alpha$.

**Lema 3.17** *Neka su $\mathbf{H}$ i $\mathbf{K}$ podgrupe grupe $\mathbf{G}$. Tada je*

$$[\mathbf{H} : \mathbf{H} \cap \mathbf{K}] \leq [\mathbf{G} : \mathbf{K}] \quad i \quad [\mathbf{G} : \mathbf{H} \cap \mathbf{K}] \leq [\mathbf{G} : \mathbf{H}] \cdot [\mathbf{G} : \mathbf{K}].$$

*Ako je $G = HK$, jednakost važi u oba slučaja. Uz uslov da je podgrupa $\mathbf{K}$ konačnog indeksa iz prve jednakosti proizilazi $G = HK$ (ako je i podgrupa $\mathbf{H}$ konačnog indeksa, onda druga jednakost daje $G = HK$, no dokaz se ponovo svodi na prvi slučaj).*

**Dokaz.** $\phi : h(H \cap K) \longrightarrow hK$ je "jedan-jedan" preslikavanje skupa levih koseta podgrupe $\mathbf{H} \cap \mathbf{K}$ u $\mathbf{H}$ u skup svih levih koseta podgrupe $\mathbf{K}$ u $\mathbf{G}$. Proveru dobre definisanosti ostavljamo kao vežbu. Ako je pak $h_1K = h_2K$ za $h_1$, $h_2$ iz $H$, onda je $h_2^{-1}h_1 \in H \cap K$ pa je $h_1(H \cap K) = h_2(H \cap K)$. Prema tome je $[\mathbf{H} : \mathbf{H} \cap \mathbf{K}] \leq [\mathbf{G} : \mathbf{K}]$, a onda i $[\mathbf{G} : \mathbf{H} \cap \mathbf{K}] = [\mathbf{G} : \mathbf{H}] \cdot [\mathbf{H} : \mathbf{H} \cap \mathbf{K}] \leq [\mathbf{G} : \mathbf{H}] \cdot [\mathbf{G} : \mathbf{K}]$.

Ako je $G = HK$, tada je $\{hK \mid h \in H\}$ skup svih levih koseta podgrupe $\mathbf{K}$ u $\mathbf{G}$, $\phi$ je, znači, preslikavanje "na" i stoga $[\mathbf{H} : \mathbf{H} \cap \mathbf{K}] = [\mathbf{G} : \mathbf{K}]$ i $[\mathbf{G} : \mathbf{H} \cap \mathbf{K}] = [\mathbf{G} : \mathbf{H}] \cdot [\mathbf{G} : \mathbf{K}]$.

S druge strane, iz $[\mathbf{G} : \mathbf{K}] \in \omega$ i $[\mathbf{H} : \mathbf{H} \cap \mathbf{K}] = [\mathbf{G} : \mathbf{K}]$ opet proizilazi da je $\phi$ "na" preslikavanje. $\{hK \mid h \in H\}$ je, dakle, skup svih levih koseta podgrupe $\mathbf{K}$ (u $\mathbf{G}$) te je $G = \bigcup\{hK \mid h \in H\} = HK$.



Primetimo da samo $[\mathbf{H} : \mathbf{H} \cap \mathbf{K}] = [\mathbf{G} : \mathbf{K}]$ nije dovoljno da bi se dobilo $G = HK$. Kontraprimer sa grupom $\mathbf{Ra}$ i njenim podgrupama $\mathbf{Z}$ i $\mathbf{O}$ (jedinična podgrupa) to potvrđuje: $[\mathbf{Z} : \mathbf{Z} \cap \mathbf{O}] = [\mathbf{Ra} : \mathbf{O}] = \aleph_0$, ali $Ra \neq Z + O = Z$.□

**Korolar 3.18** *(Teorema Poincaréa). Presek konačne familije podgrupa konačnog indeksa je podgrupa konačnog indeksa.*

**Dokaz.** 3.17 u saradnji sa indukcijom implicira: ako su $\mathbf{H}_1, \ldots, \mathbf{H}_n$ podgrupe grupe $\mathbf{G}$, onda je

$$[\mathbf{G} : \mathbf{H}_1 \cap \ldots \cap \mathbf{H}_n] \leq \prod_{i=1}^{n} [\mathbf{G} : \mathbf{H}_i].□$$

**Napomena.** Gornje tvrđenje ne mora da važi ako je familija podgrupa beskonačna. Tako je, za pozitivan prirodan broj $n$, $n\mathbf{Z}$ podgrupa grupe $\mathbf{Z}$ konačnog indeksa $(n)$, ali $\bigcap_{n\in\omega\setminus\{0\}} n\mathbf{Z} = \mathbf{O}$ to očigledno nije.□

**Korolar 3.19** *Ako su indeksi podgrupa $\mathbf{H}$ i $\mathbf{K}$ konačni i uzajamno prosti brojevi, tada je $[\mathbf{G} : \mathbf{H} \cap \mathbf{K}] = [\mathbf{G} : \mathbf{H}] \cdot [\mathbf{G} : \mathbf{K}]$ i $G = HK$.*

**Dokaz.** Prema 3.12 i 3.17, $[\mathbf{G} : \mathbf{H} \cap \mathbf{K}]$ je takođe konačni kardinal i $[\mathbf{G} : \mathbf{H}]$, $[\mathbf{G} : \mathbf{K}]$ su njegovi delioci. No onda i $[\mathbf{G} : \mathbf{H}] \cdot [\mathbf{G} : \mathbf{K}]$ deli $[\mathbf{G} : \mathbf{H} \cap \mathbf{K}]$, dakle, $[\mathbf{G} : \mathbf{H}] \cdot [\mathbf{G} : \mathbf{K}] \leq [\mathbf{G} : \mathbf{H} \cap \mathbf{K}]$, tj. $[\mathbf{G} : \mathbf{H}] \cdot [\mathbf{G} : \mathbf{K}] = [\mathbf{G} : \mathbf{H} \cap \mathbf{K}]$, pa je $G = HK$.□

**Lema 3.20** *Ako je domen grupe $\mathbf{G}$ "pokriven" s konačno mnogo desnih koseta podgrupa $\mathbf{H}_1, \ldots, \mathbf{H}_n$ (tj. njihova je unija), onda je bar jedna od datih podgrupa konačnog indeksa.*

**Dokaz.** Indukcijom po broju podgrupa, $n$. Slučaj $n = 1$ je trivijalan. Pretpostavimo da je $n$ veće od 1, da je za svako $k$ manje od $n$ tvrđenje tačno za svakih $k$ podgrupa i da je ispunjen uslov leme za $n$ podgrupa. Ako se svi desni koseti podgrupe $\mathbf{H}_n$ javljaju među kosetima koji pokrivaju domen $G$, a takvih je, po uslovu, konačno mnogo, $\mathbf{H}_n$ je konačnog indeksa. Ako, s druge strane, recimo, koset $H_ng$ nije prisutan, dok npr. koseti $H_ng_1, \ldots, H_ng_i$ jesu, tada je, s obzirom na disjunknost desnih koseta iste podgrupe, $H_ng$ podskup unije konačno mnogo desnih koseta podgrupa $\mathbf{H}_1, \ldots, \mathbf{H}_{n-1}$. Proizilazi da je svaki desni koset podgrupe $\mathbf{H}_n$ podskup unije konačno mnogo desnih podgrupa $\mathbf{H}_1, \ldots, \mathbf{H}_{n-1}$, te je i domen $G$ unija konačno mnogo desnih koseta podgrupa $\mathbf{H}_1, \ldots, \mathbf{H}_{n-1}$, ne nužno onih iz već datog "pokrivača". Prema induktivnoj hipotezi, jedna od podgrupa $\mathbf{H}_1, \ldots, \mathbf{H}_{n-1}$ je konačnog indeksa.□

**Lema 3.21** *Neka su $\mathbf{H}$ i $\mathbf{K}$ podgrupe grupe $\mathbf{G}$. Tada važi:*

*(a)* $|HK| = |H| \cdot [\mathbf{K} : \mathbf{H} \cap \mathbf{K}]$. *Posebno, ako su $\mathbf{H}$ i $\mathbf{K}$ konačne grupe, imamo:* $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$;

*(b) $HK$ je domen podgrupe grupe $\mathbf{G}$ akko je $HK = KH$ (tj. akko su skupovi $H$ i $K$ permutabilni).*

**Dokaz**. ($a$) Ako je $\{(H \cap K)k_i \mid i \in I\}$ skup svih međusobno disjunktnih desnih koseta podgrupe $\mathbf{H} \cap \mathbf{K}$ u grupi $\mathbf{K}$ (jasno, $|I| = [\mathbf{K} : \mathbf{H} \cap \mathbf{K}]$), onda je $\{Hk_i \mid i \in I\}$ particija skupa $HK$; ako je $h \in H$ i $k \in K$, tada je, za neko $i$ iz $I$ i neko $a$ iz $H \cap K$, $k = ak_i$ i $hk = (ha)k_i \in Hk_i$, pa je $HK = \bigcup\{Hk_i \mid i \in I\}$; za različite indekse $i$ i $j$ je $Hk_i \cap Hk_j = \emptyset$ (u suprotnom bi bilo $k_i = hk_j$ za neko $h$ iz $H$, odatle $h \in H \cap K$ i $(H \cap K)k_i = (H \cap K)k_j$, kontradikcija). Prema tome je $|HK| = |H| \cdot |I| = |H| \cdot [\mathbf{K} : \mathbf{H} \cap \mathbf{K}]$.

($b$) Za domene podgrupa $\mathbf{H}$ i $\mathbf{K}$ je, očigledno, $KH = (HK)^{-1}$. Prema tome, ako je $HK = KH$, imamo $HK = (HK)^{-1}$, a zbog permutabilnosti skupova $H$ i $K$ evidentno važi i $(HK)(HK) \subseteq HK$; dakle, $HK$ je domen podgrupe (videti napomenu uz lemu 3.2). I obrat je već dokazan.□

**Napomena**. U slučaju kada su podgrupe $\mathbf{H}$ i $\mathbf{K}$ grupe $\mathbf{G}$ permutabilne, tj. kada je $HK = KH$, podgrupu sa domenom $HK$ obeležavaćemo jednostavno sa $\mathbf{HK}$ (ili neki put sa $\mathbf{H} \cdot \mathbf{K}$).

Ako je baš $\mathbf{G} = \mathbf{H} \cdot \mathbf{K}$ i $\mathbf{H} \cap \mathbf{K} = \mathbf{E}$, onda je $\mathbf{K}$ *komplement* podgrupe $\mathbf{H}$ (kao što je i $\mathbf{H}$ komplement podgrupe $\mathbf{K}$). Ako je $\mathbf{K}$ i normalna podgrupa, onda je ona *normalni komplement* podgrupe $\mathbf{H}$ (videti naredni paragraf kao i paragraf o poludirektnim proizvodima).

Već smo konstatovali da je unija lanca (pod)grupa (pod)grupa. No to je samo poseban slučaj jednog mnogo opštijeg stava koji upravo dajemo. Ali prvo

**Definicija 3.22** *Parcijalno uređeni skup (sistem)* $\mathcal{I} = \langle I, \leq \rangle$ *je usmeren skup (sistem) (eng. directed partially ordered set) akko svaka dva elementa imaju zajedničku gornju granicu* $(\forall i, j \, \exists k \;\; i \leq k, j \leq k)$.

*Usmerena familija grupa (eng. directed family of groups) je uređena trojka*

$$\langle \mathcal{I} \, (= \langle I, \leq \rangle), \{\mathbf{G}_i \mid i \in I\}, \{\varphi_{ij} \mid i \leq j\} \rangle,$$

*gde je* $\mathcal{I}$ *usmereni parcijalno uređeni skup, za svako* $i$ *iz* $I$ *je* $\mathbf{G}_i = \langle G_i, \cdot_i \rangle$ *grupa, a za* $i \leq j$ *je* $\varphi_{ij}$ *(izabrano) homomorfno preslikavanje grupe* $\mathbf{G}_i$ *u* $\mathbf{G}_j$*; pri tom još važi: za svako* $i$ *je* $\varphi_{ii} = \imath_{G_i}$ *i ako je* $i \leq j \leq k$*, onda je* $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$.

Neka je data usmerena familija grupa $\langle \mathcal{I}, \{\mathbf{G}_i \mid i \in I\}, \{\varphi_{ij} \mid i \leq j\} \rangle$. Na skupu $G_\infty = \bigcup_{i \in I} G_i$ definišimo relaciju $\sim$ sa: ako je $a \in G_i$, $b \in G_j$, onda je $a \sim b$ akko je $(a)\varphi_{ik} = (b)\varphi_{jk}$ za neko $k \geq i, j$. $\sim$ je relacija ekvivalencije skupa $G_\infty$. Refleksivnost je posledica činjenice da je $\varphi_{ii}$ identično preslikavanje. Simetričnost je očigledna. Što se tiče tranzitivnosti, neka je $a \sim b$ i $b \sim c$, $a \in G_i$, $b \in G_j$, $c \in G_k$ i neka je $(a)\varphi_{im} = (b)\varphi_{jm}$ $(m \geq i, j)$, $(b)\varphi_{jn} = (c)\varphi_{kn}$ $(n \geq j, k)$. Ako je $r$ gornja granica za $m$ i $n$, onda imamo: $(a)\varphi_{ir} = ((a)\varphi_{im})\varphi_{mr} = ((b)\varphi_{jm})\varphi_{mr} = (b)\varphi_{jr} = ((b)\varphi_{jn})\varphi_{nr} = ((c)\varphi_{kn})\varphi_{nr} = (c)\varphi_{kr}$, pa je i $a \sim c$. Obeležimo sa $[a]$ klasu relacije ekvivalencije $\sim$ kojoj pripada element $a$ $(\in G_\infty)$, a na skupu $\{[a] \mid a \in G_\infty\}$ definišimo



operaciju $\bullet$ na sledeći način: ako $a \in G_i$, $b \in G_j$ i ako je $k \geq i, j$, tada $[a] \bullet [b] = [(a)\varphi_{ik} \cdot_k (b)\varphi_{jk}]$. Definicija operacije $\bullet$ je korektna. Prvo, ne zavisi od izbora elementa $k$; jer, ako je i $l \geq i, j$ i $m \geq l, k$, onda je: $((a)\varphi_{ik} \cdot_k (b)\varphi_{jk})\varphi_{km} = (a)\varphi_{im} \cdot_m (b)\varphi_{jm} = ((a)\varphi_{il})\varphi_{lm} \cdot_m ((b)\varphi_{jl})\varphi_{lm} = ((a)\varphi_{il} \cdot_l (b)\varphi_{jl})\varphi_{lm}$, te je $(a)\varphi_{ik} \cdot_k (b)\varphi_{jk} \sim (a)\varphi_{jl} \cdot_l (b)\varphi_{jl}$, tj. $[(a)\varphi_{ik} \cdot_k (b)\varphi_{jk}] = [(a)\varphi_{il} \cdot_l (b)\varphi_{jl}]$. Drugo, ne zavisi od izbora reprezenata klasa. Neka je $a \sim c$, $b \sim d$, $a \in G_i$, $b \in G_j$, $c \in G_p$, $d \in G_r$ i neka je $(a)\varphi_{iq} = (c)\varphi_{pq}$, $(b)\varphi_{js} = (d)\varphi_{rs}$. Za $t \geq q, s$ je: $(a)\varphi_{it} \cdot_t (b)\varphi_{jt} = ((a)\varphi_{iq})\varphi_{qt} \cdot_t ((b)\varphi_{js})\varphi_{st} = ((c)\varphi_{pq})\varphi_{qt} \cdot_t ((d)\varphi_{rs})\varphi_{st}) = (c)\varphi_{pt} \cdot_t (d)\varphi_{rt}$; dakle, $[a] \bullet [b] = [(a)\varphi_{it} \cdot_t (b)\varphi_{jt}] = [(c)\varphi_{pt} \cdot_t (d)\varphi_{rt}] = [c] \bullet [d]$.

Sa uvedenom notacijom važi

**Lema 3.23** ($a$) *Grupoid* $\mathbf{G}_\infty = \langle G_\infty, \bullet \rangle$ *je grupa, tzv. usmereni limit date usmerene familije grupa.*

($b$) *Preslikavanje* $\varphi_{i\infty} : G_i \longrightarrow G_\infty$ *dato sa* $(a)\varphi_{i\infty} = [a]$ *homomorfno je preslikavanje grupe* $\mathbf{G}_i$ *u grupu* $\mathbf{G}_\infty$.

**Dokaz**. ($a$) Proverimo prvo asocijativnost (indekse više nećemo objašnjavati – iz konteksta je jasno o čemu je reč).

$$([a] \bullet [b]) \bullet [c] = [(a)\varphi_{ik} \cdot_k (b)\varphi_{jk}] \bullet [c] = [((a)\varphi_{ik} \cdot_k (b)\varphi_{jk})\varphi_{km} \cdot_m (c)\varphi_{lm}] =$$

$$[((a)\varphi_{im} \cdot_m (b)\varphi_{jm}) \cdot_m (c)\varphi_{lm}] = [(a)\varphi_{im} \cdot_m ((b)\varphi_{jm} \cdot_m (c)\varphi_{lm})] =$$

$$[a] \bullet [(b)\varphi_{jm} \cdot_m (c)\varphi_{lm}] = [a] \bullet ([b] \bullet [c]).$$

Naravno, za svako $i, j$ iz $I$ je $e_i \sim e_j$, gde su, podrazumeva se, $e_i$ i $e_j$ jedinični elementi grupa, respektivno, $\mathbf{G}_i$ i $\mathbf{G}_j$, a $[e_i]$ je jedinični element polugrupe $\mathbf{G}_\infty$. I na kraju, trivijalno: $[a]^{-1} = [a^{-1}]$.

($b$) $(a \cdot_i b)\varphi_\infty = [a \cdot_i b] = [a] \bullet [b] = (a)\varphi_{i\infty} \bullet (b)\varphi_{i\infty}$.□

**Napomena**. Ako je svaki homomorfizam $\varphi_{ij}$ injektivan, onda je i svaki homomorfizam $\varphi_{i\infty}$ injektivan; ako je $a, b \in G_i$ i $a \neq b$, tada je, očigledno, i $[a] \neq [b]$ (na umu nam je i da je $\varphi_{ii}$ identično preslikavanje). U tom slučaju možemo opet celu stvar svesti na uniju lanca grupa, jer važi

**Lema 3.24** *(Lema prenosa). Neka je* $\varphi$ *utapanje (injektivni homomorfizam) grupe* $\mathbf{A} = \langle A, \cdot \rangle$ *u grupu* $\mathbf{D} = \langle D, \odot \rangle$*. Tada postoji grupa* $\mathbf{C}$ *čija je jedna podgrupa* $\mathbf{A}$ *i koja je izomorfna sa* $\mathbf{D}$*, pri čemu postoji izomorfizam* $\theta \in Is(\mathbf{C}, \mathbf{D})$ *takav da je* $\theta|_A = \varphi$.

**Dokaz**. Pretpostavićemo, naravno, da $\varphi$ nije surjektivno preslikavanje. Neka je $B$ ma koji skup disjunktan sa $A$ i kardinalnosti $|D \setminus (A)\varphi|$, a $\theta$ bijektivno preslikavanje skupa $A \cup B = C$ na skup $D$ za koje je $\theta|_A = \varphi$. Definišimo na skupu $A \cup B$ operaciju $*$ sa:

$$x * y = ((x)\theta \odot (y)\theta)\theta^{-1}.$$

Grupoid $\mathbf{C} = \langle C, * \rangle$ je grupa. Zaista, za $x, y, z \in C$ je:

$$(x * y) * z = ((x * y)\theta \odot (z)\theta)\theta^{-1} = ((((x)\theta \odot (y)\theta)\theta^{-1})\theta \odot (z)\theta)\theta^{-1} =$$

$$(((x)\theta \odot (y)\theta) \odot (z)\theta)\theta^{-1} = ((x)\theta \odot ((y)\theta \odot (z)\theta))\theta^{-1} =$$

$$((x)\theta \odot (((y)\theta \odot (z)\theta)\theta^{-1})\theta)\theta^{-1} = ((x)\theta \odot (y * z)\theta)\theta^{-1} = x * (y * z).$$

Jedinični element, $e$, grupe $\mathbf{A}$ je i jedinični element polugrupe $\mathbf{C}$:

$$x * e = ((x)\theta \odot (e)\theta)\theta^{-1} = ((x)\theta \odot (e)\varphi)\theta^{-1} =$$

$$((x)\theta \odot e_D)\theta^{-1} = ((x)\theta)\theta^{-1} = x.$$

Jasno, i $x * e = x$. Inverzni element elementa $x$ je $(((x)\theta)^{-1})\theta^{-1}$:

$$x * (((x)\theta)^{-1})\theta^{-1} = ((x)\theta \odot ((((x)\theta)^{-1})\theta^{-1})\theta)\theta^{-1} =$$

$$((x)\theta \odot ((x)\theta)^{-1})\theta^{-1} = (e_D)\theta^{-1} = e.$$

Naravno, lako se proverava i da je $(((x)\theta)^{-1})\theta^{-1} * x = e$, ali za to nema ni potrebe (dovoljan je, rekli smo već, jedan desni jedinični element za koji svaki element ima desni inverzni). $\theta$ je ujedno i izomorfno preslikavanje grupe $\mathbf{C}$ na grupu $\mathbf{D}$. Bijektivnost je data, a:

$$(x * y)\theta = (((x)\theta \odot (y)\theta)\theta^{-1})\theta = (x)\theta \odot (y)\theta. \square$$

**Korolar 3.25** *Svaki neprazan skup može biti domen (bar jedne) grupe.*

**Dokaz.** Neka je $A$ neprazan skup kardinalnosti $\lambda$ ($\geq 1$) i $\mathbf{B} = \langle B, \odot \rangle$ grupa kardinalnosti $\lambda$ – takva uvek postoji; ako je $\lambda$ pozitivan prirodan broj, onda je npr. $\mathbf{Z}_\lambda$ grupa reda $\lambda$; ako je $\lambda \geq \aleph_0$, onda je npr. direktni proizvod $\prod_{\alpha<\lambda} \mathbf{Z}^\alpha$, gde je, za svako $\alpha < \lambda$, $\mathbf{Z}^\alpha$ "kopija" aditivne grupe celih brojeva, grupa reda $\lambda$ (videti paragraf o direktnim proizvodima). Ako je, dalje, $\varphi$ bijektivno preslikavanje skupa $A$ na skup $B$, tada je, za operaciju $*$ na skupu $A$ definisanoj sa: $x * y = ((x)\varphi \odot (y)\varphi)\varphi^{-1}$, grupoid $\mathbf{A} = \langle A, * \rangle$ grupa, izomorfna grupi $\mathbf{B}$. Dokaz je uglavnom sadržan u dokazu prethodne leme.$\square$

# 4 Normalne i neke druge podgrupe

Normalne podgrupe, ekvivalent relacijama kongruencija, od posebnog su značaja. Delom se to već naslućuje iz teorema o izomorfizmu (paragraf 8), potpunije iz celog teksta, a još potpunije iz još potpunijeg teksta o grupama (ukratko, bez njih se ne može u teoriji grupa).



**Definicija 4.1** *Podgrupa* $\mathbf{H}$ *grupe* $\mathbf{G}$ *je normalna (pišemo* $\mathbf{H} \lhd \mathbf{G}$*) akko važi* $\forall g \in G\ gH = Hg$, *tj.* $\forall g \in G\, \forall h \in H\ \exists h_1, h_2 \in H\, (gh = h_1 g \wedge hg = gh_2)$.

*Neprazni podskup* $A$ *domena* $G$ *grupe* $\mathbf{G}$ *je normalan podskup grupe* $\mathbf{G}$ *akko je unija klasa konjugovanih elemenata (tj. akko važi* $\forall a \in A\, \forall g \in G\ g^{-1}ag \in A$*).*

**Lema 4.2** *Neka je* $\mathbf{H} \leq \mathbf{G}$. *Tada su sledeći uslovi ekvivalentni:*

(1) $\mathbf{H}$ *je normalna podgrupa;*

(2) $\forall g \in G\ g^{-1}Hg = H$;

(3) $\forall g \in G\ g^{-1}Hg \subseteq H$ *(drugim rečima: ako je* $a \in H$, *onda su i svi konjugati od* $a$ *u* $H$, *ili: ako je* $\phi \in Inn(\mathbf{G})$, *onda je* $(\mathbf{H})\phi \leq \mathbf{H}$*).*

**Dokaz.** Primetimo samo: ako je $g^{-1}Hg \subset H$ za neko $g \in G$, onda je $H \subset gHg^{-1}$.$\square$

Tačka (3) nam kaže da smo normalne podgrupe mogli okarakterisati i kao podgrupe invarijantne za unutrašnje automorfizme.

*Trivijalne normalne podgrupe* grupe $\mathbf{G}$ su sama grupa $\mathbf{G}$ i jedinična podgrupa.

Grupa bez netrivijalnih normalnih podgrupa se zove *prosta grupa*. Jasno, po definiciji je jedinična grupa prosta, a Abelova nejedinična grupa je prosta akko joj je red prost broj (videti 5.6, 7.2).

**Lema 4.3** (*a*) *Normalna podgrupa je permutabilna sa svakom drugom;*

(*b*) *Ako su* $\mathbf{H}_1, \ldots, \mathbf{H}_n$ *normalne podgrupe grupe* $\mathbf{G}$, *onda je:*

$$|H_1 \ldots H_n| = \frac{\prod_{i=1}^{n} |H_i|}{\prod_{i=1}^{n-1} |H_1 \ldots H_i \cap H_{i+1}|}.$$

**Dokaz.** (*a*) Trivijalno. Primetimo samo da iz permutabilnosti dve podgrupe ne sledi nužno normalnost (barem) jedne od njih.

(*b*) Prema tački (*b*) leme 3.21, $\mathbf{H}_1 \ldots \mathbf{H}_i$ ($1 \leq i \leq n$) je podgrupa grupe $\mathbf{G}$, pa je tvrđenje neposredna posledica tačke (*a*) iste leme (u dokazu koristiti indukciju).$\square$

**Primer 4.4** *(a) U* 3.4(*c*) *podgrupe grupe* $\mathbf{GL}_n(\mathbf{Re})$ *date u* (*i*) *i* (*ii*) *su normalne, ostale nisu ako je* $n > 1$.

*(b) U* 3.4(*d*), *ako je* $|A \setminus X| \geq 2$, *podgrupa iz* (*i*) *nije normalna. Podgrupa iz* (*ii*) *je (uvek) normalna.*

(*c*) *Naravno, uvek je* $\mathbf{Z}(\mathbf{G}) \lhd \mathbf{G}$. *Takođe, podgrupe indeksa* 2 *su uvek normalne.*

**Dokaz.** Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$ indeksa 2 i neka $g \in G \setminus H$. Onda je $\{H, gH\}$ skup levih i $\{H, Hg\}$ skup desnih koseta podgrupe $\mathbf{H}$, pa je $gH = Hg = G \setminus H$.

(*d*) $\mathbf{Inn(G)} = \langle Inn(\mathbf{G}), \circ\rangle$ *(videti 2.10(b)) je normalna podgrupa grupe* $\mathbf{Aut(G)}$.

**Dokaz.** Zaista, prema 2.15, $\mathbf{Inn(G)}$ je grupa, dakle, podgrupa grupe $\mathbf{Aut(G)}$. Osim toga, ako je $\phi \in Aut(\mathbf{G})$ i $u_a \in Inn(\mathbf{G})$, onda je $\phi^{-1} \circ u_a \circ \phi = u_{(a)\phi}$.

(*e*) *Ako je* $\mathbf{H} \lhd \mathbf{G}$ *i* $\mathbf{K} \leq \mathbf{G}$, $HK$ *je domen podgrupe. Ako je i* $\mathbf{K} \lhd \mathbf{G}$, $HK$ *je domen normalne podgrupe.*

(*f*) *Ako važi* $\forall \alpha < \lambda\ \mathbf{H}_\alpha \lhd \mathbf{G}_\alpha$, *gde su* $\{\mathbf{H}_\alpha \mid \alpha < \lambda\}$ *i* $\{\mathbf{G}_\alpha \mid \alpha < \lambda\}$ *lanci grupa, onda je* $\bigcup_{\alpha<\lambda} \mathbf{H}_\alpha \lhd \bigcup_{\alpha<\lambda} \mathbf{G}_\alpha$.

(*g*) *Ako je* $A$ *normalni podskup grupe* $\mathbf{G}$, $\mathbf{C}(A)$ *je normalna podgrupa.*□

**Napomena.** Svojstvo normalnosti nije tranzitivno, tj. iz $\mathbf{H} \lhd \mathbf{K} \lhd \mathbf{G}$ ne sledi nužno i $\mathbf{H} \lhd \mathbf{G}$. Sledeći primer to pokazuje.

**Primer 4.5** *Neka je* $\mathbf{G}$ *grupa sa normalnom podgrupom* $\mathbf{H}$ *koja sadrži centar grupe i za koju postoji* $\phi \in Aut(\mathbf{G})$ *tako da* $(H)\phi \not\subseteq H$. *Tada je* $\langle \{u_h \mid h \in H\}, \circ\rangle$ *normalna podgrupa grupe* $\mathbf{Inn(G)}$, *ali ne i grupe* $\mathbf{Aut(G)}$.

**Dokaz.** Za bilo koje $a \in G$ i bilo koje $h \in H$ je $(u_a^{-1} \circ u_h \circ u_a = u_{a^{-1}} \circ u_h \circ u_a = u_{a^{-1}ha})$, ali ako $h \in H$ i $(h)\phi \notin H$, onda $\phi^{-1} \circ u_h \circ \phi = u_{(h)\phi} \notin \{u_h \mid h \in H\}$.

Naravno, da bi naš primer bio punovažan treba nam bar jedna grupa $\mathbf{G}$ sa podgrupom $\mathbf{H}$ koja ispunjava date uslove. Nju dajemo u 5.7(*a*).

Jedan drugi primer možemo odmah ponuditi. Podgrupa

$$\mathbf{K} = \langle \{\imath, \sigma, \rho^2, \sigma\rho^2\}, \circ\rangle$$

je normalna podgrupa dijedarske grupe stepena 4 (videti primer 3.4(*e*)), $\mathbf{H} = \langle \{\imath, \sigma\}, \circ\rangle$ je normalna podgrupa grupe $\mathbf{K}$, ali ne i dijedarske grupe.□

**Definicija 4.6** *Podgrupe* $\mathbf{H}$ *i* $\mathbf{K}$ *grupe* $\mathbf{G}$ *su konjugovane akko je* $K = g^{-1}Hg$ *za neko* $g \in G$. *Pisaćemo i* $\mathbf{K} = g^{-1}\mathbf{H}g$.

**Lema 4.7** (*a*) *Relacija konjugovanosti podgrupa je relacija ekvivalencije na skupu svih podgrupa;*

(*b*) *Podgrupa* $\mathbf{N}$ *je normalna akko je jednaka svim svojim konjugatima.*

**Dokaz.** (*a*) je trivijalno, a (*b*) već dato (4.2 (1) $\Longleftrightarrow$ (2)).□

**Lema 4.8** *Ako je* $\mathbf{H} \leq \mathbf{G}$, *tada je* $\mathbf{Core(H)} \stackrel{\text{def}}{=} \bigcap\{g^{-1}\mathbf{H}g \mid g \in G\} \lhd \mathbf{G}$. $\mathbf{Core(H)}$ *je ujedno maksimalna normalna podgrupa grupe* $\mathbf{G}$, *s obzirom na inkluziju, koja je sadržana u* $\mathbf{H}$.



**Dokaz.** Prvi deo tvrđenja je očigledan, jer prema 4.2 i definiciji podgrupe $\mathbf{Core(H)}$ imamo: $\mathbf{Core(H)} \lhd \mathbf{G}$ akko $\forall a \in G\ \forall c \in Core(\mathbf{H})\ a^{-1}ca \in Core(\mathbf{H})$ akko $\forall a, b \in G\ \forall c \in Core(\mathbf{H})\ a^{-1}ca \in b^{-1}Hb$ akko $\forall a, b \in G\ \forall c \in Core(\mathbf{H})\ c \in (ba^{-1})^{-1}H(ba^{-1})$ akko $\forall g \in G\ \forall c \in Core(\mathbf{H})\ c \in g^{-1}Hg$.

Mogli smo i ovako rezonovati: za svaki injektivni endomorfizam $\phi$ i svaku familiju podgrupa $\{\mathbf{H}_i \mid i \in I\}$ važi: $(\bigcap\{\mathbf{H}_i \mid i \in I\})\phi = \bigcap\{(\mathbf{H}_i)\phi \mid i \in I\}$ (inkluzija $\leq$ je očigledna, i važi za svaki endomorfizam, a inkluzija $\geq$ je posledica injektivnosti). Posebno, u konkretnom slučaju imamo za svako $a$ iz $G$: $a^{-1}\mathbf{Core(H)}a = a^{-1}\bigcap\{b^{-1}\mathbf{H}b \mid b \in G\}a = \bigcap\{a^{-1}b^{-1}\mathbf{H}ba \mid b \in G\} = \bigcap\{g^{-1}\mathbf{H}g \mid g \in G\} = \mathbf{Core(H)}$.

Neka je sada $\mathbf{K} \leq \mathbf{H}$ i $\mathbf{K} \lhd \mathbf{G}$. Kako je, za svako $g \in G$, $\mathbf{K} = g^{-1}\mathbf{K}g \leq g^{-1}\mathbf{H}g$, to je $\mathbf{K} \leq \bigcap\{g^{-1}\mathbf{H}g \mid g \in G\} = \mathbf{Core(H)}$.□

**Napomena.** Podgrupa $\mathbf{Core(H)}$ zove se *srž* ili *jezgro*, eng. *core* - otuda i oznaka, ili, "topološkim" rečnikom, *normalna unutrašnjost* (eng. *normal interior*) podgrupe $\mathbf{H}$.

**Lema 4.9** *Neka je* $\mathbf{G}$ *grupa,* $\mathbf{H} \leq \mathbf{G}$, $\emptyset \neq A \subseteq G$ *i* $N_{\mathbf{H}}(A) \stackrel{\text{def}}{=} \{h \in H \mid hA = Ah\}$. *Tada je* $\mathbf{N_H}(A) = \langle N_{\mathbf{H}}(A), \cdot\rangle$ *podgrupa grupe* $\mathbf{H}$, *tzv. normalizator skupa* $A$ *u* $\mathbf{H}$. *Posebno, ako je* $A = \{a\}$, *koristićemo, umesto* $\mathbf{N_H}(\{a\})$, *standardnije* $\mathbf{C_H}(a)$ - *u pitanju je centralizator elementa* $a$ *u* $\mathbf{H}$. *Ako je* $\mathbf{A} = \langle A, \cdot\rangle$ *podgrupa, pisaćemo i* $\mathbf{N_H(A)}$ *i tu podgrupu zvati normalizatorom podgrupe* $\mathbf{A}$ *u* $\mathbf{H}$. *Ako je* $\mathbf{H} = \mathbf{G}$, *često se, kad kontekst dozvoljava, koristi* $\mathbf{N}(A)$, *tj.* $\mathbf{N(A)}$, *umesto* $\mathbf{N_G}(A)$, *odnosno* $\mathbf{N_G(A)}$. *Za* $\mathbf{A} \leq \mathbf{G}$ *je* $\mathbf{N(A)}$ *maksimalna podgrupa grupe* $\mathbf{G}$ *koja sadrži* $\mathbf{A}$ *kao normalnu podgrupu. Takođe,* $\mathbf{A} \lhd \mathbf{G}$ *akko je* $\mathbf{N(A)} = \mathbf{G}$.

**Lema 4.10** *Centralizator normalne podgrupe je normalna podgrupa.*

**Lema 4.11** *Neka je* $\mathbf{H}$ *podgrupa grupe* $\mathbf{G}$. *Tada je*

$$|\{g^{-1}\mathbf{H}g \mid g \in G\}| = [\mathbf{G} : \mathbf{N(H)}];$$

*rečima: kardinalnost klase ekvivalencija, s obzirom na relaciju konjugovanosti podgrupa, koja sadrži* $\mathbf{H}$ *jednaka je indeksu normalizatora podgrupe* $\mathbf{H}$ *ili, jednostavnije i neformalnije, broj konjugata podgrupe* $\mathbf{H}$ *jednak je indeksu njenog normalizatora.*

**Dokaz.** $F : g^{-1}Hg \longrightarrow N(\mathbf{H})g$ je biunivoko preslikavanje skupa konjugata podgrupe $\mathbf{H}$ u skup desnih koseta njenog normalizatora. Jer, "na" je po definiciji, a s obzirom na : $b^{-1}\mathbf{H}b = c^{-1}\mathbf{H}c$ akko $(bc^{-1})^{-1}\mathbf{H}bc^{-1} = \mathbf{H}$ akko $bc^{-1} \in N(\mathbf{H})$ akko $b \in N(\mathbf{H})c$ akko $N(\mathbf{H})b = N(\mathbf{H})c$, $F$ je i dobro definisano (pravac ($\Longrightarrow$)) i "jedan-jedan".

Primetimo da nigde u dokazu nismo koristili uslov $\mathbf{H} \leq \mathbf{G}$, dakle, tvrđenje analogno gornjem važi za svaki podskup skupa $G$, te kao poseban zaključak izvodimo:

*broj elemenata konjugovanih sa $a$ jednak je indeksu centralizatora $\mathbf{C}(a)$; posebno, FC-elementi su elementi čiji su centralizatori konačnog indeksa.*□

**Korolar 4.12** *Neka je u grupi $\mathbf{G}$ $\mathcal{R}$ skup predstavnika klasa relacije konjugovanosti elemenata kardinalnosti veće od 1. Tada je*

$$|G| = |Z(G)| + \sum_{g \in \mathcal{R}} [\mathbf{G} : \mathbf{C}(g)].$$

**Dokaz**. Jasno, $[\mathbf{G} : \mathbf{C}(g)] = 1$ akko $g \in Z(G)$ (naravno, imamo u vidu i činjenicu da je relacija konjugovanosti elemenata relacija ekvivalencije na skupu $G$).□

**Korolar 4.13** *Centar grupe reda $p^m$, gde je $m \geq 1$ i $p$ prost broj, je nejedinična podgrupa.*

**Dokaz**. Neka je $\mathbf{G}$ grupa reda $p^m$. Prema oznakama iz prethodnog korolara je, za svako $g \in \mathcal{R}$, $\mathbf{C}(g)$ prava podgrupa grupe $\mathbf{G}$; dakle, $p$ deli $\sum_{g \in \mathcal{R}} [\mathbf{G} : \mathbf{C}(g)]$, a onda i $|Z(\mathbf{G})|$. Videti i 16.20.□

**Korolar 4.14** *Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$ i $\mathcal{A}$ familija podskupova domena $G$ takva da je, za svako $A \in \mathcal{A}$ i svako $h \in H$, $h^{-1}Ah \in \mathcal{A}$. Ako je $\sim_H$ relacija (ekvivalencije) na skupu $\mathcal{A}$ definisana sa: $A \sim_H B$ akko $\exists h \in H$ $B = h^{-1}Ah$, a $\mathcal{R}$ skup predstavnika klasa ekvivalencija relacije $\sim_H$, onda je*

$$|\mathcal{A}| = \sum_{R \in \mathcal{R}} [\mathbf{H} : \mathbf{N}_{\mathbf{H}}(R)].$$

**Korolar 4.15** *Normalizatori konjugovanih podgrupa su istog indeksa.*

**Lema 4.16** *Ako su $\mathbf{H}$ i $\mathbf{K}$ podgrupe grupe $\mathbf{G}$ i ako je $\mathbf{K} = g^{-1}\mathbf{H}g$, tada je $\mathbf{N}(\mathbf{K}) = g^{-1}\mathbf{N}(\mathbf{H})g$ i $[\mathbf{N}(\mathbf{H}) : \mathbf{H}] = [\mathbf{N}(\mathbf{K}) : \mathbf{K}]$.*

**Dokaz**. $a \in N(\mathbf{K})$ akko $a^{-1}Ka = K$ akko $a^{-1}g^{-1}Hag = g^{-1}Hg$ akko $(gag^{-1})^{-1}Hgag^{-1} = H$ akko $gag^{-1} \in N(\mathbf{H})$ akko $a \in g^{-1}N(\mathbf{H})g$.

$\psi = u_g|_{N(\mathbf{H})}$ $(u_g : x \longrightarrow g^{-1}xg)$ je izomorfno preslikavanje grupe $\mathbf{N}(\mathbf{H})$ u $\mathbf{N}(\mathbf{K})$ i $(H)\psi = K$, odakle proizilazi drugi deo tvrđenja.□

**Korolar 4.17** *Konjugovane podgrupe su istog indeksa.*

4.15 i 4.17 su, napomenimo i to, samo poseban slučaj sledećeg, opštijeg stava, koji je opet poseban slučaj teoreme 8.7.



**Lema 4.18** *Neka su $\mathbf{G}$ i $\mathbf{H}$ izomorfne grupe, $\varphi \in Is(\mathbf{G}, \mathbf{H})$ i $\mathbf{A}$ i $\mathbf{B}$ podgrupe, respektivno, grupa $\mathbf{G}$ i $\mathbf{H}$ takve da je $(A)\varphi = B$. Tada je $[\mathbf{G} : \mathbf{A}] = [\mathbf{H} : \mathbf{B}]$.*

**Dokaz**. Jasno, $F : \{Ag \mid g \in G\} \longrightarrow \{Bh \mid h \in H\}$ dato sa: $(Ag)F = B(g)\varphi$ biunivoko je preslikavanje skupa desnih koseta podgrupe $\mathbf{A}$ u skup desnih koseta podgrupe $\mathbf{B}$.□

**Korolar 4.19** *Ako je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$ konačnog indeksa, onda postoji normalna podgrupa grupe $\mathbf{G}$ konačnog indeksa koja je ujedno i podgrupa grupe $\mathbf{H}$.*

**Dokaz**. Kako je $\mathbf{H}$ podgrupa konačnog indeksa, to je i njen normalizator konačnog indeksa, pa $\mathbf{H}$ ima samo konačno mnogo konjugata. Neka su to $\mathbf{H} = \mathbf{H}_0, \ldots, \mathbf{H}_{n-1}$. Prema 4.8 i 4.17 $\mathbf{Core}(\mathbf{H}) = \mathbf{H}_0 \cap \ldots \cap \mathbf{H}_{n-1} (\leq \mathbf{H})$ je normalna podgrupa grupe $\mathbf{G}$ konačnog indeksa.□

Ovaj korolar ćemo kasnije još jednom dokazati (*repetitium est mater studiorum*) - videti odeljak o grupama permutacija - 9.35. To, dakako, ne znači da u ovaj dokaz treba sumnjati.

**Lema 4.20** *Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$. Tada važi: $\forall a, b \in G$ $aH \cdot bH = abH$ akko je $\mathbf{H}$ normalna podgrupa ($aH \cdot bH$ je, naravno, skup $\{(ah_1)(bh_2) \mid h_1, h_2 \in H\}$).*

**Dokaz**. Pretpostavimo prvo da važi $\forall a, b \in G$ $aH \cdot bH = abH$ i neka je $h \in H, g \in G$. No onda je, zbog $g^{-1}hg \in g^{-1}H \cdot gH = H$, $\mathbf{H}$ normalna podgrupa.

Primetimo da je uvek $abH \subseteq aH \cdot bH$. Ako je $\mathbf{H}$ i normalna podgrupa grupe $\mathbf{G}$, za proizvoljne elemente $h_1, h_2 \in H$ imaćemo: $ah_1bh_2 = ab(b^{-1}h_1b)h_2 \in abH$, pa važi i $aH \cdot bH \subseteq abH$.□

**Korolar 4.21** *Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$. Korespondencija*

$$\cdot : \{aH \mid a \in G\} \times \{bH \mid b \in G\} \longrightarrow \{cH \mid c \in G\}$$

*data sa $\cdot(aH, bH) = abH$ algebarska je operacija na skupu $\{aH \mid a \in G\}$ akko je $\mathbf{H}$ normalna podgrupa.*

**Dokaz**. Neka $\mathbf{H}$ nije normalna podgrupa. Tada je, za neko $a, b \in G$, $abH \subset aH \cdot bH$, pa postoje elementi $h_1, h_2 \in H$ takvi da $(ah_1)(bh_2) \notin abH$. I sada $aH = (ah_1)H$, $bH = (bh_2)H$, ali $abH \neq (ah_1)(bh_2)H$.

Ako je pak $\mathbf{H} \lhd \mathbf{G}$, lako se proverava da je $\cdot$ algebarska operacija, tj. da iz $aH = a_1H$ i $bH = b_1H$ sledi $abH = a_1b_1H$.□

**Korolar 4.22** *Neka je* $\mathbf{H}$ *normalna podgrupa grupe* $\mathbf{G}$. *Tada je*

$$\mathbf{G/H} = \langle \{aH \mid a \in G\}, \cdot \rangle,$$

*gde je* $aH \cdot bH \stackrel{\text{def}}{=} abH$, *grupa, tzv. faktor grupa grupe* $\mathbf{G}$ *po podgrupi* $\mathbf{H}$.

**Dokaz.** Već smo videli da je $\mathbf{G/H}$ grupoid, asocijativnost očigledno važi, $H$ je neutralni element, a $(aH)^{-1} = a^{-1}H$.□

U vezi sa prethodnom lemom i njenim korolarima uočimo da važi

**Lema 4.23** *Neka je* $\mathbf{G} = \langle G, \cdot \rangle$ *grupa i neka je za particiju* $\mathcal{P}$ *njenog domena* $\mathbf{P} = \langle \mathcal{P}, \bullet \rangle$ *grupa, gde je, za* $A, B \in \mathcal{P}$, $A \bullet B \stackrel{\text{def}}{=} AB$. *Tada je* $\mathbf{P}$ *faktor grupa grupe* $\mathbf{G}$ *po nekoj normalnoj podgrupi.*

**Dokaz.** Neka je $H \in \mathcal{P}$ jedinični element grupe $\mathbf{P}$. Skup $H$ je domen normalne podgrupe grupe $\mathbf{G}$. Jer, zbog $H \bullet H = HH = H$, skup $H$ je zatvoren za "množenje", a ako je $a \in H$, tada je i $a^{-1} \in H$; pretpostavka $a^{-1} \in K \neq H$ bi dala $e = aa^{-1} \in HK = K$, i stoga $H = He \subseteq HK = K$, kontradikcija. Isto tako $b \in K$ implicira $b^{-1} \in K^{-1}$ (gde je, jasno, $K^{-1}$ inverzni element elementa $K$ u grupi $\mathbf{P}$ – nije, naravno, isključena mogućnost da je $K = K^{-1}$); jer, ako je $b^{-1} \in L$, tada je $e = bb^{-1} \in KL = H$ pa $L = K^{-1}$. Odatle odmah sledi normalnost podgrupe $\mathbf{H}$: za $a \in H$ i $b \in K$ je: $b^{-1}ab \in K^{-1}HK = K^{-1} \bullet H \bullet K = H$. Dalje, ako je $b \in K$, onda je $K = bH$. Inkluzija $\supseteq$ je očigledna: $bH \subseteq KH = K$. S druge strane, za $c \in K$ imamo: $c = b(b^{-1}c) \in bK^{-1}K = bH$. Konačno, operacija $\bullet$ odgovara standardno definisanom "množenju" u faktor grupi $\mathbf{G/H}$: ako je $K = bH$ i $L = cH$, onda je $K \bullet L = (bH) \bullet (cH) = (bH)(cH) = (bc)H$ (zbog normalnosti podgrupe $\mathbf{H}$).□

**Lema 4.24** *Neka je* $\varphi : G \longrightarrow H$ *homomorfno preslikavanje grupe* $\mathbf{G}$ *u grupu* $\mathbf{H}$ *i neka je* $Ker(\varphi) \stackrel{\text{def}}{=} \{a \in G \mid (a)\varphi = e_H\}$. *Tada je* $\mathbf{Ker}(\varphi) = \langle Ker(\varphi), \cdot \rangle$ *normalna podgrupa grupe* $\mathbf{G}$.

**Dokaz.** $Ker(\varphi) \neq \emptyset$ jer $e_G \in Ker(\varphi)$. Ako je $a, b \in Ker(\varphi)$ i $g \in G$, onda je $(ab^{-1})\varphi = (a)\varphi((b)\varphi)^{-1} = e_H$ i $(g^{-1}ag)\varphi = ((g)\varphi)^{-1}e_H(g)\varphi = e_H$, pa je $\mathbf{Ker}(\varphi) \lhd \mathbf{G}$.□

I skup $Ker(\varphi)$ i podgrupu $\mathbf{Ker}(\varphi)$ zvaćemo *jezgrom* homomorfizma $\varphi$. Notacija je po engleskoj reči *kernel* (= jezgro).

**Teorema 4.25** *Podgrupa* $\mathbf{H}$ *grupe* $\mathbf{G}$ *je normalna akko je jezgro nekog homomorfizma.*

**Dokaz.** Neka je $\mathbf{H} \lhd \mathbf{G}$. Preslikavanje $\varphi : G \longrightarrow G/H$ $(= \{gH \mid g \in G\})$, gde je $(a)\varphi \stackrel{\text{def}}{=} aH$, homomorfno je preslikavanje grupe $\mathbf{G}$ na grupu $\mathbf{G/H}$ i $Ker(\varphi) = H$ (jasno, $aH = H$ akko $a \in H$).■



**Napomena.** Homomorfizam $\varphi : a \longrightarrow aH$ je tzv. *prirodni (kanonički) homomorfizam* i kad god se govori o homomorfnom preslikavanju grupe $\mathbf{G}$ u grupu $\mathbf{G/H}$ mi ćemo ga (ukoliko ne naglasimo drugačije) podrazumevati.

**Lema 4.26** (*a*) *Ako je* $\mathbf{H}$ *prava podgrupa konačne grupe* $\mathbf{G}$, *tada je*

$$\bigcup_{g \in G} g^{-1}Hg \neq G;$$

(*b*) *Ako je* $\mathbf{H}$ *prava podgrupa konačnog indeksa grupe* $\mathbf{G}$, *tada je*

$$\bigcup_{g \in G} g^{-1}Hg \neq G.$$

**Dokaz.** Naravno, (*b*) uključuje (*a*), ali je za dokaz tačke (*b*) zahvalno znati (*a*) i zato smo to tvrđenje izdvojili.

(*a*) Kako $\mathbf{H}$ ima najviše $[\mathbf{G} : \mathbf{H}]$ konjugata, a sve te podgrupe imaju bar jedan zajednički element, to je

$$|\bigcup_{g \in G} g^{-1}Hg| \leq 1 + (|H| - 1)[\mathbf{G} : \mathbf{H}] = 1 + |G| - [\mathbf{G} : \mathbf{H}] < |G|.$$

(*b*) Prema 4.19 postoji normalna podgrupa konačnog indeksa $\mathbf{N}$ grupe $\mathbf{G}$ koja je sadržana u $\mathbf{H}$. $\mathbf{H/N}$ je prava podgrupa konačne grupe $\mathbf{G/N}$, pa prema (*a*) postoji element $aN$ koji ne pripada skupu $\bigcup_{g \in G}(g^{-1}N)H/N(gN)$. No onda $a \notin \bigcup_{g \in G} g^{-1}Hg$ (ako bi bilo $a = g^{-1}hg$ za neko $g \in G$ i neko $h \in H$, sledilo bi $aN = (g^{-1}N)(hN)(gN) \in (g^{-1}N)H/N(gN)$, kontradikcija).□

**Korolar 4.27** *Ako je* $\mathbf{H}$ *prava podgrupa konačne grupe* $\mathbf{G}$ *i* $\mathbf{H} \cap g^{-1}\mathbf{H}g = \mathbf{E}$ *za svako* $g \in G \setminus H$, *tada je* $|G \setminus \bigcup_{g \in G} g^{-1}Hg| = [\mathbf{G} : \mathbf{H}] - 1$.

**Dokaz.** Primetimo samo, ako je i to uopšte potrebno: ako je $\mathbf{H} \neq \mathbf{E}$, tada je, pod datim uslovima, $\mathbf{N(H)} = \mathbf{H}$.□

**Lema 4.28** *Neka je* $\mathbf{H}$ *normalna podgrupa grupe* $\mathbf{G}$. *Tada važi:*

(*a*) *Za svaku podgrupu* $\mathbf{K}$ *grupe* $\mathbf{G}$ *je*

$$(gH)^{-1}((\mathbf{KH})/\mathbf{H})gH = ((g^{-1}\mathbf{K}g)\mathbf{H})/\mathbf{H};$$

(*b*) *Ako su* $\mathbf{K}_1$ *i* $\mathbf{K}_2$ *konjugovane podgrupe grupe* $\mathbf{G}$, *tada su* $(\mathbf{K}_1\mathbf{H})/\mathbf{H}$ *i* $(\mathbf{K}_2\mathbf{H})/\mathbf{H}$ *konjugovane podgrupe grupe* $\mathbf{G/H}$;

(*c*) *Ako su* $\mathbf{M}_1/\mathbf{H}$ *i* $\mathbf{M}_2/\mathbf{H}$ *konjugovane podgrupe grupe* $\mathbf{G/H}$, *onda su* $\mathbf{M}_1$ *i* $\mathbf{M}_2$ *konjugovane podgrupe grupe* $\mathbf{G}$.

**Dokaz.** (*a*) Direktna posledica činjenice da je za svaku podgrupu $\mathbf{K}$ grupe $\mathbf{G}$ domen grupe $(\mathbf{KH})/\mathbf{H}$ skup $\{kH \mid k \in K\}$.

(*b*) Direktna posledica prethodne tačke.

(*c*) Ako je $(gH)^{-1}\mathbf{M}_1/\mathbf{H}\,gH = \mathbf{M}_2/\mathbf{H}$, onda je $g^{-1}\mathbf{M}_1g = \mathbf{M}_2$. Tako je recimo, za $a \in M_1$, $(g^{-1}ag)H = g^{-1}HaHgH \in (gH)^{-1}M_1/H\,gH = M_2/H$, pa je, za neko $b \in M_2$, $g^{-1}ag \in bH \subseteq M_2$; dakle, $g^{-1}M_1g \subseteq M_2$. Po simetriji stvari je $gM_2g^{-1} \subseteq M_1$, odnosno $M_2 \subseteq g^{-1}M_1g$.□

**Korolar 4.29** *U grupi reda $p^m$, gde je $p$ prost broj i $m \geq 1$, svaka prava podgrupa je strogo sadržana u svom normalizatoru.*

**Dokaz.** Indukcijom po $m$. Slučaj $m = 1$ je trivijalan. Pretpostavimo da je tvrđenje tačno za sve grupe reda $p^k$, gde je $1 \leq k < m$ $(> 1)$ i neka je $\mathbf{H}$ prava podgrupa neabelove grupe $\mathbf{G}$ reda $p^m$. Ako je $\mathbf{Z(G)}$ podgrupa grupe $\mathbf{H}$, onda je $\mathbf{H/Z(G)}$ prava podgrupa grupe $\mathbf{G/Z(G)}$, reda manjeg od $p^m$ (4.13), i po induktivnoj hipotezi je strogo sadržana u svom normalizatoru. Ako je $gZ(\mathbf{G})$ element normalizatora koji nije u podgrupi, onda je $g$ element normalizatora podgrupe $\mathbf{H}$, ali ne i podgrupe $\mathbf{H}$. Ako pak $\mathbf{Z(G)} \not\leq \mathbf{H}$, tada je $\mathbf{H} < \mathbf{HZ(G)} \leq \mathbf{N(H)}$.□

**Napomena.** Prethodni rezultat je samo poseban slučaj opšteg stava da je svaka nilpotentna grupa $N$-grupa – videti 48.9($a$), 48.27 i 48.28 kao i napomenu posle korolara 48.36.

**Definicija 4.30** ($a$) *Podgrupa $\mathbf{H}$ grupe $\mathbf{G}$ je karakteristična akko je $(\mathbf{H})\varphi \leq \mathbf{H}$ za svako $\varphi \in Aut(\mathbf{G})$;*

*Grupa je karakteristično prosta akko nema netrivijalnih karakterističnih podgrupa.*

($b$) *Podgrupa $\mathbf{H}$ grupe $\mathbf{G}$ je potpuno invarijantna akko je $(\mathbf{H})\varphi \leq \mathbf{H}$ za svako $\varphi \in End(\mathbf{G})$.*

Uočimo da kao i u slučaju normalnih podgrupa, s tim što se tamo radilo o unutrašnjim automorfizmima (videti 4.2), imamo:

$\mathbf{H}$ *je karakteristična podgrupa akko važi* $\forall \varphi \in Aut(\mathbf{G})$ $(\mathbf{H})\varphi = \mathbf{H}$.

**Lema 4.31** *Svojstva karakterističnosti i potpune invarijantnosti su tranzitivna, tj. ako je $\mathbf{H}$ karakteristična (potpuno invarijantna) podgrupa grupe $\mathbf{K}$ i $\mathbf{K}$ karakteristična (potpuno invarijantna) podgrupa grupe $\mathbf{G}$, tada je $\mathbf{H}$ karakteristična (potpuno invarijantna) podgrupa grupe $\mathbf{G}$.*

**Dokaz.** Za oba svojstva dokaz je isti. Recimo, neka je $\mathbf{H}$ karakteristična podgrupa grupe $\mathbf{K}$, $\mathbf{K}$ karakteristična podgrupa grupe $\mathbf{G}$ i $\varphi \in Aut(\mathbf{G})$. Onda je $(\mathbf{K})\varphi = \mathbf{K}$ pa je $\varphi|_K \in Aut(\mathbf{K})$. Stoga je $(\mathbf{H})\varphi|_K = \mathbf{H}$, no $(\mathbf{H})\varphi|_K = (\mathbf{H})\varphi$.□

Za podgrupu $\mathbf{H}$ grupe $\mathbf{G}$ očigledno važi:

$\mathbf{H}$ *je potpuno invarijantna* $\Longrightarrow$ $\mathbf{H}$ *je karakteristična* $\Longrightarrow$ $\mathbf{H}$ *je normalna.*

Nemamo, međutim, implikacije u suprotnom smeru.

U Kleinovoj grupi su sve podgrupe reda 2 normalne, ali ne i karakteristične – videti i 4.36.

Posmatrajmo sada grupu $\mathbf{GL}_n(\mathbf{Re})$ realnih, regularnih matrica formata $n \times n$ (2.4($d$)). Iz teorije matrica je poznato da je $Z(\mathbf{GL}_n(\mathbf{Re})) = \{\alpha I \mid \alpha \in Re \setminus \{0\}\}$, i naravno, to je svojstvo svakog centra, $\mathbf{Z(GL}_n\mathbf{(Re))}$ je karakteristična podgrupa. Lako je pak proveriti da je preslikavanje $\varphi : GL_n(\mathbf{Re}) \to GL_n(\mathbf{Re})$, gde je



$$(A)\varphi \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 0 & \dots & ln|det(A)| \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix},$$

endomorfizam grupe $\mathbf{GL}_n(\mathbf{Re})$, ali $(Z(\mathbf{GL}_n(\mathbf{Re})))\varphi \not\subseteq Z(\mathbf{GL}_n(\mathbf{Re}))$.

**Lema 4.32** *Skup svih $FC$-elemenata grupe je domen karakteristične podgrupe, tzv. $FC$-centra grupe.*

**Dokaz.** Jasno, bar je jedinični element $FC$-element. Ako su pak $a$ i $b$ $FC$-elementi, tj. ako su njihovi centralizatori konačnog indeksa (videti dokaz leme 4.11), onda je, s obzirom da je $\mathbf{C}(b) = \mathbf{C}(b^{-1})$ i $\mathbf{C}(a) \cap \mathbf{C}(b^{-1}) \leq \mathbf{C}(ab^{-1})$, i centralizator elementa $ab^{-1}$ konačnog indeksa (3.12), te je skup $FC$-elemenata domen podgrupe (mogli smo, naravno, i direktno da zaključimo da ako su $a = a_1, \dots, a_k$ i $b = b_1, \dots, b_m$ svi konjugati elemenata $a$ i $b$, tada su konjugati elementa $a^{-1}$ inverzni elementi konjugata $a$, a konjugati elementa $ab$ su, ne nužno različiti, elementi $a_ib_j$, $i = 1, \dots, k$, $j = 1, \dots, m$. Pošto je, za ma koji automorfizam $\varphi$, $C((a)\varphi) = (C(a))\varphi$ (što nam uzgred dokazuje da je centar grupe karakteristična podgrupa), proizilazi i da je slika $FC$-elementa opet $FC$-element (4.18).□

**Lema 4.33** *Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$. Tada je $\bigcap\{(\mathbf{H})\varphi \mid \varphi \in Aut(\mathbf{G})\}$ maksimalna (s obzirom na inkluziju) karakteristična podgrupa grupe $\mathbf{G}$ sadržana u $\mathbf{H}$, tzv. karakteristično jezgro podgrupe $\mathbf{H}$.*

**Dokaz.** Analogan dokazu leme 4.8.□

**Lema 4.34** *Ako je $\mathbf{H} \leq \mathbf{K} \lhd \mathbf{G}$ i $\mathbf{H}$ karakteristična podgrupa grupe $\mathbf{K}$, tada je $\mathbf{H}$ normalna podgrupa grupe $\mathbf{G}$.*

**Napomena.** Treba i ovo reći: iz $\mathbf{H} < \mathbf{K} < \mathbf{G}$ i $\mathbf{H}$ je karakteristična (potpuno invarijantna) podgrupa grupe $\mathbf{G}$ ne sledi nužno i da je $\mathbf{H}$ karakteristična (potpuno invarijantna) podgrupa grupe $\mathbf{K}$. Tako npr. $\mathbf{Z(GL}_n\mathbf{(Re))}$ nije karakteristična podgrupa grupe dijagonalnih, regularnih matrica $\mathbf{D}$, jer za, recimo, $\varphi \in Aut(\mathbf{D})$, gde je $(diag(a_1, a_2, \dots, a_n))\varphi = diag(a_1^{-1}, a_2, \dots, a_n)$, $(Z(\mathbf{GL}_n(\mathbf{Re})))\varphi \not\subseteq Z(\mathbf{GL}_n(\mathbf{Re}))$.

**Lema 4.35** *Neka je grupa $\mathbf{G}$ unija rastućeg lanca karakterističnih podgrupa: $\mathbf{G} = \bigcup_{n\in\omega} \mathbf{G}_n$ (za $k < m$ je $\mathbf{G}_k \leq \mathbf{G}_m$). Ako je, za svako $n \in \omega$, $\mathbf{Aut(G}_n\mathbf{)}$ Abelova grupa, onda je i $\mathbf{Aut(G)}$ Abelova grupa. Ako nijedna grupa $\mathbf{Aut(G}_n\mathbf{)}$ $(n \in \omega)$ nema element reda $r$, tada ni $\mathbf{Aut(G)}$ nema element reda $r$.*

**Dokaz**. Neka $\varphi, \psi \in Aut(\mathbf{G})$ i $g \in G$, recimo $g \in G_n$. Kako je $\mathbf{G}_n$ karakteristična podgrupa, to su $\varphi|_{G_n}$, $\psi|_{G_n}$, $(\varphi \circ \psi)|_{G_n} = \varphi|_{G_n} \circ \psi|_{G_n}$ i $(\psi \circ \varphi)|_{G_n} = \psi|_{G_n} \circ \varphi|_{G_n}$ automorfizmi grupe $\mathbf{G}_n$, pa je: $(g)(\varphi \circ \psi) = (g)(\varphi \circ \psi)|_{G_n} = (g)(\varphi|_{G_n} \circ \psi|_{G_n}) = (g)(\psi|_{G_n} \circ \varphi|_{G_n}) = (g)(\psi \circ \varphi)|_{G_n} = (g)(\psi \circ \varphi)$. Analogno se dokazuje i drugi deo tvrđenja.□

**Primer 4.36** *Za svako polje $\langle F, +, \cdot \rangle$ je njegova aditivna grupa $\langle F, + \rangle$ karakteristično prosta.*

**Dokaz**. Ako je $a$ nenula element polja, onda je preslikavanje $\varphi_a : x \longrightarrow ax$ automorfizam njegove aditivne grupe (videti 2.10($f$)). Neka je $\mathbf{H} = \langle H, + \rangle$ prava nenula podgrupa aditivne grupe $\mathbf{F} = \langle F, + \rangle$ (polja $\langle F, +, \cdot \rangle$). Ako je $b$ nenula element podgrupe $\mathbf{H}$ i ako $c$ nije u $\mathbf{H}$, onda $(b)\varphi_{cb^{-1}} = c \notin H$.□

**Definicija 4.37** *Prava podgrupa $\mathbf{H}$ grupe $\mathbf{G}$ je maksimalna akko nije sadržana ni u jednoj drugoj pravoj podgrupi (znači: iz $\mathbf{H} \leq \mathbf{K} \leq \mathbf{G}$ sledi $\mathbf{K} = \mathbf{H}$ ili $\mathbf{K} = \mathbf{G}$).*

*Prava podgrupa $\mathbf{H}$ grupe $\mathbf{G}$ je maksimalna podgrupa sa svojstvom $\mathcal{P}$ akko ima svojstvo $\mathcal{P}$ i nije sadržana ni u jednoj drugoj pravoj podgrupi sa svojstvom $\mathcal{P}$.*

*Nejedinična normalna podgrupa grupe $\mathbf{G}$ je minimalna normalna podgrupa akko ne sadrži strogo nijednu drugu normalnu podgrupu grupe $\mathbf{G}$, osim, naravno, jedinične.*

*Podgrupa $\mathbf{H}$ konačne grupe $\mathbf{G}$ je Hallova podgrupa akko je*

$$([\mathbf{G} : \mathbf{H}], |H|) = 1.$$

*Podgrupa $\mathbf{H}$ konačne grupe $\mathbf{G}$ je specijalna akko za svako $a \in G$ i svako $b \in G \setminus H$ postoji jedinstveno $h \in H$ takvo da je $a^{-1}ba = h^{-1}bh$.*

**Lema 4.38** ($a$) *Neka je $\mathbf{G}$ grupa i $A$ neprazan podskup njenog domena koji ne sadrži jedinični element. Tada postoji maksimalna podgrupa grupe $\mathbf{G}$ sa svojstvom da joj je domen disjunktan sa $A$;*

($b$) *Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$, $A$ neprazan podskup domena grupe $\mathbf{G}$ i neka je $A \cap H = B$. Tada postoji maksimalna podgrupa grupe $\mathbf{G}$ koja sadrži $\mathbf{H}$ i čiji domen u preseku sa $A$ daje $B$.*

**Dokaz**. ($a$) Direktna posledica Zornove leme. Familija $\mathcal{F} = \{\mathbf{K} \mid \mathbf{K} < \mathbf{G}, K \cap A = \emptyset\}$ je neprazna familija ($\mathbf{E} \in \mathcal{F}$) i unija svakog lanca podgrupa iz $\mathcal{F}$ je opet u $\mathcal{F}$ (dakle, za svaki lanac postoji gornje ograničenje), pa postoji maksimalni element u $\mathcal{F}$.

($b$) Jasno (ako je ($a$) jasno).□

**Korolar 4.39** *Svaka neabelova grupa ima maksimalnu Abelovu podgrupu.*



**Dokaz**. Za familiju podgrupa $\mathcal{F} = \{\mathbf{A} \mid \mathbf{A}$ je Abelova podgrupa grupe $\mathbf{G}\}$, uređenu relacijom inkluzije, važe uslovi leme Zorna, pa u $\mathcal{F}$ imamo (barem jedan) maksimalni element; no to je i maksimalna Abelova podgrupa grupe $\mathbf{G}$.□

Grupe $\mathbf{p}^\infty$, $\mathbf{Ra}$ i $\mathbf{Re}$ nemaju nijednu maksimalnu podgrupu – videti 7.11 i 33.7.

Jasno, podgrupa čiji je indeks prost broj je maksimalna (3.11). Dati uslov nije i potreban za maksimalnost podgrupe. Zapravo važi:

**Lema 4.40** *Za svaki prirodan broj $n > 1$ postoji grupa sa maksimalnom podgrupom indeksa $n$.*

**Dokaz**. Videti 9.46($a$).□

**Definicija 4.41** *Grupa $\mathbf{G}$ je $R$-grupa akko, za svako $a, b \in G$ i svaki pozitivan prirodan broj $n$, iz $a^n = b^n$ sledi $a = b$.*

*Podgrupa $\mathbf{H}$ $R$-grupe $\mathbf{G}$ je izolovana akko, za svako $g \in G$ i svaki pozitivan prirodan broj $n$, iz $g^n \in H$ sledi $g \in H$; drugim rečima: podgrupa $\mathbf{H}$ je izolovana akko za svako $h \in H$ i svaki pozitivan prirodan broj $n$ rešenje jednačine $h = x^n$, ukoliko postoji u $\mathbf{G}$, pripada podgrupi $\mathbf{H}$.*

U vezi sa terminom *izolovana podgrupa* videti i definiciju 37.1.

Očigledno, $R$-grupe su torziono slobodne. Takođe, svaka Abelova torziono slobodna grupa je $R$-grupa.

Dokazi naredne dve leme su trivijalni.

**Lema 4.42** *Presek familije izolovanih podgrupa $R$-grupe je izolovana podgrupa.*

**Lema 4.43** *Normalna podgrupa $\mathbf{H}$ $R$-grupe $\mathbf{G}$ je izolovana akko je faktor grupa $\mathbf{G}/\mathbf{H}$ torziono slobodna.*

**Definicija 4.44** *Neka je $M$ podskup domena $R$-grupe $\mathbf{G}$. Presek svih izolovanih podgrupa grupe $\mathbf{G}$ čiji domeni sadrže $M$ je tzv. izolatorsko zatvorenje skupa $M$ ili kraće, izolator skupa $M$, u oznaci $\mathbf{I}(M)$. Ako je $M$ baš domen podgrupe $(\mathbf{M})$, pisaćemo i $\mathbf{I}(\mathbf{M})$.*

Naravno, izolator skupa $M$ je najmanja izolovana podgrupa grupe koja sadrži $M$.

**Lema 4.45** ($a$) *Neka je $M$ neprazan podskup $R$-grupe $\mathbf{G}$. Tada je $\mathbf{C}(M)$, centralizator skupa $M$, izolovana podgrupa grupe $\mathbf{G}$.*

($b$) *Centar $R$-grupe je izolovana podgrupa.*

**Dokaz.** ($a$) Neka je $a^n \in C(M)$, gde je $n$ pozitivan prirodan broj. Tada je, za svako $g \in M$, $(g^{-1}ag)^n = g^{-1}a^n g = a^n$, pa $g^{-1}ag = a$ i $a \in C(M)$.□

**Lema 4.46** *Ako su za elemente $a, b$ R-grupe $\mathbf{G}$ i pozitivne prirode brojeve $m, n$ elementi $a^m$ i $b^n$ uzajamno permutabilni, onda su uzajamno permutabilni i elementi $a$ i $b$.*

**Dokaz.** Ako je $n = 1$, tj. $a^m b = ba^m$, tada je, kao i maločas, $(b^{-1}ab)^m = b^{-1}a^m b = a^m$, te $b^{-1}ab = a$, odnosno, $ab = ba$. Generalno, iz $a^m b^n = b^n a^m$ sledi $(a^{-m}ba^m)^n = b^n$, odatle $a^m b = ba^m$, i dalje, $ab = ba$.□

**Lema 4.47** *Torziono slobodna grupa $\mathbf{G}$ je R-grupa akko je $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ R-grupa.*

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{G}$ $R$-grupa. Tada je $\mathbf{Z}(\mathbf{G})$ izolovana podgrupa pa je faktor grupa $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ torziono slobodna. Neka je, za elemente $a, b$ grupe $\mathbf{G}$ i neki pozitivan prirodan $n$, $(aZ(\mathbf{G}))^n = (bZ(\mathbf{G}))^n$, tj. $a^n Z(\mathbf{G}) = b^n Z(\mathbf{G})$. Onda je, za neko $c \in Z(\mathbf{G})$, $b^n = a^n c$, te su elementi $a^n$ i $b^n$ uzajamno permutabilni. Prema prethodnoj lemi uzajamno su permutabilni i elementi $a$ i $b$. Sledi: $c = a^{-n}b^n = (a^{-1}b)^n$, dakle $a^{-1}b \in Z(\mathbf{G})$, odnosno $aZ(\mathbf{G}) = bZ(\mathbf{G})$.

($\Longleftarrow$) Neka je $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ $R$-grupa i neka je, za elemente $a, b$ grupe $\mathbf{G}$ i neko $n > 0$, $a^n = b^n$. Tada je $(aZ(\mathbf{G}))^n = (bZ(\mathbf{G})^n$, te je $a^{-1}b \in Z(\mathbf{G})$. Ako je, za $c \in Z(\mathbf{G})$, $b = ac$, onda je $b^n = (ac)^n = a^n c^n$, znači $c^n = e$ i $a = b$.□

**Lema 4.48** *Neka je $\mathbf{A}$ podgrupa R-grupe $\mathbf{G}$. Tada je $(\mathbf{I}(\mathbf{A}))u_g = \mathbf{I}(g^{-1}\mathbf{A}g)$ za svako $u_g \in Inn(\mathbf{G})$.*

**Dokaz.** Trivijalno. Ako je $\mathbf{B}$ izolovana podgrupa, onda je i $(\mathbf{B})u_g = g^{-1}\mathbf{B}g$ izolovana podgrupa; iz $c^n \in g^{-1}Bg$ sledi $gc^n g^{-1} = (gcg^{-1})^n \in B$ pa $gcg^{-1} \in B$ i $c \in g^{-1}Bg$. Odatle:

$$(\mathbf{I}(\mathbf{A}))u_g = (\bigcap\{\mathbf{B} \mid \mathbf{A} \leq \mathbf{B}\ (\leq \mathbf{G}),\ \mathbf{B} \text{ je izolovana podgrupa}\})u_g =$$

$$\bigcap\{g^{-1}\mathbf{B}g \mid \mathbf{A} \leq \mathbf{B},\ \mathbf{B} \text{ je izolovana podgrupa}\} =$$

$$\bigcap\{g^{-1}\mathbf{B}g \mid g^{-1}\mathbf{A}g \leq g^{-1}\mathbf{B}g,\ g^{-1}\mathbf{B}g \text{ je izolovana podgrupa}\} = \mathbf{I}(g^{-1}\mathbf{A}g).$$□

# 5 Mreže podgrupa

O mrežama podgrupa ćemo ovom prilikom u samo nekoliko reči. Na tu temu ćemo se još vraćati, ali sve se svodi na osnovne činjenice koje su sastavni deo svake "priče" o grupama.



**Definicija 5.1** *Neka je $\mathbf{G}$ grupa i $A$ podskup skupa $G$. Podgrupa generisana skupom $A$ (u oznaci $\langle A\rangle$) je najmanja podgrupa grupe $\mathbf{G}$ čiji domen sadrži $A$, tj. $\langle A\rangle = \bigcap\{\mathbf{H} \leq \mathbf{G} \mid A \subseteq H\}$.*

*Grupa $\mathbf{G}$ je konačno generisana akko je generisana nekim konačnim podskupom svog domena. Posebno, grupa $\mathbf{G}$ je ciklična akko je generisana nekim jednoelementnim podskupom.*

*Grupa je lokalno konačna akko svaki konačan podskup njenog domena generiše konačnu podgrupu.*

Ako je $A$ konačan skup, npr. $A = \{a_0, \ldots, a_{n-1}\}$, pisaćemo $\langle a_0, \ldots, a_{n-1}\rangle$ pre nego korektno $\langle\{a_0, \ldots, a_{n-1}\}\rangle$. Isto tako reći ćemo da je $\langle a_0, \ldots, a_{n-1}\rangle$ (pod)grupa generisana elementima $a_0, \ldots, a_{n-1}$; dakle, nešto preformulisano: grupa je ciklična akko je generisana jednim elementom.

Domen podgrupe $\langle A\rangle$ obeležavaćemo sa $\langle A\rangle$.

Jasno, $\langle\emptyset\rangle = \mathbf{E}$ i $\langle G\rangle = \mathbf{G}$.

Primetimo da je lokalno konačna grupa trivijalno periodična; obrat, međutim, ne mora da važi. Važi, naime, sledeći stav ([54]):

*Za svaki prost broj $p$ i svaki prirodan broj $k$ veći od 1 poznat je primer beskonačne $p$-grupe generisane skupom kardinalnosti $k$.*

Ovim je ujedno dat (negativan) odgovor na dugo nerešiv Burnsideov problem: *da li je konačno generisana periodična grupa konačna?* (pogledati i [3], [63]).

**Lema 5.2** *Neka je $\emptyset \neq A \subseteq G$. Tada je*

$$\langle A\rangle = \{a_{i_1}^{\alpha_1} \cdot \ldots \cdot a_{i_k}^{\alpha_k} \mid \alpha_j \in \{1, -1\},\ a_{i_j} \in A,\ k \in \omega\};$$

*rečima, $\langle A\rangle$ je skup konačnih proizvoda elemenata iz $A \cup A^{-1}$, gde je $A^{-1} \stackrel{\text{def}}{=} \{a^{-1} \mid a \in A\}$.*

*Posebno, ako su svi elementi iz $A$ konačnog reda, $\langle A\rangle$ je skup konačnih proizvoda elemenata iz $A$.*

**Dokaz.** Trivijalan. Inkluzija ($\supseteq$) je jasna, a skup konačnih proizvoda elemenata iz $A \cup A^{-1}$ je, opet očigledno, domen podgrupe.□

**Korolar 5.3** ($a$) *Neka je $\mathbf{G}$ grupa i $A \subseteq G$. Onda važi: $a \in \langle A\rangle$ akko postoji konačan niz elemenata $a_0, \ldots, a_{n(a)-1} = a$ $(n(a) \geq 1)$ takav da je za svako $i$, $0 \leq i < n(a)$, $a_i$ ili element iz $A$ ili $e$ ili $\exists j < i$ i $a_i = a_j^{-1}$ ili $\exists j, k < i$ i $a_i = a_j \cdot a_k$.*

($b$) $|\langle A\rangle| \leq |A| + \aleph_0$. *Posebno, ako je $|A| \geq \aleph_0$, onda je $|\langle A\rangle| = |A|$.*

**Dokaz.** Recimo samo: mogućnost $a = e$ je tu jedino zbog slučaja $A = \emptyset$.□

**Korolar 5.4** *Neka je podgrupa* $\mathbf{H}$ *grupe* $\mathbf{G}$ *generisana skupom* $A$. *Tada važi:*

(*a*) $\mathbf{H}$ *je Abelova akko su elementi iz* $A$ *uzajamno permutabilni;*

(*b*) $\mathbf{H}$ *je potpuno invarijantna (karakteristična, normalna) akko je za svako* $a \in A$ *i svako* $\varphi \in End(\mathbf{G})$ $(\varphi \in Aut(\mathbf{G}),\ \varphi \in Inn(\mathbf{G}))$ $(a)\varphi \in H$.

Prema tome, podgrupe $\mathbf{G}^k \stackrel{\text{def}}{=} \langle\{g^k \mid g \in G\}\rangle$ $(k \in \omega)$ grupe $\mathbf{G}$ su potpuno invarijantne.

**Korolar 5.5** *Ako je* $\varphi$ *homomorfno preslikavanje grupe* $\mathbf{G}$, *generisane skupom* $A$, *na grupu* $\mathbf{H}$, *tada je grupa* $\mathbf{H}$ *generisana skupom* $(A)\varphi$; *posebno, ako je* $\mathbf{G}$ *ciklična, onda je i* $\mathbf{H}$ *ciklična grupa.*

*Ako je* $\phi, \psi \in Hom(\mathbf{G}, \mathbf{K})$ *i* $\forall a \in A\ \ (a)\phi = (a)\psi$, *tada je* $\phi = \psi$.

**Korolar 5.6** *Za konačne grupe važi:*

(*a*) *Red elementa deli red grupe;*

(*b*) *Ako je red grupe prost broj, grupa je ciklična.*

(*c*) *Grupa čiji je red stepen prostog broja* $p$ *je* $p$*-grupa.*

Kasnije ćemo pokazati da u slučaju konačnih grupa važi i obrat tačke (*c*) (16.18), a sada ćemo, vežbe radi, iskoristiti poslednji rezultat (tačka (*a*)) u dokazu sledećeg tvrđenja iz teorije brojeva:

*Fermatova teorema (Pierre Fermat,* 1601-1665*). Ako je* $(a, n) = 1$, $a \in Z$, $n \in \omega$, *tada je* $a^{\varphi(n)} \equiv 1\ (mod\ n)$ *(*$\varphi$ *- Eulerova funkcija).*

Neka je $(a, n) = 1$ i $a = bn + c$, $1 \leq c < n$. Jasno, onda je i $(c, n) = 1$, pa je $\underbrace{c \cdot_n \ldots \cdot_n c}_{\varphi(n)-puta} = c^{\varphi(n)} - [\frac{c^{\varphi(n)}}{n}]\ n = 1$ (videti primere 2.4(*b*) i 3.4(*e*)).

Prema tome, $a^{\varphi(n)} = (bn + c)^{\varphi(n)} = \sum_{k=0}^{\varphi(n)-1} \binom{\varphi(n)}{k} (bn)^{\varphi(n)-k} c^k + c^{\varphi(n)} = \sum_{k=0}^{\varphi(n)-1} \binom{\varphi(n)}{k} (bn)^{\varphi(n)-k} c^k + [\frac{c^{\varphi(n)}}{n}]\, n + 1$, dakle $n | (a^{\varphi(n)} - 1)$.

**Primer 5.7** (*a*) *Podgrupa multiplikativne grupe kompleksnih regularnih matrica formata* $2 \times 2$ *generisana matricama* $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ *i* $B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$ *je reda* 8. *To je tzv. grupa kvaterniona i obično se obeležava sa* $\mathbf{Q}$ *(koristi se i* $\mathbf{Q}_8$*).*



**Dokaz.** Kako je $A^2 = B^2 = (AB)^2\ (= -I)$ i $A^4 = I$, a odatle $BA = A^3B$, imamo:

| $\cdot$ | $I$ | $A$ | $A^2$ | $A^3$ | $B$ | $AB$ | $A^2B$ | $A^3B$ |
|---|---|---|---|---|---|---|---|---|
| $I$ | $I$ | $A$ | $A^2$ | $A^3$ | $B$ | $AB$ | $A^2B$ | $A^3B$ |
| $A$ | $A$ | $A^2$ | $A^3$ | $I$ | $AB$ | $A^2B$ | $A^3B$ | $B$ |
| $A^2$ | $A^2$ | $A^3$ | $I$ | $A$ | $A^2B$ | $A^3B$ | $B$ | $AB$ |
| $A^3$ | $A^3$ | $I$ | $A$ | $A^2$ | $A^3B$ | $B$ | $AB$ | $A^2B$ |
| $B$ | $B$ | $A^3B$ | $A^2B$ | $AB$ | $A^2$ | $A$ | $I$ | $A^3$ |
| $AB$ | $AB$ | $B$ | $A^3B$ | $A^2B$ | $A^3$ | $A^2$ | $A$ | $I$ |
| $A^2B$ | $A^2B$ | $AB$ | $B$ | $A^3B$ | $I$ | $A^3$ | $A^2$ | $A$ |
| $A^3B$ | $A^3B$ | $A^2B$ | $AB$ | $B$ | $A$ | $I$ | $A^3$ | $A^2$. |

Primetimo da su sve podgrupe grupe $\mathbf{Q}$ normalne. Prave (netrivijalne) podgrupe su reda 2 ili 4. Za one reda 4, dakle indeksa 2, već znamo da su normalne, a jedina podgrupa reda 2, $\langle\{I, A^2\}, \cdot\rangle$, je baš centar grupe $\mathbf{Q}$ (u proveri ovoga dovoljno je, naravno, samo pokazati da je $A^2$ jedini element, pored jediničnog, permutabilan sa generatornim elementima grupe $A$ i $B$). Navodimo ovom prilikom i definicije:

*Hamiltonova grupa (William Rowan Hamilton,* 1805-1865*) je neabelova grupa čije su sve podgrupe normalne. Kasnije ćemo pokazati da svaka Hamiltonova grupa ima za podgrupu grupu kvaterniona (*20.1*);*

*Abelove i Hamiltonove grupe čine klasu Dedekindovih grupa (Richard Julius Wilhelm Dedekind,* 1831-1916*).*

S grupom $\mathbf{Q}$, kao što smo obećali, vraćamo dug iz 4.5. Podgrupa $\langle\{I, A^2, B, A^2B\}, \cdot\rangle$, označimo je sa $\mathbf{H}$, normalna je i sadrži centar, a za automorfizam $\varphi$ određen sa $(A)\varphi = B$, $(B)\varphi = A$ (onda je npr. $(A^3B)\varphi = AB$) imamo $(H)\varphi = \{I, A, A^2, A^3\} \neq H$.

(*b*) *Dijedarska grupa stepena* $n$ *(*3.4(*e*)*) generisana je elementima* $\sigma_y$ *i* $\rho_{\frac{2\pi}{n}}$ *za koje važi:* $\sigma_y^2 = (\rho_{\frac{2\pi}{n}})^n = \imath$ *i* $\rho_{\frac{2\pi}{n}} \sigma_y = \sigma_y (\rho_{\frac{2\pi}{n}})^{n-1} = \sigma_y (\rho_{\frac{2\pi}{n}})^{-1}$.

**Dokaz.** Samo podsećamo: izometrija je određena slikom triju tačaka.

(*c*) *Podgrupa grupe* $\mathbf{GL}_2(\mathbf{Re})$ *generisana matricama*

$$A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \ i \ B = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$$

*je beskonačna, a elementi su joj konačni proizvodi matrica* $A$ *i* $B$ *koje se u njima naizmenično pojavljuju (videti komentar uz* 2.7*); drugim rečima, njeni nejedinični elementi su oblika* $C_1 \cdot \ldots \cdot C_k$, $k \geq 1$, *gde je* $C_i$ *ili* $A$ *ili* $B$ *i* $C_i \neq C_{i+1}$.

**Definicija 5.8** *Frattinijeva podgrupa (G. Frattini,* 1852 - 1925*) grupe* $\mathbf{G}$, *u oznaci* $\mathbf{Fr}(\mathbf{G})$ *(koristi se i* $\mathbf{Frat}(\mathbf{G})$, $\Phi(\mathbf{G})$*), presek je svih maksimalnih podgrupa grupe* $\mathbf{G}$, *ukoliko takvih ima, u suprotnom je* $\mathbf{Fr}(\mathbf{G}) = \mathbf{G}$.

**Lema 5.9** *Domen Frattinijeve podgrupe grupe* $\mathbf{G}$ *je skup svih elemenata koji se mogu eliminisati iz svakog skupa generatora (cele) grupe.*

**Dokaz**. Neka je $D$ skup svih elemenata (grupe $\mathbf{G}$) koji se mogu eliminisati iz svakog generatornog skupa grupe. $D$ je, naravno, neprazan skup jer je barem $e \in D$. Dokazaćemo (1) $(Fr(\mathbf{G}))^c \subseteq D^c$ i (2) $D^c \subseteq (Fr(\mathbf{G}))^c$ (gde je, za $A \subseteq G$, $A^c = G \setminus A$ – komplement skupa $A$).

(1) Neka je $a \in (Fr(\mathbf{G}))^c$. Onda $a$ nije element neke maksimalne podgrupe $\mathbf{M}$, pa je $M \cup \{a\}$ generatorni skup grupe $\mathbf{G}$ iz koga se $a$ ne može eliminisati.

(2) Neka je sada $a \in D^c$ i neka je $a \in A\ (\subseteq G)$, $G = \langle A \rangle$ i $G \neq \langle A \setminus \{a\} \rangle$. Tada $a \notin \langle A \setminus \{a\} \rangle$, te postoji maksimalna podgrupa grupe $\mathbf{G}$, recimo $\mathbf{M}$, koja sadrži podgrupu $\langle A \setminus \{a\} \rangle$ i čiji element nije $a$. No, $\mathbf{M}$ je, zapravo, i maksimalna podgrupa grupe $\mathbf{G}$; jer, ako je $\mathbf{M}$ prava podgrupa podgrupe $\mathbf{N}$, onda je $a \in N$ i kako je već $A \setminus \{a\} \subseteq N$, sledi $\mathbf{N} = \mathbf{G}$.□

**Korolar 5.10** *Neka je* $\mathbf{H}$ *podgrupa grupe* $\mathbf{G}$, $\mathbf{Fr(G)}$ *konačno generisana grupa i* $\mathbf{G} = \mathbf{Fr(G)} \cdot \mathbf{H}$. *Tada je* $\mathbf{G} = \mathbf{H}$.

**Dokaz**. Ako je $\mathbf{Fr(G)} = \langle g_1, \ldots, g_n \rangle$, tada je prema prethodnoj lemi:

$$\mathbf{G} = \langle \{g_1, \ldots, g_n\} \cup H \rangle = \langle \{g_1, \ldots, g_{n-1}\} \cup H \rangle = \cdots = \langle \{g_1\} \cup H \rangle = \langle H \rangle.\square$$

**Korolar 5.11** *Ako je Frattinijeva podgrupa grupe* $\mathbf{G}$ *konačno generisana, a faktor grupa* $\mathbf{G/Fr(G)}$ *generisana skupom* $\{g_i Fr(\mathbf{G}) \mid i \in I\}$, *onda je grupa* $\mathbf{G}$ *generisana skupom* $\{g_i \mid i \in I\}$.

**Dokaz**. Neka je $\mathbf{H} = \langle \{g_i \mid i \in I\} \rangle$. Tada je $\mathbf{G} = \mathbf{Fr(G)} \cdot \mathbf{H}$ i prema prethodnom korolaru $\mathbf{G} = \mathbf{H}$.□

**Korolar 5.12** *Ako je* $\mathbf{G}$ *konačno generisana prosta grupa, onda je* $\mathbf{Fr(G)}$ *jedinična podgrupa.*

**Korolar 5.13** *Grupa je bez maksimalnih podgrupa akko se svaki njen element može eliminisati iz svakog njenog generatornog skupa.*

**Definicija 5.14** *Grupa ispunjava uslov rastućih lanaca akko je svaki rastući niz njenih podgrupa konačan, tj. akko važi: ako je* $\mathbf{A}_0 \leq \mathbf{A}_1 \leq \cdots \leq \mathbf{A}_k \leq \cdots$ *rastući niz podgrupa, onda je, za neki prirodan broj* $n$, $\mathbf{A}_n = \mathbf{A}_{n+1} = \mathbf{A}_{n+2} = \cdots$.

*Jednostavnije i bez dodatnih objašnjenja: grupa ispunjava uslov rastućih lanaca akko je svaki strogo rastući lanac podgrupa konačan.*

*Grupa ispunjava uslov opadajućih lanaca akko je svaki opadajući lanac njenih podgrupa konačan.*

*Grupa* $\mathbf{G}$ *ispunjava uslov maksimalnosti (minimalnosti) podgrupa akko svaka neprazna familija* $\mathcal{F}$ *njenih podgrupa sadrži podgrupu koja nije sadržana*



*ni u jednoj drugoj podgrupi (ne sadrži ni jednu drugu podgrupu) familije* $\mathcal{F}$. *Analogno se definiše uslov maksimalnosti (minimalnosti) normalnih (karakterističnih, potpuno invarijantnih) podgrupa.*

**Napomena.** Umesto termina *rastući lanac* mogli smo u prethodnoj definiciji koristiti, a mnogi bi to i radije učinili, termin *neopadajući lanac* (naravno, onda bi *strogo rastući lanac* postao *rastući lanac*); slična je situacija i sa opadajućim i strogo opadajućim lancima. No mišljenja smo da je navedeno tumačenje termina rastući (opadajući) lanac podgrupa češće u upotrebi.

**Lema 5.15** *Neka je data grupa* $\mathbf{G}$. *Sledeći uslovi su ekvivalentni:*

($a$) $\mathbf{G}$ *ispunjava uslov rastućih lanaca;*

($b$) *Svaka podgrupa grupe* $\mathbf{G}$ *je konačno generisana;*

($c$) $\mathbf{G}$ *ispunjava uslov maksimalnosti podgrupa.*

**Dokaz**. ($a$) $\Longrightarrow$ ($b$) Pretpostavimo da važi ($a$) i neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$, a $h_0$ (ma koji) njen element. Ako je $\langle h_0 \rangle$ prava podgrupa grupe $\mathbf{H}$, biramo element $h_1 \in H \setminus \langle h_0 \rangle$. Ukoliko je i $\langle h_0, h_1 \rangle$ prava podgrupa, biramo element $h_2 \in H \setminus \langle h_0, h_1 \rangle$ i nastavljamo postupak. No s obzirom da je lanac $\langle h_0 \rangle < \langle h_0, h_1 \rangle < h_0, h_1, h_2 \rangle < \cdots$ konačan, mora i $\mathbf{H}$ biti konačno generisana podgrupa.

($b$) $\Longrightarrow$ ($c$) Pretpostavimo da neprazna familija podgrupa $\mathcal{F}$ grupe $\mathbf{G}$ ne ispunjava uslov maksimalnosti podgrupa. U tom slučaju postoji strogo rastući niz podgrupa iz $\mathcal{F}$: $\mathbf{H}_0 < \mathbf{H}_1 < \cdots < \mathbf{H}_n < \cdots$, a unija tog lanca $\mathbf{H} = \bigcup_{i \in \omega} \mathbf{H}_i$ nije konačno generisana grupa; $\mathbf{H} = \langle h_0, \ldots, h_m \rangle$ i $h_k \in H_{i_k}$, $k = 0, \ldots, m$, dalo bi $\mathbf{H}_r = \mathbf{H}_{r+1} = \cdots = \mathbf{H}$, gde je $r = max\{i_0, \ldots, i_m\}$).

($c$) $\Longrightarrow$ ($a$) Neka važi ($c$) i neka je $\mathbf{H}_0 \leq \mathbf{H}_1 \leq \cdots$ rastući niz podgrupa grupe $\mathbf{G}$. Ako je $\mathbf{H} = \mathbf{H}_n$ maksimalni element (s obzirom na inkluziju) familije $\mathcal{F} = \{\mathbf{H}_i \mid i \in \omega\}$, onda je $\mathbf{H}_n = \mathbf{H}_{n+1} = \cdots$.□

Analogno tvrđenje imamo za uslov maksimalnosti normalnih podgrupa. No prvo

**Definicija 5.16** *Neka su* $A$ *i* $B$ *podskupovi domena grupe* $\mathbf{G}$. *Tada sa* $A^B$ *označavamo podgrupu, kao i njen domen,* $\langle \{b^{-1}ab \mid a \in A, b \in B\} \rangle$ *(naravno, ostaje standardna upotreba oznake* $A^B$ *za skup funkcija* $\{f \mid f : A \longrightarrow B\}$, *a iz konteksta će uvek biti jasno na šta se data oznaka odnosi). Ako su* $A$ *i* $B$ *domeni podgrupa, koristićemo za formiranu podgrupu oznaku* $\mathbf{A^B}$, *a za njen domen ostaje* $A^B$.

*Neka je* $\mathbf{G}$ *grupa i* $A \subseteq G$ $(\mathbf{A} \leq \mathbf{G})$. *Najmanja normalna podgrupa grupe* $\mathbf{G}$ *koja sadrži* $A$ *zove se normalno zatvorenje skupa* $A$ *(podgrupe* $\mathbf{A}$*). Za njegovo obeležavanje koristi se, pored već uvedene oznake* $A^{\mathbf{G}}$ $(\mathbf{A}^{\mathbf{G}})$ *(videti napomenu dole), takođe* $[A]_{\mathbf{G}}$, *odnosno (kada je podgrupa u pitanju)* $[\mathbf{A}]_{\mathbf{G}}$, *ili samo* $[A]$, *tj.* $[\mathbf{A}]$.

*Grupa je lokalno konačna i normalna akko je normalno zatvorenje svakog konačnog podskupa njenog domena konačna podgrupa.*

**Napomena.** U knjizi A. Kuroša koristi se termin *lokalno normalna grupa* umesto lokalno konačna i normalna grupa. Korektnije je, međutim, imajući u vidu opštu definiciju o lokalnim svojstvima (pogledati paragraf "Lokalna svojstva"), lokalno konačna i normalna grupa. Ovo je, uostalom, primedba i K. Hirscha, prevodioca Kuroševe knjige na engleski, a "pun" termin se koristi, recimo, i u knjizi D. Robinsona. U našem nemaru dozvolićemo sebi luksuz da se služimo sa oba termina.

Jasno, $[A] = \bigcap\{\mathbf{N} \mid \mathbf{N} \lhd \mathbf{G} \text{ i } A \subseteq N\} = \langle\{g^{-1}ag \mid g \in G, a \in A\}\rangle = \langle\bigcup\{g^{-1}Ag \mid g \in G\}\rangle = A^{\mathbf{G}}$. Karakterizacija normalnog zatvorenja podgrupe je data u 6.16.

**Lema 5.17** *(Lema Dicmana). Neka je $M$ konačan normalan podskup domena grupe $\mathbf{G}$ koji se sastoji od elemenata konačnog reda. Tada je $\langle M\rangle$ konačna normalna podgrupa grupe $\mathbf{G}$.*

**Dokaz.** Ako je $|M| = m$ i $n$ najmanji zajednički sadržalac redova elemenata iz $M$, onda se svaki element iz $\langle M\rangle$ može predstaviti kao proizvod od ne više od $m(n-1)$ elemenata iz $M$ (prema tome je i $\langle M\rangle$ konačna podgrupa). Zaista, neka je $g = a_1 \dots a_k \in \langle M\rangle$, $a_i \in M$, $1 \leq i \leq k$, i neka je $k > m(n-1)$. Onda se bar jedan element iz $M$, recimo $a$, javlja barem $n$ puta u tom proizvodu. Neka je $i$ najmanji indeks za koji je $a_i = a$. Tada je (pretpostavićemo odmah $i > 1$):

$$g = a_1 \dots a_{i-1}a_ia_{i+1} \dots a_k = aa^{-1}a_1aa^{-1}a_2a \dots a^{-1}a_{i-1}aa^{-1}a_ia_{i+1} \dots a_k =$$

$$aa'_1a'_2 \dots a'_{i-1}a_{i+1} \dots a_k.$$

Ovim smo "izvukli" jedno $a$ na prvo mesto. U daljem postupku, polazeći od proizvoda $a'_1 \dots a'_{i-1}a_{i+1} \dots a_k$, izvukli bismo opet "prvo po redu" $a$ na prvo mesto, i uopšte, nakon $n$ takvih koraka dobili bismo $g = a^nh$, gde je sa $h$ jednostavno obeležen "ostatak". No, $a^n = e$, a $g = h$ je sada proizvod od $k-n$ elemenata iz $M$ (jer je $M$ normalan podskup). Ako je $k - n \leq m(n-1)$ gotovi smo, u suprotnom postupak se ponavlja sa (eventualno nekim novim) elementom koji se javlja barem $n$ puta. Konačno ćemo tako dobiti element $g$ predstavljen kao proizvod od ne više od $m(n-1)$ elemenata iz $M$.□

**Korolar 5.18** *Grupa je periodična $FC$-grupa akko je lokalno konačna i normalna.*

*Periodična Abelova grupa je lokalno konačna.*

**Dokaz.** Neka je $g$ element lokalno konačne i normalne grupe $\mathbf{G}$. On je tada sadržan u nekoj konačnoj normalnoj podgrupi $\mathbf{H}$ (grupe $\mathbf{G}$), koja, jasno, sadrži i sve njegove konjugate, dakle, $g$ je $FC$-element.□



**Definicija 5.19** *Grupa $\mathbf{G}$ ima svojstvo $\mathcal{P}$ rezidualno akko za svaki element $g \in G \setminus \{e\}$ postoji normalna podgrupa $\mathbf{N}_g$ grupe $\mathbf{G}$ takva da faktor grupa $\mathbf{G}/\mathbf{N}_g$ ima svojstvo $\mathcal{P}$ i $g \notin N_g$.*

Grupa $\mathbf{Z}$ ima npr. svojstvo konačnosti rezidualno, tj. rezidualno je konačna. Jer, ako je $(0 \neq)\ m \in Z$ i $p$ prost broj koji nije faktor broja $m$, onda $m \notin pZ$ i $\mathbf{Z}/p\mathbf{Z}$ je reda $p$. Ovo je uostalom, kao što ćemo kasnije videti (23.3($h$)), samo specijalan slučaj opšteg stava da je svaka slobodna grupa rezidualno konačna.

U daljem ćemo, govoreći generalno o nekom svojstvu grupe, ukoliko jedino ne naglasimo drugačije, podrazumevati da se to svojstvo ne tiče prirode elemenata ili operacije; dakle, ako ga ima neka grupa, imaće ga i sve grupe njoj izomorfne.

**Korolar 5.20** *Ako je $\mathbf{G}$ $FC$-grupa, onda je $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ periodična, rezidualno konačna grupa;*

**Dokaz.** Neka $a$ nije element centra grupe $\mathbf{G}$. Onda, za neko $b$ $(\in G)$, $a \notin C(b)$ i kako je $\mathbf{C}(b)$ konačnog indeksa (4.11), to je $\mathbf{C}(b)/\mathbf{Z}(\mathbf{G})$ podgrupa konačnog indeksa grupe $\mathbf{G}/\mathbf{Z}(\mathbf{G})$. Prema 4.19, $\mathbf{Core}(\mathbf{C}(b)/\mathbf{Z}(\mathbf{G}))$ je normalna podgrupa konačnog indeksa grupe $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ koja, jasno, ne sadrži element $aZ(\mathbf{G})$, dakle, $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ je rezidualno konačna grupa. Neka je, dalje, $g$ ma koji element grupe $\mathbf{G}$ i $\{d_1, \dots, d_k\}$ desna transverzala centralizatora elementa $g$. Prema 3.18, $\mathbf{C} = \mathbf{C}(d_1) \cap \dots \cap \mathbf{C}(d_k)$ je podgrupa konačnog indeksa pa je $\mathbf{Core}(\mathbf{C})$ normalna podgrupa konačnog indeksa. Stoga je, za neki pozitivan prirodan broj $m$, $g^m \in Core(\mathbf{C})$, posebno, $g^m$ je permutabilan sa svakim od elemenata $d_1, \dots, d_m$. No kako je $\mathbf{G} = \langle C(g) \cup \{d_1, \dots, d_k\}\rangle$, proizilazi da je $g^m$ element centra, te je $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ i periodična grupa.□

**Lema 5.21** *Sledeći uslovi su ekvivalentni za grupu $\mathbf{G}$:*

*($a$) $\mathbf{G}$ ispunjava uslov rastućih lanaca normalnih podgrupa;*

*($b$) Svaka normalna podgrupa grupe $\mathbf{G}$ je normalno zatvorenje nekog konačnog skupa;*

*($c$) $\mathbf{G}$ ispunjava uslov maksimalnosti normalnih podgrupa.*

**Dokaz.** Videti (i iskoristiti) dokaz prethodne leme.□

**Lema 5.22** *Sledeći uslovi su ekvivalentni za grupu $\mathbf{G}$:*

*($a$) $\mathbf{G}$ ispunjava uslov opadajućih lanaca (normalnih) podgrupa;*

*($b$) $\mathbf{G}$ ispunjava uslov minimalnosti (normalnih) podgrupa.*

Očigledno, ako grupa $\mathbf{G}$ ispunjava uslov rastućih lanaca, onda i svaka njena prava podgrupa ispunjava taj uslov. Obrat ne važi: svaka prava podgrupa

grupe $\mathbf{p}^\infty$ je konačna, dakle, ispunjava uslov rastućih lanaca, ali ga sama grupa $\mathbf{p}^\infty$ ne ispunjava.

Za uslov opadajućih lanaca imamo, međutim, očigledno:

*grupa* $\mathbf{G}$ *ispunjava uslov opadajućih lanaca akko svaka njena prava podgrupa ispunjava taj uslov.*

Grupe $\mathbf{p}^\infty$, $\mathbf{Ra}$ i $\mathbf{Re}$ ne ispunjavaju uslov maksimalnosti, a aditivne grupe racionalnih i realnih brojeva ne ispunjavaju ni uslov minimalnosti podgrupa. Prüferova grupa pak zadovoljava uslov minimalnosti, dok s druge strane aditivna grupa celih brojeva ispunjava uslov maksimalnosti ali ne i minimalnosti podgrupa. Uočimo da je podgrupa grupe $\mathbf{Z}$ maksimalna akko je generisana prostim brojem (7.2), pa je $\mathbf{Fr}(\mathbf{Z}) = \mathbf{O}$ (dosledno aditivnoj notaciji jediničnu podgrupu obeležavamo sa $\mathbf{O}$).

**Lema 5.23** *Ako grupa* $\mathbf{G}$ *ispunjava uslov minimalnosti normalnih podgrupa, onda ima jedinstvenu minimalnu podgrupu konačnog indeksa koja je i karakteristična.*

**Dokaz.** Uslov minimalnosti normalnih podgrupa nam garantuje egzistenciju jedinstvene minimalne normalne podgrupe konačnog indeksa, neka je to $\mathbf{F}$; u pitanju je najmanji element familije podgrupa $\mathcal{F} = \{\mathbf{N} \lhd \mathbf{G} \mid [\mathbf{G} : \mathbf{N}] < \infty\}$. Ako je $\mathbf{K}$ podgrupa konačnog indeksa, tada je i $\mathbf{Core}(\mathbf{K})$ podgrupa konačnog indeksa, pa je prema 3.18 $\mathbf{F} \cap \mathbf{Core}(\mathbf{K})$ (normalna) podgrupa konačnog indeksa. Stoga je $\mathbf{F} \leq \mathbf{Core}(\mathbf{K}) \leq \mathbf{K}$; dakle, $\mathbf{F}$ se sadrži u svim podgrupama konačnog indeksa. Kao jedinstvena minimalna podgrupa konačnog indeksa, $\mathbf{F}$ je i karakteristična (videti komentar uz 4.17). Recimo još da se podgrupa $\mathbf{F}$ zove *konačni ostatak* (eng. *finite residual*) grupe $\mathbf{G}$.□

**Korolar 5.24** *Ako su* $\mathbf{H}_i$, $i \in I$, *potpuno invarijantne (karakteristične, normalne) podgrupe grupe* $\mathbf{G}$, *onda su i* $\bigcap_{i\in I} \mathbf{H}_i$ *i* $\langle \bigcup_{i\in I} H_i \rangle$ *potpuno invarijantne (karakteristične, normalne) podgrupe grupe* $\mathbf{G}$.

*Posebno, unija lanca karakterističnih (potpuno invarijantnih) podgrupa je karakteristična (potpuno invarijantna) podgrupa.*

**Dokaz.** Dovoljno je podsetiti se da je za svako preslikavanje $\varphi$: $(\bigcap_{i\in I} H_i)\varphi \subseteq \bigcap_{i\in I}(H_i)\varphi$ i $(\bigcup_{i\in I} H_i)\varphi = \bigcup_{i\in I}(H_i)\varphi$. Ostalo je stvar definicija, s tim što se u dokazu drugog dela prvoga dela tvrđenja koristi i 5.5.□

**Korolar 5.25** *Frattinijeva podgrupa je karakteristična.*

**Dokaz.** Recimo samo: izomorfna slika maksimalne podgrupe je maksimalna podgrupa.□

U narednih nekoliko stavova koristićemo pojam mreže. Zato prvo



**Definicija 5.26** *Mreža* $\mathbf{L} = \langle L, +, \cdot \rangle$ *je algebra sa dve binarne operacije za koje važi:*

(1) $a + a = a$, $a \cdot a = a$ *– zakoni idempotencije;*

(2) $a + b = b + a$, $a \cdot b = b \cdot a$ *– zakoni komutativnosti;*

(3) $(a + b) + c = a + (b + c)$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *– zakoni asocijativnosti; i*

(4) $a \cdot (a + b) = a$, $a + (a \cdot b) = a$ *– zakoni apsorbcije.*

*Mreža je modularna akko iz* $a+c = c$ $(\iff a \cdot c = a)$ *sledi* $(a+b)\cdot c = a+b\cdot c$.

*Mreža je distributivna akko je svaka od operacija distributivna u odnosu na drugu:* $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$, $(a \cdot b) + c = (a + c) \cdot (b + c)$.

Očigledno, distributivnost povlači modularnost. Obrat, međutim, ne važi.

Relacija $\leq$ u mreži $\mathbf{L}$ definisana sa $a \leq b \iff a \cdot b = a$ $(\iff a + b = b)$ je takvo parcijalno uređenje da za svaki dvočlani (prema tome i svaki konačan) podskup postoji infinum i supremum. Pri tome je $inf\{a, b\} = a \cdot b$, $sup\{a, b\} = a + b$. S druge strane, u svakom parcijalno uređenom skupu $\mathbf{L} = \langle L, \leq \rangle$, u kome svi konačni podskupovi imaju infinum i supremum, moguće je definisati binarne operacije $\cdot$ i $+$ koje zadovoljavaju aksiome mreže. Sada je, naravno, $a \cdot b = inf\{a, b\}$, $a + b = sup\{a, b\}$. U upotrebi je često i ova druga prezentacija mreže kao posebnog parcijalno uređenog skupa.

Mreža $\mathbf{L}$ je *kompletna* akko za svaki podskup $A$ od $L$ postoje elementi $supA$ i $infA$ sa svojstvom:

$\forall a \in A$ $a \cdot supA = a$ i ako je, za (neko) $b$ i svako $a \in A$, $a \cdot b = a$, onda je $b \cdot supA = supA$; $supA$ se obeležava i sa $\sum_{a\in A} a$.

$\forall a \in A$ $a \cdot infA = infA$ i ako je, za (neko) $b$ i svako $a \in A$, $a \cdot b = b$, tada je $b \cdot infA = b$; $infA$ se obeležava i sa $\prod_{a\in A} a$.

Kompletna mreža $\mathbf{L}$ je *kompletno modularna* akko za bilo koja dva podskupa $\{a_i \mid i \in I\}$ i $\{b_i \mid i \in I\}$ skupa $L$ takva da $a_i \leq b_j (\iff a_i \cdot b_j = a_i)$ za $i \neq j$ važi: $\sum_{i\in I} a_i \cdot \prod_{i\in I} b_i = \sum_{i\in I} a_i \cdot b_i$.

Očigledno, kompletna kompletno modularna mreža je i modularna. Obrat u opštem slučaju ne važi.

**Lema 5.27** *Neka su* $L$, $L_n$, $L_k$ *i* $L_{p.i}$, *respektivno, skupovi svih, odnosno svih normalnih, karakterističnih i potpuno invarijantnih podgrupa (proizvoljne) grupe* $\mathbf{G}$. *Neka je u svim slučajevima operacija* $\vee$ *definisana sa:* $\mathbf{A} \vee \mathbf{B} = \langle A \cup B \rangle$. *Tada su* $\mathbf{L}_n = \langle L_n, \vee, \cap \rangle$, $\mathbf{L}_k = \langle L_k, \vee, \cap \rangle$ *i* $\mathbf{L}_{p.i} = \langle L_{p.i}, \vee, \cap \rangle$ *kompletne kompletno modularne mreže, podmreže kompletne mreže svih podgrupa* $\mathbf{L} = \langle L, \vee, \cap \rangle$.

**Dokaz.** Da su u pitanju mreže, šta više kompletne mreže, lako se proverava – uvek je $sup\{\mathbf{A}_i \mid i \in I\} = \langle \bigcup_{i\in I} A_i \rangle$, $inf\{\mathbf{A}_i \mid i \in I\} = \bigcap_{i\in I} \mathbf{A}_{i\in I}$; jasno,

u slučaju mreža $\mathbf{L}_n$, $\mathbf{L}_k$, $\mathbf{L}_{p.i}$ imamo u vidu i korolar 5.24. Nešto manje je očigledna kompletna modularnost ovih mreža. Kako je normalnost podgrupa sve što nam za to treba, u dokazu ćemo se skoncentrisati na mrežu $\mathbf{L}_n$.

Neka su $\{\mathbf{A}_i \mid i \in I\}$ i $\{\mathbf{B}_i \mid i \in I\}$ skupovi normalnih podgrupa takvi da je $\mathbf{A}_i \leq \mathbf{B}_j$ za sve različite indekse $i, j$ iz $I$ . Na nama je da pokažemo:

$$\langle \bigcup_{i\in I} A_i\rangle \cap \bigcap_{i\in I} \mathbf{B}_i = \langle \bigcup_{i\in I}(A_i \cap B_i)\rangle.$$

Inkluzija $\geq$ važi uvek. Naime, u svakoj kompletnoj mreži $\langle L, +, \cdot\rangle$, uz pretpostavku (neformalno zapisanu sa) $\forall j,k \in I\ (j \neq k \implies a_j \leq b_k)$, imamo: $\sum_{i\in I} a_i \cdot b_i \leq \sum_{i\in I} a_i \cdot \prod_{i\in I} b_{i\in I}$. Jer, $\forall m \in I\ a_m \cdot b_m \leq a_m$ implicira $\sum_{i\in I} a_i \cdot b_i \leq \sum_{i\in I} a_i$, a $\forall m \in I\ a_m \cdot b_m \leq b_m$ i $\forall j,k \in I\ (j \neq k \implies a_j \cdot b_j \leq a_j \leq b_k)$ daju: $\forall l \in I\ \sum_{i\in I} a_i \cdot b_i \leq b_l$, pa je $\sum_{i\in I} a_i \cdot b_i \leq \prod_{i\in I} b_i$; prema tome, $\sum_{i\in I} a_i \cdot b_i \leq \sum_{i\in I} a_i \cdot \prod_{i\in I} b_i$.

S druge strane, ako je $g$ nejedinični element grupe $\langle \bigcup_{i\in I} A_i\rangle \cap \bigcap_{i\in I} \mathbf{B}_i$, on je proizvod nekih elemenata unije $\bigcup_{i\in I} A_i$, recimo $g = a_1 \cdot \ldots \cdot a_n$, gde je $a_j \in A_{i_j}$, $i_j \in I$ i $i_j \neq i_k$ za $j \neq k$. Kako je i $g \in B_{i_1}$ i $a_k \in B_{i_1}$ za $1 < k \leq n$ (jer $\mathbf{A}_{i_k} \leq \mathbf{B}_{i_1}$), proizilazi $a_1 \in B_{i_1}$, tj. $a_1 \in A_{i_1} \cap B_{i_1}$. Analogno je, za $1 < j \leq n$, $a_j \in A_{i_j} \cap B_{i_j}$, pa je $g \in \langle \bigcup_{i\in I}(A_i \cap B_i)\rangle$.□

Modularnost mreža $\mathbf{L}_n$, $\mathbf{L}_k$ i $\mathbf{L}_{p.i}$, koja, kao što smo već konstatovali, proizilazi iz kompletne modularnosti, i inače se lako direktno dokazuje. Ovom prilikom iskoristićemo (delimično) sledeći rezultat iz teorije mreža i dati još jedan dokaz modularnosti ovih mreža.

**Lema 5.28** *(a) Mreža je modularna akko ne sadrži petoelementnu podmrežu oblika* $\langle\{a \cdot c = b \cdot c,\ a,\ b,\ c,\ a + c = b + c\}, +, \cdot\rangle$, *gde je još* $a + b = b\ (\iff a \cdot b = a)$;

*(b) Mreža je distributivna akko ne sadrži ni petoelementnu podmrežu iz tačke (a) ni petoelementnu podmrežu oblika* $\langle\{a \cdot b = a \cdot c = b \cdot c,\ a,\ b,\ c,\ a + b = a + c = b + c\}, +, \cdot\rangle$;

*(c) Mreža je kompletna akko za svaki podskup $A$ domena postoji $supA$ $(infA)$.*

**Lema 5.29** *(a) Neka su* $\mathbf{A}$ *i* $\mathbf{B}$ *podgrupe grupe* $\mathbf{G}$ *i neka je* $\mathbf{C}$ *normalna podgrupa grupe* $\mathbf{G}$. *Ako je* $\mathbf{A} \leq \mathbf{B}$, $\mathbf{A} \cap \mathbf{C} = \mathbf{B} \cap \mathbf{C}$ *i* $\mathbf{AC} = \mathbf{BC}$, *tada je* $\mathbf{A} = \mathbf{B}$;

*(b) Mreže* $\mathbf{L}_n$, $\mathbf{L}_k$ *i* $\mathbf{L}_{p.i}$ *su modularne.*

**Dokaz.** *(a)* Neka je $b \in B$. Onda je, prema uslovima leme, $b = ac$ za neko $a \in A$ i neko $c \in C$. Odatle je $c = a^{-1}b \in B \cap C = A \cap C$, stoga i $b \in A$.

*(b)* Prema *(a)* u datim mrežama nema za modularnost "zabranjenih" podmreža.□



**Napomena.** U opštem, mreža svih podgrupa neke grupe ne mora biti modularna. Tako npr. ako je $\mathbf{S}_4$ grupa permutacija skupa $\{0, 1, 2, 3\}$ sa elementima $\mathbf{i}$, $\mathbf{i} = 1, \ldots, \mathbf{24}$ ($\mathbf{i}$ je $i$-ta po redu permutacija u leksikografskom poretku), njene podgrupe

$$\mathbf{A}_4 = \langle\{\mathbf{1}, \mathbf{4}, \mathbf{5}, \mathbf{8}, \mathbf{9}, \mathbf{12}, \mathbf{13}, \mathbf{16}, \mathbf{17}, \mathbf{20}, \mathbf{21}, \mathbf{24}\}, \circ\rangle,$$

$$\mathbf{B} = \langle\{\mathbf{1}, \mathbf{4}, \mathbf{5}\}, \circ\rangle \text{ i } \mathbf{C} = \langle\{\mathbf{1}, \mathbf{15}\}, \circ\rangle$$

generišu za modularnost "zabranjenu" podmrežu (očigledno je $\mathbf{A}_4 \cap \mathbf{C} = \mathbf{B} \cap \mathbf{C} = \mathbf{E}$, a lako se proverava da je $\langle B \cup C\rangle = \langle A_4 \cup C\rangle = \mathbf{A}_4\mathbf{C} = \mathbf{S}_4$).

S druge strane, Kleinova grupa je tek jedan od primera grupa čije mreže normalnih podgrupa nisu distributivne (videti odeljak o lokalno cikličnim grupama).

**Definicija 5.30** *Relacija $\rho \subseteq G \times G$ je relacija kongruencije grupe $\mathbf{G} = \langle G, \cdot\rangle$ akko je relacija ekvivalencije domena grupe saglasna sa operacijom grupe, što znači: ako je $a\rho b$ i $c\rho d$ (tj. ako je $(a, b), (c, d) \in \rho$), tada je i $(a \cdot c)\rho(b \cdot d)$ $((a \cdot c, b \cdot d) \in \rho)$.*

**Napomena.** Lako se pokazuje da je presek i proizvod relacija kongruencije grupe opet relacija kongruencije. Podsećamo: proizvod relacija $\rho$ i $\sigma$, u oznaci $\rho \circ \sigma$, definiše se sa

$$a\,(\rho \circ \sigma)\,b \iff \exists c\,(a\rho c \wedge c\sigma b).$$

Osvrnimo se samo na proizvod. Refleksivnost je očigledna. Neka je dalje $a(\rho \circ \sigma)b$. Tada je za neko $c$ $a\rho c$ i $c\sigma b$. No onda je $(bc^{-1})a\rho(bc^{-1})c$, tj. $bc^{-1}a\rho b$, odnosno, $b\rho bc^{-1}a$; analogno, $c(c^{-1}a)\sigma b(c^{-1}a)$ daje $bc^{-1}a\sigma a$, pa je i $b(\rho \circ \sigma)a$. Iz simetričnosti relacije $\rho \circ \sigma$ proizilazi i permutabilnost relacija $\rho$ i $\sigma$: $\rho \circ \sigma = (\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \rho^{-1} = \sigma \circ \rho$. Tranzitivnost takođe direktno dobijamo: $(\rho \circ \sigma) \circ (\rho \circ \sigma) = \rho \circ (\sigma \circ \rho) \circ \sigma = \rho \circ \rho \circ \sigma \circ \sigma = \rho \circ \sigma$. Saglasnost sa operacijom grupe se još lakše proverava.

Kako su relacije kongruencije grupe uzajamno permutabilne (s obzirom na proizvod), proizilazi da je supremum dve relacije kongruencije $\rho$ i $\sigma$ upravo njihov proizvod. Jer, ako je za relacije kongruencije $\rho, \sigma$ i $\theta$ grupe $\mathbf{G}$ $\rho, \sigma \subseteq \theta$ i $a(\rho \circ \sigma)b$, dakle $a\rho c$ i $c\sigma b$ za neko $c$, tada je $a\theta c$ i $c\theta b$, stoga i $a\theta b$. Zbog refleksivnosti relacija imamo pak trivijalno $\rho, \sigma \subseteq \rho \circ \sigma$.

**Lema 5.31** *Neka je* $\mathbf{G}$ *grupa. Tada je* $\mathbf{Con(G)} = \langle Con(\mathbf{G}), \circ, \cap\rangle$, *gde je* $Con(\mathbf{G})$ *skup svih relacija kongruencije grupe* $\mathbf{G}$, *kompletna kompletno modularna mreža, izomorfna mreži normalnih podgrupa grupe* $\mathbf{G}$ – $\mathbf{L}_n$.

**Dokaz.** Ostavljamo kao laku vežbu (posle gornje napomene) proveru da je $\mathbf{Con(G)}$ mreža. Mi ćemo pak pokazati da je preslikavanje $\psi$ skupa $L_n$ u skup $Con(\mathbf{G})$ definisano sa: $(\mathbf{N})\psi = \rho_{\mathbf{N}}$, gde je: $a\,\rho_{\mathbf{N}}\,b$ akko $aN = bN$ (prema 3.6

i 4.20, $\rho_{\mathbf{N}}$ je relacija kongruencije grupe $\mathbf{G}$), izomorfizam mreža $\mathbf{L}_n$ i $\mathbf{Con}(\mathbf{G})$.

$\psi$ je injektivno, jer ako su $\mathbf{N}_1$ i $\mathbf{N}_2$ normalne podgrupe i $N_1 \neq N_2$, npr. $\exists a \in N_1 \setminus N_2$, onda je $a \,\rho_{\mathbf{N}_1}\, e$, ali nije $a \,\rho_{\mathbf{N}_2}\, e$ ($e$ je, jasno, jedinični element grupe). Dalje, ako je $\rho$ relacija kongruencije, tada je $[e]_\rho \stackrel{\text{def}}{=} \{g \in G \mid e\,\rho\, g\}$ domen normalne podgrupe, obeležimo je sa $\mathbf{N}_\rho$, i važi: $[a]_\rho = a\,[e]_\rho$. No sada je $\rho = (\mathbf{N}_\rho)\psi$:

$$a\,\rho\, b \iff [a]_\rho = [b]_\rho \iff a\,[e]_\rho = b\,[e]_\rho \iff a\,\rho_{\mathbf{N}_\rho}\, b,$$

te je $\psi$ i surjektivno. Konačno, $\psi$ je i homomorfno preslikavanje jer je $\rho_{\mathbf{N}_1 \cap \mathbf{N}_2} = \rho_{\mathbf{N}_1} \cap \rho_{\mathbf{N}_2}$ i $\rho_{\mathbf{N}_1 \mathbf{N}_2} = \rho_{\mathbf{N}_1} \circ \rho_{\mathbf{N}_2}$. Zaista:

$$a\,\rho_{\mathbf{N}_1\mathbf{N}_2}\, b \iff \exists n_1 \in N_1\, \exists n_2 \in N_2 \;\; b = a n_1 n_2 \iff$$

$$\exists c\,(a\,\rho_{\mathbf{N}_1}\, c \wedge c\,\rho_{\mathbf{N}_2}\, b) \iff a\,(\rho_{\mathbf{N}_1} \circ \rho_{\mathbf{N}_2})\, b$$

(u slučaju pretposlednje ekvivalencije, kada je u pitanju implikacija $\Longrightarrow$, za $c$ uzimamo $an_1$, kada je u pitanju implikacija $\Longleftarrow$, imamo: $\exists c\, \exists n_1 \in N_1\, \exists n_2 \in N_2\,(c = an_1 \wedge b = cn_2)$);

$$a\,\rho_{\mathbf{N}_1 \cap \mathbf{N}_2}\, b \iff a^{-1}b \in N_1 \cap N_2 \iff a^{-1}b \in N_1 \wedge a^{-1}b \in N_2 \iff$$

$$a\,\rho_{\mathbf{N}_1}\, b \wedge a\,\rho_{\mathbf{N}_2}\, b \iff a\,(\rho_{\mathbf{N}_1} \cap \rho_{\mathbf{N}_2})\, b. \square$$

**Napomena.** U nekim knjigama se umesto o faktor grupi grupe po nekoj njenoj normalnoj podgrupi govori o faktor grupi grupe po (odgovarajućoj) relaciji kongruencije; tako se i piše umesto, recimo, $\mathbf{G}/\mathbf{H}$, $\mathbf{G}/\rho$ (gde je $\rho = \rho_{\mathbf{H}}$), a umesto o kosetima podgrupe $\mathbf{H}$, kao elementima faktor grupe, sada je reč o klasama ekvivalencije relacije $\rho$. Gornja lema nam pokazuje da se radi o dvema verzijama iste "priče". No sa stanovišta univerzalne algebre rad sa relacijama kongruencije je prirodniji utoliko što je opšteg karaktera. Kod grupa (kao i npr. prstena) među klasama ekvivalencije se izdvaja ona koja odgovara jediničnom elementu (nula elementu prstena) i koja je domen normalne podgrupe grupe (ideala prstena) (i pomoću koje su određene sve druge klase ekvivalencije). Kada je reč o ma kakvoj, ničem specifikovanoj univerzalnoj algebri i (nekoj) njenoj relaciji kongruenciji, klase te relacije su "ravnopravne" i u tom slučaju možemo samo govoriti o faktor algebri date algebre po (datoj) relaciji kongruencije.

## 6 Izvodne podgrupe

Izvodne podgrupe (i uopšte izvodni nizovi) pratiće nas kroz ceo tekst (izuzetak je, jasno, poglavlje o Abelovim grupama). Već lema 6.8 umnogome objašnjava specifičnost izvodne podgrupe, a konačnost izvodnih lanaca karakteriše klasu



rešivih grupa (interesantnu iz mnogo razloga – jedan je, svakako, uslovljenost rešenja algebarske jednačine pomoću radikala rešivošću odgovarajuće grupe Galois; o teoriji Galois videti u, recimo, [132]).

**Definicija 6.1** (*a*) *Komutator elemenata $a$ i $b$ grupe $\mathbf{G}$, u oznaci $[a,b]$, je proizvod $a^{-1}\,b^{-1}\,a\,b$. Rekurzivno se definiše:*

$$[a,b]_0 = b, \;\; [a,b]_n = [a,\,[a,b]_{n-1}] \;\; za \;\; n \geq 1,$$

*kao i, za $n > 2$:*

$$[a_1, \ldots, a_{n-1}, a_n] = [[a_1, \ldots, a_{n-1}], a_n].$$

*Element $a$ je nilelement (ili Engel element) akko za svako $b$ postoji prirodan broj $n$ (koji je u funkciji od $b$) takav da je $[a,b]_n = e$.*

(*b*) *Izvodna (komutatorska) podgrupa grupe $\mathbf{G}$ je podgrupa generisana skupom svih komutatora. Obeležava se sa $\mathbf{G}'$.*

*Ako su $A$ i $B$ neprazni podskupovi skupa $G$, tada je $[A, B]$ podgrupa $\langle\{[a,b] \mid a \in A, b \in B\}\rangle = [B, A]$ - videti 6.2(b). Njen domen ćemo prirodno označavati sa $[A, B]$. Istu notaciju koristićemo i u slučaju kada su $A$ i $B$ domeni podgrupa, ali tada ćemo pisati i $[\mathbf{A}, \mathbf{B}]$ - domen podgrupe ostaje $[A, B]$.*

(*c*) *Niz podgrupa $\mathbf{G}^{(n)}$, $n \in \omega$, grupe $\mathbf{G}$, gde je $\mathbf{G}^{(0)} \stackrel{\text{def}}{=} \mathbf{G}$ i, za $n \geq 1$, $\mathbf{G}^{(n)} \stackrel{\text{def}}{=} (\mathbf{G}^{(n-1)})'$, izvodni je niz grupe $\mathbf{G}$.*

**Napomena.** Očigledno, $\mathbf{G}$ je Abelova grupa akko je $\mathbf{G}' = \mathbf{E}$. S druge strane, niti $\mathbf{Z}(\mathbf{G}) = \mathbf{E}$ povlači nužno $\mathbf{G}' = \mathbf{G}$ (videti 9.26), niti iz $\mathbf{G} = \mathbf{G}'$ mora da sledi $\mathbf{Z}(\mathbf{G}) = \mathbf{E}$. Zaista, neka je $\mathbf{H}$ podgrupa grupe $\mathbf{GL}_n(\mathbf{Re})$, $n = 2m > 2$, generisana matricama $I + \lambda I_{ik}$, $i \neq k$, gde je $I_{ik}$ matrica čiji su svi elementi nula, osim elementa u $i$-toj vrsti i $k$-toj koloni koji je jednak 1. Tada je $\mathbf{H} = \mathbf{H}'$, jer je $(I + \lambda I_{ij})^{-1} = I - \lambda I_{ij}$, a ako su $i, j, k$ tri različita indeksa, onda je

$$I + \lambda I_{ij} = (I + \lambda I_{ik})(I + I_{kj})(I - \lambda I_{ik})(I - I_{kj}) = [I - \lambda I_{ik},\, I - I_{kj}].$$

Lako je pak videti da je $-I \in H$ (pa je $\mathbf{Z}(\mathbf{H}) \neq \mathbf{E}$). Dovoljno je da to pokažemo na primeru matrica formata $2 \times 2$ (opšte rešenje onda sledi koristeći se množenjem matrica "podeljenih" na adekvatno izabrane blokove). Tako imamo:

$$(I + I_{12}) \cdot (I - I_{21}) = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix},$$

$$(I - I_{21}) \cdot (I + I_{12}) = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix};$$

odatle je

$$(I + I_{12}) \cdot (I - I_{21}) \cdot (I - I_{21}) \cdot (I + I_{21}) = \begin{bmatrix} -1 & 0 \\ -2 & -1 \end{bmatrix}$$

i, konačno:

$$\begin{bmatrix} -1 & 0 \\ -2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} = -I.$$

Navešćemo ovom prilikom neka od svojstava izvodnih podgrupa koja će nam kasnije biti od koristi.

**Lema 6.2** *Komutatori grupe* $\mathbf{G}$ *zadovoljavaju sledeće relacije:*

(*a*) *Ako je* $\varphi \in End(\mathbf{G})$, *onda je* $[a,b]\varphi = [a\varphi, b\varphi]$. *Posebno:* $[a,b]u_g = g^{-1}[a,b]g = [g^{-1}ag, g^{-1}bg]$;

(*b*) $[a,b]^{-1} = [b,a]$;

(*c*) $[a^{-1},b] = a[a,b]^{-1}a^{-1}$; $[a,b^{-1}] = b[a,b]^{-1}b^{-1}$;

(*d*) $[ab,c] = b^{-1}[a,c]\,b\,[b,c]$;

(*e*) $[a,bc] = [a,c]\,c^{-1}\,[a,b]\,c$;

(*f*) $b^{-1}[[a,b^{-1}],c]\,bc^{-1}\,[[b,c^{-1}],a]\,ca^{-1}\,[[c,a^{-1}],b]\,a = e$;

(*g*) $[a,c,a^{-1}ba]\cdot[b,a,b^{-1}cb]\cdot[c,b,c^{-1}ac] = e$;

(*h*) *Za svaki ceo broj* $z$ *je*

$[a^z,b] = a^{-(z-1)}[a,b]a^{z-1}\cdot a^{-(z-2)}[a,b]a^{z-2}\cdot\ldots\cdot a^{-1}[a,b]a\cdot[a,b]$.

*Posebno, ako je* $[a,b] \in Z(\langle a,b\rangle)$, *onda je*

$[a^z,b] = [a,b]^z$.

**Dokaz**. Prost račun. (*f*) i (*g*) su nešto zamorniji, (*h*) se dokazuje za prirodne brojeve indukcijom koristeći se tačkom (*d*), a prelaz na negativne cele brojeve je trivijalan.

(*f*) je, prema (*b*), ekvivalentno sa

$$b^{-1}[b^{-1},a]\,c^{-1}[a,b^{-1}]\,cbc^{-1}\,[c^{-1},b]\,a^{-1}\,[b,c^{-1}]\,aca^{-1}\,[a^{-1},c]\,b^{-1}[c,a^{-1}]\,ba = e,$$

što je, dalje, ekvivalentno sa

$$[b^{-1},a]\,c^{-1}[a,b^{-1}]\,cbc^{-1}[c^{-1},b]\,a^{-1}[b,c^{-1}]\,aca^{-1}[a^{-1},c]\,b^{-1}[c,a^{-1}]\,a = [b^{-1},a],$$

tj. sa

$$c^{-1}[a,b^{-1}]\,cbc^{-1}[c^{-1},b]\,a^{-1}[b,c^{-1}]\,aca^{-1}[a^{-1},c]\,b^{-1}[c,a^{-1}]\,a = e.$$

No

$$c^{-1}[a,b^{-1}]\,bb^{-1}cbc^{-1}[c^{-1},b]\,a^{-1}[b,c^{-1}]\,cc^{-1}aca^{-1}[a^{-1},c]\,b^{-1}[c,a^{-1}]\,a =$$



$$c^{-1}[a,b^{-1}]\,b\,[b,c^{-1}]\,[c^{-1},b]\,a^{-1}[b,c^{-1}]\,c\,[c,a^{-1}]\,[a^{-1},c]\,b^{-1}[c,a^{-1}]\,a =$$

$$c^{-1}[a,b^{-1}]\,ba^{-1}\,[b,c^{-1}]\,cb^{-1}[c,a^{-1}]\,a =$$

$$c^{-1}a^{-1}bab^{-1}ba^{-1}b^{-1}cbc^{-1}cb^{-1}c^{-1}aca^{-1}a = e.$$

(*g*)

$$[a,c,a^{-1}ba] = [a,c]^{-1}(a^{-1}ba)^{-1}[a,c]a^{-1}ba =$$

$$c^{-1}a^{-1}ca\cdot a^{-1}b^{-1}a\cdot a^{-1}c^{-1}ac\cdot a^{-1}ba = c^{-1}a^{-1}cb^{-1}c^{-1}\cdot aca^{-1}ba =$$

$$(cbc^{-1}ac)^{-1}\cdot(aca^{-1}ba).$$

Analogno:

$$[b,a,b^{-1}cb] = (aca^{-1}ba)^{-1}\cdot(bab^{-1}cb),$$

$$[c,b,c^{-1}ac] = (bab^{-1}cb)^{-1}\cdot(cbc^{-1}ac),$$

i, očigledno, nakon "množenja" dobijamo jedinični element.□

**Korolar 6.3** (*a*) *Ako je* $\mathbf{G}' \leq \mathbf{Z}(\mathbf{G})$, *onda je za svako* $a,b,c \in G$:

$$[ab,c] = [a,c]\cdot[b,c] \quad i \quad [a,bc] = [a,c]\cdot[a,b].$$

*Posebno, za* $z \in Z$ *imamo:*

$$[a^z,b] = [a,b]^z = [a,b^z].$$

(*b*) *Ako je* $[a,b] \in Z(\mathbf{G})$, *tada je:*

$$[a^{-1},b] = [a,b^{-1}] = [a,b]^{-1} = [b,a], \quad [a^{-1},b^{-1}] = [a,b]$$

*i*

$$(ab)^z = [b,a]^{\frac{1}{2}z(z-1)}a^zb^z.$$

**Dokaz**. (*a*) Direktna posledica tačaka (*d*), (*e*) i (*h*) prethodne leme i uslova korolara.

(*b*) Prvi deo tvrđenja je očigledan, a indukcijom pokazujemo prvo da za svaki prirodan broj $n$ važi i njegov drugi deo.

Slučaj $n = 0$ je trivijalan. Pretpostavimo da je tvrđenje tačno za $n$ ($\geq 0$), dakle:

$$(ab)^n = [b,a]^{\frac{1}{2}n(n-1)}a^nb^n \qquad (I).$$

Zbog ($[a,b]^{-1} =$) $[b,a] \in Z(\mathbf{G})$ je:

$$aba^nb^n = aa^nb\cdot b^{-1}a^{-n}ba^n\cdot b^n = a^{n+1}b[b,a^n]b^n =$$

$$a^{n+1}b[b,a]^nb^n = [b,a]^na^{n+1}b^{n+1} \qquad (II),$$

a $(I)$ i $(II)$ nam daju:

$$aba^nb^n = ab\cdot(ab)^n\cdot[b,a]^{-\frac{1}{2}n(n-1)} = [b,a]^n\cdot a^{n+1}b^{n+1},$$

odnosno

$$(ab)^{n+1} = [b,a]^{\frac{1}{2}(n+1)[(n+1)-1]}a^{n+1}b^{n+1},$$

što pokazuje da je navedena relacija tačna i za $n+1$.

Sada, za $n>0$, direktno dobijamo primenom već izvedenih relacija:

$$(ab)^{(-n)} = ((ab)^{-1})^n = (b^{-1}a^{-1})^n = [a^{-1},b^{-1}]^{\frac{1}{2}n(n-1)}(b^{-1})^n(a^{-1})^n =$$

$$([b,a]^{\frac{1}{2}(-n)(n-1)}b^{-n}a^{-n} = [b,a]^{\frac{1}{2}(-n)(n-1)}b^{-n}a^{-n} =$$

$$[b,a]^{\frac{1}{2}(-n)(n-1)}b^{-n}a^{-n}b^na^na^{-n}b^{-n} = [b,a]^{\frac{1}{2}(-n)(n-1)}[b^n,a^n]a^{-n}b^{-n} =$$

$$[b,a]^{\frac{1}{2}(-n)(n-1)}[b,a]^{n^2}a^{-n}b^{-n} = [b,a]^{\frac{1}{2}(-n)[(-n)-1]}a^{-n}b^{-n}.\square$$

**Korolar 6.4** *Za elemente $a,b,c$ grupe $\mathbf{G}$ važi:*

*$(a)$ ako je $c\in C([a,b])$, onda je $[a,bc]=[a,c]\cdot[a,b]$ i $[ac,b]=[a,b]\cdot[c,b]$;*

*$(b)$ ako je $[a,b]\in C(a)\cap C(b)$ i $k,m\in Z$, onda je $[a^k,b^m]=[a,b]^{km}$, $(ab)^m=[a,b]^{\frac{1}{2}m(m-1)}a^mb^m$.*

**Korolar 6.5** *Ako je centar grupe $\mathbf{G}$ konačnog indeksa, onda je izvodna podgrupa grupe $\mathbf{G}$ konačna.*

**Dokaz.** Neka je $[\mathbf{G}:\mathbf{Z(G)}]=n$ i neka je $\{a_1,\dots,a_n\}$ jedna transverzala centra grupe. Prema $6.2(d),(e)$, skup svih komutatora grupe $\mathbf{G}$ je $\mathcal{G}=\{[a_i,a_j]\mid 1\le i,j\le n\}$ (ne isključujemo mogućnost da su neki od nabrojanih komutatora jednaki, a evidentno neki su baš jedinični element); jer je, za elemente $c,d$ centra: $[a_ic,a_jd]=[a_i,a_j]$. S druge strane, kako je, za bilo koje elemente $a,b,c,d$, $[a,b]\cdot[c,d]=[c,d]\cdot[[c,d]^{-1}a[c,d],[c,d]^{-1}b[c,d]]$, preostaje nam da pokažemo da je $(n+1)$-vi stepen svakog elementa iz $\mathcal{G}$ proizvod $n$ elemenata iz $\mathcal{G}$; odatle onda sledi da je svaki element izvodne podgrupe proizvod od najviše $n^3$ elemenata skupa $\mathcal{G}$. Ali, za svako $a,b$ je $[a,b]^n\in Z(\mathbf{G})$, pa je $[a,b]^{n+1}=[a,b]\cdot b^{-1}\cdot[a,b]^n\cdot b=[a,b]b^{-1}[a,b]b\cdot b^{-1}[a,b]^{n-1}b=[a,b^2]\cdot[b^{-1}ab,b]^{n-1}.\square$

**Lema 6.6** *Ako je, za elemente $a,b$ grupe $\mathbf{G}$, $a^3=(ab)^3=(ab^{-1})^3=e$, onda je $[a,b,b]=e$.*

**Dokaz.** Pokazaćemo da je $b$ permutabilno sa $a^{-1}ba$, samim tim i sa $b^{-1}\cdot(a^{-1}ba)=[b,a]=[a,b]^{-1}$, a tada su i $b^{-1}$ i $[b,a]=[a,b]^{-1}$ permutabilni, pa je

$$[a,b,b]=[a,b]^{-1}b^{-1}[a,b]b=e.$$

Zaista, imamo: $b\cdot a^{-1}ba=a^{-1}ba\cdot b$ akko je (posle "množenja" sleva sa $a^{-1}ba^{-1}$) $(a^{-1}b)^3\cdot a=a^{-1}ba^{-2}bab$ akko je $a=a^{-1}b(ab)^2$ akko je $a=a^{-2}(ab)^3$ akko je $a=a^{-2}.\square$



**Korolar 6.7** $\mathbf{G}^{(n)}$ *je potpuno invarijantna podgrupa grupe $\mathbf{G}$ za svaki prirodan broj $n$.*

**Dokaz.** Prema $6.2(a)$ i $4.31.\square$

**Lema 6.8** *Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$. Tada je $\mathbf{G}'\le\mathbf{H}$ akko je $\mathbf{H}$ normalna podgrupa i $\mathbf{G/H}$ Abelova grupa.*

**Dokaz.** ($\Longrightarrow$) Neka je $a\in H$ i $g\in G$. Kako je, prema uslovu leme, $[g,a^{-1}]\in H$, to je $g^{-1}ag\in Ha=H$, te je $\mathbf{H}\lhd\mathbf{G}$. Isto tako je, za svako $a,b\in G$, $aH\cdot bH=abH=baH=bH\cdot aH$ (jasno, $abH=baH\iff[a,b]\in H$).$\square$

**Lema 6.9** *Za domen $G'$ izvodne podgrupe grupe $\mathbf{G}$ važi:*

$$G'=\{\,a_1^{-1}\cdot\ldots\cdot a_n^{-1}\cdot a_1\cdot\ldots\cdot a_n\mid a_i\in G,\ n\ge 2\}.$$

**Dokaz.** Proveravamo prvo da važi inkluzija ($\subseteq$).

Primetimo da je prema $5.26(a)$ svaki element iz $G'$ konačan proizvod komutatora. Indukcijom po broju komutatora u proizvodu $(k)$ dokazujemo sada da je svaki element iz $G'$ oblika $a_1^{-1}\dots a_n^{-1}a_1\dots a_n$ za neko $n\ge 2$.

Za $k=1$ to proizilazi iz same definicije komutatora, pa pretpostavimo da je tvrđenje tačno za $k$ ($\ge 1$). No onda je:

$$[a_1,b_1]\dots[a_k,b_k][a_{k+1},b_{k+1}] = c_1^{-1}\dots c_n^{-1}\,c_1\dots c_n\,[a_{k+1},b_{k+1}] =$$

$$(c_n\dots c_1)^{-1}c_1\dots c_na_{k+1}^{-1}(b_{k+1}^{-1}a_{k+1})b_{k+1}(c_n\dots c_1)c_1^{-1}\dots c_n^{-1}a_{k+1}(a_{k+1}^{-1}b_{k+1})b_{k+1}^{-1}.$$

I za inkluziju ($\supseteq$) koristimo indukciju, naravno, ovog puta po $n$.

Za $n=2$ je, trivijalno, $a_1^{-1}a_2^{-1}a_1a_2=[a_1,a_2]\in G'$, a uz induktivnu hipotezu za $n\ge 2$ imamo i za slučaj $n+1$:

$$a_1^{-1}\dots a_{n-1}^{-1}a_n^{-1}a_{n+1}^{-1}a_1\dots a_{n-1}\,a_n\,a_{n+1} =$$

$$a_1^{-1}\dots a_{n-1}^{-1}(a_{n+1}\,a_n)^{-1}a_1\dots a_{n-1}(a_{n+1}\,a_n)\cdot a_n^{-1}a_{n+1}^{-1}\,a_n\,a_{n+1} =$$

$$a_1^{-1}\dots a_{n-1}^{-1}(a_{n+1}a_n)^{-1}a_1\dots a_n(a_{n+1}\,a_n)\cdot[a_n,\,a_{n+1}]\in G'.\square$$

**Lema 6.10** *Neka su $\mathbf{A}$, $\mathbf{B}$ i $\mathbf{C}$ normalne podgrupe grupe $\mathbf{G}$. Tada važi:*

*$(a)$ $[\mathbf{A},\mathbf{B}]$ je normalna podgrupa grupe $\mathbf{G}$ sadržana u $\mathbf{A}\cap\mathbf{B}$. Posebno, $[\mathbf{A},\mathbf{B}]$ je normalna podgrupa grupe $\mathbf{G}$ sadržana u $\mathbf{A}$;*

*$(b)$ $[[\mathbf{A},\mathbf{B}],\mathbf{C}]\le[[\mathbf{C},\mathbf{A}],\mathbf{B}]\cdot[[\mathbf{B},\mathbf{C}],\mathbf{A}]=[[\mathbf{B},\mathbf{C}],\mathbf{A}]\cdot[[\mathbf{C},\mathbf{A}],\mathbf{B}]$;*

*$(c)$ $[\mathbf{AB},\mathbf{C}]=[\mathbf{A},\mathbf{C}]\cdot[\mathbf{B},\mathbf{C}]$.*

**Dokaz.** ($a$) Trivijalno. 6.2($a$) daje takođe: ako su $\mathbf{A}$ i $\mathbf{B}$ karakteristične (potpuno invarijantne) podgrupe, onda je i $[\mathbf{A},\mathbf{B}]$ karakteristična (potpuno invarijantna) podgrupa.

($b$) Prema ($a$) su $[[\mathbf{B},\mathbf{C}],\mathbf{A}]$, $[[\mathbf{C},\mathbf{A}],\mathbf{B}]$, a onda i njihov proizvod, normalne podgrupe grupe $\mathbf{G}$. Dalje, ako je $[\mathbf{A},\mathbf{B}]=\mathbf{D}$, generatorni skup grupe $[[\mathbf{A},\mathbf{B}],\mathbf{C}]$ je skup $\{[d,c] \mid d\in D, c\in C\}$. $d\in D$ je pak oblika $d_1\dots d_n$ ($n$ je, jasno, u funkciji od $d$), gde je $d_i$ ili $[a_i,b_i]$ ili $[b_i,a_i]$ za neko $a_i\in A$, $b_i\in B$. Koristeći 5.26($a$),($c$) lako se pokazuje, indukcijom po $n$, da je $[d,c]$ proizvod konjugata elemenata $[d_i,c]$. Slučaj $n=1$ je očigledan, a ako tvrđenje važi za $n\,(\geq 1)$, onda je

$$[d_1\dots d_nd_{n+1},\,c]=d_{n+1}^{-1}[d_1\dots d_n,\,c]\,d_{n+1}\,[d_{n+1},\,c]=$$

prema induktivnoj hipotezi za neko $g_i\in G$, $i=1,\dots n$,

$$d_{n+1}^{-1}\,(\prod_{i=1}^{n} g_i^{-1}\,[d_i,\,c]\,g_i)\,d_{n+1}\,[d_{n+1},\,c]=\prod_{i=1}^{n}(g_i\,d_{n+1})^{-1}\,[d_i,\,c]\,(g_i\,d_{n+1})\,[d_{n+1},\,c].$$

S obzirom na normalnost podgrupa $[[B,\,C],\,A]$, $[[C,\,A],\,B]$ dovoljno je, znači, pokazati da je za $a\in A$, $b\in B$ i $c\in C$:

$$[[a,b],c],\,[[b,a],c]\in[[C,\,A],\,B]\cdot[[B,\,C],\,A].$$

6.2($f$) daje

$$b\,[[a,b],\,c]\,b^{-1}c^{-1}[[b^{-1},c^{-1}],\,a]\,ca^{-1}[[c,a^{-1}],\,b^{-1}]\,a=e,$$

a odatle je

$$[[a,b],\,c]=b^{-1}a^{-1}[b^{-1},[c,a^{-1}]]\,ac^{-1}\,[a,[b^{-1},c^{-1}]]\,cb=$$

$$(ab)^{-1}\,[b^{-1},[c,a^{-1}]]\,(ab)\,(cb)^{-1}[a,[b^{-1},c^{-1}]]\,cb=$$

$$\{(ab)^{-1}\,[[c,a^{-1}],b^{-1}]\,(ab)\}^{-1}\,\{(cb)^{-1}[[b^{-1},c^{-1}],a]\,(cb)\}^{-1}\in$$

$$[[C,\,A],\,B]\cdot[[B,\,C],\,A]=[[B,\,C],\,A]\cdot[[C,\,A],\,B].$$

Slično se proverava i da je $[[b,a],c]\in[[B,\,C],\,A]\cdot[[C,\,A],\,B]$, samo nam sada treba i relacija $[X,\,Y]=[Y,\,X]$.

($c$) Podgrupa $[\mathbf{AB},\mathbf{C}]$ je generisana skupom $\{[ab,c] \mid a\in A, b\in B, c\in C\}$ i kako je $[ab,c]=(b^{-1}[a,c]\,b)\,[b,c]\in[A,\,C]\,[B,\,C]$, to je $[\mathbf{AB},\mathbf{C}]\leq[\mathbf{A},\mathbf{C}]\cdot[\mathbf{B},\mathbf{C}]$.

Inkluzija ($\supseteq$) je očigledna: $[\mathbf{A},\mathbf{C}]\leq[\mathbf{AB},\mathbf{C}]$ i $[\mathbf{B},\mathbf{C}]\leq[\mathbf{AB},\mathbf{C}]$.□

**Korolar 6.11** *(Kalužin, M. Hall) Neka su* $\mathbf{A}$, $\mathbf{B}$ *i* $\mathbf{C}$ *podgrupe grupe* $\mathbf{G}$. *Ako su dve od podgrupa* $[[\mathbf{A},\mathbf{B}],\mathbf{C}]$, $[[\mathbf{B},\mathbf{C}],\mathbf{A}]$, $[[\mathbf{C},\mathbf{A}],\mathbf{B}]$ *sadržane u nekoj normalnoj podgrupi grupe* $\mathbf{G}$, *onda je i treća.*



**Dokaz.** Videti dokaz druge tačke prethodne leme.□

**Lema 6.12** *Neka su* $\mathbf{A}$ *i* $\mathbf{B}$ *podgrupe grupe* $\mathbf{G}$. *Tada je* $[\mathbf{A},\mathbf{B}]\lhd\langle A\cup B\rangle$.

**Dokaz.** Neka je $a,a_1\in A$ i $b\in B$. Iz $[aa_1,b]=a_1^{-1}[a,b]\,a_1\,[a_1,b]$, tj. $a_1^{-1}\,[a,b]\,a_1=[aa_1,b]\,[a_1,b]^{-1}\in[A,\,B]$, proizilazi $\mathbf{A}\leq\mathbf{N}([A,\,B])$.

Isto tako je, za $a\in A$ i $b,b_1\in B$, $[a,bb_1]=[a,b_1]\,b_1^{-1}[a,b]\,b_1$, odnosno $b_1^{-1}[a,b]\,b_1=[a,b_1]^{-1}\,[a,bb_1]\in[A,\,B]$, te je i $\mathbf{B}\leq\mathbf{N}([A,\,B])$. Stoga je $\langle A\cup B\rangle\leq\mathbf{N}([A,\,B])$, a trivijalno $[\mathbf{A},\mathbf{B}]\leq\langle A\cup B\rangle$.□

**Lema 6.13** ($a$) *Ako je* $\mathbf{A}$ *podgrupa grupe* $\mathbf{G}$ *i* $[\mathbf{A},\,\mathbf{G}']=\mathbf{E}$, *tada je i* $[\mathbf{A}',\,\mathbf{G}]$ *jedinična podgrupa.*

($b$) *Ako je* $\mathbf{A}$ *normalna podgrupa grupe* $\mathbf{G}$ *i* $\mathbf{A}\cap\mathbf{G}'=\mathbf{E}$, *tada je* $\mathbf{A}\leq\mathbf{Z}(\mathbf{G})$.

**Dokaz.** ($a$) Neka je $a,b\in A$ i $c\in G$. Već smo koristili

$$[[a,b],c]=b^{-1}a^{-1}[b^{-1},[c,a^{-1}]]\,ac^{-1}[a,[b^{-1},c^{-1}]]\,cb$$

(videti dokaz leme 6.10($b$)). No po uslovu je $[b^{-1},[c,a^{-1}]]=[a,[b^{-1},c^{-1}]]=e$ (u pitanju su elementi grupe $[A,\,G']$), pa je i $[[a,b],c]=e$. Ali onda je i $[h,g]=e$ za svako $h\in A'$ i svako $g\in G$ (videti 6.2($e$) i prvi deo dokaza tačke 6.10($b$) – staviti $\mathbf{A}=\mathbf{B}$, $\mathbf{C}=\mathbf{G}$).

($b$) Trivijalno.□

Primetimo da obrat tačke ($a$) ne važi. Tako za podgrupu

$$\mathbf{H}=\langle\{\imath,(01)(23),(02)(13),(03)(12)\},\cdot\rangle$$

grupe $\mathbf{S}_4$ (videti deo o simetričnim grupama) imamo $[\mathbf{H}',\mathbf{S}_4]=\mathbf{E}$, ali $[\mathbf{H},\mathbf{S}_4']\neq\mathbf{E}$.

**Lema 6.14** *Neka je* $A$ *neprazan podskup domena, a* $\mathbf{H}$ *i* $\mathbf{K}$ *podgrupe grupe* $\mathbf{G}$ *generisane, respektivno, skupovima* $B$ *i* $C$. *Tada važi:*

($a$) $A^{\mathbf{H}}=\langle A,[A,H]\rangle$ *i* $A^{\mathbf{H}}$ *je normalna podgrupa grupe* $\langle A,H\rangle$;

($b$) $[A,H]^{\mathbf{H}}=[A,H]$;

($c$) $[A,H]=[A,B]^H$ $(=\langle\{h^{-1}[a,b]h \mid a\in A, b\in B, h\in H\}\rangle)$;

($d$) $[H,K]=[B,C]^{HK}$ $(=\langle\{(hk)^{-1}[b,c]hk \mid b\in B, c\in C, h\in H, k\in K\}\rangle)$.

**Dokaz.** ($a$) Prvi deo tvrđenja je direktna posledica identiteta $h^{-1}ah=[h,a^{-1}]a$, drugi je očigledan.

($b$) Inkluzija $\supseteq$ je jasna, a prema 6.2($e$) je: $h^{-1}[a,h_1]h=[a,h]^{-1}[a,h_1h]$ $(\in[A,H])$.

($c$) Prethodna tačka dokazuje inkluziju $\supseteq$, a druga inkluzija je posledica identiteta: $[a,b^{-1}] = (b[a,b]b^{-1})^{-1}$, $[a,b_1b_2] = [a,b_1]b_2^{-1}[a,b_1]b_2$ (6.2($c$),($e$)). Naravno, indukcija završava posao.

($d$) Dvostruka primena prethodne tačke: $[H,K] = [H,C]^K = ([B,C]^H)^K = [B,C]^{HK}$.□

**Lema 6.15** *Neka su* $\mathbf{H}$ *i* $\mathbf{K}$ *podgrupe grupe* $\mathbf{G}$, $\mathbf{H}$ *normalna podgrupa grupe* $\mathbf{K}$ *i neka je* $\emptyset \neq A \subseteq H$. *Tada je* $A^{\mathbf{H}}$ *normalna podgrupa grupe* $A^{\mathbf{K}}$.

**Lema 6.16** *Normalno zatvorenje podgrupe* $\mathbf{A}$ *grupe* $\mathbf{G}$ *je podgrupa* $[\mathbf{G},\mathbf{A}]\,\mathbf{A}$.

**Dokaz**. $[\mathbf{G},\mathbf{A}]$ je normalna podgrupa grupe $\mathbf{G}$ prema 6.12, a prema 6.14($a$) važi:

$$[\mathbf{A}] = A^{\mathbf{G}} = \langle A, [A,G]\rangle = [\mathbf{G},\mathbf{A}]\,\mathbf{A}.\square$$

**Korolar 6.17** *Ako su* $\mathbf{A}$ *i* $\mathbf{B}$ *podgrupe grupe* $\mathbf{G}$, *onda je* $[\langle A \cup B\rangle] = [\mathbf{A}][\mathbf{B}]$.

**Dokaz**. Trivijalno $[\mathbf{A}][\mathbf{B}] \leq [\langle A \cup B\rangle]$. Očigledno je i $\langle A \cup B\rangle \leq [\mathbf{A}][\mathbf{B}]$ pa je $[\langle A \cup B\rangle] = [\mathbf{A}][\mathbf{B}]$.□

U opštem ne važi za bilo koje dve podgrupe (neke grupe $\mathbf{G}$) $[\mathbf{A} \cap \mathbf{B}] = [\mathbf{A}] \cap [\mathbf{B}]$ (jasno, inkluzija $\leq$ je uvek data). U grupi $\mathbf{A}_5$ (videti deo o simetričnim grupama) imamo recimo, za $\mathbf{A} = \langle(012)\rangle$ i $\mathbf{B} = \langle(123)\rangle$: $[\mathbf{A} \cap \mathbf{B}] = \mathbf{E}$ i $[\mathbf{A}] \cap [\mathbf{B}] = \mathbf{A}_5$. Situacija se ne menja ni ako je jedna od podgrupa normalna. Npr. u $\mathbf{S}_5$ je $[\mathbf{A}_5 \cap \langle(01)\rangle] = \mathbf{E}$ i $[\mathbf{A}_5] \cap [\langle(01)\rangle] = \mathbf{A}_5$ (u proveri koristiti 9.23 i 9.24).

Zapravo možemo izvesti ovakav stav.

**Lema 6.18** *Ako grupa* $\mathbf{G}$ *sadrži podgrupu* $\mathbf{H}$ *konačnog indeksa koja nije normalna, onda postoje dve podgrupe* $\mathbf{A}$ *i* $\mathbf{B}$ *takve da je* $[\mathbf{A} \cap \mathbf{B}]$ *prava podgrupa grupe* $[\mathbf{A}] \cap [\mathbf{B}]$.

**Dokaz**. Pretpostavimo da za svake dve podgrupe $\mathbf{A}$ i $\mathbf{B}$ grupe $\mathbf{G}$ važi: $[\mathbf{A} \cap \mathbf{B}] = [\mathbf{A}] \cap [\mathbf{B}]$. Indukcija nam onda kaže da je za svaki konačan skup podgrupa $\mathbf{A}_0, \ldots, \mathbf{A}_m$: $[\bigcap_{i=0}^m \mathbf{A}_i] = \bigcap_{i=0}^m [\mathbf{A}_i]$.

S obzirom na uslove $\mathbf{H}$ ima konačno mnogo konjugata (4.11). Neka su to $\mathbf{H} = \mathbf{H}_0, \mathbf{H}_1, \ldots, \mathbf{H}_k$, $k \geq 1$. Međutim, $[\bigcap_{i=0}^k \mathbf{H}_i] = \bigcap_{i=0}^k \mathbf{H}_i = \mathbf{Core}(\mathbf{H})$ (4.8), dok $\bigcap_{i=0}^k [\mathbf{H}_i] \geq \langle H_0 \cup \ldots \cup H_k\rangle$; naša pretpostavka je, dakle, pogrešna.□

**Korolar 6.19** *Konačna grupa je Dedekindova akko je* $[\mathbf{A} \cap \mathbf{B}] = [\mathbf{A}] \cap [\mathbf{B}]$ *za svake dve njene podgrupe* $\mathbf{A}$ *i* $\mathbf{B}$.

**Definicija 6.20** *Grupa* $\mathbf{G}$ *ima eksponent* $n$ *akko je* $n$ *najmanji pozitivan prirodan broj za koji je* $g^n = e$ *za svako* $g \in G$.



U 10.33 je pokazano da su Abelove grupe čiji je eksponent prost broj $p$ direktni proizvod cikličnih grupa reda $p$. Grupe eksponenta 2 su uvek Abelove.

**Lema 6.21** *U grupi eksponenta* 3 *normalno zatvorenje svake ciklične podgrupe je Abelova grupa.*

**Dokaz**. Neka je grupa $\mathbf{G}$ eksponenta 3. Ma koji njen element $a$ je, prema dokazu leme 6.6, permutabilan sa svim svojim konjugatima, pa je, za sve cele brojeve $k,l$ i svaki element $g$ grupe $\mathbf{G}$, $a^k$ permutabilno sa $g^{-1}a^lg = (g^{-1}ag)^l$. Proizilazi da su elementi generatornog skupa normalnog zatvorenja ciklične grupe $\langle a\rangle$ permutabilni:

$$(g^{-1}a^kg)\cdot(g_1^{-1}a^lg_1) = g_1^{-1}\cdot(g_1g^{-1}a^kgg_1^{-1})\cdot a^l\cdot g_1 =$$

$$g_1^{-1}a^l\cdot g_1g^{-1}a^kgg_1^{-1}\cdot g_1 = (g_1^{-1}a^lg_1)\cdot(g^{-1}a^kg).\square$$

**Lema 6.22** *Ako je* $\mathbf{N}$ *normalna podgrupa grupe* $\mathbf{G}$, *onda je*

$$(\mathbf{G}/\mathbf{N})^{(i)} = (\mathbf{G}^{(i)}\mathbf{N})/\mathbf{N}.$$

**Dokaz**. Indukcijom. Ako je $i = 1$ i $gN \in (G/N)'$ imamo:

$$gN = [a_1N,b_1N]\ldots[a_kN,b_kN] = [a_1,b_1]N\ldots[a_k,b_k]N =$$

$$([a_1,b_1]\ldots[a_k,b_k])N = g'N \in G'N/N,$$

gde je $g' = [a_1,b_1]\ldots[a_k,b_k] \in G'$.

Ako je pak $gN \in G'N/N$, $g = g'n$, $g' \in G'$, $n \in N$, sledi:

$$gN = g'nN = g'N = ([a_1,b_1]\ldots[a_k,b_k])N =$$

$$[a_1,b_1]N\ldots[a_k,b_k]N = [a_1N,b_1N]\ldots[a_kN,b_kN] \in (G/N)'.$$

Pretpostavimo da je tvrđenje tačno za svako $k \leq i$ ($\geq 1$). Tada je $(\mathbf{G}/\mathbf{N})^{(i+1)} = ((\mathbf{G}/\mathbf{N})^{(i)})' = (\mathbf{G}^{(i)}\mathbf{N}/\mathbf{N})'$. Elementi grupe $\mathbf{G}^{(i)}\mathbf{N}/\mathbf{N}$ su oblika $aN$, gde je $a \in G^{(i)}$, pa su elementi grupe $(\mathbf{G}^{(i)}\mathbf{N}/\mathbf{N})'$ oblika

$$[a_1N,b_1N]\ldots[a_mN,b_mN] = ([a_1,b_1]\ldots[a_m,b_m])N;$$

dakle, to su ujedno i elementi grupe $\mathbf{G}^{(i+1)}\mathbf{N}/\mathbf{N}$ (podrazumevamo, naravno: $a_1, b_1, \ldots, a_m, b_m \in G^{(i)}$). Druga inkluzija se izvodi analogno.□

# 7 Ciklične grupe

U narednih nekoliko stavova iznosimo osnovne osobine cikličnih grupa.

**Lema 7.1** *Ciklične grupe istog reda su izomorfne.*

**Dokaz.** Neka je $\mathbf{G} = \langle a \rangle$ reda $n$. Preslikavanje $\varphi : a^m \longrightarrow m$, $0 \leq m < n$, izomorfno je preslikavanje grupe $\mathbf{G}$ u grupu $\mathbf{Z}_n = \langle n, +_n \rangle$ (videti primer 2.4($a$)). U pitanju je, očigledno, bijekcija, a kako je $a^k \cdot a^l = a^{k+_n l}$ (dokaz je indukcijom po npr. $l$, imajući u vidu da je $a^n = e$), to je

$$(a^k \cdot a^l)\varphi = (a^{k+_n l})\varphi = k +_n l = (a^k)\varphi +_n (a^l)\varphi,$$

te je $\varphi$ i homomorfno preslikavanje.

Ciklične grupe beskonačnog reda izomorfne su aditivnoj grupi celih brojeva $\mathbf{Z}$. Dokaz je analogan.□

S obzirom na gornju lemu uobičajeno je da se ciklična grupa reda $n$ obeležava sa $\mathbf{C}_n$ (samo je jedna takva do na izomorfizam). U dokazu njenih svojstava obično ćemo koristiti grupu $\mathbf{Z}_n$. Kada su u pitanju beskonačne ciklične grupe, jasno, grupa $\mathbf{Z}$ će biti osnovni primer.

**Teorema 7.2** ($a$) *Podgrupa ciklične grupe je ciklična;*

($b$) *Podgrupa ciklične grupe je potpuno invarijantna;*

($c$) *U cikličnoj grupi $\mathbf{Z}_n$ je, za $k < n$, $\langle k \rangle = \langle (k, n) \rangle$.*
*Red elementa $k$ je $\frac{n}{(n,k)}$;*

($d$) *Ako su $k$ i $r$ delioci broja $n$, u $\mathbf{Z}_n$ važi: $\langle k \rangle \leq \langle r \rangle$ akko $r|k$. Za svako $k, r < n$, $r|k$ implicira $\langle k \rangle \leq \langle r \rangle$.*

*U beskonačnoj cikličnoj grupi $\mathbf{Z}$ važi: $\langle k \rangle \leq \langle l \rangle$ akko $l|k$.*

($e$) *U $\mathbf{Z}_n$ važi: $\langle k \rangle = \langle l \rangle$ akko je $(n, k) = (n, l)$; $\langle k \rangle \leq \langle l \rangle$ akko $(n, l)|(n, k)$;*

($f$) *$\langle k \rangle = \mathbf{Z}_n$ akko $(k, n) = 1$; ako je $(k, n) = 1$, $k < n$, jednačina $\underbrace{x +_n \cdots +_n x}_{k-puta} = s$ ima jedinstveno rešenje za svako $s < n$;*

($g$) *Za svaki delioc $k$ broja $n$ grupa $\mathbf{Z}_n$ ima jedinstvenu podgrupu reda $k$;*

($h$) *Grupa $\mathbf{Z}_k$ je homomorfna slika grupe $\mathbf{Z}_n$ akko $k|n$. Svaka konačna ciklična grupa je homomorfna slika beskonačne ciklične grupe;*

($i$) *U $\mathbf{Z}_n$ važi:*

$$\langle k \rangle \cap \langle r \rangle = \langle NZS(k, r) - [\frac{NZS(k, r)}{n}] n \rangle, \quad \langle k \rangle + \langle r \rangle = \langle (k, r) \rangle.$$

*Analogna tvrđenja važe za grupu $\mathbf{Z}$ - naravno, sada nema nikakvih kongruencija po nekakvom modulu;*



($j$) *Za $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ ($p_i$ prost broj, $p_i \neq p_j$ za $i \neq j$, $\alpha_i \geq 1$) je $\mathbf{Fr}(\mathbf{Z}_n) = \langle \prod_{i=1}^{k} p_i \rangle$ ako $\exists j$ $\alpha_j > 1$, u suprotnom je $\mathbf{Fr}(\mathbf{Z}_n) = \mathbf{O}$.*

**Dokaz.** ($a$) Neka je $\mathbf{O} \neq \mathbf{H} \leq \mathbf{Z}_n$ i neka je $h (< n)$ najmanji pozitivan broj koji se javlja u $H$. Tada je $\mathbf{H} = \langle h \rangle$. Jer, neka je $0 \neq l \in H$ i pretpostavimo $l = ph + r$, $0 \leq r < k$, $p \geq 1$. Onda je $l = \underbrace{h +_n \cdots +_n h}_{p-puta} +_n r = p \cdot_n h +_n r$, pa kako $l, p \cdot_n h \in H$, to je i $r \in H$ ($r = l +_n (n - p) \cdot_n h$) i stoga je $r = 0$.

($b$) Jasno; ako je $\mathbf{H} = \langle h \rangle$ i $\varphi \in End(\mathbf{Z}_n)$, onda je

$$(h)\varphi = \underbrace{(1 +_n \cdots +_n 1)}_{h-puta}\varphi = \underbrace{(1)\varphi +_n \cdots +_n (1)\varphi}_{h-puta} = h \cdot_n (1)\varphi = \underbrace{h +_n \cdots +_n h}_{(1)\varphi-puta},$$

pa je $(H)\varphi \subseteq H$.

($c$) Neka je $(k, n) = r$ i neka su $u$ i $v$ celi brojevi takvi da je $uk + vn = r$. Ako je $u = pn + q$, $0 < q < n$, imamo:

$$\underbrace{k +_n \cdots +_n k}_{q-puta} = q \cdot_n k = qk - [\frac{qk}{n}] n = r - (vn + pnk) - [\frac{r - (vn + pnk)}{n}] n =$$

$$r - [\frac{r}{n}] n = r,$$

pa je $\langle r \rangle \leq \langle k \rangle$, a trivijalno $\langle k \rangle \leq \langle r \rangle$.

($d$) Neka je $\langle k \rangle \leq \langle r \rangle$. Kako $r|n$, $r$ je najmanji (pozitivan) prirodan broj koji se javlja u $\langle r \rangle$. Prema tome je, za neko $p$, $0 < p < \frac{n}{r}$: $k = \underbrace{r +_n \cdots +_n r}_{p-puta} = \underbrace{r + \cdots + r}_{p-puta} = rp$ i $r|k$.

Implikaciju ($\Longleftarrow$) odista ne treba objašnjavati.

($e$) Direktna posledica tačaka ($c$) i ($d$).

($f$) Prvi deo tvrđenja je direktna posledica tačke ($c$). Zaključujemo: ciklična grupa reda $n$ ima $\varphi(n)$ generatornih elemenata.

Generatorni elementi grupe $\mathbf{Z}$ su 1 i -1.

Ako je $(k, n) = 1$, $k$ je generatorni element grupe $\mathbf{Z}_n$, pa je za neko $p$, $0 < p < n$: $s = \underbrace{k +_n \cdots +_n k}_{p-puta}$, tj. $s = p \cdot_n k = \underbrace{p +_n \cdots +_n p}_{k-puta}$.

Rešenje je jedinstveno, jer ako $u, v < n$ i $\underbrace{u +_n \cdots +_n u}_{k-puta} = \underbrace{v +_n \cdots +_n v}_{k-puta}$, tj. $uk - [\frac{uk}{n}] n = vk - [\frac{vk}{n}] n$, sledi $n|k(u - v)$, odnosno $n|(u - v)$, te je $u = v$.

Važi inače (dokaz je analogan): ako je element $a$ (ma koje grupe) $\mathbf{G}$ reda $n$ i ako je $k$ ceo broj takav da je $(k, n) = 1$, onda jednačina $a^s = x^k$, $0 \leq s < n$,

ima rešenje u $\mathbf{G}$. No u opštem nemamo jedinstveno rešenje. Tako je npr. u $\mathbf{Z}_6$:

$$2 = 1 +_6 1 = 4 +_6 4,\ 2 = 2 +_6 2 +_6 2 +_6 2 = 5 +_6 5 +_6 5 +_6 5.$$

$(g)$ Neka je $\frac{n}{k} = r$. Jasno, $\langle r\rangle$ je podgrupa grupe $\mathbf{Z}_n$ reda $k$. Neka je i $\langle p\rangle$ podgrupa reda $k$. Zbog $\langle p\rangle = \langle (n,p)\rangle$ je $\frac{n}{(n,p)} = k$, te je $(n,p) = r$ i $\langle p\rangle = \langle r\rangle$.

$(h)$ Neka je $\mathbf{Z}_k$ homomorfna slika grupe $\mathbf{Z}_n$. Prema 8.1, $k|n$.

Pretpostavimo sada $n = kr$. Preslikavanje $\varphi : m \longrightarrow m - [\frac{m}{k}]k,\ 0 \leq m < n$, homomorfno je preslikavanje grupe $\mathbf{Z}_n$ na grupu $\mathbf{Z}_k$. Zaista, $\varphi$ je očigledno surjekcija, a za $p, q < n$ je:

$$(p +_n q)\varphi = p + q - [\frac{p+q}{n}]n - [\frac{p+q-[\frac{p+q}{n}]n}{k}]k =$$

$$p + q - [\frac{p+q}{k}]k = (p - [\frac{p}{k}]k) +_k (q - [\frac{q}{k}]k) = (p)\varphi +_k (q)\varphi.$$

Slično se pokazuje: preslikavanje $\varphi : Z \longrightarrow Z_n$ dato sa $(k)\varphi = k - [\frac{k}{n}]n$ homomorfno je preslikavanje grupe $\mathbf{Z}$ na grupu $\mathbf{Z}_n$ (za svako $n \geq 1$).

$(i)$ Posmatraćemo samo grupu $\mathbf{Z}_n$ (dokazi za $\mathbf{Z}$ su u osnovi isti – ali lakši). Naravno, $(0,n)$ biće $n$.

Prema $(a)$ je $\langle k\rangle \cap \langle r\rangle = \langle (k,n)\rangle \cap \langle (r,n)\rangle$. Neka je $(k,n) = q$ i $(r,n) = t$. Uočimo prvo da važi:

$$(NZS(k,r) - [\frac{NZS(k,r)}{n}]n,\ n) = (NZS(k,r),\ n) = NZS(q,t).$$

Zaista, neka je $k = \prod_i p_i^{\alpha_i}$, $r = \prod_i p_i^{\beta_i}$, $n = \prod_i p_i^{\gamma_i}$ (skoro svi stepeni – svi sem konačno mnogo – jednaki su 0, $p_i$ prolazi skupom svih prostih brojeva). Sada je:

$$q = \prod_i p_i^{min(\alpha_i,\gamma_i)},\quad t = \prod_i p_i^{min(\beta_i,\gamma_i)},$$

$$NZS(q,t) = \prod_i p_i^{max(min(\alpha_i,\gamma_i),min(\beta_i,\gamma_i))},\quad NZS(k,r) = \prod_i p_i^{max(\alpha_i,\beta_i)}.$$

Jasno, $NZS(q,t)|n$ i $NZS(q,t)|NZS(k,r)$. S druge strane, ako $m = \prod_i p_i^{\delta_i}$ deli i $n$ i $NZS(k,r)$, onda je $\delta_i \leq \gamma_i$ i $\delta_i \leq max(\alpha_i,\beta_i)$, pa je

$$\delta_i \leq max(min(\alpha_i,\gamma_i), min(\beta_i,\gamma_i)),$$

dakle $m$ deli $NZS(q,t)$.

Ako $NZS(k,r)$ nije deljivo sa $n$, onda je $NZS(q,t)$ manje od $n$, i prema $(d)$ je $\langle NZS(q,t)\rangle \leq \langle q\rangle \cap \langle t\rangle$. Opet, ako je $m \in \langle q\rangle \cap \langle t\rangle$, tada je $m$ deljivo i sa $q$ i sa $t$, jer su to delioci broja $n$, pa je $m$ deljivo i sa $NZS(q,t)$, dakle $m \in \langle NZS(q,t)\rangle$. Ako je $NZS(k,r)$ deljivo sa $n$, tada je $NZS(q,t) = n$ i



$\langle q\rangle \cap \langle t\rangle = \mathbf{O}$; opet, ako je $m \in \langle q\rangle \cap \langle t\rangle$, onda je $m$ deljivo sa $n$, te mora biti 0.

U drugom delu imamo: ako je $k, r \neq 0$ (izbegavamo trivijalne slučajeve) i ako je, za cele brojeve $u, v$, $uk + vr = (k,r)$ i $u = pn + u_1$, $v = qn + v_1$, $0 \leq u_1, v_1 < n$, onda je $(u_1 \cdot_n k) +_n (v_1 \cdot_n r) = (k,r)$.

$(j)$ Ako je $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, tada su $\langle p_1\rangle, \ldots, \langle p_k\rangle$ maksimalne podgrupe (prema $(c)$, $(d)$ i $(f)$), pa je prema $(i)$, uz uslov $\exists j\ \alpha_j > 1$:

$$\mathbf{Fr}(\mathbf{Z}_n) = \langle p_1\rangle \cap \ldots \cap \langle p_k\rangle = \langle NZS(p_1, \ldots, p_k)\rangle = \langle p_1 \ldots p_k\rangle.$$

Za $\alpha_1 = \cdots = \alpha_k = 1$ je, jasno, $\mathbf{Fr}(\mathbf{Z}_n) = \mathbf{O}$.

Ranije smo već videli $\mathbf{Fr}(\mathbf{Z}) = \mathbf{O}$.■

**Napomena**. Neko će naći jednostavnijim da dokaze pojedinih tačaka ove teoreme izvede prvo za aditivnu grupu celih brojeva, a onda, koristeći tačku $(h)$, i za konačne ciklične grupe. Ostavljamo taj put kao vežbu.

**Korolar 7.3** *Neka je $\varphi$ homomorfno preslikavanje grupe $\mathbf{Z}_n$ na grupu $\mathbf{Z}_k$ $(k|n)$ iz dokaza tačke $(h)$ prethodne teoreme. Tada je svaki generatorni element grupe $\mathbf{Z}_k$ slika bar jednog generatornog elementa grupe $\mathbf{Z}_n$.*

**Dokaz**. Neka je $r$ generatorni element grupe $\mathbf{Z}_k$ (dakle, $(r,k) = 1$) i neka je $n = k \cdot m$. Kako je $Ker(\varphi) = \{kt \mid 0 \leq t \leq m-1\}$, važi: $(\{r\})\varphi^{-1}) = \{r + kt \mid 0 \leq t \leq m-1\}$. Stoga treba da pokažemo da je bar jedan od elemenata $r + kt$, $0 \leq t \leq m-1$, uzajamno prost sa $n$. S obzirom da su $k$ i $r$ uzajamno prosti, prema poznatoj teoremi P. G. L. Dirichleta (Peter Gustav Lejeune Dirichlet, 1805 -1859) – citiramo je: *aritmetički niz $\langle a + bc\rangle_{c\geq 0}$, gde su $a$ i $b$ uzajamno prosti prirodni brojevi, sadrži beskonačno mnogo prostih brojeva* – postoji prirodan broj $u$ (zapravo je beskonačno mnogo takvih – možemo uzeti najmanji među njima) takav da je $r + ku$ prost broj. Ako je $u$ manje od $m-1$, imamo odmah rešenje; ako je $u \geq m$, tada je traženo rešenje $r + ku - [\frac{r+ku}{n}]n$ – to je broj oblika $r + ks$ za neko $s \in \{0, \ldots, m-1\}$ (jer $k \cdot m = n$) i evidentno je uzajamno prost sa $n$.□

**Korolar 7.4** *Grupa $\mathbf{G}$ je ciklična akko ima element $g$ takav da je za svako homomorfno preslikavanje $\varphi$ proizvoljne grupe $\mathbf{H}$ u $\mathbf{G}$ ispunjeno: ako je $g \in (H)\varphi$, onda je $\varphi$ surjektivno.*

**Dokaz**. ($\Longrightarrow$) Neka je $\mathbf{G}$ ciklična grupa generisana sa $g$, $\varphi \in Hom(\mathbf{H}, \mathbf{G})$ i $g \in (H)\varphi$, recimo $g = (h)\varphi$. Jasno, tada je, za svaki element $g^k$ grupe $\mathbf{G}$, $(h^k)\varphi = ((h)\varphi)^k = g^k$.

($\Longleftarrow$) Neka je $g$ element grupe $\mathbf{G}$ sa datim svojstvom. Po pretpostavci je svako homomorfno preslikavanje $\varphi$ grupe $\mathbf{Z}$ na cikličnu grupu $\langle g\rangle$ surjektivno pa je $\mathbf{G}$ ciklična grupa generisana sa $g$.□

**Korolar 7.5** *(a) Neka je $n$ prirodan broj i neka je $D$ skup svih njegovih pozitivnih delilaca ($D = \{d \mid 1 \leq d \leq n,\ d|n\}$). Tada je*

$$n = \sum_{d\in D} \varphi(d),$$

*gde je, podsećamo, $\varphi(d)$ vrednost Eulerove funkcije za broj $d$;*

*(b) Grupa konačnog reda $n$ je ciklična akko za svaki delilac $d$ broja $n$ ima najviše jednu podgrupu reda $d$.*

**Dokaz.** *(a)* Neka je $\mathbf{G}$ grupa reda $n$ i neka je $\mathcal{C}_\mathbf{G} = \{\mathbf{C}_i \mid i \in I\}$ skup svih njenih cikličnih podgrupa. Ako je $g(\mathbf{C}_i)$ skup generatora ciklične grupe $\mathbf{C}_i$ onda je, jasno, za različite indekse $i, j$ iz $I$, $g(\mathbf{C}_i) \cap g(\mathbf{C}_j) = \emptyset$ i $G = \bigcup_{i\in I} g(\mathbf{C}_i)$, pa je $|G| = \sum_{i\in I} |g(\mathbf{C}_i)|$.

Posebno, kada je u pitanju ciklična grupa $\mathbf{Z}_n$ reda $n$ imamo, prema tački $(g)$ prethodne teoreme, za svako $d \in D$, tačno jednu cikličnu podgrupu reda $d$, što zajedno sa tačkom $(f)$ iste teoreme daje:

$$n = |Z_n| = \sum_{d\in D} |g(\mathbf{Z}_d)| = \sum_{d\in D} \varphi(d).$$

*(b)* Naravno, treba dokazati samo implikaciju ($\Longleftarrow$). Neka je $\mathbf{G}$ grupa reda $n$, sa najviše jednom podgrupom reda $d$ za $d \in D$. S obzirom na upravo rečeno važi:

$$n = |G| \leq \sum_{d\in D} \varphi(d) = n,$$

pa proizilazi da $\mathbf{G}$ mora imati i cikličnu podgrupu reda $n$, tj. da i sama mora biti ciklična.□

**Korolar 7.6** *Neka je $A = \{n_1, \ldots, n_k\}$ (bilo koji) konačan skup prirodnih brojeva. Tada postoji konačna nejedinična grupa $\mathbf{G}$ u kojoj sve jednačine $x^{n_i} = a$, $1 \leq i \leq k$, $a \in G$, imaju rešenje.*

**Dokaz.** Prema tački $(f)$ prethodne teoreme za grupu $\mathbf{G}$ možemo uzeti bilo koju cikličnu grupu čiji je red uzajamno prost sa svakim elementom iz $A$ (npr. $|G| = \prod_{i=1}^{k} n_i + 1$).□

**Korolar 7.7** *Ako grupa $\mathbf{G}$ reda $2n$ ima element reda $n$, onda ima i najmanje $\tau(n) - 1$ netrivijalnih normalnih podgrupa, gde je $\tau(n)$ broj delilaca broja $n$ (uključujući 1 i $n$).*

**Dokaz.** Neka je $a \in G$ element reda $n$. Tada je $\mathbf{A} = \langle a\rangle$ normalna podgrupa grupe $\mathbf{G}$ (jer je indeksa 2), a svaka njena podgrupa je, kao potpuno invarijantna, i normalna podgrupa grupe $\mathbf{G}$ (4.34). Prema tački $(g)$ prethodne teoreme, $\mathbf{A}$ ima $\tau(n)$ podgrupa (uključujući i jediničnu).□

Prema 5.11 važi



**Lema 7.8** *Konačna grupa $\mathbf{G}$ je ciklična akko je $\mathbf{G}/\mathbf{Fr}(\mathbf{G})$ ciklična.*

**Definicija 7.9** *Neka je $A$ skup (sistem) generatora grupe $\mathbf{G}$ ($\mathbf{G} = \langle A\rangle$). $A$ je ireducibilan sistem generatora akko ni jedan njegov pravi podskup ne generiše celu grupu.*

**Primer 7.10** *(a) Svaki od skupova $\{1\}$, $\{2, 3\}$, $\{6, 10, 15\}$ je ireducibilan sistem generatora grupe $\mathbf{Z}$. Uopšte, za svaki prirodan broj $n > 0$ grupa $\mathbf{Z}$ ima ireducibilni sistem generatora (zapravo, takvih ima beskonačno mnogo) od $n$ elemenata.*

*(b) Skupovi*

$$P = \{p \mid p \text{ je prost broj}\},$$

$$\{p_1 \ldots p_n \mid n \in \omega,\ p_i \text{ } i\text{-ti (po redu) prost broj}\}$$

*su ireducibilni sistemi generatora multiplikativne grupe pozitivnih racionalnih brojeva $\langle Ra^+, \cdot\rangle$.*

*$Q = P \cup \{-1\}$ je ireducibilan sistem generatora multiplikativne grupe nenula racionalnih brojeva.*

*Neka $p, k \in P$. Podgrupa $\mathbf{H}_{p,k} = \langle Q \setminus \{p\} \cup \{p^k\}\rangle$ je indeksa $k$, stoga i maksimalna. Takođe je $\mathbf{H} = \langle P\rangle$ maksimalna podgrupa (indeksa 2), te je $\mathbf{Fr}(\langle Ra \setminus \{0\}, \cdot\rangle) = \mathbf{E}$;*

*(c) $\{(0\,1), (1\,2), \ldots, (n-2\ n-1)\}$ i $\{(0\,1), (0\,1\ldots n-1)\}$ su ireducibilni sistemi generatora grupe $\mathbf{S}_n$ (videti 9.10).*

*(d) Aditivna grupa racionalnih brojeva i Prüferova $p$-grupa (primer 3.4(b)) nemaju ireducibilan sistem generatora.*

**Dokaz.** Neka je $\mathbf{Ra} = \langle A\rangle$, $a, b \in A$, $a \neq b$ i $ab \neq 0$. Onda je, za neko $k, l \in Z \setminus \{0\}$, $ka = lb$ i kako postoji $m \in Z$ i $c \in \langle A \setminus \{a\}\rangle$ takvi da je $(1/k)a = ma + c$, to je $a = m(ka) + kc = (ml)b + kc \in \langle A \setminus \{a\}\rangle$. Proizilazi da je i $A \setminus \{a\}$ generatorni skup grupe $\mathbf{Ra}$.

Što se Prüferove grupe tiče jedan njen generatorni skup je $A = \{a_k \mid k \in \omega\}$, gde je $a_k = e^{2\pi i/p^k}$. S obzirom da je $a_r = a_s^{p^{s-r}}$ za $r < s$, svaki beskonačan podskup skupa $A$ je, takođe, generatorni skup grupe $\mathbf{p}^\infty$. Neka je i $B$ skup generatora. No, ako je $b \in \langle a_{k+1}\rangle \setminus \langle a_k\rangle$, onda je $\langle b\rangle = \langle a_{k+1}\rangle$ (teorema 5.28$(d)$,$(f)$) te i svaki beskonačan podskup od $B$ generiše celu grupu.

**Napomena.** Uočimo da smo usput i ovo pokazali:

*svaki element grupa $\mathbf{Ra}$ i $\mathbf{p}^\infty$ može se eliminisati iz bilo kojeg generatornog skupa tih grupa;*

*svaka prava podgrupa grupe $\mathbf{p}^\infty$ je konačna i ciklična – prave podgrupe su, kao što smo videli $\langle a_k\rangle$, $k \in \omega$.*□

Videćemo kasnije da je Prüferova $p$-grupa i jedina beskonačna Abelova grupa sa svojstvom da su joj sve prave podgrupe konačne (37.29). Što se tiče prvog dela napomene, prema 5.9 sledi

**Korolar 7.11** *Grupe* **Ra** *i* $\mathbf{p}^\infty$ *nemaju maksimalnih podgrupa.*

**Napomena.** U odeljku o deljivim grupama daćemo jedan drugi, "nezavisan", dokaz da grupe **Ra** i $\mathbf{p}^\infty$ nemaju maksimalnih podgrupa (33.7), koji je onda, prema prethodnom korolaru, i drugi, indirektan dokaz da se svaki njihov element može eliminisati iz svakog njihovog generatornog skupa.

**Korolar 7.12** *Beskonačna ciklična grupa ne ispunjava uslov minimalnosti podgrupa.*

*Svaka grupa koja ispunjava uslov minimalnosti podgrupa je periodična.*

**Dokaz.** Prvi deo tvrđenja je direktna posledica tačke $(d)$ prethodne teoreme. Npr. $\langle 2\rangle > \langle 2^2\rangle > \cdots > \langle 2^n\rangle > \cdots$ je beskonačan (strogo) opadajući niz podgrupa grupe **Z**. Drugi deo je neposredna posledica prvog; dodajmo samo: njegov obrat ne važi (videti komentar uz 13.4).□

Jasno, ako je grupa **G** konačno generisana, tada svaki njen generatorni skup sadrži ireducibilan konačni podskup. Takođe, takve grupe ne mogu biti beskonačna unija lanca strogo rastućih pravih podgrupa (videti i 5.15). Ovo nam, pored već navedenog, daje i drugi dokaz da grupe **Ra** i $\mathbf{p}^\infty$ nisu konačno generisane:

$$\mathbf{Ra} = \bigcup_{n\in\omega} \langle \frac{1}{n!}\rangle, \quad \mathbf{p}^\infty = \bigcup_{n\in\omega} \langle e^{2\pi i/p^n}\rangle,$$

a odatle sledi da je svaka konačno generisana podgrupa grupe **Ra** ciklična. Važi inače, dokaz ostavljamo za vežbu, $\langle \frac{p}{q}, \frac{r}{s}\rangle = \langle \frac{NZD(p,r)}{NZS(q,s)}\rangle$, i uopšte:

$$\langle \frac{p_1}{q_1}, \ldots, \frac{p_k}{q_k}\rangle = \langle \frac{NZD(p_1,\ldots,p_k)}{NZS(q_1,\ldots,q_k)}\rangle.$$

Grupa sa svojstvom da je svaka konačno generisana podgrupa ciklična zove se *lokalno ciklična*. Rezimiramo: **Ra** i $\mathbf{p}^\infty$ su lokalno ciklične grupe. Zapravo klasifikacija lokalno cikličnih grupa (videti paragraf 34 - 34.10) upravo je određena ovim grupama. I treba li reći da je svaka konačna lokalno ciklična grupa ciklična.

Kad grupa **G** nije konačno generisana, svi generatorni sistemi su, to smo već konstatovali, iste kardinalnosti - $|G|$.

Prüferove i primarne ciklične grupe (dakle, podgrupe Prüferovih grupa) vezuje svojstvo kocikličnosti (uporediti ga sa onim iz 7.4).

**Definicija 7.13** *Abelova grupa* **A** *je kociklična akko sadrži element* $a$ *takav da važi: homomorfno preslikavanje* $\varphi$ *grupe* **A** *u (proizvoljnu) nenula grupu* **B** *je injektivno akko* $a \notin Ker(\varphi)$. *Pomenuti element* $a$ *(ukoliko postoji) zovemo kocikličnim elementom grupe* **A**.



**Lema 7.14** *Abelova grupa je kociklična akko sadrži nenula podgrupu sadržanu u svakoj drugoj nenula podgrupi, tj. drugim rečima, akko je presek svih nenula podgrupa nenula podgrupa.*

**Dokaz.** ($\Longrightarrow$) Neka je $a$ kocikličnі element Abelove grupe **A**. Kako za svaku nenula podgrupu **B** postoji prirodni homomorfizam $\varphi_B : A \longrightarrow A/B$ koji, naravno, nije injektivan, to je $a$ elemet svake nenula podgrupe. Stoga $\bigcap\{\mathbf{B} \mid \mathbf{O} \neq \mathbf{B} \leq \mathbf{A}\} = \langle a\rangle$.

($\Longleftarrow$) Neka je nenula podgrupa $\mathbf{A}_1$ presek svih nenula podgrupa grupe **A**. Jasno, $\mathbf{A}_1$ mora biti ciklična grupa prostog reda. Neka je $a$ jedan njen generatorni element. $a$ je onda i kocikličan, jer ako $\varphi \in Hom(\mathbf{A},\mathbf{B})$ i $a \notin Ker(\varphi)$, onda je $\mathbf{Ker}(\varphi)$ nula (jedinična) podgrupa i $\varphi$ je injektivno preslikavanje.□

**Lema 7.15** *Grupa je kociklična akko je ili primarna ciklična ili Prüferova, tj. akko je podgrupa Prüferove grupe.*

**Dokaz.** ($\Longrightarrow$) Neka je $a$ kocikličnі element Abelove grupe **A**. Prema prethodnoj lemi ciklična grupa $\langle a\rangle$ je prostog reda, recimo $p$. Sledi i da je **A** periodična $p$-grupa (u beskonačnim cikličnim i konačnim cikličnim grupama čiji redovi sadrže više različitih prostih faktora ne postoji nenula podgrupa sadržana u svakoj drugoj nenula podgrupi). Indukcijom po $n$ pokazujemo da grupa **A** ima najviše jednu podgrupu reda $p^n$ i da ta, ukoliko postoji, mora biti ciklična. Za $n = 1$ imamo baš (samo) $\langle a\rangle$. Pretpostavimo da je tvrđenje tačno za svako $k \leq n$ i neka je $\mathbf{B} = \langle b\rangle$ jedina podgrupa reda $p^n$, a **C** i **D** neka su podgrupe reda $p^{n+1}$. Ako je $c \in C \setminus B$, $d \in D \setminus B$, tada je $red(c) = red(d) = p^{n+1}$ (pretpostavka da je npr. $red(c) = p^k < p^{n+1}$ značila bi da imamo bar dve ciklične grupe reda $p^k$ - odgovarajuću podgrupu grupe **B** i $\langle c\rangle$). Neka je, za neke cele brojeve $r$ i $s$: $(p,r) = (p,s) = 1$ i $pc = rb$, $pd = sb$. Ako je $rr_1 + up^n = 1$, $ss_1 + vp^n = 1$, $c_1 = r_1c$, $d_1 = s_1b$, onda je $\langle c\rangle = \langle c_1\rangle$ i $\langle d\rangle = \langle d_1\rangle$ (zbog $(p,r_1) = (p,s_1) = 1$), a $pc_1 = pr_1c = rr_1b = (1 - up^n)b = b$, i isto tako $pd_1 = b$. Odatle je $p(c_1 - d_1) = 0$, pa je, kao element reda $p$ ili nula element, $c_1 - d_1$ u podgrupi **B**. Neka je $c_1 = d_1 + tb = (1 + tp)d_1$. Proizilazi: $\langle c\rangle = \langle c_1\rangle = \langle (1 + tp_1)d_1\rangle \leq \langle d_1\rangle = \langle d\rangle$, stoga i $\langle c\rangle = \langle d\rangle$. Podgrupe grupe **A** su, dakle, linearno uređene te je **A** ili konačna ciklična $p$-grupa ili, ukoliko nema maksimalne podgrupe, Prüferova $\mathbf{p}^\infty$ grupa.

($\Longleftarrow$) Očigledno.□

# 8 Teoreme o izomorfizmu

Teoreme o izomorfizmu, lema Zassenhausa i teorema 8.7 jedno su od osnovnih "oruđa" u radu sa grupama. Stoga ih treba, zajedno sa dokazima, potpuno "usvojiti" (ovo ne znači, naravno, da ostala tvrđenja ovog paragrafa ne zaslužuju dužnu pažnju).

**Teorema 8.1** *(Prva teorema o izomorfizmu ili Teorema o homomorfizmu). Neka je $\varphi$ homomorfno preslikavanje grupe $\mathbf{G}$ na grupu $\mathbf{H}$. Tada je grupa $\mathbf{H}$ izomorfna grupi $\mathbf{G/Ker}(\varphi)$.*

**Dokaz.** Korespondencija $\psi : G/Ker(\varphi) \longrightarrow H$, data sa $(g\,Ker(\varphi))\psi \stackrel{\text{def}}{=} (g)\varphi$, izomorfno je preslikavanje grupe $\mathbf{G/Ker}(\varphi)$ na grupu $\mathbf{H}$. Proverićemo samo da je $\psi$ dobro definisano i $1-1$:

$$aKer(\varphi) = bKer(\varphi) \Longleftrightarrow a^{-1}b \in Ker(\varphi) \Longleftrightarrow (a^{-1}b)\varphi = e_H \Longleftrightarrow$$

$$(a)\varphi = (aKer(\varphi))\psi = (bKer(\varphi))\psi = (b)\varphi.\blacksquare$$

Prema teoremama 4.25 i 8.1, $\{\mathbf{G/H} \mid \mathbf{H} \lhd \mathbf{G}\}$ je skup svih homomorfnih slika (do na izomorfizam) grupe $\mathbf{G}$ i već ta činjenica ukazuje na izuzetan značaj pojma normalne podgrupe. No još mnogo važnih "rola" imaju normalne podgrupe u teoriji grupa.

**Korolar 8.2** *Ako je $\varphi$ homomorfno preslikavanje proste grupe $\mathbf{G}$ u grupu $\mathbf{H}$, onda je $\varphi$ ili trivijalan homomorfizam ili utapanje (injektivni homomorfizam) grupe $\mathbf{G}$ u grupu $\mathbf{H}$.*

**Dokaz.** Jezgro homomorfizma $\varphi$ može biti samo ili cela grupa $\mathbf{G}$ ili jedinična podgrupa. U prvom slučaju je $(\mathbf{G})\varphi \cong \mathbf{G/Ker}(\varphi)$ jedinična podgrupa grupe $\mathbf{H}$, u drugom izomorfna slika grupe $\mathbf{G}$.$\square$

**Lema 8.3** *Ako je $\mathbf{H} \lhd \mathbf{G}$ i $\mathbf{K} \leq \mathbf{G}$, onda je $\mathbf{H} \cap \mathbf{K} \lhd \mathbf{K}$.*

**Korolar 8.4** *Neka je nejedinična grupa $\mathbf{G}$ unija podgrupa $\mathbf{H}_i$, $i \in I$, gde je indeksni skup $I$ uređen relacijom $\leq$ tako da za svako $i, j \in I$ postoji $k \in I$ za koje je $i \leq k$, $j \leq k$ (u pitanju je, dakle, usmereni skup - 3.22), i neka je $\mathbf{H}_i \leq \mathbf{H}_j$ za $i \leq j$ (iz čisto praktičnih razloga koristimo istu oznaku za relaciju na indeksnom skupu i relaciju inkluzije podgrupa). Tada važi: ako za svako $i \in I$ postoji $j \in I$ za koje je $i \leq j$ i $\mathbf{H}_j$ prosta grupa, onda je i $\mathbf{G}$ prosta grupa.*

**Dokaz.** Iz datih uslova sledi da za svaku netrivijalnu podgrupu $\mathbf{H}$ grupe $\mathbf{G}$ postoji $j \in I$, tako da je $\mathbf{H}_j$ prosta grupa i $\{e\} \neq H \cap H_j \subset H_j$. Zaista, neka je $a$ nejedinični element podgrupe $\mathbf{H}$ i $\mathbf{H}_k$ prosta grupa koja nije sadržana u $\mathbf{H}$ (takva postoji jer je $\mathbf{H}$ prava podgrupa). Ako je $a \in H_l$ i $k, l \leq i$, a $\mathbf{H}_i \leq \mathbf{H}_j$, gde je $\mathbf{H}_j$ prosta grupa, onda imamo: $\{e\} \neq \langle a \rangle \subseteq H \cap H_j \subset H_j$. Prema tome bi pretpostavka da je $\mathbf{H}$ normalna podgrupa vodila u kontradikciju ($\mathbf{H} \cap \mathbf{H}_i$ bi bila netrivijalna normalna podgrupa proste grupe $\mathbf{H}_j$).$\square$



**Teorema 8.5** *(Lema Zassenhausa). Neka su $\mathbf{H}$, $\mathbf{H}_1$, $\mathbf{K}$, $\mathbf{K}_1$ podgrupe grupe $\mathbf{G}$ takve da je $\mathbf{H}_1 \lhd \mathbf{H}$ i $\mathbf{K}_1 \lhd \mathbf{K}$. Tada je:*

$$\mathbf{H}_1(\mathbf{H} \cap \mathbf{K}_1) \lhd \mathbf{H}_1(\mathbf{H} \cap \mathbf{K}), \quad \mathbf{K}_1(\mathbf{H}_1 \cap \mathbf{K}) \lhd \mathbf{K}_1(\mathbf{H} \cap \mathbf{K})$$

*i*

$$\mathbf{H}_1(\mathbf{H} \cap \mathbf{K})/\mathbf{H}_1(\mathbf{H} \cap \mathbf{K}_1) \cong \mathbf{K}_1(\mathbf{H} \cap \mathbf{K})/\mathbf{K}_1(\mathbf{H}_1 \cap \mathbf{K}).$$

**Dokaz.** Prema prethodnoj lemi je $\mathbf{H}_1 \cap (\mathbf{H} \cap \mathbf{K}) = \mathbf{H}_1 \cap \mathbf{K} \lhd \mathbf{H} \cap \mathbf{K}$ i $\mathbf{H} \cap \mathbf{K}_1 \lhd \mathbf{H} \cap \mathbf{K}$, pa je i $(\mathbf{H}_1 \cap \mathbf{K})(\mathbf{H} \cap \mathbf{K}_1)$ normalna podgrupa grupe $\mathbf{H} \cap \mathbf{K}$. Pokazaćemo sada da je korespondencija $\varphi : H_1(H \cap K) \longrightarrow (H \cap K)/((H_1 \cap K)(H \cap K_1))$, gde je, za $h \in H_1$ i $a \in H \cap K$, $(ha)\varphi \stackrel{\text{def}}{=} (H_1 \cap K)(H \cap K_1)a$, homomorfno preslikavanje grupe $\mathbf{H}_1(\mathbf{H} \cap \mathbf{K})$ na faktor grupu $(\mathbf{H} \cap \mathbf{K})/((\mathbf{H}_1 \cap \mathbf{K})(\mathbf{H} \cap \mathbf{K}_1))$ ($\mathbf{H}_1(\mathbf{H} \cap \mathbf{K})$ je domen podgrupe grupe $\mathbf{H}$ jer je $\mathbf{H}_1 \lhd \mathbf{H}$). $\varphi$ je dobro definisano, s obzirom da ako je $h_1 a = h_2 b$, $h_1, h_2 \in H_1$, $a, b \in H \cap K$, onda je $h_2^{-1} h_1 = ba^{-1} \in H_1 \cap (H \cap K) = H_1 \cap K \subseteq (H_1 \cap K)(H \cap K_1)$, dakle, $(h_1 a)\varphi = (h_2 b)\varphi$. $\varphi$ je, jasno, "na", a važi takođe i:

$$(h_1 a\, h_2 b)\varphi = (h_1 a h_2 a^{-1}\, ab)\varphi = (H_1 \cap K)(H \cap K_1)\, ab =$$

$$(H_1 \cap K)(H \cap K_1)a\,(H_1 \cap K)(H \cap K_1)b = (h_1 a)\varphi\,(h_2 b)\varphi.$$

Kako je $\mathbf{Ker}(\varphi) = \mathbf{H}_1(\mathbf{H} \cap \mathbf{K}_1)$ (inkluzija $\geq$ je očigledna, a s druge strane, ako je $(ha)\varphi = (H_1 \cap K)(H \cap K_1)$, tj. $a \in (H_1 \cap K)(H \cap K_1)$, tada je, za neko $b \in H_1 \cap K$ i neko $c \in H \cap K_1$, $a = bc$ i prema tome $ha = (hb)c \in H_1(H \cap K_1)$), imamo:

$$(\mathbf{H}_1(\mathbf{H} \cap \mathbf{K}))/(\mathbf{H}_1(\mathbf{H} \cap \mathbf{K}_1)) \cong (\mathbf{H} \cap \mathbf{K})/((\mathbf{H}_1 \cap \mathbf{K})(\mathbf{H} \cap \mathbf{K}_1)).$$

Po simetriji stvari je i

$$(\mathbf{K}_1(\mathbf{H} \cap \mathbf{K}))/(\mathbf{K}_1(\mathbf{H}_1 \cap \mathbf{K})) \cong (\mathbf{H} \cap \mathbf{K})/((\mathbf{H}_1 \cap \mathbf{K})(\mathbf{H} \cap \mathbf{K}_1)).\blacksquare$$

**Korolar 8.6** *(Druga teorema o izomorfizmu). Ako su $\mathbf{A}$ i $\mathbf{B}$ podgrupe grupe $\mathbf{G}$ takve da je $\mathbf{A} \lhd \langle A \cup B \rangle$, tada je*

$$\langle A \cup B \rangle/\mathbf{A} \cong \mathbf{B}/(\mathbf{A} \cap \mathbf{B}).$$

**Dokaz.** Direktna posledica leme Zassenhausa - staviti $\mathbf{H} = \langle A \cup B \rangle$, $\mathbf{H}_1 = \mathbf{A}$, $\mathbf{K} = \mathbf{B}$ i $\mathbf{K}_1 = \mathbf{E}$.

Primetimo da je, s obzirom na uslov korolara, $\langle A \cup B \rangle = \mathbf{AB}$, te ćemo obično pisati

$$\mathbf{AB}/\mathbf{A} \cong \mathbf{B}/(\mathbf{A} \cap \mathbf{B}).\square$$

**Teorema 8.7** *(Teorema o korespondenciji). Neka je $\varphi$ homomorfno preslikavanje grupe $\mathbf{G}$ na grupu $\mathbf{H}$. Tada postoji izomorfizam mreža $\langle\{\mathbf{B} \mid \mathbf{B} \leq \mathbf{H}\}, \vee, \cap\rangle$ i $\langle\{\mathbf{A} \mid \mathbf{Ker}(\varphi) \leq \mathbf{A} \leq \mathbf{G}\}, \vee, \cap\rangle$ za koji važi: odgovarajuće podgrupe su istog indeksa, normalnost jedne povlači normalnost njoj korespondentne i u tom slučaju su njihove faktor grupe izomorfne.*

**Dokaz.** Preslikavanje $\psi : \{\mathbf{B} \mid \mathbf{B} \leq \mathbf{H}\} \longrightarrow \{\mathbf{A} \mid \mathbf{Ker}(\varphi) \leq \mathbf{A} \leq \mathbf{G}\}$, gde je $(\mathbf{B})\psi \stackrel{\text{def}}{=} (\mathbf{B})\varphi^{-1}$ (videti 3.3($c$)), izomorfizam je datih mreža sa navedenim svojstvima.

$\psi$ je "jedan - jedan", jer ako je $\mathbf{B_1} \neq \mathbf{B_2}$ i, recimo, $h \in B_1 \setminus B_2$ i $(g)\varphi = h$, onda je $g \in (B_1)\varphi^{-1} \setminus (B_2)\varphi^{-1}$. $\psi$ je i "na", pošto je $\mathbf{A} = ((\mathbf{A})\varphi)\varphi^{-1}$ (videti i 2.16) ako je $\mathbf{Ker}(\varphi) \leq \mathbf{A} (\leq \mathbf{G})$. Zaista, ako je $g \in ((A)\varphi)\varphi^{-1}$, onda postoji $a \in A$ takvo da je $(a)\varphi = (g)\varphi$, odatle je $a^{-1}g \in Ker(\varphi)$, te je $g \in a\,Ker(\varphi) \subseteq A$.

Korespondencija $\theta : \{g(B)\varphi^{-1} \mid g \in G\} \longrightarrow \{hB \mid h \in H\}$, gde je $(g(B)\varphi^{-1})\theta \stackrel{\text{def}}{=} (g)\varphi\, B$, biunivoko je preslikavanje skupa levih koseta podgrupe $(\mathbf{B})\varphi^{-1}$ u skup levih koseta podgrupe $\mathbf{B}$, pa je $[\mathbf{G} : (\mathbf{B})\varphi^{-1}] = [\mathbf{H} : \mathbf{B}]$.

Lako se proverava i da je $\mathbf{B} \lhd \mathbf{H}$ akko je $(\mathbf{B})\varphi^{-1} \lhd \mathbf{G}$, pa ako je $\mathbf{B} \lhd \mathbf{H}$, $\theta$ je izomorfno preslikavanje grupe $\mathbf{G}/(\mathbf{B})\varphi^{-1}$ na grupu $\mathbf{H}/\mathbf{B}$.

Svojstvo homomorfnosti preslikavanja $\psi$ u odnosu na operacije $\vee$ i $\cap$ takođe se neposredno proverava. Imamo direktno $(\mathbf{B_1} \cap \mathbf{B_2})\varphi^{-1} = (\mathbf{B_1})\varphi^{-1} \cap (\mathbf{B_2})\varphi^{-1}$, i očigledno $\langle (B_1)\varphi^{-1} \cup (B_2)\varphi^{-1}\rangle \subseteq \langle B_1 \cup B_2\rangle\varphi^{-1}$, a i inkluzija $\supseteq$ se lako proverava. No to je i suvišno ako mreže posmatramo kao parcijalne uređene skupove s obzirom na relaciju inkluzije - jasno, ako je $\mathbf{B_1}$ strogo sadržano u $\mathbf{B_2}$, onda je i $(\mathbf{B_1})\varphi^{-1}$ strogo sadržano u $(\mathbf{B_2})\varphi^{-1}$. Konstatujmo konačno, a to smo mogli i ranije učiniti: bijekcija domena dveju mreža je izomorfizam tih mreža ako i samo ako ima svojstvo homomorfnosti u odnosu na jednu od operacija.■

**Napomena.** U vezi ove teoreme videti i 4.18.

Obično ćemo kod primene teoreme 8.7 imati da je $\mathbf{H}$ neka faktor grupa $\mathbf{G/N}$ grupe $\mathbf{G}$ i $\varphi$ prirodni homomorfizam, te će korespondentne podgrupe biti $\mathbf{K}$ i $\mathbf{K/N}$, gde je $\mathbf{N} \leq \mathbf{K} \leq \mathbf{G}$. Tako ćemo često koristiti sledeći

**Korolar 8.8** *(Treća teorema o izomorfizmu). Neka je $\mathbf{N}$ normalna podgrupa grupe $\mathbf{G}$ i neka je $\mathbf{N} \leq \mathbf{K} \leq \mathbf{G}$. Tada važi: $\mathbf{K} \lhd \mathbf{G}$ akko $\mathbf{K/N} \lhd \mathbf{G/N}$, i ako je $\mathbf{K} \lhd \mathbf{G}$, onda je*

$$\mathbf{G/K} \cong \mathbf{(G/N)/(K/N)}.$$

Primetimo da korespondencija $\mathbf{K} \longrightarrow (\mathbf{K})\varphi$ bez uslova $\mathbf{N} \leq \mathbf{K}$ nije nužno jednoznačna. Tako npr. ako je $\mathbf{G} = \mathbf{Z}$, $\mathbf{N} = 24\mathbf{Z} = \langle\{24k \mid k \in Z\}, +\rangle$, $\mathbf{K_1} = 6\mathbf{Z}$ i $\mathbf{K_2} = 30\mathbf{Z}$, onda je $(\mathbf{K_1})\varphi = (\mathbf{K_2})\varphi = \mathbf{K_1/N}$, gde je $\varphi : Z \longrightarrow Z/N$ prirodni homomorfizam.



**Lema 8.9** *Neka su $\mathbf{A}$ i $\mathbf{B}$ normalne podgrupe grupe $\mathbf{G}$ takve da je $\mathcal{S} = \{[a,b] \mid a \in A, b \in B\}$ konačan skup. Tada je i grupa $[\mathbf{A},\mathbf{B}]$ konačna.*

**Dokaz.** Neka je $\mathbf{H} = \mathbf{AB}$ i $\mathbf{C} = [\mathbf{A},\mathbf{B}]$. Zbog normalnosti podgrupa $\mathbf{A}$ i $\mathbf{B}$, preslikavanje $\Phi : H \longrightarrow S_{\mathcal{S}}$, definisano sa: $(h)\Phi \stackrel{\text{def}}{=} u_h|_{\mathcal{S}}$, homomorfno je preslikavanje grupe $\mathbf{H}$ u simetričnu grupu $\mathbf{S}_{\mathcal{S}}$ skupa $\mathcal{S}$. Naravno, $\mathbf{K} = \mathbf{Ker}(\Phi)$ je podgrupa konačnog indeksa grupe $\mathbf{H}$, sadržana u centralizatoru podgrupe $\mathbf{C}$ (ako je $h \in K$, onda je, za svako $[a,b] \in [A,B]$, $h^{-1}[a,b]h = [a,b]$, tj. $h[a,b] = [a,b]h$). Stoga je $\mathbf{C} \cap \mathbf{K}$ podgrupa centra grupe $\mathbf{C}$ i to konačnog indeksa (jer: $\mathbf{C}/(\mathbf{C} \cap \mathbf{K}) \cong (\mathbf{CK})/\mathbf{K} \leq \mathbf{H}/\mathbf{K}$). Prema 6.5, $\mathbf{C'}$ je konačna grupa, ujedno i normalna podgrupa grupe $\mathbf{H}$ (6.10, 4.34). Neka je $\overline{\mathbf{H}} = \mathbf{H}/\mathbf{C'}$, $\overline{\mathbf{A}} = \mathbf{A}/\mathbf{C'}$, $\overline{\mathbf{B}} = \mathbf{B}/\mathbf{C'}$ i $\overline{\mathbf{C}} = \mathbf{C}/\mathbf{C'}$. Očigledno, ako je $a \in A$ i $c \in C \subseteq B$, onda je $[aC', cC'] = [a,c]C'$, te postoji samo konačno mnogo komutatora oblika $[\overline{a},\overline{c}]$, $\overline{a} \in \overline{A}$, $\overline{c} \in \overline{C}$. Opet, pošto je $\overline{\mathbf{C}}$ Abelova grupa i uz to normalna podgrupa grupe $\overline{\mathbf{H}}$ (8.7), imamo: $[\overline{a},\overline{c}]^2 = ((\overline{a})^{-1}(\overline{c})^{-1}\overline{a})\cdot\overline{c}\cdot((\overline{a})^{-1}(\overline{c})^{-1}\overline{a})\cdot\overline{c} = ((\overline{a})^{-1}(\overline{c})^{-1}\overline{a})^2\cdot(\overline{c})^2 = (\overline{a})^{-1}(\overline{c})^{-2}\overline{ac}^2 = [\overline{a},\overline{c}^2]$. Sledi da je grupa $[\overline{\mathbf{A}},\overline{\mathbf{C}}] = \overline{\mathbf{D}}$ konačna normalna podgrupa grupe $\overline{\mathbf{H}}$. Pređimo, konačno, na faktor grupu $\overline{\overline{\mathbf{H}}} = \overline{\mathbf{H}}/\overline{\mathbf{D}}$ i njene podgrupe $\overline{\overline{\mathbf{A}}} = \overline{\mathbf{A}}/\overline{\mathbf{D}}$, $\overline{\overline{\mathbf{B}}} = \overline{\mathbf{B}}/\overline{\mathbf{D}}$ i $\overline{\overline{\mathbf{C}}} = \overline{\mathbf{C}}/\overline{\mathbf{D}}$. Naravno, $\overline{\overline{\mathbf{C}}} = [\overline{\overline{\mathbf{A}}},\overline{\overline{\mathbf{B}}}]$ i podgrupa $\overline{\overline{\mathbf{A}}}$ je sadržana u centarlizatoru podgrupe $\overline{\overline{\mathbf{C}}}$. Odatle, ako je $x \in \overline{\overline{A}}$ i $y \in \overline{\overline{B}}$ (zbog preglednosti teksta koristimo $x$ i $y$ umesto očekivanih $\overline{\overline{a}}$ i $\overline{\overline{b}}$), onda je $[x,y]^2 = x^{-1}y^{-1}\cdot xyx^{-1}y^{-1}\cdot xy = x^{-1}y^{-1}x^2yx^{-1} = x\cdot x^{-2}y^{-1}x^2y\cdot x^{-1} = x^{-2}y^{-1}x^2y = [x^2,y]$; dakle, kvadrat komutatora je komutator. Prema uslovima leme i analogiji sa dokazom leme 6.5 proizilazi da je $\overline{\overline{\mathbf{C}}}$ konačna grupa, a tada i $\overline{\mathbf{C}}$, a tada i $\mathbf{C}$.□

**Lema 8.10** ($a$) *Neka je $\mathbf{H}$ karakteristična podgrupa grupe $\mathbf{G}$ i neka je $\mathbf{K/H}$ karakteristična podgrupa grupe $\mathbf{G/H}$. Tada je $\mathbf{K}$ karakteristična podgrupa grupe $\mathbf{G}$;*

($b$) *Neka su $\mathbf{H}$ i $\mathbf{N}$ karakteristične podgrupe grupe $\mathbf{G}$ i neka je $\mathbf{H}$ podgrupa grupe $\mathbf{N}$, a $\mathbf{K/H}$ karakteristična podgrupa grupe $\mathbf{N/H}$. Tada je $\mathbf{K}$ karakteristična podgrupa grupe $\mathbf{G}$.*

**Dokaz.** ($a$) Neka je $\varphi$ automorfizam grupe $\mathbf{G}$. Tada je preslikavanje $\overline{\varphi} : G/H \longrightarrow G/H$ dato sa: $(aH)\overline{\varphi} = (a)\varphi H$ automorfizam faktor grupe $\mathbf{G/H}$. Jer, s obzirom da je $\mathbf{H}$ karakteristična podgrupa, sledi za ma koje elemente $a,b$ grupe $\mathbf{G}$: $aH = bH$ akko $b^{-1}a \in H$ akko $(b^{-1}a)\varphi \in H$ akko $(a)\varphi H = (b)\varphi H$, pa je $\overline{\varphi}$ dobro definisano i injektivno, a surjektivnost i homomorfnost su očigledni. No tada je $\mathbf{K/H} = (\mathbf{K/H})\overline{\varphi} = (\mathbf{K})\varphi/\mathbf{H}$ i, odatle, $\mathbf{K} = (\mathbf{K})\varphi$.

($b$) Neka je $\varphi$ automorfizam grupe $\mathbf{G}$. Tada je $\psi = \varphi|_N$ automorfizam grupe $\mathbf{N}$ koji ostavlja fiksnom podgrupu $\mathbf{H}$ (koja inače ne mora biti karakteristična podgrupa grupe $\mathbf{N}$), te je, kao u prethodnom slučaju, $K = (K)\psi = (K)\varphi$.□

**Korolar 8.11** *Ako je normalna podgrupa $\mathbf{N}$ grupe $\mathbf{G}$ sadržana u $\mathbf{Fr(G)}$, onda je $\mathbf{Fr(G/N)} = \mathbf{Fr(G)/N}$.*

**Korolar 8.12** *Sve maksimalne podgrupe grupe* $\mathbf{G}$ *su normalne akko je* $\mathbf{G}' \leq \mathbf{Fr}(\mathbf{G})$.

**Dokaz**. Tvrđenje trivijalno važi ako $\mathbf{G}$ nema maksimalnih podgrupa – tada je $\mathbf{Fr}(\mathbf{G}) = \mathbf{G}$ (o Abelovim grupama bez maksimalnih podgrupa videti u 33.7). Pretpostavimo zato da $\mathbf{G}$ ima maksimalnih podgrupa.

($\Longrightarrow$) Ako je $\mathbf{M}$ maksimalna podgrupa grupe $\mathbf{G}$, onda je $\mathbf{G}/\mathbf{M}$ grupa prostog reda (jer nema netrivijalnih podgrupa), dakle ciklična, dakle Abelova. Stoga je $\mathbf{G}' \leq \mathbf{M}$ (6.8) pa je i $\mathbf{G}' \leq \mathbf{Fr}(\mathbf{G})$.

($\Longleftarrow$) Već dokazano (opet 6.8); za svaku maksimalnu podgrupu $\mathbf{M}$ je: $\mathbf{G}' \leq \mathbf{Fr}(\mathbf{G}) \leq \mathbf{M}$.□

**Korolar 8.13** (*a*) *Ako je* $\mathbf{H}$ *normalna Hallova podgrupa grupe* $\mathbf{G}$, *onda je ona ujedno i jedina podgrupa grupe* $\mathbf{G}$ *reda* $|H|$;

(*b*) *Ako su* $\mathbf{H}$ *i* $\mathbf{K}$ *Hallove podgrupe grupe* $\mathbf{G}$ *istog reda, onda je* $\mathbf{N_K(H)} = \mathbf{H} \cap \mathbf{K}$.

(*c*) *Ako je* $\mathbf{H}$ *Hallova i* $\mathbf{K}$ *normalna podgrupa grupe* $\mathbf{G}$, *onda je* $\mathbf{H} \cap \mathbf{K}$ *Hallova podgrupa grupe* $\mathbf{K}$, *a* $(\mathbf{HK})/\mathbf{K}$ *Hallova podgrupa grupe* $\mathbf{G}/\mathbf{K}$.

**Dokaz**. (*a*) Neka je $\mathbf{i}$ $\mathbf{K}$ podgrupa grupe $\mathbf{G}$ reda $|H|$. Kako je, prema drugoj teoremi o izomorfizmu, $\mathbf{HK}/\mathbf{H} \cong \mathbf{K}/(\mathbf{H} \cap \mathbf{K})$, sledi:

$$[\mathbf{G} : \mathbf{HK}] = \frac{|G|}{|HK|} = \frac{\frac{|G|}{|H|}}{\frac{|HK|}{|H|}} = \frac{\frac{|G|}{|H|}}{\frac{|K|}{|H \cap K|}} = \frac{[\mathbf{G} : \mathbf{H}] \cdot |H \cap K|}{|H|}.$$

Dakle, $|H|$ deli $|H \cap K|$ pa je $\mathbf{H} \leq \mathbf{K}$, odnosno $\mathbf{H} = \mathbf{K}$.

(*b*) Obeležićemo, u cilju pojednostavljenja notacije, $\mathbf{N_K(H)}$ sa $\mathbf{N}$. $\mathbf{H}$ je normalna podgrupa grupe $\langle H \cup N \rangle = \mathbf{HN}$, te imamo $\mathbf{HN}/\mathbf{H} \cong \mathbf{N}/(\mathbf{H} \cap \mathbf{N})$ i odatle $[\mathbf{NH} : \mathbf{H}] = [\mathbf{N} : \mathbf{H} \cap \mathbf{N}]$. S obzirom da je $\mathbf{H}$ Hallova podgrupa i svake druge podgrupe grupe $\mathbf{G}$ koja je sadrži, proizilazi $([\mathbf{HN} : \mathbf{H}], |H|) = 1$, prema tome i $([\mathbf{N} : \mathbf{H} \cap \mathbf{N}], |H|) = 1$. Pošto je $\mathbf{N}$ podgrupa grupe $\mathbf{K}$ i $|H| = |K|$, mora biti $[\mathbf{N} : \mathbf{H} \cap \mathbf{N}] = 1$, pa je $\mathbf{N} \leq \mathbf{H}$.

(*c*) Iz $(\mathbf{HK})/\mathbf{K} \cong \mathbf{H}/(\mathbf{H} \cap \mathbf{K})$ sledi:

$$[\mathbf{HK} : \mathbf{H}] = \frac{|HK|}{|H|} = \frac{|K|}{|H \cap K|} = [\mathbf{K} : \mathbf{H} \cap \mathbf{K}],$$

pa $[\mathbf{K} : \mathbf{H} \cap \mathbf{K}]$ deli $[\mathbf{G} : \mathbf{H}]$, i jasno, $|H \cap K|$ deli $|H|$. Odatle, $(|H \cap K|, [\mathbf{K} : \mathbf{H} \cap \mathbf{K}]) = 1$.

Očigledno; $[\mathbf{G}/\mathbf{K} : (\mathbf{HK})/\mathbf{K}] = [\mathbf{G} : \mathbf{HK}]$ deli $[\mathbf{G} : \mathbf{H}]$, a $\frac{|HK|}{|K|} = \frac{|H|}{|H \cap K|}$ deli $|H|$.□

**Korolar 8.14** *Ako grupa* $\mathbf{G}$ *ispunjava uslov rastućih (opadajućih) lanaca, tj. uslov maksimalnosti (minimalnosti) podgrupa, onda i svaka njena homomorfna slika ispunjava uslov rastućih (opadajućih) lanaca.*



**Korolar 8.15** *Ako normalna podgrupa* $\mathbf{N}$ *grupe* $\mathbf{G}$ *i faktor grupa* $\mathbf{G}/\mathbf{N}$ *ispunjavaju uslov maksimalnosti (minimalnosti) podgrupa (normalnih podgrupa), onda i grupa* $\mathbf{G}$ *ispunjava taj uslov.*

**Dokaz**. Dajemo ga samo za "obične" podgrupe. Dokaz je u osnovi isti i za normalne podgrupe (videti 5.21).

Krenimo od maksimalnosti. Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$. Prema drugoj teoremi o izomorfizmu je $(\mathbf{NH})/\mathbf{N} \cong \mathbf{H}/(\mathbf{H} \cap \mathbf{N})$, pa je $\mathbf{H}/(\mathbf{H} \cap \mathbf{N})$ konačno generisana grupa (jer je svaka podgrupa grupe $\mathbf{G}/\mathbf{N}$ konačno generisana). Podgrupa $\mathbf{H} \cap \mathbf{N}$ je takođe, kao podgrupa grupe $\mathbf{N}$, konačno generisana. No onda je, očigledno, i $\mathbf{H}$ konačno generisana grupa.

Neka sada grupe $\mathbf{N}$ i $\mathbf{G}/\mathbf{N}$ ispunjavaju uslov minimalnosti i neka je $\mathbf{H}_0 > \mathbf{H}_1 > \cdots$ strogo opadajući lanac podgrupa grupe $\mathbf{G}$. Tada je $\mathbf{H}_0 \cap \mathbf{N} \geq \mathbf{H}_1 \cap \mathbf{N} \geq \cdots$ opadajući lanac podgrupa grupe $\mathbf{N}$, pa je, počev od nekog $m$, $\mathbf{H}_m \cap \mathbf{N} = \mathbf{H}_{m+1} \cap \mathbf{N} = \cdots$. Slično, $(\mathbf{H}_0 \cdot \mathbf{N})/\mathbf{N} \geq (\mathbf{H}_1 \cdot \mathbf{N})/\mathbf{N} \geq \cdots$ je opadajući lanac podgrupa faktor grupe $\mathbf{G}/\mathbf{N}$, te je, za neki prirodan broj $n$, $(\mathbf{H}_n \cdot \mathbf{N})/\mathbf{N} = (\mathbf{H}_{n+1} \cdot \mathbf{N})/\mathbf{N} = \cdots$. Ako je $r = max\{m, n\}$, onda je, prema 5.29(*a*), $\mathbf{H}_r = \mathbf{H}_{r+1} = \cdots$.□

**Korolar 8.16** *Neka su* $\mathbf{H}$ *i* $\mathbf{K}$ *normalne podgrupe grupe* $\mathbf{G}$, $\mathbf{K} \leq \mathbf{H}$ *i neka su* $\mathbf{G}/\mathbf{H}$ *i* $\mathbf{H}/\mathbf{K}$ *torziono slobodne grupe. Onda je i* $\mathbf{G}/\mathbf{K}$ *torziono slobodna grupa.*

**Lema 8.17** *Ako je* $\mathbf{H}$ *izolovana normalna podgrupa R-grupe* $\mathbf{G}$ *i ako je* $\mathbf{G}/\mathbf{H}$ *takođe R-grupa, tada postoji uzajamno jednoznačna korespondencija između izolovanih podgrupa grupe* $\mathbf{G}$ *koje sadrže* $\mathbf{H}$ *i izolovanih podgrupa faktor grupe* $\mathbf{G}/\mathbf{H}$.

**Dokaz**. (Jedna) korespondencija je, što se i prirodno očekuje, ona iz 8.7.

Neka je $\mathbf{K}/\mathbf{H}$ izolovana podgrupa grupe $\mathbf{G}/\mathbf{H}$ i neka je, za $a \in G$ i pozitivan prirodan broj $n$, $a^n \in K$. Tada je $a^n H = (aH)^n \in K/H$ pa je i $aH \in K/H$. Stoga je, za neko $b \in K$, $aH = bH$, a odatle je $a \in bH \subseteq K$.

Ako je $\mathbf{H}$ podgrupa izolovane podgrupe $\mathbf{K}$ grupe $\mathbf{G}$ i ako je $(aH)^n = a^n H \in K/H$, onda je, kao maločas, $a^n \in K$, tj. $a \in K$, te je $aH \in K/H$.□

**Lema 8.18** *(Lema Grüna). Ako je* $\mathbf{Z}(\mathbf{G}) \neq \mathbf{E}$ *i* $\mathbf{Z}(\mathbf{G}/\mathbf{Z}(\mathbf{G})) \neq \mathbf{E}$, *tada postoji netrivijalni endomorfizam grupe* $\mathbf{G}$ *koji je preslikava u njen centar.*

**Dokaz**. Neka je $\mathbf{Z}_1 = \mathbf{Z}(\mathbf{G})$, $\mathbf{Z}_2/\mathbf{Z}_1 = \mathbf{Z}(\mathbf{G}/\mathbf{Z}(\mathbf{G}))$ i $a \in Z_2 \setminus Z_1$. Za svako $g \in G$ je $[a, g] \in Z_1$; jer, $(ag)Z_1 = aZ_1 \cdot gZ_1 = gZ_1 \cdot aZ_1 = (ga)Z_1$. Definišimo preslikavanje $\varphi : G \longrightarrow Z_1$ sa: $(g)\varphi = [a, g]$. U pitanju je netrivijalni homomorfizam. Svakako je, za neko $g \in G$, $[a, g] \neq e$ (pošto $a \notin Z_1$). Što se tiče homomorfnosti preslikavanja $\varphi$, imamo (zbog $[x, a^{-1}] = [a^{-1}, x]^{-1} \in Z_1$ za svako $x$):

$$(g)\varphi \cdot (h)\varphi = [a, g] \cdot [a, h] = a^{-1}g^{-1}ag \cdot a^{-1}h^{-1}ah = a^{-1} \cdot [g, a^{-1}] \cdot h^{-1}ah =$$

$$a^{-1}h^{-1}\cdot[g,a^{-1}]\cdot ah = a^{-1}h^{-1}\cdot g^{-1}aga^{-1}\cdot ah = a^{-1}(gh)^{-1}a(gh) =$$
$$[a,gh] = (gh)\varphi.\square$$

**Lema 8.19** *Ako je* $\mathbf{G}$ *neabelova grupa, faktor grupa* $\mathbf{G/Z(G)}$ *nije unija rastućeg lanca cikličnih grupa; posebno,* $\mathbf{G/Z(G)}$ *nije ciklična grupa.*

**Dokaz.** Neka je $\mathbf{G}$ neabelova grupa i neka je $\mathbf{G/Z(G)} = \bigcup_{\alpha<\lambda}\mathbf{H}_\alpha/\mathbf{Z(G)}$, gde je, za $\alpha<\lambda$, $\mathbf{H}_\alpha/\mathbf{Z(G)}$ ciklična grupa i ako je $\alpha<\beta$ onda je $\mathbf{H}_\alpha/\mathbf{Z(G)} \leq \mathbf{H}_\beta/\mathbf{Z(G)}$. Ako je $\mathbf{H}_\alpha/\mathbf{Z(G)} = \langle g_\alpha Z(\mathbf{G})\rangle$, tada je $\mathbf{H}_\alpha = \langle Z(\mathbf{G})\cup\{g_\alpha\}\rangle$ i, jasno, $\mathbf{H}_\alpha$ je Abelova grupa. Kako je $\mathbf{G} = \bigcup_{\alpha<\lambda}\mathbf{H}_\alpha$, proizilazi da je i $\mathbf{G}$ Abelova grupa, kontradikcija.$\square$

**Korolar 8.20** *Neka je* $p$ *prost broj. Tada važi:*

($a$) *Sve grupe reda* $p^2$ *su Abelove;*

($b$) *Neabelove grupe reda* $p^3$ *imaju centar reda* $p$.

**Dokaz.** Direktna posledica prethodne leme i 4.13.$\square$

**Lema 8.21** *Za svaku grupu* $\mathbf{G}$ *važi*

$$\mathbf{G/Z(G)} \cong \mathbf{Inn(G)}.$$

**Dokaz.** Preslikavanje $\psi : a \longrightarrow u_a$, gde je, podsećamo, $(g)u_a = g^{-1}ag$, homomorfno je preslikavanje grupe $\mathbf{G}$ na grupu $\mathbf{Inn(G)}$ (videti 2.10($b$)), a jezgro tog homomorfizma je baš $\mathbf{Z(G)}$.$\square$

**Korolar 8.22** *Ako je* $\mathbf{G}$ *neabelova grupa, onda* $\mathbf{Aut(G)}$ *nije ciklična grupa.*

**Dokaz.** Već ga imamo: 8.19 i 8.21, uz asistenciju 7.2($a$).$\square$

**Lema 8.23** *Ako je* $\mathbf{G}$ *grupa bez centra (tj.* $\mathbf{Z(G)} = \mathbf{E}$ *- videti* 3.4($a$)*), onda je centralizator (pod)grupe unutrašnjih automorfizama u grupi automorfizama grupe* $\mathbf{G}$, $\mathbf{C_{Aut(G)}(Inn(G))}$, *jedinična grupa; posebno, grupa* $\mathbf{Aut(G)}$ *je bez centra.*

**Dokaz.** Neka je $\varphi$ ($\in Aut(\mathbf{G})$) element centralizatora podgrupe $\mathbf{Inn(G)}$ u grupi $\mathbf{Aut(G)}$. Onda je, za svako $g\in G$, $\varphi^{-1}\circ u_g\circ\varphi = u_g$, tj. $u_{(g)\varphi} = u_g$. Stoga je, za svako $a\in G$, $g^{-1}\cdot a\cdot g = ((g)\varphi)^{-1}\cdot a\cdot(g)\varphi$, pa je $(g)\varphi\cdot g^{-1}\in Z(\mathbf{G}) = \{e\}$, odnosno $(g)\varphi = g$ i $\varphi = \imath_G$.$\square$

Obrat ovog tvrđenja ne važi. Tako npr. grupa automorfizama Kleinove grupe (2.4($e$)) je grupa permutacija $\mathbf{S}_3$ (videti 2.10($d$)) - svako biunivoko preslikavanje skupa $\{e, a, b, c\}$ sa fiksnom tačkom $e$ je automorfizam), dakle, grupa bez centra.



Konstatujmo uzgred, s obzirom da su, na primer, grupe $\mathbf{S}_3$ i $\mathbf{Aut(S}_3\mathbf{)}$ izomorfne (videti 9.29), da neizomorfne grupe mogu imati izomorfne grupe automorfizama. Drugi jedan takav primer nam daju grupe $\mathbf{Z}$ i $\mathbf{Z}_3$ čije su grupe automorfizama izomorfne sa $\mathbf{Z}_2$. Još mnogo takvih primera možemo lako naći koristeći sledeći stav

**Lema 8.24** $\mathbf{Aut(Z}_n\mathbf{)} \cong \langle\{a \mid 0<a<n,\ (a,n)=1\}, \cdot_n\rangle$ *za svako* $n\geq 1$.

**Dokaz.** Automorfizam grupe $\mathbf{Z}_n$ određen je slikom elementa 1, a to opet mora biti element uzajamno prost sa $n$. Za prirodan broj $a$ koji je manji od $n$ i sa njime uzajamno prost, obeležimo sa $\varphi_a$ funkciju koja preslikava $Z_n$ u $Z_n$, a definisana je sa: $(b)\varphi_a = b\cdot_n a$ (posebno $(1)\varphi_a = a$). Tvrdimo: $\varphi_a$ je automorfizam grupe $\mathbf{Z}_n$.

$\varphi_a$ je "jedan - jedan"; jer ako je $(b)\varphi_a = (c)\varphi_a$, tj. $b\cdot_n a = ba - [\frac{ba}{n}]n = ca - [\frac{ca}{n}]n = c\cdot_n a$, tada je $\frac{(b-c)a}{n} = [\frac{ba}{n}] - [\frac{ca}{n}] \in Z$, pa $n|(b-c)a$, odnosno, zbog $(a,n)=1$, $n|(b-c)$, i (s obzirom da je $0\leq b,c<n$) $b=c$.

$\varphi_a$ je "na", jer jednačina $x\cdot_n a = b$ ima uvek rešenje u $\mathbf{Z}_n$, pošto $a$ ima inverzni ($a^{-1}$) u polugrupi $\langle n, \cdot_n\rangle$ ($x = b\cdot_n a^{-1}\in Z_n$).

$\varphi_a$ je i homomorfizam: $(b+_n c)\varphi_a = (b+_n c)\cdot_n a = b\cdot_n a +_n c\cdot_n a = (b)\varphi_a +_n (c)\varphi_a$ (videti 2.4($a$),($b$)).

No, $\{\varphi_a \mid 1\leq a<n, (a,n)=1\}$ je i skup svih automorfizama grupe $\mathbf{Z}_n$. Slika elementa 1 za ma koji automorfizam mora, već smo rekli, biti generatorni element. Prema tome, ako je $\psi\in Aut(\mathbf{Z}_n)$, onda je $(1)\psi = a$ za neko $a$ uzajamno prosto sa $n$, i, odatle, za svako $b\in Z_n$:

$$(b)\psi = \underbrace{(1+_n\cdots+_n 1)}_{b-puta}\psi = \underbrace{(1)\psi+_n\cdots+_n(1)\psi}_{b-puta} = \underbrace{a+_n\cdots+_n a}_{b-puta} = b\cdot_n a = (b)\varphi_a;$$

Definišimo sada preslikavanje $F : Aut(\mathbf{Z}_n)\longrightarrow\{a \mid a<n, (a,n)=1\}$ sa $(\varphi_a)F = a$. $F$ je, očigledno, dobro definisano i bijektivno preslikavanje, ali i homomorfizam; $(1)(\varphi_a\circ\varphi_b) = (a)\varphi_b = a\cdot_n b$, pa je $\varphi_a\circ\varphi_b = \varphi_{a\cdot_n b}$.$\square$.

Lako se proverava da je npr. $\mathbf{Aut(Z}_8\mathbf{)} \cong \mathbf{Aut(Z}_{12}\mathbf{)}$. Kako je $\mathbf{Aut(Z}_{12}\mathbf{)}$ Kleinova grupa, zaključujemo da grupa automorfizama ciklične grupe nije nužno ciklična.

Ostavljamo kao laku vežbu za proveru:

$$\mathbf{Aut(Z}_3\mathbf{)} \cong \mathbf{Aut(Z}_4\mathbf{)} \cong \mathbf{Aut(Z}_6\mathbf{)} \cong \mathbf{Z}_2,\ \ \mathbf{Aut(Z}_{18}\mathbf{)} \cong \mathbf{Z}_6.$$

Uopšte $\mathbf{Aut(Z}_{2^n}\mathbf{)}$, $n\geq 3$, nije ciklična grupa, jer su elementi $2^n-1$ i $2^{n-1}-1$ grupe $\langle\{k<2^n \mid (k,n)=1\}, \cdot_{2^n}\rangle$ reda 2, dok ciklična grupa parnog reda ima samo jedan element reda 2 (videti 7.2($g$) kao i 10.45($a$),($b$)).

S druge strane važi

**Lema 8.25** *Za prost broj* $p$ *je* $\mathbf{Aut(Z}_p\mathbf{)} \cong \mathbf{Z}_{p-1}$.

**Dokaz.** $\mathbf{Aut}(\mathbf{Z}_p) \cong \langle \{q \mid 0 < q < p\}, \cdot_p \rangle$, a ovo je pak multiplikativna grupa polja $\langle p, +_p, \cdot_p \rangle$. Preostaje da se pozovemo na lemu 19.17.□

Generalno važi

**Lema 8.26** *Za neparan prost broj $p$ je* $\mathbf{Aut}(\mathbf{Z}_{p^n}) \cong \mathbf{Z}_{p^{n-1}(p-1)}$.

**Dokaz.** Prema 8.24, $|Aut(\mathbf{Z}_{p^n})| = |\{a \mid 0 < a < p^n,\ (a,p^n) = 1\}| = \varphi(p^n) = p^{n-1}(p-1)$. Neka je $(0 <)\ b < p$ element grupe $\langle \{a \mid 0 < a < p\},\ (a,p) = 1\}, \cdot_p \rangle$ reda $p-1$ (upravo smo pokazali da je data grupa ciklična). Ako je $m$ red elementa $b$ u grupi $\langle \{a \mid 0 < a < p^n,\ (a,p^n) = 1\}, \cdot_{p^n} \rangle$ ($\cong \mathbf{Aut}(\mathbf{Z}_{p^n})$), onda iz $b^m - [\frac{b^m}{p^n}]p^n = 1$ sledi, posebno, $b^m \equiv 1 (mod\, p)$, pa $p-1$ deli $m$. Stoga je, za $m = l \cdot (p-1)$, $c = b^l$ element reda $p-1$. Uočimo dalje da važi: ako je za cele brojeve $k$ i $q \geq 1$: $k \equiv 1\ (mod\ p^q)$ i $k \not\equiv 1\ (mod\ p^{q+1})$, tada je $k^p \equiv 1\ (mod\ p^{q+1})$ i $k^p \not\equiv 1\ (mod\ p^{q+2})$. Zaista, za neki ceo broj $r$ koji nije deljiv sa $p$ je $k = 1 + rp^q$ i

$$k^p = 1 + \binom{p}{1} rp^q + \binom{p}{2} (rp^q)^2 + \cdots + \binom{p}{p-1} (rp^q)^{p-1} + (rp^q)^p =$$

$$1 + rp^{q+1} + \frac{p-1}{2} r^2 p^{2q+1} + \cdots + r^{p-1} p^{(p-1)q+1} + r^p p^{qp},$$

dakle, za neki ceo broj $s$ je $k^p = 1 + rp^{q+1} + sp^{q+2}$ (zbog $q \geq 1$ je $2q+1, 3q \geq q+2$); primetimo da tvrđenje ne važi za $q = 1$ i $p = 2$. Iz navedenog sledi da je element $d = 1+p$ reda $p^{n-1}$. Pokazujemo to indukcijom. $1+p \equiv 1\ (mod\ p)$ i $1+p \not\equiv 1\ (mod\ p^2)$ implicira $(1+p)^p \equiv 1\ (mod\ p^2)$ i $(1+p)^p \not\equiv 1\ (mod\ p^3)$, i ako je, za svako $1 \leq t < u < n-1$, $(1+p)^{p^t} \equiv 1\ (mod\ p^{t+1})$ i $(1+p)^{p^t} \not\equiv 1\ (mod\ p^{t+2})$, tada je $(1+p)^{p^u} = ((1+p)^{p^{u-1}})^p \equiv 1\ (mod\ p^{u+1})$ i $(1+p)^{p^u} \not\equiv 1\ (mod\ p^{u+2})$. Sada je, naravno:

$$\underbrace{(1+p) \cdot_{p^n} \cdots \cdot_{p^n} (1+p)}_{p^{n-1}-puta} = (1+p)^{p^{n-1}} - [\frac{(1+p)^{p^{n-1}}}{p^n}]p^n =$$

$$1 + vp^n - [\frac{1+vp^n}{p^n}]p^n \text{ (za neki ceo broj } v \text{ koji nije deljiv sa } p) = 1,$$

i za $t < n-1$ (tj. $t+1 < n$):

$$\underbrace{(1+p) \cdot_{p^n} \cdots \cdot_{p^n} (1+p)}_{p^t-puta} = (1+p)^{p^t} - [\frac{(1+p)^{p^t}}{p^n}]p^n =$$

$$1 + zp^{t+1} - [\frac{1+zp^{t+1}}{p^n}]p^n \text{ (za neki ceo broj } z \text{ koji nije deljiv sa } p) \neq 1.$$



Izvodimo konačno: red elementa $cd$ je, zbog $(red(c), red(d)) = (p-1, p^{n-1}) = 1$ i komutativnosti grupe, $p^n(p-1)$, te je $\langle \{a \mid 0 < a < p^n,\ (a,p) = 1\}, \cdot_{p^n} \rangle$ ciklična grupa.

Recimo još: grupa $\mathbf{Aut}(\mathbf{Z}_{2^n})$ je opisana u primeru 10.45($b$); videti i 10.47.□

**Teorema 8.27** *(N/C-teorema). Ako je* $\mathbf{H}$ *podgrupa grupe* $\mathbf{G}$, *onda je faktor grupa* $\mathbf{N(H)/C(H)}$ *izomorfna podgrupi grupe* $\mathbf{Aut(H)}$.

**Dokaz.** Preslikavanje $\psi : N(\mathbf{H}) \longrightarrow Aut(\mathbf{H})$ dato sa (za $a \in N(\mathbf{H})$) $(a)\psi \stackrel{def}{=} u_a|_H$ homomorfno je preslikavanje grupe $\mathbf{N(H)}$ u grupu $\mathbf{Aut(H)}$, a jezgro tog homomorfizma je baš $\mathbf{C(H)}$. Prema tome:

$$\mathbf{N(H)/C(H)} \cong (\mathbf{N(H)})\psi \leq \mathbf{Aut(H)}.\blacksquare$$

**Korolar 8.28** *Ako je* $\mathbf{H}$ *normalna ciklična podgrupa grupe* $\mathbf{G}$ *takva da je* $\mathbf{G/H}$ *prosta neabelova grupa, onda je* $\mathbf{H}$ *centar grupe* $\mathbf{G}$.

**Dokaz.** Podgrupa $\mathbf{H}$ je, kao Abelova, podgrupa svog centralizatora, a ovaj je pak, kao centralizator normalne podgrupe, i sam normalna podgrupa grupe $\mathbf{G}$. Ostaje da se pozovemo na prethodnu teoremu, teoremu 8.7 i lemu 8.24 (i jasno, na ostale uslove korolara).□

# 9 Grupe permutacija

Konačne grupe permutacija su, već smo naglasili u uvodnom delu, i prve formalno "otkrivene" grupe. Rezultat da su alternativne grupe stepena većeg od 4 neabelove proste grupe jedan je od ključnih u teoriji Galois. Dalje, svaka grupa se može utopiti u neku simetričnu grupu. Sve ovo i još mnogo toga drugog čine grupe permutacija interesantnim i korisnim za izučavanje i primenu. Ovde i ovom prilikom samo najosnovnije.

**Definicija 9.1** *Dve permutacije skupa $A$ su disjunktne akko je svaki element iz $A$ fiksna tačka bar jedne od njih.*

Lako se proverava da su disjunktne permutacije permutabilne (s obzirom na kompoziciju preslikavanja).

Neka je $\alpha$ element simetrične grupe $\mathbf{S}_A$ (2.4($e$)). Definišimo na skupu $A$ relaciju $\equiv_\alpha$ sa: $a \equiv_\alpha b$ akko $\exists k \in Z\ \ (a)\alpha^k = b$. Očigledno, $\equiv_\alpha$ je relacija ekvivalencije; njene klase ekvivalencije zvaćemo orbitama. Orbita $\mathcal{O}$ pak određuje preslikavanje $\alpha_{\mathcal{O}} \in S_A$, gde je

$$(a)\alpha_{\mathcal{O}} = \begin{cases} (a)\alpha & a \in \mathcal{O} \\ a & \text{inače.} \end{cases}$$

Jasno, za dve različite orbite $\mathcal{O}_1$, $\mathcal{O}_2$ odgovarajuće permutacije $\alpha_{\mathcal{O}_1}$, $\alpha_{\mathcal{O}_2}$ su disjunktne. Naravno, ako je $|\mathcal{O}| = 1$, onda je $\alpha_{\mathcal{O}} = \imath$. Stoga su za nas od interesa samo orbite kardinalnosti veće od 1. Ako takvih ima konačno mnogo, neka su npr. $\mathcal{O}_1, \ldots, \mathcal{O}_n$ sve takve, tada je $\alpha = \alpha_{\mathcal{O}_0} \circ \cdots \circ \alpha_{\mathcal{O}_n}$. Kada je samo jedna orbita, recimo $\mathcal{O}$, kardinalnosti veće od 1 i uz to još konačna, permutaciju zovemo *ciklusom* ili, preciznije, *r-ciklusom* (odnosno *ciklusom dužine r*) ako je $|\mathcal{O}| = r$. Posebno, ciklus dužine 2 se zove *transpozicija*, dužine 3 *tercet*.

Iz prethodnog sledi

**Lema 9.2** *Svaka konačna permutacija, tj. permutacija koja gotovo sve elemente (sve sem konačno mnogo njih) ostavlja fiksnim, proizvod je disjunktnih ciklusa.*

**Napomena**. Kako se u opštoj priči obično elementi skupa o čijim se permutacija govori označavaju malim latiničnim slovima, a same permutacije malim grčkim slovima, to ćemo često pisati, recimo, $a\alpha$ umesto formalnog $(a)\alpha$.

Ako je $\alpha$ $r$-ciklus i $\mathcal{O} = \{a = a\alpha^0, \ldots, a\alpha^{r-1}\}$ (jasno, $a\alpha^r = a$ - videti narednu lemu) njemu odgovarajuća orbita kardinalnosti $r$, permutaciju $\alpha$ ćemo jednostavno predstaviti sa $(a\ a\alpha \ldots a\alpha^{r-1})$. Tako je npr. $(0\,2\,3) \in S_5$ tercet $\{(0,2),(1,1),(2,3),(3,0),(4,4)\}$. Naravno, iz konteksta će uvek biti jasno o kom je skupu (čiju grupu permutacija posmatramo) reč. Kada se radi o grupama simetrija skupova konačne kardinalnosti $n$, a sve takve su međusobno izomorfne (2.10($d$)), gotovo po pravilu ćemo za predstavnika te klase grupa uzimati grupu $\mathrm{S}_n$.

Uobičajeno je da se permutacija skupa $n$ - $\{(0,a_0),\ldots,(n-1,a_{n-1})\}$ - predstavlja šemom: $\begin{pmatrix} 0 & \ldots & n-1 \\ a_0 & \ldots & a_{n-1} \end{pmatrix}$; jednostavnije je i preglednije, a olakšava i množenje. S obzirom da su elementi domena dati u prirodnom poretku, kodomen proizvoda permutacija $\alpha$ i $\beta$ dobija se tako što se ispišu elementi kodomena permutacije $\beta$ redom kojim ih "očitavaju" elementi kodomena permutacije $\alpha$ (imati u vidu da 0 "očitava" prvi element, 1 drugi itd., kao i da je, po definiciji kompozicije preslikavanja, $a(\alpha \circ \beta) = (a\alpha)\beta$). Ilustrujmo to sledećim primerom: neka je $\alpha = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 1 & 0 \end{pmatrix}$ i $\beta = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 1 & 0 & 2 \end{pmatrix}$; onda je $\alpha \circ \beta = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 1 & 3 \end{pmatrix}$ (drugi element kodomena permutacije $\beta$ je 0, treći 2, prvi 1 i nulti 3).

Koji put se u pojednostavljenju notacije ide još korak dalje, pa se permutacije (skupa $n$) predstavljaju kao uređene $n$-torke elemenata kodomena. Za nas je to neprihvatljivo jer je u koliziji sa navedenim načinom zapisivanja ciklusa kome, zbog 9.2, dajemo prednost.



**Lema 9.3** ($a$) *Ciklus dužine r je reda r;*

($b$) *Red konačne permutacije je prost broj p akko je ona proizvod disjunktnih ciklusa dužine p;*

**Dokaz**. ($a$) Neka je $\alpha = (0 \ldots r-1)$ $r$-ciklus simetrične grupe $\mathrm{S}_A$, $r \subseteq A$ ($A$ može biti i beskonačan skup). Očigledno, $a \neq a\alpha^k$ za $0 < k < r$, $a\alpha^r = a$ i, za $0 \leq m < r$, $(a\alpha^m)\alpha^r = (a\alpha^r)\alpha^m = a\alpha^m$. No zbog nekih kasnijih tvrđenja korisno je uočiti sledeće:

$$i\alpha^k = i +_r k \quad \text{za} \quad 0 \leq i \leq r-1 \ \text{ i } \ k \in Z,$$

i naravno, $a\alpha^k = a$ za $a \notin r$. Pretpostavimo prvo da je $k$ prirodan broj i izvedimo dokaz indukcijom.

Jasno, $i\alpha^0 = i = i +_r 0$ i, za $0 \leq i < r-1$, $i\alpha = i+1 = i +_r 1$, i $(r-1)\alpha = 0 = (r-1) +_r 1$, a iz $i\alpha^k = i +_r k$ sledi: $i\alpha^{k+1} = (i\alpha^k)\alpha = (i +_r k)\alpha = (i +_r k) +_r 1 = i +_r (k +_r 1) = i +_r (k+1)$ $(= i+k+1-[\frac{i+k+1}{r}]r)$.

Ako je pak $-k$ negativan ceo broj i $-k = mr + p$, $0 \leq p < r$, onda je $i\alpha^{-k} = i\alpha^p =$ (prema upravo dokazanom) $i +_r p = i +_r (-k)$.

Prema tome (ponavljamo dokaz leme), $i\alpha^r = i +_r r = i$, a ako je $i\alpha^m = i$, tj. $i + m - [\frac{i+m}{r}]r = i$, onda $r|m$.

($b$) Prema ($a$) i 2.7($d$).□

Recimo još da naš izbor ciklusa ne utiče na opštost razmatranja. Da smo posmatrali ciklus $\beta = (i_0 \ldots i_{r-1})$, račun bi se samo preneo na indekse. Imali bi, dakle, za $m$ iz $r$ i ceo broj $k$, $i_m\beta^k = i_{m+_r k}$.

**Definicija 9.4** *Permutacija $\alpha$ grupe $\mathrm{S}_n$ je regularna akko je ili identično preslikavanje ($\imath_n$) ili ako je bez fiksnih tačaka i proizvod je disjunktnih ciklusa iste dužine.*

**Napomena**. Gornja definicija se može na prirodan način proširiti i na slučaj simetričnih grupa $\mathrm{S}_A$, gde je $A$ neki beskonačan skup:

*permutacija $\alpha$ grupe $\mathrm{S}_A$ je regularna akko je ili identično preslikavanje ili ne ostavlja ni jedan element fiksnim i sve su joj orbite iste kardinalnosti.*

Lako se pokazuje da grupa $\mathrm{S}_A$ ima netrivijalnih regularnih permutacija (videti 9.30; čitaocu ostavljamo za vežbu čisto skupovni dokaz). Naravno, u slučaju kad je $A$ beskonačan skup ne možemo govoriti o proizvodu "odgovarajućih ciklusa" - permutacija determinisanih orbitama.

**Lema 9.5** *Permutacija $\alpha$ grupe $S_n$ je regularna akko je stepen nekog $n$-ciklusa.*

**Dokaz**. Neka je $n = kl$ i neka je $\alpha$ proizvod $l$ ciklusa dužine $k$, recimo:

$$\alpha = (0\,l \ldots (k-1)l)(1\,1+l \ldots 1+(k-1)l) \ldots (l-1\,(l-1)+l \ldots (l-1)+(k-1)l)$$

(izbor je, kao i u 9.3, nebitan; učinjeni nas oslobađa rada sa indeksima). Tada je $\alpha = \beta^l$, gde je $\beta$ $n$-ciklus $(0\,1\ldots kl-1)$. Zaista, ako je $0 \le u \le l-1$ i $0 \le v < k-1$, onda je $(u+vl)\alpha = u+(v+1)l$, ali je i (videti dokaz leme 9.3) $(u+vl)\beta^l = u+vl+l-[\frac{u+vl+l}{n}]\,n = u+(v+1)l$; isto tako: $(u+(k-1)l)\alpha = u$, no i $(u+(k-1)l)\beta^l = u+(k-1)l+l-[\frac{u+(k-1)l+l}{n}]\,n = u+kl-n-[\frac{u}{n}]\,n = u$.

Neka je sada $\alpha = \beta^p$, $\beta = (0\,1\ldots n-1)$ i $0 < p < n$. Ako je $(n,p) = q$ i $n = qr$, $p = qs$, $\alpha$ je proizvod $q$ ciklusa dužine $r$. Konkretno:

$$\alpha = \prod_{k=0}^{q-1}(k\;\; k+p\;\; k+2\cdot_n p \ldots k+(r-1)\cdot_n p).$$

Kao vežbu ostavljamo proveru nekih detalja; recimo da je, za $0 \le u_1, u_2 \le q-1$ i $0 \le v_1, v_2 \le r-1$, $u_1+v_1\cdot_n p = u_2+v_2\cdot_n p$ akko je $u_1 = u_2$ i $v_1 = v_2$, kao i da je $u+v\cdot_n p < n$. Ako je $v < r-1$ imamo:

$$(u+\;v\cdot_n p)\beta^p = (u+\;v\cdot_n p)+_n p =$$

$$u+vp-[\frac{vp}{n}]\,n+p-[\frac{u+vp-[\frac{vp}{n}]\,n+p}{n}]\,n =$$

$$u+(v+1)p-[\frac{u+(v+1)p}{n}]\,n = u+_n(v+1)p = u+_n(v+1)\cdot_n p =$$

$$u+(v+1)\cdot_n p = (u+v\cdot_n p)\alpha$$

(koristili smo $a+_n bc = a+_n(b\cdot_n c)$ i gore navedenu činjenicu: $u+v\cdot_n p < n$).

Posebno je, za $v = r-1$, tj. $v+1 = r$:

$$(v+1)\cdot_n p = r\cdot_n p = rp-[\frac{rp}{n}]\,n = rqs-[\frac{rqs}{rq}]\,rq = rqs-rqs = 0,$$

pa je, opet, $(u+(r-1)\cdot_n p)\beta^p = u = (u+(r-1)\cdot_n p)\alpha$.□

**Korolar 9.6** *Ako je $\alpha$ $r$-ciklus, onda je $\alpha^k$ $(0 \le k \le r-1)$ proizvod $(r,k)$ disjunktnih ciklusa dužine $\frac{r}{(r,k)}$.*

**Dokaz**. Videti dokaz prethodne leme (pravac $\Longleftarrow$).□

**Lema 9.7** *(a) Svaki ciklus je proizvod transpozicija;*

*(b) Svaka konačna permutacija je proizvod transpozicija.*

**Dokaz**. (a) $(0\,1\,2\ldots r-1) = (0\,1)(0\,2)\ldots(0\,r-1)$.

(b) Prema 9.2 i (a).□

**Teorema 9.8** *Permutacije $\alpha$ i $\beta$ (grupe $S_A$) su konjugovani elementi akko se među skupovima orbita relacija $\equiv_\alpha$ i $\equiv_\beta$ može uspostaviti uzajamno jednoznačna korespondencija takva da su odgovarajuće orbite iste kardinalnosti.*



**Dokaz**. U osnovi tvrđenja je sledeća očigledna činjenica: ako je $\beta = \gamma^{-1}\alpha\gamma$ i $a\alpha = b$, onda je $(a\gamma)\beta = b\gamma$.

($\Longrightarrow$) Neka je, za neko $\gamma \in S_A$, $\beta = \gamma^{-1}\alpha\gamma$, i neka je $[a]_\alpha$ orbita relacije $\equiv_\alpha$ određena elementom $a$ ($[a]_\alpha \stackrel{\text{def}}{=} \{a\alpha^k \mid k \in Z\}$). Tada je $|[a]_\alpha| = |[a\gamma]_\beta|$. Zaista, preslikavanje $F : a\alpha^k \longrightarrow (a\gamma)\beta^k$ je biunivoko: ako je $a\alpha^k = a$, onda je $(a\alpha^k)F = (a\gamma)\beta^k = a\gamma(\gamma^{-1}\alpha\gamma)^k = a\gamma$; ako je, s druge strane, $(a\gamma)\beta^m = a\gamma$, tj. $a\gamma(\gamma^{-1}\alpha^m\gamma) = a\gamma$, sledi $(a\alpha^m)\gamma = a\gamma$, i kako je $\gamma$ injektivno, $a\alpha^m = a$.

Očigledno, preslikavanje $\Phi : \{[a]_\alpha \mid a \in A\} \longrightarrow \{[b]_\beta \mid, b \in A\}$, gde je $([a]_\alpha)\Phi \stackrel{\text{def}}{=} [a\gamma]_\beta$, bijektivno je preslikavanje (skupa svih orbita relacije $\equiv_\alpha$ na skup svih orbita relacije $\equiv_\beta$) koje ispunjava uslov teoreme.

($\Longleftarrow$) Pretpostavimo sada da postoji uzajamno jednoznačna korespondencija među skupovima orbita relacija $\equiv_\alpha$ i $\equiv_\beta$ koja vezuje orbite iste kardinalnosti. Neka je $R$ skup reprezenata orbita relacije $\equiv_\alpha$ i neka je, za $a \in R$, $b$ reprezent orbite (relacije $\equiv_\beta$) korespondentne orbiti $[a]_\alpha$. Preslikavanje $\gamma_a$ : $[a]_\alpha \longrightarrow [b]_\beta$ definisano sa $(a\alpha^k)\gamma_a = b\beta^k$ bijektivno je zbog $|[a]_\alpha| = |[b]_\beta|$, pa je $\gamma = \bigcup_{a\in R}\gamma_a \in S_A$, a važi i $\beta = \gamma^{-1}\alpha\gamma$; odista: $(a\alpha^k)(\gamma\beta) = (b\beta^k)\beta = b\beta^{k+1} = (a\alpha^{k+1})\gamma = (a\alpha^k)(\alpha\gamma)$.■

U slučaju konačnih permutacija gornja teorema se jednostavno formuliše:

*permutacije su konjugovane akko imaju istu cikličnu strukturu (to će reći, u njihovom razlaganju na proizvod disjunktnih ciklusa javlja se isti broj ciklusa iste, date, dužine).*

**Primer 9.9** *(a)*

$$(0\;\;1\;2\;\;3\;\;4\;\;5\;\;6\;\;7\;\;8\;\;9\;\;10\;\;11)^8 =$$

$$(0\;\;8\;\;2\cdot_{12}8)(1\;\;1+8\;\;1+2\cdot_{12}8)(2\;\;2+8\;2+2\cdot_{12}8)(3\;\;3+8\;\;3+2\cdot_{12}8) =$$

$$(0\;\;8\;\;4)(1\;\;9\;\;5)(2\;\;10\;\;6)(3\;\;11\;\;7).$$

*(b)*

$$(0\;\;1\;\;2\;\;3\;\;4\;\;5\;\;6\,7\;\;8\;\;9\;\;10\;\;11\;\;12\;\;13\;\;14)^9 =$$

$$(0\;\;1\cdot_{15}9\;\;2\cdot_{15}9\;\;3\cdot_{15}9\;\;4\cdot_{15}9)(1\;\;1+1\cdot_{15}9\;\;1+2\cdot_{15}9\;\;1+3\cdot_{15}9\;\;1+4\cdot_{15}9)\circ$$

$$(2\;\;2+1\cdot_{15}9\;\;2+2\cdot_{15}9\;\;2+3\cdot_{15}9\;\;2+4\cdot_{15}9) =$$

$$(0\;\;9\;\;3\;\;12\;\;6)(1\;\;10\;\;4\;\;13\;\;7)(2\;\;11\;\;5\;\;14\;\;8).$$

*(c) Neka su*

$$\alpha = (0\;\;3\;\;5\;\;7)(6\;\;8\;\;10)(1\;\;9\;\;11)(2\;\;13)$$

*i*

$$\beta = (1\;\;3\;\;6\;\;8)(2\;\;5\;\;7)(4\;\;0\;\;9)(2\;\;14)$$

*permutacije grupe* $S_{15}$*; napominjemo da cikluse dužine* 1 *ne pišemo - u nekim knjigama se to čini, pa bi "puni" oblik permutacije* $\alpha$ *bio*

$$(0\ 3\ 5\ 7)(6\ 8\ 10)(1\ 9\ 11)(2\ 13)(4)(12)(14).$$

*Tada je:*

$$\beta = \gamma_1^{-1}\alpha\gamma_1 = \gamma_2^{-1}\alpha\gamma_2 = \cdots = \gamma_{864}^{-1}\alpha\gamma_{864},$$

*gde je npr.*

$$\gamma_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 1 & 4 & 12 & 3 & 10 & 6 & 2 & 8 & 5 & 0 & 7 & 9 & 11 & 14 & 13 \end{pmatrix};$$

$$\gamma_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 1 & 2 & 12 & 3 & 10 & 6 & 4 & 8 & 0 & 5 & 9 & 7 & 11 & 14 & 13 \end{pmatrix};$$

$$\gamma_3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 8 & 4 & 12 & 1 & 10 & 3 & 2 & 6 & 5 & 0 & 7 & 9 & 11 & 14 & 13 \end{pmatrix}.$$

Dokonim i strpljivim se prepušta da pronađu preostalih 861 "$\gamma$".□

**Napomena.** Nije teško proveriti da ako su permutacije $\alpha$ i $\beta$ grupe $S_n$ proizvod (disjunktnih) $k_1$ ciklusa dužine $r_1, \ldots, k_m$ ciklusa dužine $r_m$ (gde je $r_i \neq r_j$ za $i \neq j$ i $\sum_{i=1}^{m} k_i r_i = n$), tada je $\beta = \gamma^{-1}\alpha\gamma$ za $\prod_{i=1}^{m}(k_i! r_i^{k_i})$ permutacija "gama".

Ako je $|A| > \aleph_0$, onda je, za sve konjugovane elemente $\alpha, \beta$ grupe $S_A$, $|\{\gamma \in S_A \mid \gamma^{-1}\alpha\gamma = \beta\}| = 2^{|A|}$; ako je $|A| = \aleph_0$, kardinalnost skupa $\{\gamma \in S_A \mid \gamma^{-1}\alpha\gamma = \beta\}$ je ili $\aleph_0$ ili $2^{\aleph_0}$.

U daljem, do kraja ovog paragrafa, razmatraćemo neka od osnovnih svojstava grupe $S_n$. Naravno, slučajevi $n = 1$ i $n = 2$ nisu baš interesantni.

**Lema 9.10** *Simetrična grupa* $S_n$ *(*$n \geq 3$*) generisana je svakim od skupova:*
(*a*) $\{(0\,1), (0\,2), \ldots, (0\,n-1)\}$,
(*b*) $\{(0\,1), (0\,1\ldots n-1)\}$.

**Dokaz.** (*a*) Kako je $(i\ j) = (0\ i)(0\ j)(0\ i)$, grupa $\langle\{(0\ 1), \ldots, (0\ n-1)\}\rangle$ sadrži sve transpozicije, dakle i sve permutacije (9.7(*b*)).

(*b*) Prema 9.8 (i 9.3), za $0 \leq k \leq n-2$ imamo:

$$(0\ 1\ldots n-1)^{n-k}(0\ 1)(0\ 1\ldots n-1)^k =$$

$$(0(0\ 1\ldots n-1)^k\ 1(0\ 1\ldots n-1)^k) = (k\ k+1).$$

Čitaocu ostavljamo kao vežbu da gornji rezultat dobije koristeći se samo lemom 9.3.



Sada još samo treba uočiti da transpozicije $(0\ 1), (1\ 2), \ldots, (n-2\ n-1)$ daju sve one iz skupa u tački (*a*); no:

$$(0\ j) = \alpha^{-1}(j-1\ j)\alpha,$$

gde je $\alpha = (j-1\ j-2)(j-2\ j-3)\ldots(2\ 1)(1\ 0)$.□

**Definicija 9.11** *Neka je data permutacija* $\alpha \in S_n$. $\alpha$ *čini inverziju, s obzirom na elemente* $i, j < n$ *akko je* $i < j$ *i* $i\alpha > j\alpha$. *Broj svih inverzija permutacije* $\alpha$ *obeležićemo sa* $I(\alpha)$.

*Permutacija je parna akko je* $I(\alpha)$ *paran broj, u suprotnom je neparna.*

**Primer 9.12** *Permutacija* $\alpha = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix}$ *je parna* ($I(\alpha) = 6$), *dok je permutacija* $\beta = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 0 & 1 \end{pmatrix}$ *neparna* ($I(\alpha) = 9$).

**Lema 9.13** *Permutacije* $\alpha$ *i* $(i\ j)\alpha$ *(grupe* $S_n$*) su suprotne parnosti. Posebno, svaka transpozicija je neparna permutacija.*

**Dokaz.** Neka je $\alpha = \begin{pmatrix} 0 & \ldots & i & \ldots & j & \ldots & n-1 \\ a_0 & \ldots & a_i & \ldots & a_j & \ldots & a_{n-1} \end{pmatrix}$. Razmotrimo sledeće slučajeve: I $j = i+1$; II $j > i+1$.

Slučaj I

$$(i\ i+1)\alpha = \begin{pmatrix} 0 & \ldots & i & i+1 & \ldots & n-1 \\ a_0 & \ldots & a_{i+1} & a_i & \ldots & a_{n-1} \end{pmatrix},$$

pa nije teško uvideti da je

$$I((i\ i+1)\alpha) = \begin{cases} I(\alpha)+1 & \text{ako je } a_i < a_{i+1} \\ I(\alpha)-1 & \text{ako je } a_i > a_{i+1} \end{cases}$$

Slučaj II Ovog puta imamo:

$$(i\ i{+}1)(i{+}1\ i{+}2)\ldots(j{-}2\ j{-}1)(j{-}1\ j)(j{-}1\ j{-}2)\ldots(i{+}2\ i{+}1)(i{+}1\ i)\alpha$$

$$= (i\ j)\alpha = \begin{pmatrix} 0 & \ldots & i & \ldots & j & \ldots & n-1 \\ a_0 & \ldots & a_j & \ldots & a_i & \ldots & a_{n-1} \end{pmatrix},$$

i kako se radi o sukcesivnom množenju sa $2(j-i)-1$ transpozicija tipa $(k\ k{+}1)$, opet proizilazi da su $\alpha$ i $(i\ j)\alpha$ suprotne parnosti.□

U prethodnom primeru je bilo $\beta = (0\,2)\alpha$.

**Korolar 9.14** *Permutacija je parna akko je proizvod parnog broja transpozicija.*

**Dokaz**. Neka je $\alpha$ parna permutacija. Već znamo da je proizvod transpozicija (9.7), recimo $\alpha = \alpha_1 \dots \alpha_m$, gde su $\alpha_i$, $i = 1, \dots, m$, transpozicije. Prema prethodnoj lemi $m-1$ mora biti neparan broj, tj. $m$ mora biti paran broj.

Pravac ($\Longleftarrow$) je jednako tako jasan.□

**Napomena**. Jedna permutacija se može na bezbroj načina predstaviti kao proizvod transpozicija, ono što je fiksno to je parnost odnosno neparnost broja faktora u tim proizvodima. Tako su npr. dve takve prezentacije za permutaciju $\alpha$ iz 9.12:

$$\alpha = (0\ 2)(0\ 4)(0\ 1)(0\ 3) = (1\ 2)(0\ 1)(1\ 2)(0\ 4)(0\ 1)(0\ 3).$$

Prema 9.7 i 9.14 proizilazi odmah i

**Korolar 9.15** *Ciklus dužine $r$ je parna permutacija akko je $r$ neparan broj.*

**Teorema 9.16** *Skup svih parnih permutacija grupe $\mathbf{S}_n$, $n \geq 2$, domen je normalne podgrupe indeksa 2.*

**Dokaz**. Proizvod parnih permutacija je opet parna permutacija (svaka je proizvod parnog broja transpozicija, pa je i nihov proizvod opet proizvod parnog broja transpozicija), te je

$$\mathbf{A}_n \stackrel{\text{def}}{=} \langle \{\alpha \in S_n \mid \alpha \text{ je parna permutacija}\}, \circ \rangle$$

podgrupa grupe $\mathbf{S}_n$. Pošto parnih permutacija ima koliko i neparnih ($\alpha \longrightarrow (0\ 1)\alpha$ je biunivoko preslikavanje skupa parnih permutacija u skup neparnih permutacija), to je $|A_n| = \frac{n!}{2}$, tj. $[\mathbf{S}_n : \mathbf{A}_n] = 2$. Stoga je i $\mathbf{A}_n \lhd \mathbf{S}_n$ (videti 4.4($c$)); primetimo: normalnost podgrupe $\mathbf{A}_n$ proizilazi direktno i prema 9.8 (konjugat transpozicije je opet transpozicija).■

Podgrupu parnih permutacija $\mathbf{A}_n$ grupe $\mathbf{S}_n$ zovemo *alternativnom grupom (stepena $n$)*.

**Lema 9.17** *Za $n \geq 3$ grupa $\mathbf{A}_n$ je generisana skupom svih terceta.*

**Dokaz**. Neka je $\mathbf{H}$ podgrupa generisana skupom svih terceta (njeni elementi su, prema tome, konačni proizvodi terceta). Maločas smo konstatovali da su ciklusi neparne dužine parne permutacije, znači, $\mathbf{H} \leq \mathbf{A}_n$. S druge strane je, zbog $(i\ j)(k\ m) = (i\ j\ k)(k\ i\ m)$ i već viđenog: $(i\ j)(i\ k) = (i\ j\ k)$, i $\mathbf{A}_n \leq \mathbf{H}$.□

**Lema 9.18** ($a$) *Ako je $n$ neparan broj veći od 1, grupa $\mathbf{A}_n$ je generisana skupom*

$$\{(0\ 1 \dots n-1), (0\ 1\ 2)\};$$

($b$) *Ako je $n$ paran broj veći od 2, grupa $\mathbf{A}_n$ je generisana skupom*

$$\{(0\ 1 \dots n-2), (n-3\ n-2\ n-1)\}.$$



**Dokaz**. ($a$) Prema prethodnoj lemi dovoljno je pokazati da podgrupa generisana permutacijama $(0\ 1 \dots n-1)$ i $(0\ 1\ 2)$ sadrži sve tercete. Pretpostavićemo da je $n$ veći od 3 (slučaj $n = 3$ je suviše trivijalan). Uočimo prvo da je za $0 \leq k \leq n-3$:

$$(0\ 1 \dots n-1)^{-k}(0\ 1\ 2)(0\ 1 \dots n-1)^k =$$

$$(0(0\ 1 \dots n-1)^k\ 1(0\ 1 \dots n-1)^k\ 2(0\ 1 \dots n-1)^k) =$$

$$(k\ k+1\ k+2).$$

No kada su nam na raspolaganju svi terceti oblika $(k\ k+1\ k+2)$ (i, naravno, njima inverzni), lako dobijamo i sve ostale; jer, za $1 \leq k \leq n-3$ imamo:

$$\alpha^{-1}(k\ k+1\ k+2)\alpha = (0\ 1\ k+2),$$

gde je

$$\alpha = (k-1\ k+1\ k)(k-2\ k\ k-1)\dots(1\ 3\ 2)(0\ 2\ 1),$$

a

$$(0\ 1\ j)(0\ 1\ k)(0\ j\ 1) = (0\ k\ j),\ j \neq k,\ j,k \geq 2,$$

i

$$(0\ k\ j)(0\ i\ m)(0\ j\ k) = (j\ i\ m),$$

gde su $i, j, k, m$ međusobno različiti elementi skupa $n$ veći od 0.

($b$) Za $2 \leq k \leq n-1$ je:

$$(0\ 1 \dots n-2)^{-k}(n-3\ n-2\ n-1)(0\ 1 \dots n-2)^k =$$

$$((n-3)(0\ 1 \dots n-2)^k\ (n-2)(0\ 1 \dots n-2)^k\ (n-1)(0\ 1 \dots n-2)) =$$

$$((n-3) +_{n-1} k\ (n-2) +_{n-1} k\ n-1) = (k-2\ k-1\ n-1).$$

Dakle, terceti $(0\ 1\ n-1), (1\ 2\ n-1), \dots, (n-3\ n-2\ n-1)$ su tu, a onda i

$$(1\ 2\ n-1)(0\ 1\ n-1) = (0\ 1\ 2)$$

$$(2\ 3\ n-1)(1\ 2\ n-1) = (1\ 2\ 3)$$

$$\vdots$$

$$(n-3\ n-2\ n-1)(n-4\ n-3\ n-1) = (n-4\ n-3\ n-2),$$

pa nastavljamo kao u ($a$).□

**Korolar 9.19** $\mathbf{A}_n$ *je potpuno invarijantna podgrupa i za* $n$ *veće od* 2 *generisana je svakim od skupova terceta:*

$$\{(0\ 1\ 2), (1\ 2\ 3), \ldots, (n-3\ n-2\ n-1)\},$$

$$\{(0\ 1\ 2), (0\ 1\ 3), \ldots, (0\ 1\ n-1)\},$$

$$\{(0\ 1\ n-1), (1\ 2\ n-1), \ldots, (n-3\ n-2\ n-1)\}.$$

*(Ovim, naravno, nije iscrpljen sav "izbor" - videti i komentar uz* 9.39*).*

**Lema 9.20** *Neka je* $n$ *veće od* 2. *Ako normalna podgrupa* $\mathbf{H}$ *grupe* $\mathbf{A}_n$ *sadrži bar jedan tercet, tada je* $\mathbf{H} = \mathbf{A}_n$.

**Dokaz.** Primetimo prvo da u grupi $\mathbf{S}_n$ ciklusa dužine $k$ ima $\frac{V_k^n}{k}$ ($V_k^n$ - broj varijacija bez ponavljanja od $n$ elemenata $k$-te klase), posebno terceta ima $\frac{n(n-1)(n-2)}{3}$. Kako su svi terceti konjugovani, indeks centralizatora (ma kog) terceta je $\frac{n(n-1)(n-2)}{3}$, tj. centralizator je reda $3 \cdot (n-3)!$.

Pretpostavimo sada da je $\mathbf{H} \lhd \mathbf{A}_n$, $n \geq 4$ (slučaj $n = 3$ je trivijalan) i $\alpha = (i\ j\ k) \in H$. Prema 9.17 dovoljno je pokazati da $\mathbf{H}$ sadrži sve tercete. Jasno, $\{\gamma^{-1}\alpha\gamma \mid \gamma \in A_n\} \subseteq H$, a $|\{\gamma^{-1}\alpha\gamma \mid \gamma \in A_n\}| = [\mathbf{A}_n : \mathbf{C}_{\mathbf{A}_n}(\alpha)]$ (podsetimo se: $C_{\mathbf{A}_n}(\alpha) = \{\beta \in A_n \mid \beta\alpha = \alpha\beta\} = C(\alpha) \cap A_n$).

Ako je $n > 4$, $\mathbf{C}(\alpha)$ nije podgrupa grupe $\mathbf{A}_n$ jer je $(l\ m) \in C(\alpha) \setminus A_n$, gde $l, m \in n \setminus \{i, j, k\}$. Prema drugoj teoremi o izomorfizmu je

$$(\mathbf{C}(\alpha)\,\mathbf{A}_n)/\mathbf{A}_n \cong \mathbf{C}(\alpha)/(\mathbf{A}_n \cap \mathbf{C}(\alpha)),$$

i kako je $\mathbf{C}(\alpha)\mathbf{A}_n = \mathbf{S}_n$, $|C_{\mathbf{A}_n}(\alpha)| = \frac{|C(\alpha)|}{2}$. Proizilazi:

$$[\mathbf{A}_n : \mathbf{C}_{\mathbf{A}_n}(\alpha)] = [\mathbf{S}_n : \mathbf{C}(\alpha)],$$

pa su svih $\frac{n(n-1)(n-2)}{3}$ terceta u $\mathbf{H}$.

Ako je $n = 4$, $|\mathbf{C}(\alpha)| = 3$ i prema tome: $C(\alpha) = \{\imath, \alpha, \alpha^{-1}\} \subseteq A_4$ i $|\{\gamma^{-1}\alpha\gamma \mid \gamma \in A_4\}| = 4$. No sada u $H$ već imamo pet elemenata (naravno, $\imath \in H$), ali tada je $\mathbf{H} = \mathbf{A}_4$. Ne može, naime, biti $|H| = 6$. Novi tercet u $H$ znači zapravo četiri nova elementa, a ako je pak $(p\ q)(r\ s) \in H$, onda je i $(p\ q\ r)(p\ q)(r\ s)(p\ r\ q) \in H$, tj. $(p\ r)(q\ s) \in H$.□

Iz razmatranja u ovom dokazu sledi direktno

**Korolar 9.21** *Grupa* $\mathbf{A}_4$ *nema podgrupu reda* 6.

**Dokaz.** U $A_4$ od 12 elemenata osam su terceti.□

**Korolar 9.22** *Ako podgrupa* $\mathbf{H}$ *grupe* $\mathbf{S}_n$ *nije ujedno i podgrupa grupe* $\mathbf{A}_n$, *onda ona ima isti broj parnih i neparnih permutacija; posebno,* $\mathbf{H}$ *je podgrupa parnog reda i ima podgrupu indeksa* 2 ($\mathbf{H} \cap \mathbf{A}_n$).



**Napomena**. Dokaz leme 9.20 može biti i znatno kraći.

Neka je $n \geq 5$ i $(i\ j\ k) \in H$. No onda za svaki tercet $(p\ q\ r)$ postoji parna permutacija $\alpha$ takva da je $\alpha^{-1}(i\ j\ k)\alpha = (p\ q\ r)$ ($\in H$). Jer kako imamo na raspolaganju dovoljno elemenata, uvek se permutiranjem, po potrebi, dva elemenata $s, t$ različita od $i, j, k$, može permutacija $\begin{pmatrix} \ldots & i & \ldots & j & \ldots & k & \ldots \\ \ldots & p & \ldots & q & \ldots & r & \ldots \end{pmatrix}$ učiniti parnom.

Iz ovog dokaza ne slede, međutim, direktno i dokazi korolara date leme, stoga ga i nismo stavili u prvi plan.

**Teorema 9.23** *Grupa* $\mathbf{A}_n$ *je prosta za* $n \neq 4$.

**Dokaz**. Slučajevi $n = 1, 2, 3$ su trivijalni. Grupa $\mathbf{A}_4$ ima normalnu (Kleinovu) podgrupu

$$\mathbf{H} = \langle\{\imath, (0\ 1)(2\ 3), (0\ 2)(1\ 3), (0\,3)(1\ 2)\}, \circ\rangle.$$

$\mathbf{H}$ je, štaviše, normalna podgrupa (cele) grupe $\mathbf{S}_4$ - konjugat bilo kog njenog nejediničnog elementa je opet proizvod dve disjunktne transpozicije, a svi takvi proizvodi su u $\mathbf{H}$. Mogli smo i ovako rezonovati (što ipak daje duže rešenje): s obzirom da je $\mathbf{S}_4 = \langle(0\ 1)(0\ 1\ 2\ 3)\rangle$, dovoljno je samo proveriti: $(0\ 1)H = H(0\ 1)$ i $(0\ 1\ 2\ 3)H = H(0\ 1\ 2\ 3)$. Za one lenje, svejedno, dajemo:

$$(0\ 1)H = H(0\ 1) = \{(0\ 1), (2\ 3), (0\ 3\ 1\ 2), (0\ 2\ 1\ 3)\};$$

$$(0\ 1\ 2\ 3)H = H(0\ 1\ 2\ 3) = \{(0\ 1\ 2\ 3), (1\ 3), (0\ 2), (0\ 3\ 2\ 1)\}.$$

Pretpostavimo sada: $\mathbf{E} \neq \mathbf{H} \lhd \mathbf{A}_n$ i $n \geq 5$. Prema 9.20 dovoljno je da pokažemo da $H$ sadrži bar jedan tercet.

Neka je $\imath \neq \alpha \in H$ i $\alpha = \alpha_1 \ldots \alpha_m$, gde su $\alpha_i$, $1 \leq i \leq m$, disjunktni ciklusi dužina, respektivno, $r_i$ ($> 1$) (naravno, moguće je da za $i \neq j$ bude $r_i = r_j$). Ako je $m = 1$ i $r_1 = 3$, gotovi smo. Razmotrimo stoga teže slučajeve.

Neka je jedan ciklus, zašto da to ne bude $\alpha_1$? dužine $\geq 4$; recimo, $\alpha = (0\ 1\ 2\ 3\ldots)\beta$, gde je $\beta$ proizvod ostalih ciklusa, ukoliko ih uopšte ima, ili $\imath$. Tada je

$$(0\ 2\ 1)\alpha(0\ 1\ 2) = (0\ 2\ 1)(0\ 1\ 2\ 3\ldots)\beta(0\ 1\ 2) =$$

$$(0\ 2\ 1)(0\ 1\ 2\ 3\ldots)(0\ 1\ 2)\beta = (1\ 2\ 0\ 3\ldots)\beta \in H,$$

i dalje

$$\alpha^{-1}(1\ 2\ 0\ 3\ldots)\beta = (0\ 1\ 2\ 3\ldots)^{-1}(1\ 2\ 0\ 3\ldots)\beta^{-1}\beta = (0\ 1\ 3) \in H.$$

Preostaje mogućnost da su ciklusi $\alpha_i$, $1 \leq i \leq m$, bilo terceti bilo transpozicije. Ako imamo samo jedan tercet, opet neka to bude $\alpha_1$, onda odmah: $\alpha^2 = \alpha_1^2\beta^2 = \alpha_1^2 \in H$, i ponovo $\mathbf{H} = \mathbf{A}_n$ ($\alpha_1^2$ je, jasno, tercet, a $\beta^2 = \imath$ jer je $\beta$ proizvod disjunktnih transpozicija ili $\imath$). Ako je pak bar dva terceta: $\alpha = (0\ 1\ 2)(3\ 4\ 5)\beta$, sledi:

$$\gamma = (2\ 4\ 3)\alpha(2\ 3\ 4) = (2\ 4\ 3)(0\ 1\ 2)(3\ 4\ 5)(2\ 3\ 4)\beta =$$

$$(0\ 1\ 3)(2\ 5\ 4)\beta \in H$$

i

$$\alpha\gamma = (0\ 1\ 2)(3\ 4\ 5)\beta(0\ 1\ 3)(2\ 5\ 4)\beta =$$

$$(0\ 1\ 2)(3\ 4\ 5)(0\ 1\ 3)(2\ 5\ 4)\beta^2 = (0\ 3\ 2\ 1\ 5)\beta^2 \in H,$$

no ovo nas vraća na prvi slučaj.

Pretpostavimo konačno da su svi ciklusi $\alpha_i$, $1 \leq i \leq m$, transpozicije (jasno, mora ih biti paran broj). Ako ih ima samo dve, npr. $\alpha = (0\ 1)(2\ 3)$, onda je (ne zaboravimo $n \geq 5$):

$$(0\ 4\ 1)\alpha(4\ 0\ 1) = (0\ 4\ 1)(0\ 1)(2\ 3)(0\ 1\ 4) = (1\ 4)(2\ 3) \in H$$

i

$$(0\ 1)(2\ 3)(1\ 4)(2\ 3) = (0\ 1)(1\ 4)(2\ 3)^2 = (0\ 4\ 1) \in H.$$

Na kraju, ako je $\alpha = (0\ 1)(2\ 3)(4\ 5)(6\ 7)\beta$, koristimo:

$$\gamma = (1\ 2)(3\ 4)\alpha(1\ 2)(3\ 4) =$$

$$(1\ 2)(3\ 4)(0\ 1)(2\ 3)(4\ 5)(6\ 7)(1\ 2)(3\ 4)\beta =$$

$$(0\ 2)(1\ 4)(3\ 5)(6\ 7)\beta \in H$$

i

$$\alpha\gamma = (0\ 1)(2\ 3)(4\ 5)(6\ 7)\beta(0\ 2)(1\ 4)(3\ 5)(6\ 7)\beta =$$

$$(0\ 1)(2\ 3)(4\ 5)(0\ 2)(1\ 4)(3\ 5) = (0\ 4\ 3)(1\ 2\ 5) \in H,$$

a ovo implicira, maločas je pokazano, $\mathbf{H} = \mathbf{A}_n$.■

**Napomena.** Čitaocu koji misli da je izborom ciklusa uskraćena opštost diskusije i koji bi prema tome izabrao ciklus $\alpha = (i_0\ i_1\ i_2\ i_3 \ldots)$, skrećemo pažnju da bismo u tom (njegovom) slučaju mogli npr. prvo biunivoko preslikati $n$ u $n$, $\varphi : n \longrightarrow n$ tako da je $(i_k)\varphi = k$ i onda posmatrati u $\mathbf{S}_{(n)\varphi} = \mathbf{S}_n$ podgrupu odgovarajuću (njegovoj) podgrupi $\mathbf{H}$. Onom ko i dalje insistira na ciklusu $(i_0\ i_1\ i_2\ i_3 \ldots)$ preostaje da zameni svuda – ovo se odnosi na ceo dokaz – 0, 1, 2, 3 ... sa $i_0, i_1, i_2, i_3, \ldots$ i prosto račun "prenese na indekse".

**Korolar 9.24** *Ako je $n > 2$ i $n \neq 4$, $\mathbf{A}_n$ je jedina netrivijalna normalna podgrupa grupe $\mathbf{S}_n$.*



**Dokaz.** Upravo smo u grupi $\mathbf{S}_4$ našli dve netrivijalne normalne podgrupe: $\mathbf{A}_4$ i $\mathbf{H} = \langle\{(0\ 1)(2\ 3), (0\ 2)(1\ 3), (0\ 3)(1\ 2)\}, \circ\rangle$ – zapravo, s nešto truda može se pokazati da ih više i nema kao i da je $\mathbf{H}$ jedina netrivijalna normalna podgrupa grupe $\mathbf{A}_4$.

Neka je sada $n > 2$ i $n \neq 4$ i pretpostavimo da je $\mathbf{N}$ prava netrivijalna normalna podgrupe grupe $\mathbf{S}_n$. Prema 8.3, $\mathbf{N} \cap \mathbf{A}_n \lhd \mathbf{A}_n$, i kako je $\mathbf{A}_n$ prosta grupa, ili je $(a)$ $\mathbf{N} \cap \mathbf{A}_n = \mathbf{A}_n$ ili $(b)$ $\mathbf{N} \cap \mathbf{A}_n = \mathbf{E}$. $(a)$ odmah daje $\mathbf{N} = \mathbf{A}_n$ ($\mathbf{A}_n$ je indeksa 2 i prema tome maksimalna). Ako važi $(b)$, onda mora biti $\mathbf{N} = \mathbf{E}$. U suprotnom, $|N| = 2$ (korolar 9.22) i neparna permutacija $(\alpha)$ iz $N$ bila bi permutabilna sa svim elementima grupe $\mathbf{S}_n$ (jer je za svako $\beta$, $\beta^{-1}\alpha\beta = \alpha$) i, s obzirom da je reda 2, proizvod (neparnog broja) disjunktnih transpozicija. No ako je $\alpha = (i\ \ j)\beta$, gde je $\beta$ ili $\imath$ ili proizvod ostalih transpozicija ukoliko ih ima, onda je $(i\ k)\alpha \neq \alpha(i\ k)$ za $k \neq j$.□

**Korolar 9.25** *Za $n \geq 4$, grupa $\mathbf{A}_n$ je bez centra. Za $n \geq 3$, grupa $\mathbf{S}_n$ je bez centra.*

**Korolar 9.26** *Za $n > 4$, $\mathbf{S}_n' = \mathbf{A}_n' = \mathbf{A}_n$;*
$\mathbf{S}_3' = \mathbf{A}_3$, $\mathbf{A}_3' = \mathbf{E}$;
$\mathbf{S}_4' = \mathbf{A}_4$, $\mathbf{A}_4' = \langle\{\imath, (0\ 1)(2\ 3), (0\ 2)(1\ 3), (0\ 3)(1\ 2)\}, \circ\}\rangle$.

**Dokaz.** Direktno sledi iz 5.26 i 9.23. $\mathbf{S}_n$ nije Abelova grupa za $n \geq 3$, a za $n \geq 4$ ni $\mathbf{A}_n$ nije Abelova grupa. Prema tome, $\mathbf{S}_n'$ i $\mathbf{A}_n'$ su minimalne (s obzirom na inkluziju) normalne nejedinične podgrupe čije su faktor grupe komutativne. Faktor grupa $\mathbf{S}_4/\mathbf{A}_4'$ nije komutativna – pošto su $(0\ \ 1)\,A_4'$ i $(0\ \ 1\ \ 2\ \ 3)\,A_4'$ njeni generatorni elementi, dovoljno je samo proveriti da je $(0\ \ 1)\,A_4'\,(0\ \ 1\ \ 2\ \ 3)\,A_4' \neq (0\ \ 1\ \ 2\ \ 3)\,A_4'\,(0\ \ 1)\,A_4'$, tj. $(0\ \ 2\ \ 3)\,A_4' \neq (1\ \ 2\ \ 3)\,A_4'$.□

Iskoristićemo ovom prilikom grupe simetrija da damo primer beskonačne proste grupe (posle će ih biti još).

**Primer 9.27** *Neka je $\mathbf{S}_{\omega,n}$ podgrupa grupe $\mathbf{S}_\omega$ sa domenom $\{\alpha \in S_\omega \mid \forall i \geq n\ (i)\alpha = i\}$. Očigledno je $\mathbf{S}_{\omega,n} \cong \mathbf{S}_n$, a $\bigcup_{n\in\omega}\mathbf{S}_{\omega,n}$ je grupa svih konačnih permutacija skupa $\omega$, dakle i normalna podgrupa grupe $\mathbf{S}_\omega$ (4.4(b)). Neka je, analogno, $\mathbf{A}_{\omega,n}$ podgrupa sa domenom $\{\alpha \in S_{\omega,n} \mid \alpha$ je parna permutacija$\}$ – parnost definišemo kao i u slučaju permutacija konačnog skupa $n$, s obzirom na prirodno uređenje skupa $\omega$; broj inverzija je, naravno, konačan, jer gotovo svi elementi (svi sem konačno mnogo) ostaju fiksnim. Jasno, opet je $\mathbf{A}_{\omega,n} \cong \mathbf{A}_n$, a $\bigcup_{n\in\omega}\mathbf{A}_{\omega,n} = \mathbf{A}_\infty$, tzv. beskonačna alternativna grupa, prosta je grupa generisana skupom svih terceta i normalna je podgrupa grupa $\mathbf{S}_\omega$ i $\bigcup_{n\in\omega}\mathbf{S}_{\omega,n}$. Važi i $[\bigcup_{n\in\omega}\mathbf{S}_{\omega,n} : \mathbf{A}_\infty] = 2$.*

**Dokaz.** $\mathbf{A}_\infty$ je podgrupa indeksa 2 grupe $\bigcup_{n\in\omega}\mathbf{S}_{\omega,n}$ jer je za svako $\alpha \in S_{\omega,n}$ ili $\alpha$ ili $(0\ \ 1)\,\alpha$ element njenog domena. Prema 8.4, $\mathbf{A}_\infty$ je prosta grupa. Vežbe radi dajemo i naredni (duži) dokaz za to.

Neka je $\mathbf{E} \neq \mathbf{N} \lhd \mathbf{A}_\infty$. Kao i u slučaju leme 9.20 (videti napomenu posle 9.22), dovoljno je pokazati da $N$ sadrži bar jedan tercet. Neka je $\alpha$ nejedinični element grupe $\mathbf{N}$ koji nije tercet (u suprotnom, dokaz je već tu). Onda postoji tercet $\beta$ takav da je $\alpha\beta \neq \beta\alpha$; ako je $\alpha = (i\,j\ldots)\gamma$, gde je $\gamma$ proizvod ostalih disjunktnih ciklusa, ukoliko ih ima, ili $\imath$, tada je npr. $(i\ k\ m)\alpha \neq \alpha(i\ k\ m)$ za bilo koji prirodan broj $k$ koji $\alpha$ ostavlja fiksnim i bilo koje $m$ različito od $i$ i $k$. $(\alpha\beta\alpha^{-1} \circ \beta^{-1})$ je element grupe $\mathbf{N}$ različit od jediničnog i kako je proizvod dva terceta "pomera" najviše šest elemenata. Neka je skup elemenata koji se javlja u tercetima $\alpha\beta\alpha^{-1}$ i $\beta^{-1}$ podskup skupa $\{i_0,\ldots,i_5\}$ i neka je $\mathbf{H}$ podgrupa grupe $\mathbf{A}_\infty$ sa domenom $\{\gamma \in A_\omega \mid \forall i \notin \{i_0,\ldots,i_5\}\ (i)\gamma = i\}$. $\mathbf{H}$ je prosta grupa (jer je $\mathbf{H} \cong \mathbf{A}_6$) i pošto je $\mathbf{E} \neq \mathbf{N} \cap \mathbf{H} \lhd \mathbf{H}$, sledi $\mathbf{N} \cap \mathbf{H} = \mathbf{H}$, tj. $\mathbf{H} \leq \mathbf{N}$, te u $N$ imamo tercet.□

**Definicija 9.28** *Grupa* $\mathbf{G}$ *je savršena (kaže se i kompletna) akko je bez centra* ($\mathbf{Z(G)} = \mathbf{E}$) *i ako je* $\mathbf{Aut(G)} = \mathbf{Inn(G)}$ *(svi automorfizmi su unutrašnji).*

Primetimo da je savršena grupa izomorfna sa svojom grupom automorfizama (8.21).

**Teorema 9.29** *Grupa* $\mathbf{S}_n$ *je savršena za* $n \neq 2, 6$.

**Dokaz.** Treba samo da proverimo jednakost grupa $\mathbf{Aut}(\mathbf{S}_n)$ i $\mathbf{Inn}(\mathbf{S}_n)$ (videti 9.25). Prepostavićemo odmah: $2 < n \neq 6$.

Neka je $T_k$, $k \leq \frac{n}{2}$, skup svih proizvoda od $k$ disjunktnih transpozicija. Jasno, $T_k$ je klasa konjugovanih elemenata (9.8) i

$$|T_k| = \frac{1}{k!}\prod_{i=0}^{k-1}\begin{pmatrix} n-2i \\ 2 \end{pmatrix}$$

(delimo sa $k!$ jer je u proizvodu disjunktnih ciklusa nebitan njihov redosled). $\bigcup_{k=1}^{[\frac{n}{2}]} T_k$ je skup svih permutacija reda 2 (9.3($b$)), i ako je $u_\alpha \in Inn(\mathbf{S}_n)$, tada je, za svako $k$, $(T_k)u_\alpha = T_k$; zbog 9.8 je, jasno, $(T_k)u_\alpha \subseteq T_k$; ako je pak $(i_0\ j_0)\ldots(i_{k-1}\ j_{k-1}) \in T_k$, onda je, opet prema 9.8:

$$((i_0\alpha^{-1}\ \ j_0\alpha^{-1})\ldots(i_{k-1}\alpha^{-1}\ \ j_{k-1}\alpha^{-1}))u_\alpha = (i_0\ j_0)\ldots(i_{k-1}\ j_{k-1}).$$

Dokazaćemo prvo da je $(T_1)\Phi = T_1$ za svako $\Phi \in Aut(\mathbf{S}_n)$ i onda odatle izvesti da je $\Phi$ unutrašnji automorfizam. Mi već znamo da je $(T_1)\Phi = T_k$ za neko $k$ (2.9($a$),($c$)). No jednakost

$$\frac{1}{k!}\prod_{i=0}^{k-1}\begin{pmatrix} n-2i \\ 2 \end{pmatrix} = \begin{pmatrix} n \\ 2 \end{pmatrix}$$

tj.

$$(n-2)\ldots(n-2k+2)(n-2k+1) = k!\,2^{k-1}$$



nije moguća za $k \neq 1$ i $n \neq 6$. Zaista, kako je $2k \leq n$, $(n-2)\ldots(n-2k+1) \geq (2k-2)!$ i, za $k \geq 4$, $(2k-2)! > k!\,2^{k-1}$ (dokaz indukcijom), mora biti $k \leq 3$. Za $k = 2$, međutim, jednačina $(n-2)(n-3) = 2!\,2$ nema celobrojna rešenja, a ako je $k = 3$ (znači $n \geq 6$), imamo $(n-2)(n-3)(n-4)(n-5) = 3!\,2^2$ i jedina (celobrojna) rešenja su 1 i 6 ( 24 se na samo jedan način može predstaviti kao proizvod četiri različita faktora: $24 = 4 \cdot 3 \cdot 2 \cdot 1$).

Neka je, dalje, za dato $i < n$ ($n \geq 3$ i $n \neq 6$), $T(i)$ skup svih transpozicija u kojima se javlja $i$. Tada važi: $\forall i \exists_1 j\ (T(i))\Phi = T(j)$. Pokažimo to. Transpozicije se, upravo smo videli, preslikavaju u transpozicije, a ako $(i\ k), (i\ m) \in T(i)$, s obzirom da je $(i\ k)(i\ m) \neq (i\ m)(i\ k)$, a onda i $(i\ k)\Phi\,(i\ m)\Phi \neq (i\ m)\Phi\,(i\ k)\Phi$, moraju slike transpozicija $(i\ k)$ i $(i\ m)$ da imaju zajednički element (u suprotnom bi bile permutabilne). S druge strane, slike elemenata $(i\ k)$, $(i\ m)$ i $(i\ p)$ ne mogu biti, respektivno, transpozicije $(j\ r)$, $(j\ t)$, $(r\ t)$, jer je permutacija $(i\ k)(i\ m)(i\ p) = (i\ k\ m\ p)$ reda 4, a $(j\ r)(j\ t)(r\ t) = (j\ t)$ reda 2. Stoga je, za neko $j$, $(T(i))\Phi \subseteq T(j)$, i po istom rezonu, za neko $k$, $(T(j))\Phi^{-1} \subseteq T(k)$. No, iz $T(i) \subseteq T(k)$ sledi $i = k$, pa je $T(i) = T(j)$.

Iz gornjeg razmatranja proizilazi da je preslikavanje $\varphi : n \longrightarrow n$ dato sa $(i)\varphi = j$ akko $(T(i))\Phi = T(j)$ bijektivno, dakle, $\varphi \in S_n$, i štaviše, $\Phi = u_\varphi$ (setimo se – za $\alpha \in S_n$ je $(\alpha)u_\varphi = \varphi^{-1}\alpha\varphi$). Jer, $(\{(i\ \ j)\})\Phi = (T(i) \cap T(j))\Phi = (T(i))\Phi \cap (T(j))\Phi = T(i\varphi) \cap T(j\varphi) = \{(i\varphi\ \ j\varphi)\} = \{(ij)\}u_\varphi$, tj. $(i\ j)\Phi = (i\ j)u_\varphi$, a onda je i $(\alpha)\Phi = (\alpha)u_\varphi$ za svako $\alpha \in S_n$ (5.5).

Grupa $\mathbf{S}_2$ očigledno nije savršena, a nije ni $\mathbf{S}_6$, što je već teže dokazati. Za to nam nedostaje (bar) jedan spoljašnji (– koji nije unutrašnji) automorfizam. Iz gornje diskusije može se relativno lako naslutiti "kandidat", veći je problem dokazati da on ispunjava uslove koji se pred (svako) izomorfno preslikavanje postavljaju. Već znamo da bi spoljašnji automorfizam, ukoliko postoji, morao preslikati (svaku) transpoziciju u proizvod triju disjunktnih transpozicija. S druge strane, kako je grupa $\mathbf{S}_6$ generisana transpozicijama $(0\ \ 1)$, $(0\ \ 2)$, $(0\ \ 3)$, $(0\ \ 4)$, $(0\ \ 5)$, svaki automorfizam je određen slikama tih transpozicija. S obzirom da je proizvod bilo koje dve od njih tercet, njihove slike ne smeju imati zajedničkih transpozicija. Pokazaćemo da je to, zapravo, i jedino ograničenje. Dalje pratimo [113].

Neka je

$\varphi_1 = (0\ \ 1)(2\ \ 5)(3\ \ 4)$, $\varphi_2 = (0\ \ 2)(1\ \ 3)(4\ \ 5)$, $\varphi_3 = (0\ \ 3)(1\ \ 5)(2\ \ 4)$,
$\varphi_4 = (0\ \ 4)(1\ \ 2)(3\ \ 5)$, $\varphi_5 = (0\ \ 5)(1\ \ 4)(2\ \ 3)$ i $\mathcal{P} = \{\varphi_i \mid i = 1,\ldots,5\}$.

Skup $\mathcal{P}$ je tranzitivan na skupu $6 = \{0,1,2,3,4,5\}$, tj. važi: za svaka dva različita elementa $i, j$ (skupa 6) postoji permutacija u $\mathcal{P}$ koja $i$ preslikava u $j$. Da se ne bismo ponavljali, ubuduće ćemo, kada govorimo o permutacijama iz $\mathcal{P}$, podrazumevati da je indeks bilo koji od elemenata skupa $\{1,2,3,4,5\}$. Jasno, $\varphi_i^2 = \imath$, a za $i \neq j$ je $k\varphi_i \neq k\varphi_j$ (odnosno $k(\varphi_i\varphi_j) \neq k$) i $i\varphi_j \neq j\varphi_i$. Ako je $\varphi_i = (0\ \ i)(j\ \ k)(r\ \ s)$, onda (za $j \neq i$) $\varphi_j$ može biti samo ili

$(0\ j)(i\ r)(k\ s)$ ili $(0\ j)(i\ s)(k\ r)$; u svakom slučaju, $\varphi_i\varphi_j$ je proizvod dva terceta te je reda 3. Stoga je

$$\varphi_i\varphi_j\varphi_i = \varphi_j\varphi_i\varphi_j \tag{1}.$$

Takođe je, za $i \neq j \neq k \neq i$,

$$i\varphi_j \neq j\varphi_k \neq k\varphi_i \tag{2};$$

jer, ako je $i\varphi_j = j\varphi_k = k\varphi_i = p\ (\neq 0,i,j,k)$ i $\{1,2,3,4,5\} = \{i,j,k,p,r\}$, proizilazi da je $q\varphi_r \neq p$ za svako $q \in 6$ $(0\varphi_r = r \neq p,\ i\varphi_r \neq i\varphi_j = p,\ j\varphi_r \neq j\varphi_k = p,\ k\varphi_r \neq k\varphi_i = p,\ r\varphi_r = 0 \neq p,\ p\varphi_r \neq p)$, kontradikcija. Važi i (opet za $i \neq j \neq k \neq i$)

$$\varphi_k(\varphi_i\varphi_j\varphi_i) = (\varphi_i\varphi_j\varphi_i)\varphi_k \tag{3}.$$

Zaista, koristeći po potrebi (1), dobijamo $\varphi_i\varphi_j\varphi_i = (0\ i\varphi_j\varphi_i)(i\ j\varphi_i)(j\ i\varphi_j)$, pa se (bar) jedna (i samo jedna) od datih triju (disjunktnih) transpozicija javlja i u $\varphi_k$. Naime, $\varphi_i$, $\varphi_j$ ne sadrže ni jednu od njih, a ako bi se, za neko $r\ (\neq i,j)$, u $\varphi_r$ javile dve, dakle i sve tri transpozicije, tj. ako bismo imali $\varphi_i\varphi_j\varphi_i = \varphi_r$, onda iz $i\varphi_j\varphi_i = r$ i $i\varphi_j = j\varphi_r$ sledi $i\varphi_j = r\varphi_i = j\varphi_r$, protivno sa (2). Ako sad uzmemo jednostavno da je $\varphi_i\varphi_j\varphi_i = (a\ b)(c\ d)(e\ f)$ i npr. $\varphi_k = (a\ b)(c\ e)(d\ f)$, onda je $(\varphi_i\varphi_j\varphi_i)\varphi_k = \varphi_k(\varphi_i\varphi_j\varphi_i) = (c\ f)(d\ e)$.

Iz $\varphi_i\varphi_j\varphi_i\varphi_k = \varphi_k\varphi_i\varphi_j\varphi_i$ i (1) dobijamo redom:

$$\varphi_j\varphi_i\varphi_k = \varphi_i\varphi_k\varphi_i\varphi_j\varphi_i,\quad \varphi_j\varphi_i\varphi_k = \varphi_i\varphi_k\varphi_j\varphi_i\varphi_j,$$

tj.

$$\varphi_j\varphi_i\varphi_k\varphi_j = \varphi_i\varphi_k\varphi_j\varphi_i \tag{4},$$

a iz (4) i (1), indukcijom po $n$ (ta indukcija nije baš dugačka): ako su $\alpha,\beta,\psi_1,\ldots,\psi_n$ različiti elementi iz $\mathcal{P}$, onda je

$$\alpha\beta\psi_1\ldots\psi_n\alpha = \beta\psi_1\ldots\psi_n\alpha\beta \tag{5}.$$

Slučaj $n = 1$ je baš (4), a uz induktivnu pretpostavku za $n$ izvodimo:

$$\alpha\beta\psi_1\ldots\psi_n\psi_{n+1}\alpha = (\alpha\beta\psi_1\ldots\psi_n\alpha)(\alpha\psi_{n+1}\alpha) =$$

$$(\beta\psi_1\ldots\psi_n\alpha\beta)(\psi_{n+1}\alpha\psi_{n+1}) = (\beta\psi_1\ldots\psi_n\psi_{n+1})(\psi_{n+1}\alpha\beta\psi_{n+1})(\alpha\psi_{n+1}) =$$

$$(\beta\psi_1\ldots\psi_{n+1})(\alpha\beta\psi_{n+1}\alpha)(\alpha\psi_{n+1}) = \beta\psi_1\ldots\psi_{n+1}\alpha\beta.$$

Prema (5) i (1) je $(\alpha\beta\psi_1\ldots\psi_n\alpha)(\alpha\beta) = (\beta\psi_1\ldots\psi_n\alpha\beta)(\alpha\beta)$, tj.

$$\alpha\beta\psi_1\ldots\psi_n\beta = (\beta\psi_1\ldots\psi_n)(\beta\alpha\beta)\beta,$$

odnosno,

$$\alpha\beta\psi_1\ldots\psi_n = \beta\psi_1\ldots\psi_n\beta\alpha \tag{6}.$$



Neka su, konačno, $a_1,\ldots,a_n$ različti elementi skupa $\{1,2,3,4,5\}$, $\alpha,\beta$ disjunktne permutacije iz $\mathbf{S}_6$ i neka je $\Phi : S_6 \longrightarrow S_6$ dato sa:

$$\imath\Phi = \imath,\ (0\ a_i)\Phi = \varphi_{a_i},$$

$$(0\ a_1\ldots a_n)\Phi = \varphi_{a_1}\ldots\varphi_{a_n},$$

$$(a_1\ldots a_n)\Phi = \varphi_{a_n}\varphi_{a_1}\ldots\varphi_{a_n}\overset{(5)}{=}\varphi_{a_1}\ldots\varphi_{a_n}\varphi_{a_1}),$$

$$(\alpha\beta)\Phi = \alpha\Phi\,\beta\Phi.$$

Tada je $\Phi \in Aut(S_6)$, a evo i dokaza. Dobra definisanost je, jasno, ekvivalentna sa uslovima: za disjunktne cikluse $\alpha = (i_1\ldots i_m)$ i $\beta = (j_1\ldots j_n)$ važi:

$(i)$ $(\alpha\beta)\Phi = (\beta\alpha)\Phi$

i

$(ii)$ $\alpha\Phi = (i_1\ldots i_m)\Phi = (i_2\ldots i_1)\Phi$.

$(i)$ Neka $\beta$ ne permutira 0 (u suprotnom polazimo od $\alpha$). Onda je $\beta\Phi = \varphi_{j_n}\varphi_{j_1}\ldots\varphi_{j_n}$, a sukcesivnom primenom (6) lako se izvodi: $(\alpha\beta)\Phi = \alpha\Phi\,\beta\Phi = \beta\Phi\,\alpha\Phi = (\beta\alpha)\Phi$.

$(ii)$ Ako $\alpha$ permutira 0, $\alpha\Phi$ je, po definiciji, jedinstveno. Ako ne, tada je $(i_1\ldots i_m)\Phi = \varphi_{i_m}\varphi_{i_1}\ldots\varphi_{i_m}\overset{(5)}{=}\varphi_{i_1}\varphi_{i_2}\ldots\varphi_{i_m}\varphi_{i_1} = (i_2\ldots i_m\ i_1)\Phi$.

$\Phi$ je i homomorfno preslikavanje. Jasno, dovoljno je pokazati da je $(\gamma\delta)\Phi = (\gamma)\Phi(\delta)\Phi$, gde je $\delta$ transpozicija i $\gamma$ proizvod međusobno disjunktnih ciklusa koji nisu disjunktni sa $\delta$. Razmotrićemo neke moguće slučajeve.

$(a)$ $\gamma = (0\ a_1\ldots a_m)$ i $\delta = (0\ b)$:

$$(\gamma)\Phi(\delta)\Phi = \varphi_{a_1}\ldots\varphi_{a_m}\varphi_b = (0\ a_1\ldots a_m\ b)\Phi = [(0\ a_1\ldots a_m)(0\ b)]\Phi.$$

$(b)$ $\gamma = (0\ a_1\ldots a_m\ c\ b_1\ldots b_n)$ i $\delta = (0\ c)$ $(m,n \geq 0)$:

$$(\gamma)\Phi(\delta)\Phi = \varphi_{a_1}\ldots\varphi_{a_m}\varphi_c\varphi_{b_1}\ldots\varphi_{b_n}\varphi_c\overset{(5)}{=}$$

$$(\varphi_{a_1}\ldots\varphi_{a_m})(\varphi_{b_n}\varphi_c\varphi_{b_1}\ldots\varphi_{b_n}) = (0\ a_1\ldots a_m)\Phi(c\ b_1\ldots b_n)\Phi\overset{(5)}{=}$$

$$[(0\ a_1\ldots a_m)(c\ b_1\ldots b_n)]\Phi = [(0\ a_1\ldots a_m\ c\ b_1\ldots b_n)(0\ c)]\Phi.$$

$(c)$ $\gamma = (0\ a_1\ldots a_m)(c\ b_1\ldots b_n)$, $\delta = (0\ c)$:

$$(\gamma)\Phi(\delta)\Phi = (0\ a_1\ldots a_m)\Phi(c\ b_1\ldots b_n)\Phi(0\ c)\Phi =$$

$$(\varphi_{a_1}\ldots\varphi_{a_m})(\varphi_c\varphi_{b_1}\ldots\varphi_{b_n}\varphi_c)\varphi_c =$$

$$\varphi_{a_1}\ldots\varphi_{a_m}\varphi_c\varphi_{b_1}\ldots\varphi_{b_n} = (0\ a_1\ldots a_m\ c\ b_1\ldots b_n)\Phi =$$

$$[(0\ a_1\ldots a_m)(c\ b_1\ldots b_n)(0\ c)]\Phi = (\gamma\delta)\Phi.$$

$(d)$ $\gamma = (c\ a_1\ldots a_m\ d\ b_1\ldots b_n)$, $\delta = (c\ d)$ $(m,n \geq 0)$:

$$(\gamma)\Phi(\delta)\Phi = (\varphi_c\varphi_{a_1}\ldots\varphi_{a_m}\varphi_d\varphi_{b_1}\ldots\varphi_{b_n}\varphi_c)(\varphi_c\varphi_d\varphi_c) =$$

$$(\varphi_c\varphi_{a_1}\dots\varphi_{a_m})(\varphi_d\varphi_{b_1}\dots\varphi_{b_n}\varphi_d)\overset{(6)}{=}(\varphi_c\varphi_{a_1}\dots\varphi_{a_m})(\varphi_c\varphi_d\varphi_{b_1}\dots\varphi_{b_n}\varphi_d)=$$

$$(\varphi_c\varphi_{a_1}\dots\varphi_{a_m}\varphi_c)(\varphi_d\varphi_{b_1}\dots\varphi_{b_n}\varphi_d)=(c\ a_1\dots a_m)\Phi\,(d\ b_1\dots b_n)\Phi=$$

$$[(c\ a_1\dots a_m)(d\ b_1\dots b_n)]\Phi=[(c\ a_1\dots a_m\ d\ b_1\dots b_n)(c\ d)]\Phi.$$

(e) $\gamma=(c\ a_1\dots a_m)(d\ b_1\dots b_n)$, $\delta=(c\ d)$.

Uočimo prvo da važi:

*ako je* $\varepsilon=(e\ f_1\dots f_m)$ *i* $\eta=(e\ h_1\dots h_n)$, *tada je*:

$$(\varepsilon\,\eta)\Phi=(\varepsilon)\Phi\,(\eta)\Phi \tag{7}.$$

Jer,

$$(\varepsilon)\Phi\,(\eta)\Phi=\varphi_e\varphi_{f_1}\dots\varphi_{f_m}\varphi_e\varphi_e\varphi_{h_1}\dots\varphi_{h_n}\varphi_e=$$

$$\varphi_e\varphi_{f_1}\dots\varphi_{f_m}\varphi_{h_1}\dots\varphi_{h_n}\varphi_e=(e\ f_1\dots f_m\ h_1\dots h_n)\Phi=$$

$$[(e\ f_1\dots f_m)(e\ h_1\dots h_n)]\Phi.$$

Odatle je

$$(\gamma)\Phi\,(\delta)\Phi=(c\ a_1\dots a_m)\Phi\,(d\ b_1\dots b_n)\Phi\,(c\ d)\Phi\overset{(7)}{=}$$

$$(c\ a_1\dots a_m)\Phi\,[(d\ b_1\dots b_n)(c\ d)]\Phi=(c\ a_1\dots a_m)\Phi\,(d\ b_1\dots b_n\ c)\Phi\overset{(7)}{=}$$

$$[(c\ a_1\dots a_m)(c\ d\ b_1\dots b_n)]\Phi=[(c\ a_1\dots a_m)(d\ b_1\dots b_n)(c\ d)]\Phi=(\gamma\,\delta)\Phi.$$

$\Phi$ je bijektivno preslikavanje, jer, naravno, $Ker(\Phi)$ može biti samo ili $S_6$ ili $A_6$ ili $E$ $(=\{\imath\})$. $S_6$ je već definicijom isključeno, a pošto je

$$[(2\ 5)(3\ 4)]\Phi=\varphi_5\varphi_2\varphi_5\varphi_4\varphi_3\varphi_4=(2\ 5)(3\ 4),$$

preostaje samo $Ker(\Phi)=E$.

Iz svega navedenog proizilazi da svako bijektivno preslikavanje skupa transpozicija $\{(0\ 1),(0\ 2),(0\ 3),(0\ 4),(0\ 5)\}$ u skup permutacija koje su proizvodi od po triju disjunktnih transpozicija i koje nemaju zajedničkih transpozicija (takve permutacije će, jasno, zadovoljavati relacije (1) – (6)) određuje jedinstven spoljašnji automorfizam. Kako takvih preslikavanja ima 720, spoljašnjih automorfizama ima koliko i unutrašnjih (8.22), dakle, ukupno 1440, pa je $\mathbf{Inn}(\mathbf{S}_6)$ (normalna) podgrupa grupe $\mathbf{Aut}(\mathbf{S}_6)$ indeksa 2.■

**Teorema 9.30** *(Teorema Cayleya). Svaka grupa* $\mathbf{G}$ *se može utopiti (izomorfno preslikati) u grupu* $\mathbf{S}_G$. *Posebno, ako je* $|G|=n$, *grupa* $\mathbf{G}$ *je izomorfna nekoj podgrupi grupe* $\mathbf{S}_n$.



**Dokaz.** Neka je, za $a\in G$, $d_a: G\longrightarrow G$ preslikavanje definisano sa: $(g)d_a=ga$ ("množenje" zdesna sa $a$). Naravno, $d_a\in S_G$, a preslikavanje $\Phi: G\longrightarrow S_G$, gde je $(a)\Phi\overset{\text{def}}{=}d_a$, injektivni je homomorfizam:

ako je $a\neq b$, onda je $(e)d_a=a\neq b=(e)d_b$, pa je $(a)\Phi=d_a\neq d_b=(b)\Phi$;

za sve elemente $c,d,g$ je $(g)d_{cd}=g(cd)=(gc)d=((g)d_c)d_d=(g)(d_c\circ d_d)$, dakle, $(cd)\Phi=d_{cd}=d_c\circ d_d=(c)\Phi\circ(d)\Phi$.

Recimo još da su sve permutacije $d_a$, $a\in G$, regularne. Jasno, za $a\neq e$, $d_a$ ne ostavlja ni jedan element fiksnim i sve orbite su iste kardinalnosti – $|\langle a\rangle|$. Naime, orbita određena elementom $b$ je baš levi koset $b\langle a\rangle$ ciklične podgrupe $\langle a\rangle$ (imati u vidu: $(b)d_a^k=(b)d_{a^k}=ba^k$).■

**Napomena.** Prethodna teorema je, recimo i to, primer takozvanog *dejstva grupe na skup*; uslediće još dosta njih (poludirektni proizvodi – 13.9, spleteni proizvodi – 14.1 itd.), ali to nećemo posebno isticati. Ukratko, homomorfno preslikavanje $\varphi$ grupe $\mathbf{G}$ u grupu simetrija skupa $X$ – $\mathbf{S}_X$ – je dejstvo grupe $\mathbf{G}$ na skup $X$. Obično se, ukoliko ne postoji mogućnost zabune (jer, naravno, može postojati više dejstava grupe $\mathbf{G}$ na skup $X$), za $g\in G$ i $x\in X$, slika elementa $x$ za permutaciju $(g)\varphi$ obeležava sa $x^g$; dakle, $x^e=x$ i $(x^{g_1})^{g_2}=x^{g_1g_2}$. Dejstvo $\varphi$ je *tranzitivno* akko važi:

$$\forall x,y\in X\,\exists g\in G\ y=x^g,$$

tj. akko je $(\mathbf{G})\varphi$ tranzitivna grupa permutacija skupa $X$ – videti 9.49. U slučaju Cayleyeve teoreme imamo upravo taj slučaj – tačka $(e)$ primera 9.50.

**Korolar 9.31** *Svaka konačna grupa se može utopiti u grupu generisanu sa dva elementa.*

**Dokaz.** Direktno prema 9.30 i 9.10$(b)$. Potpuno uopštenje ovog rezultata je dato u 14.6.□

**Korolar 9.32** *Za svaki pozitivan prirodan broj* $n$ *grupa reda* $4n+2$ *nije prosta.*

**Dokaz.** Neka je data grupa $\mathbf{G}$ reda $4n+2$, $n>0$, i neka je $g$ jedan njen element reda 2 (2.7$(e)$). Pri utapanju $\Phi: G\longrightarrow S_{4n+2}$ slika elementa $g$ će biti, kao što smo videli, regularna permutacija reda 2, dakle proizvod od $2n+1$ disjunktnih transpozicija. Prema tome, podgrupa $(\mathbf{G})\Phi$ grupe $\mathbf{S}_{4n+2}$ sadrži neparnu permutaciju i stoga ima podgrupu $\mathbf{T}$ indeksa 2. $(\mathbf{T})\Phi^{-1}$ je onda podgrupa grupe $\mathbf{G}$ indeksa 2.□

**Korolar 9.33** *Svaka grupa* $\mathbf{G}$ *se može utopiti u grupu u kojoj su svi elementi istog reda konjugovani.*

**Dokaz.** Možemo odmah pretpostaviti da je $\mathbf{G}=\mathbf{G}_0$ neprebrojiva grupa (u suprotnom mogli bismo poći od grupe $\mathbf{G}\times\prod_{\alpha<\aleph_1}\mathbf{Z}^\alpha$, gde je, za svako $\alpha<\aleph_1$,

$\mathbf{Z}^\alpha$ "kopija" aditivne grupe celih brojeva – videti naredni paragraf). Neka je $\Phi_{01}$ "standardno" utapanje grupe $\mathbf{G}_0$ u grupu $\mathbf{S}_{G_0} = \mathbf{G}_1$ ($(g)\Phi_{01} = d_g$ – 9.30). Za svako $g \in G_0$, $d_g$ je, rekli smo, regularna permutacija (neprebrojivog) skupa $G_0$ sa $|G_0|$ orbita kardinalnosti $|\langle g\rangle|$. Stoga su, prema 9.8, slike svih elemenata istog reda grupe $\mathbf{G}_0$ konjugovani elementi u $\mathbf{G}_1$. Neka je, dalje, $\Phi_{12}$ standardno utapanje grupe $\mathbf{G}_1$ u grupu $\mathbf{S}_{G_1} = \mathbf{G}_2$. Opet su slike svih elemenata istog reda grupe $\mathbf{G}_1$ konjugovani elementi u $\mathbf{G}_2$; podsećamo (2.4($d$)): grupa $\mathbf{G}_2$ je reda $2^{|G_1|}$ ($> |G_1|$ – Cantorova teorema). Nastavimo li tako rekurzivno postupak dobićemo niz grupa $\mathbf{G}_0$, $\mathbf{G}_1$, ..., $\mathbf{G}_n$, ..., gde je $\mathbf{G}_{n+1} = \mathbf{S}_{G_n}$, a za $i < j$ je $\Phi_{ij} = \Phi_{i,i+1} \circ \cdots \Phi_{j-1,j}$ utapanje grupe $\mathbf{G}_i$ u grupu $\mathbf{G}_j$. Uzećemo da je $\Phi_{ii} = \imath_{G_i}$. Dakle, $\langle(\omega, \leq), \{\mathbf{G}_i \mid i \in \omega\}, \{\Phi_{ij} \mid i, j \in \omega, i \leq j\}\rangle$ je usmerena familija, a u njenom usmerenom limitu $\mathbf{G}_\infty = \langle G_\infty, \bullet\rangle$ svi elementi istog reda su konjugovani (koristimo notaciju iz leme 3.23). Neka su, recimo, $[a]$ i $[b]$ istog reda, $a \in G_j$, $b \in G_k$ i $j \leq k$. Naravno, $red([a]) = red(a)$. $(a)\Phi_{jk}$ i $b$ su elementi istog reda grupe $\mathbf{G}_k$, pa su $((a)\Phi_{jk})\Phi_{k,k+1} = (a)\Phi_{j,k+1}$ i $(b)\Phi_{k,k+1}$ konjugovani elementi u $\mathbf{G}_{k+1}$. Ako je, za $g \in G_{k+1}$, $g^{-1}(a)\Phi_{j,k+1}g = (b)\Phi_{k,k+1}$, onda je:

$$[b] = [(b)\Phi_{k,k+1}] = [g^{-1}(a)\Phi_{j,k+1}g] = [g]^{-1} \bullet [(a)\Phi_{j,k+1}] \bullet [g] = [g]^{-1} \bullet [a] \bullet [g].\square$$

**Napomena.** Jasno, ko ne voli usmerene limite može jednostavno pretpostaviti u svakom koraku, pozivajući se na lemu prenosa, da je $\mathbf{G}_n$ baš podgrupa grupe $\mathbf{G}_{n+1}$ i onda za rešenje uzeti $\bigcup_{n\in\omega} \mathbf{G}_n$.

**Lema 9.34** *Neka je* $\mathbf{H}$ *podgrupa grupe* $\mathbf{G}$ *indeksa* $\lambda$. *Tada postoji homomorfno preslikavanje* $\Phi : G \longrightarrow S_\lambda$ *sa jezgrom* $\mathbf{Core}(\mathbf{H})$ *(već smo konstatovali* –4.8, *to je najveća normalna podgrupa grupe* $\mathbf{G}$ *sadržana u* $\mathbf{H}$*).*

**Dokaz.** Neka je $K = \{Hg_\alpha \mid \alpha \in \lambda\}$ skup desnih koseta podgrupe $\mathbf{H}$ (fiksirali smo skup reprezenata desnih koseta, tj. desnu transverzalu: $\{g_\alpha \mid \alpha \in \lambda\}$). Definišimo preslikavanje $\Phi : G \longrightarrow S_K$ sa: $(a)\Phi = \varphi_a (\in S_K)$, gde je $(Hg_\alpha)\varphi_a \stackrel{\text{def}}{=} Hg_\alpha a$ ($= Hg_\beta$ za neko $\beta \in \lambda$). $\Phi$ je homomorfizam jer je, očigledno, $\varphi_{ab} = \varphi_a \circ \varphi_b$ ($(Hg_\alpha)ab = (Hg_\alpha a)b = ((Hg_\alpha)\varphi_a)\varphi_b$).

Takođe imamo: $a \in Ker(\Phi)$ akko $\varphi_a = \imath$ akko $Hg_\alpha a = Hg_\alpha$ za svako $\alpha \in \lambda$ akko $g_\alpha a \in Hg_\alpha$ za svako $\alpha \in \lambda$ akko $a \in g_\alpha^{-1}Hg_\alpha$ za svako $\alpha \in \lambda$ akko $a \in \bigcap_{\alpha\in\lambda} g_\alpha^{-1}H\alpha$ akko $a \in \bigcap_{g\in G} g^{-1}Hg = Core(\mathbf{H})$; kod poslednje ekvivalencije koristimo: ako je $g \in Hg_\alpha$, tada je $g = hg_\alpha$ za neko $h$ iz $H$, pa je $g^{-1}Hg = g_\alpha^{-1}h^{-1}Hhg_\alpha = g_\alpha^{-1}Hg_\alpha.\square$

**Korolar 9.35** *(4.19 Drugi put – pojačana verzija). Ako je podgrupa* $\mathbf{H}$ *grupe* $\mathbf{G}$ *konačnog indeksa* $n$, *tada postoji normalna podgrupa grupe* $\mathbf{G}$ *čiji indeks deli* $n!$ *i koja je ujedno i podgrupa grupe* $\mathbf{H}$.

**Dokaz.** Koristimo notaciju iz prethodne leme. Prema prvoj teoremi o izomorfizmu je $\mathbf{G}/\mathbf{Ker}(\Phi) \cong (\mathbf{G})\Phi \leq \mathbf{S}_K \cong \mathbf{S}_n$, a $\mathbf{Ker}(\Phi) \leq \mathbf{H}$.

Čitaocu je, naravno, jasno zašto neki ovu teoremu zovu *n!-teorema.* $\square$



**Korolar 9.36** *Prosta grupa sa podgrupom indeksa* $n > 1$ *izomorfna je podgrupi grupe* $\mathbf{S}_n$, *odnosno, ako joj je red veći od* 2, *podgrupi grupe* $\mathbf{A}_n$.

**Dokaz.** Prema 9.34 i 9.22.$\square$

**Korolar 9.37** *Ako je podgrupa* $\mathbf{H}$ *konačne grupe* $\mathbf{G}$ *indeksa* $p$, *gde je* $p$ *najmanji prost faktor reda grupe* $\mathbf{G}$, *onda je* $\mathbf{H}$ *normalna podgrupa.*

**Dokaz.** Prema 9.34, $|G/Core(\mathbf{H})|$ deli $p!$ ($= |S_p|$). S obzirom na pretpostavku o $p$, $[\mathbf{G} : \mathbf{Core}(\mathbf{H})]$ je ili 1 ili $p$ (ako prost broj $q$ deli $[\mathbf{G} : \mathbf{Core}(\mathbf{H})]$, onda $q$ deli $|G|$, pa $q \geq p$). Jasno, mora biti $[\mathbf{G} : \mathbf{Core}(\mathbf{H})] = p$, te je $\mathbf{H} = \mathbf{Core}(\mathbf{H})$, tj. $\mathbf{H}$ je normalna podgrupa.$\square$

Poseban vid Cayleyeve teoreme je

**Teorema 9.38** *Neka je* $\mathbf{H}$ *podgrupa grupe* $\mathbf{G}$ *i neka je* $K$ *skup svih njenih desnih koseta. Tada je* $\mathbf{G}$ *izomorfna podgrupi grupe* $\mathbf{S}_{H\times K}$ *($H \times K = \{(h, Hg) \mid h \in H, Hg \in K\}$).*

**Dokaz.** Fiksirajmo desnu transverzalu podgrupe $\mathbf{H}$ – $\{g_\alpha \mid \alpha \in \lambda\}$; iz praktičnih razloga uzećemo da je predstavnik koseta $H$, neka je to $g_0$, jedinični element. Prema tome, $K = \{Hg_\alpha \mid \alpha \in \lambda\}$, posebno $|K| = \lambda$. Za $a \in G$ neka je $\theta_a \in S_{H\times K}$ dato sa: $(h, Hg_\alpha)\theta_a = (hh_{\alpha,a}, Hg_\beta)$, gde je $H(g_\alpha a) = Hg_\beta$, a $h_{\alpha,a}$ je element iz $H$ za koji je $g_\alpha a = h_{\alpha,a}g_\beta$. Odmah sledi da je $\theta_a \circ \theta_b = \theta_{ab}$: ako je $Hg_\alpha a = Hg_\beta$ i $Hg_\beta b = Hg_\gamma$, jasno, $Hg_\alpha(ab) = Hg_\gamma$; ako je $g_\alpha a = h_{\alpha,a}g_\beta$, $g_\beta b = h_{\beta,b}g_\gamma$ i $g_\alpha(ab) = h_{\alpha,ab}g_\gamma$, onda je $h_{\alpha,ab}g_\gamma = g_\alpha(ab) = (g_\alpha a)b = h_{\alpha,a}(g_\beta b) = h_{\alpha,a}h_{\beta,b}g_\gamma$, pa je $h_{\alpha,a}h_{\beta,b} = h_{\alpha,ab}$. Stoga je

$$(h, Hg_\alpha)(\theta_a \circ \theta_b) = ((h, Hg_\alpha)\theta_a)\theta_b = (hh_{\alpha,a}, Hg_\beta)\theta_b =$$

$$(hh_{\alpha,a}h_{\beta,b}, Hg_\gamma) = (hh_{\alpha,ab}, Hg_\alpha(ab)) = (h, Hg_\alpha)\theta_{ab}.$$

Dalje, iz $\theta_a = \theta_b$ sledi $a = b$; jer, $(e, H)\theta_a = (e, H)\theta_b$ daje redom: $Ha = Hb = Hg_\alpha$ za neko $\alpha \in \lambda$, i zbog $h_{0,a} = h_{0,b}$, $a = h_{0,a}g_\alpha = h_{0,b}g_\alpha = b$. Zaključujemo da je preslikavanje $\Theta : G \longrightarrow S_{H\times K}$, gde je $(a)\Theta \stackrel{\text{def}}{=} \theta_a$, utapanje grupe $\mathbf{G}$ u grupu $\mathbf{S}_{H\times K}$.$\blacksquare$

Prema notaciji iz ove teoreme imamo dalje

**Korolar 9.39** *Ako je grupa* $\mathbf{G}$ *generisana skupom* $A$, $\mathbf{H}$ *njena podgrupa indeksa* $\lambda$ *i* $K = \{Hg_\alpha \mid \alpha \in \lambda\}$ *skup svih desnih koseta podgrupe* $\mathbf{H}$, *tada je* $\mathbf{H}$ *generisana skupom* $\{h_{\alpha,a} \mid \alpha \in \lambda, a \in A\}$.

*(Teorema Schreiera). Ako je* $\mathbf{G}$ *konačno generisana grupa i ako je* $\mathbf{H}$ *njena podgrupa konačnog indeksa, onda je i* $\mathbf{H}$ *konačno generisana grupa.*

**Dokaz**. Koristimo dokaz prethodne teoreme. Ako je $h \in H$ i $h = a_0 \dots a_k$, $a_i \in A \cup A^{-1}$, onda je

$$(e, H)\theta_h = (e, H)\theta_{a_0 \dots a_k} = (\dots((e, H)\theta_{a_0})\dots)\theta_{a_k} = (h_{0,a_0} h_{\alpha_1,a_1} \dots h_{\alpha_k,a_k}, H),$$

gde je $Ha_0 = Hg_{\alpha_1}$ i uopšte $Hg_{\alpha_r}a_r = Hg_{\alpha_{r+1}}$, $1 \leq r \leq k$, i $g_{\alpha_r}a_r = h_{\alpha_r,a_r}g_{\alpha_{r+1}}$, a $g_0 = e$. Znači, $h = h_{0,a_0}h_{\alpha_1,a_1}\dots h_{\alpha_k,a_k}$. No ako je $a \in A$ i $Hg_\alpha a^{-1} = Hg_\beta$, odnosno $Hg_\alpha = Hg_\beta a$, tada je $g_\alpha a^{-1} = h_{\alpha,a^{-1}}g_\beta$ i $g_\beta a = h_{\beta,a}g_\alpha$. Iz ovih jednakosti sledi $g_\alpha = h_{\alpha,a^{-1}}h_{\beta,a}g_\alpha$, tj. $h_{\alpha,a^{-1}}h_{\beta,a} = e$, te je $h_{\alpha,a^{-1}} = h_{\beta,a}^{-1}$. Stoga je $\{h_{\alpha,a} \mid \alpha \in \lambda, a \in A\}$ generatorni skup grupe $\mathbf{H}$.

Odatle, ako je $\mathbf{H}$ podgrupa indeksa $m$ grupe $\mathbf{G}$ generisane sa $n$ elemenata, onda je $\mathbf{H}$ generisana sa $m \cdot n$ elemenata.□

**Napomena**. Nadovezujući se na poslednju rečenicu dokaza dodajmo: moguće je da podgrupa $\mathbf{H}$ ima i generatorni skup sa manje od $m \cdot n$ elemenata. Ciklične i simetrične grupe (uzeti za $\mathbf{H}$ alternativnu podgrupu – videti 9.18) daju bezbroj takvih primera. Drugi jedan takav slučaj opšteg karaktera je sledeći: ako je $\mathbf{G} = \langle a, b\rangle$, $\mathbf{H} < \mathbf{G}$ i $[\mathbf{G} : \mathbf{H}] = 2$, onda je $\mathbf{H}$ generisana sa tri elementa. Jer, ako npr. $a \notin H$ i ako su $g_0 = e$ i $g_1 = a$ predstavnici koseta podgrupe $\mathbf{H}$, tada je, prema korolaru, $\mathbf{H} = \langle h_{0,a}, h_{1,a}, h_{0,b}, h_{1,b}\rangle$, no $h_{0,a} = e$; $(e, H)\theta_a = (h_{0,a}, Ha)$ implicira $ea = h_{0,a}a$, tj. $h_{0,a} = e$. Ovo razmatranje ilustrujemo i primerom.

Ako u grupi $\mathbf{S}_n$, gde je $n$ neparan broj veći od 1, za generatorne elemente uzmemo $a = (0\,1)$ i $b = (0\,1\dots n-1)$, a za predstavnike koseta podgrupe $\mathbf{A}_n$ $g_0 = \imath$ (identično preslikavanje) i $g_1 = (0\,1)$, sledi da je $\mathbf{A}_n$ generisana sa $(0\,1\,2\dots n-1)$ i $(1\,0\,2\dots n-1)$; reći ćemo samo da je: $h_{0,a} = h_{1,a} = \imath$, $h_{0,b} = b$, $h_{1,b} = (1\,0\,2\dots n-1)$, a potpunu verifikaciju kao i iznalaženje raznih drugih generatornih skupova grupe $\mathbf{A}_n$ ovim putem ostavljamo za vežbu.

Primetimo još da se rezultat O. Schreiera ponovo dokazaje u 23.27.

**Teorema 9.40** *(Teorema M. Halla). Konačno generisana grupa sadrži samo konačno mnogo podgrupa datog konačnog indeksa.*

**Dokaz**. Neka je $\mathbf{G}$ konačno generisana grupa, $\mathbf{A}$ njena podgrupa, $[\mathbf{G} : \mathbf{A}] = n$ i neka su $g_0 = e, g_1, \dots, g_{n-1}$ predstavnici desnih koseta podgrupe $\mathbf{A}$. Prema 9.34, preslikavanje $\Phi_A : G \longrightarrow S_K$, gde je $K = \{A, Ag_1, \dots, Ag_{n-1}\}$ skup desnih koseta podgrupe $\mathbf{A}$, $(g)\Phi_A = \varphi_g$ i $(Ag_i)\varphi_g \stackrel{\text{def}}{=} A(g_i g)$ $(= Ag_j$ za neko $j < n)$, homomorfno je preslikavanje grupe $\mathbf{G}$ u grupu $\mathbf{S}_K$. Neka je $\psi_A$ "prirodna" bijekcija skupa $K$ na skup $n$: $(Ag_i)\psi_A \stackrel{\text{def}}{=} i$. Prema 2.10$(d)$, preslikavanje $\Psi_A : S_K \longrightarrow S_n$ dato sa (za $\alpha \in S_K$): $(\alpha)\Psi_A = \overline{\alpha}$, gde je $(i)\overline{\alpha} \stackrel{\text{def}}{=} ((Ag_i)\alpha)\psi_A$, izomorfizam je grupa $\mathbf{S}_K$ i $S_n$, pa je $\Phi_A \circ \Psi_A$ homomorfno preslikavanje grupe $\mathbf{G}$ u grupu $\mathbf{S}_n$. Ako je i $\mathbf{B}$ $(\neq \mathbf{A})$ podgrupa indeksa $n$, onda je, konstruisano analogno, i $\Phi_B \circ \Psi_B$ homomorfno preslikavanje grupe $\mathbf{G}$ u grupu $\mathbf{S}_n$ (ponovo uzimamo $g_0 = e$ za predstavnika koseta $B$). No $\Phi_A \circ \Psi_A \neq$



$\Phi_B \circ \Psi_B$. Jer ako je $a \in A \setminus B$, tada je $a(\Phi_A \circ \Psi_A) = (\varphi_a)\Psi_A = \overline{\varphi}_a$ i $(0)\overline{\varphi}_a = (0)((a)(\Phi_A \circ \Psi_A)) = ((A)\varphi_a)\psi_A = (A)\psi_A = 0$, ali jasno, zbog $Ba \neq B$, $(0)((a)(\Phi_B \circ \Psi_B)) \neq 0$.

Kako je $\mathbf{G}$ konačno generisana grupa postoji samo konačno mnogo njenih homomorfnih preslikavanja u grupu $\mathbf{S}_n$ (videti 5.5), pa i podgrupa indeksa $n$ može biti samo konačno mnogo.■

Kasnije ćemo pokazati da podgrupa konačno generisane nekomutativne grupe ne mora i sama biti konačno generisana (videti npr. 14.6, 23.28).

**Korolar 9.41** *Ako je $\mathbf{G}$ konačno generisana grupa i $\mathbf{H}$ njena podgrupa konačnog indeksa, onda postoji karakteristična podgrupa $\mathbf{K}$ grupe $\mathbf{G}$ koja je sadržana u $\mathbf{H}$ i konačnog je indeksa.*

**Dokaz**. Neka je $\mathbf{K} = \bigcap\{\mathbf{M} \leq \mathbf{G} \mid [\mathbf{G} : \mathbf{M}] = [\mathbf{G} : \mathbf{H}]\}$. Prema prethodnoj teoremi, familija podgrupa $\{\mathbf{M} \leq \mathbf{G} \mid [\mathbf{G} : \mathbf{M}] = [\mathbf{G} : \mathbf{H}]\}$ je konačna, a prema 3.18 $\mathbf{K}$ je konačnog indeksa. Jasno, $\mathbf{K}$ je i karakteristična podgrupa; uvek je, za svako $\varphi \in Aut(\mathbf{G})$ i svaku podgrupu $\mathbf{N}$, $[\mathbf{G} : \mathbf{N}] = [\mathbf{G} : (\mathbf{N})\varphi]$.□

**Korolar 9.42** *(Teorema Maljceva). Neka je $\mathbf{G}$ konačno generisana grupa takva da je presek svih njenih podgrupa konačnog indeksa jedinična podgrupa $\mathbf{E}$. Tada je svaki "na" endomorfizam grupe $\mathbf{G}$ i automorfizam.*

**Dokaz**. Neka je $\varphi$ surjektivni endomorfizam grupe $\mathbf{G}$. Prema prvoj teoremi o izomorfizmu je $\mathbf{G} = (\mathbf{G})\varphi \cong \mathbf{G}/\mathbf{Ker}(\varphi)$. Stoga, ako $\mathbf{G}$ ima npr. $m$ podgrupa indeksa $n$, onda ih toliko ima i $\mathbf{G}/\mathbf{Ker}(\varphi)$; ako su to, recimo, podgrupe $\mathbf{H}_0/\mathbf{Ker}(\varphi)$, ..., $\mathbf{H}_{m-1}/\mathbf{Ker}(\varphi)$, tada su, zbog $[\mathbf{G} : \mathbf{H}_i] = [\mathbf{G}/\mathbf{Ker}(\varphi) : \mathbf{H}_i/\mathbf{Ker}(\varphi)]$ (videti 8.8), $\mathbf{H}_i$, $i = 0, \dots, m$, sve podgrupe grupe $\mathbf{G}$ indeksa $n$. Proizilazi da je $\mathbf{Ker}(\varphi)$ sadržano u svim podgrupama grupe $\mathbf{G}$ konačnog indeksa, pa je $\mathbf{Ker}(\varphi) = \mathbf{E}$, tj. $\varphi$ je injektivno preslikavanje.□

**Lema 9.43** *Kvadratna matrica dobijena od jedinične permutiranjem kolona je tzv. permutaciona matrica.*

*Neka je $P_n$ skup svih permutacionih matrica formata $n \times n$. Tada je $\langle P_n, \cdot\rangle$ ($\cdot$ – matrično množenje) grupa izomorfna grupi $\mathbf{S}_n$.*

**Dokaz**. Neka je, za $\alpha \in S_n$, $I_\alpha$ $(\in P_n)$ matrica dobijena od jedinične permutiranjem kolona kako "nalaže" $\alpha$ (ako je npr. $i\alpha = j$, onda $i$-ta kolona dolazi na mesto $j$-te – prva kolona je 0-ta kolona, poslednja $(n-1)$-va). Naravno, preslikavanje $\psi : \alpha \longrightarrow I_\alpha$ je bijektivno preslikavanje skupa $S_n$ u skup $P_n$. Uočimo odmah da smo matricu $I_\alpha$ mogli dobiti od jedinične i permutiranjem vrsta "prema" $\alpha^{-1}$; jer ako je $i\alpha = j$, znači $j\alpha^{-1} = i$, onda je u $I_\alpha = [e_{pq}]_{0 \leq p,q \leq n-1}$ $e_{ij} = 1$, no i kada dovedemo $j$-tu vrstu na mesto $i$-te ponovo će u $i$-toj vrsti

$j$-ti element biti 1. Prema tome, slike premutacija $\alpha = \begin{pmatrix} 0 & \dots & n-1 \\ i_0 & \dots & i_{n-1} \end{pmatrix}$ (dakle, $\alpha^{-1} = \begin{pmatrix} i_0 & \dots & i_{n-1} \\ 0 & \dots & n-1 \end{pmatrix}$) i $\beta = \begin{pmatrix} j_0 & \dots & j_{n-1} \\ 0 & \dots & n-1 \end{pmatrix}$ su matrice

$$I_\alpha = \begin{bmatrix} \bar{i}_0 \\ \vdots \\ \bar{i}_{n-1} \end{bmatrix} \quad \text{i} \quad I_\beta = [\bar{j}_0 \dots \bar{j}_{n-1}],$$

gde je, jasno, $\bar{i}_k$ vektor vrsta čiji su svi elementi jednaki 0, osim $i_k$-tog koji je 1, i analogno, $\bar{j}_r$ je vektor kolona čiji su svi elementi 0, osim $j_r$-tog koji je jednak 1. Posao je gotov ako pokažemo da je $I_\alpha \cdot I_\beta = I_{\alpha\beta}$. Pa krenimo:

$$I_\alpha \cdot I_\beta = \begin{bmatrix} \bar{i}_0\bar{j}_0 & \dots & \bar{i}_0\bar{j}_{n-1} \\ \vdots & \ddots & \vdots \\ \bar{i}_{n-1}\bar{j}_0 & \dots & \bar{i}_{n-1}\bar{j}_{n-1} \end{bmatrix}, \quad \bar{i}_p\bar{j}_q = \begin{cases} 0 & i_p \neq j_q \\ 1 & i_p = j_q. \end{cases}$$

Uzmimo npr. da je $i_k = j_r$. Onda je u $k$-toj vrsti matrice $I_\alpha \cdot I_\beta$ 1 na $r$-tom mestu (dok su ostali elementi 0). S druge strane, $k(\alpha\beta) = (k\alpha)\beta = i_k\beta = j_r\beta = r$, pa je i u matrici $I_{\alpha\beta}$ u $k$-toj vrsti 1 na $r$-tom mestu.

Na kraju konstatujmo i to da je permutacija $\alpha$ parna akko $det(I_\alpha) = 1$. Dokaz sledi direktno iz činjenice da je za transpoziciju $\tau$ $det(I_\tau) = -1$ i poznatog svojstva množenja determinanata: $det(AB) = det(A) \cdot det(B)$.□

**Korolar 9.44** *Neka je, za polje* $\mathbf{F}$, $\mathbf{GL}_n(\mathbf{F})$ *grupa čiji je domen skup svih kvadratnih* $(n \times n)$ *regularnih matrica sa elementima iz* $F$ *(operacija je matrično množenje). Tada je grupa* $\mathbf{G}$ *reda* $n$ *izomorfna podgrupi grupe* $\mathbf{GL}_n(\mathbf{F})$.

Podgrupe grupe $\mathbf{S}_A$ zovemo u opštem *grupe permutacija skupa* $A$.

**Definicija 9.45** *Neka je* $\mathbf{G}$ *podgrupa grupe* $\mathbf{S}_A$. *Elementi* $a$ *i* $b$ *skupa* $A$ *su* $\mathbf{G}$*-ekvivalentni, u notaciji* $a \equiv_{\mathbf{G}} b$, *akko je* $a\alpha = b$ *za neko* $\alpha \in G$.

Očigledno, relacija $\mathbf{G}$-ekvivalentnosti je *R.S.T.* relacija (relacija ekvivalencije). Klase ekvivalencije zvaćemo *orbitama* grupe $\mathbf{G}$. Ovo je u saglasnosti sa pojmom orbite koji smo već uveli i koji odgovara slučaju kada je $\mathbf{G}$ ciklična grupa (orbite permutacije $\alpha$ odgovaraju orbitama grupe $\langle\alpha\rangle$).

Za dato $a \in A$ neka je ${}_GH_a \stackrel{\text{def}}{=} \{\alpha \in G \mid (a)\alpha = a\}$. Lako se proverava da je ovaj skup domen podgrupe $\mathbf{G}$ tzv. *stabilizator elementa* $a$ s obzirom na podgrupu $\mathbf{G}$.

Za $\alpha \in G$ neka je ${}_GF_\alpha \stackrel{\text{def}}{=} \{a \in A \mid a\alpha = a\}$.

Ako je $\mathbf{G}$ baš cela grupa simetrija pisaćemo samo $H_a$ odnosno $F_\alpha$.



**Lema 9.46** (*a*) *Za* $n$ *veće od* 1 *je* $\mathbf{H}_{n-1}$ *maksimalna podgrupa indeksa* $n$ *grupe* $\mathbf{S}_n$.

(*b*) $\mathbf{Fr}(\mathbf{S}_n) = \mathbf{E}$.

**Dokaz.** (*a*) Neka je $\mathbf{H}_{n-1} < \mathbf{K} \leq \mathbf{S}_n$. Tada u $K$ imamo ciklus $(a_0 \dots a_k\ n-1)$, $k \geq 0$, $a_i < n-1$; jer, bar jedna permutacija u $K$ ne fisira $n-1$, ona je proizvod disjunktnih ciklusa, u jednom od njih se javlja $n-1$, a drugi su, ukoliko ih ima, iz $H$. Ako je $k = 0$ i $a_0 \neq 0$, onda je $(0\ a_0)(a_0\ n-1)(0\ a_0) = (0\ n-1) \in K$, pa kako je i $(0\ 1), \dots, (0\ n-2) \in K$, $\mathbf{K} = \mathbf{S}_n$ (9.10).[5] Ako je $k \geq 1$, tada je $(a_0\ a_k) \dots (a_0\ a_1)(a_0 \dots a_k\ n-1) = (a_0\ n-1) \in K$ (pošto je $(a_0\ a_k) \dots (a_0\ a_1) \in K$) i opet je $\mathbf{K} = \mathbf{S}_n$.

Konstatujmo još: $H$, $H(0\ n-1)$, ..., $H(n-2\ n-1)$ su svi desni koseti podgrupe $\mathbf{H}$. Jasno, različiti su, jer za $i < j < n-1$ permutacija $(i\ n-1)(j\ n-1) = (i\ j\ n-1)$ nije element podgrupe $\mathbf{H}$. Ako je pak $H\beta \neq H$, $\beta = \beta_1 \dots \beta_r$, $r \geq 1$, gde su $\beta_1, \dots, \beta_r$ disjunktni ciklusi i ako je $\beta_1 = (b_0 \dots b_m\ n-1)$, $m > 1$, onda je, kao i maločas: $H\beta = H\beta_1 = H(b_0\ b_1) \dots (b_0\ b_m)(b_0\ n-1) = H(b_0\ n-1)$.

(*b*) $\mathbf{Fr}(\mathbf{S}_n) \leq \bigcap_{i<n} \mathbf{H}_i = \mathbf{E}$.□

**Lema 9.47** $|\{b \in A \mid a \equiv_{\mathbf{G}} b\}| = [\mathbf{G} : {}_G\mathbf{H}_a]$; *rečima: kardinalnost orbite grupe* $\mathbf{G}$ *određene elementom* $a$ *jednaka je indeksu stabilizatora tog elementa s obzirom na grupu* $\mathbf{G}$.

**Dokaz.** U osnovi dokaz je isti kao u 4.11.

Preslikavanje $\Phi : \{{}_GH_a\,\alpha \mid \alpha \in G\} \longrightarrow \{a\alpha \mid \alpha \in G\}$ dato sa $({}_GH_a\,\alpha)\Phi \stackrel{\text{def}}{=} a\alpha$ bijektivno je.□

Primetimo još: ako je, za neko $\alpha \in G$, $a\alpha = b$, onda je ${}_G\mathbf{H}_b = \alpha^{-1}\,{}_G\mathbf{H}_a\,\alpha$ i, naravno, $|{}_GH_a| = |{}_GH_b|$.

**Korolar 9.48** *Ako je* $A$ *konačan skup i* $\mathbf{G}$ *podgrupa grupe* $\mathbf{S}_A$, *onda je broj orbita grupe* $\mathbf{G}$ $\frac{1}{|G|}\sum_{\alpha\in G} |{}_GF_\alpha|$.

**Dokaz.** Kako je $a \in {}_GF_\alpha$ akko je $\alpha \in {}_GH_a$, u sumi $\sum_{\alpha\in G} |{}_GF_\alpha|$ svaki element $a$ je računat $|{}_GH_a|$-puta, pa su elementi iz klase ekvivalencije $\{b \in A \mid a \equiv_{\mathbf{G}} b\}$ kolektivno računati $([\mathbf{G} : {}_G\mathbf{H}_a] \cdot |{}_GH_a| =)\ |G|$-puta. Prema tome, ako je $N$ broj orbita grupe $\mathbf{G}$, onda je: $N \cdot |G| = \sum_{\alpha\in G} |{}_GF_\alpha|$.□

**Definicija 9.49** *Grupa permutacija* $\mathbf{G}$ *skupa* $A$ *je, za pozitivan prirodan broj* $k$ *kardinalnosti manje od ili jednake kardinalnosti skupa* $A$, $k$*-tostruko tranzitivna grupa stepena* $|A|$ *akko za neku datu* $k$*-torku različitih elemenata iz* $A$ *–* $(a_0, \dots, a_{k-1})$ *– postoje permutacije u* $G$ *koje je, neformalno rečeno, preslikavaju u bilo koju drugu* $k$*-torku različitih elemenata iz* $A$ *(pod tim, jasno, podrazumevamo: za ma koju* $k$*-torku različitih elemenata iz* $A$, $(b_0, \dots, b_{k-1})$,

*postoji $\alpha$ u $G$ tako da je $a_i\alpha = b_i$ za svako $i = 0, \dots, k-1$). Posebno, ako je $k = 1$, grupu $\mathbf{G}$ ćemo jednostavno zvati tranzitivnom.*

*Grupa permutacija $\mathbf{G}$ skupa $A$ je regularna akko je tranzitivna i ako je ${}_GH_a = \{\imath\}$ za svako $a \in A$.*

*Neprazni podskup $B$ skupa $A$ se zove blokom grupe permutacija $\mathbf{G}$ skupa $A$ akko je za svako $\alpha \in G$ ili $B \cap (B)\alpha = \emptyset$ ili $(B)\alpha = B$. Jednoelementni podskupovi i sam skup $A$ su tzv. trivijalni blokovi. Grupa $\mathbf{G}$ je primitivna akko nema netrivijalnih blokova.*

Iz same definicije odmah proizilazi da je red $k$-tostruko tranzitivne grupe stepena $n$ bar $V_k^n = n \dots (n-k+1)$. Osim toga, $k$-tostruko tranzitivna grupa ima zapravo svojstvo da za bilo koje dve $k$-torke $(b_0, \dots, b_{k-1})$, $(c_0, \dots, c_{k-1})$ postoji u njoj permutacija koja preslikava $b_i$ u $c_i$, $i = 0, \dots, k-1$; jer, ako je $a_i\beta = b_i$ i $a_i\gamma = c_i$, onda $\beta^{-1}\gamma$ preslikava $k$-torku $(b_0, \dots, b_{k-1})$ u $(c_0, \dots, c_{k-1})$.

**Primer 9.50** *(a)* $\langle (0\ \ 1 \dots n-1) \rangle$ *je regularna podgrupa grupe $\mathbf{S}_n$, ali nije $k$-tostruko tranzitivna ako je $n \geq 3$ i $k \geq 2$.*

**Dokaz.** Jasno; npr. $0\,(0\ \ 1 \dots n-1)^k = k$ za $0 \leq k \leq n-1$.

Primetimo još: ako je $n$ složen broj, onda data podgrupa nije primitivna. Jer, ako je $n = kr$, $1 < k, r < n$, skup $B = \{0, k, 2k, \dots, (r-1)k\}$ je (netrivijalan) blok. Setimo se da je za $\alpha = (0\ \ 1 \dots n-1)$ i $0 \leq t < n$:

$$(B)\alpha^t = \{0 +_n t,\ k +_n t, \dots, (r-1)k +_n t\}.$$

Sada se lako uočava: ako je $t \in B$, onda je $(B)\alpha^t = B$; u suprotnom, $(B)\alpha^t \cap B = \emptyset$. Npr. $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$ su (netrivijalni) blokovi grupe $\langle (0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11) \rangle$ (podgrupe grupe $\mathbf{S}_n$, $n \geq 12$).

Ako je $n$ prost broj, podgrupa je primitivna. Ovo stoga što ako je npr. $B = \{0, k, \dots\}$ blok, tada zbog $0\alpha^k = k$ i $red(\alpha) = n$ sledi $B = n$; $B \cap (B)\alpha^k \neq \emptyset$ pa je $(B)\alpha^k = B$, ali je $(k)\alpha^k = k +_n k$, $(k)\alpha^{2k} = (k +_n k)\alpha^k = k +_n k +_n k$ itd., a $k$ je (kao uostalom svaki nenula element skupa $n$) generatorni element ciklične grupe $\langle n, +_n \rangle$.

*(b)* $\langle \{\imath, (0\ \ 1)(2\ \ 3), (0\ \ 2)(1\ \ 3), (0\ \ 3)(1\ \ 2)\}, \circ \rangle$ *je regularna podgrupa grupe $\mathbf{S}_4$, ali ne i primitivna - $\{0, 1\}$ je primer netrivijalnog bloka.*

*(c) Za $n \geq 3$ grupa $\mathbf{A}_n$ je jedina prava $(n-2)$-struko tranzitivna podgrupa grupe $\mathbf{S}_n$.*

**Dokaz.** Ako je $(i_0, \dots, i_{n-3})$ bilo koja $(n-2)$-ka različitih elemenata iz $n$, postoji parna permutacija koja preslikava $m$ u $i_m$, $m = 0, \dots, n-3$; naime, ako su $i_{n-2}$ i $i_{n-1}$ preostala dva elementa $(\{i_{n-2}, i_{n-1}\} = n \setminus \{i_0, \dots, i_{n-3}\})$, tada je bilo $\begin{pmatrix} 0 & \dots & n-3 & n-2 & n-1 \\ i_0 & \dots & i_{n-3} & i_{n-2} & i_{n-1} \end{pmatrix}$ bilo $\begin{pmatrix} 0 & \dots & n-3 & n-2 & n-1 \\ i_0 & \dots & i_{n-3} & i_{n-1} & i_{n-2} \end{pmatrix}$ parna permutacija (naravno, ne i obe).



U vezi sa ovim razmatranjem videti i napomenu uz 9.22.

Već smo konstatovali da $(n-2)$-ko tranzitivna podgrupa stepena $n$ mora imati najmanje $n \cdot (n-1) \dots (n-(n-2)+1) = \frac{n!}{2}$ elemenata, a grupa $\mathbf{S}_n$ i nema drugih podgrupa reda $\frac{n!}{2}$; ($\mathbf{A}_n \neq \mathbf{H} < \mathbf{S}_n$ i $|H| = \frac{n!}{2}$ dalo bi: $\mathbf{H} \cap \mathbf{A}_n \lhd \mathbf{A}_n$ i, prema drugoj teoremi o izomorfizmu, $[\mathbf{A}_n : \mathbf{H} \cap \mathbf{A}_n] = 2$, no $\mathbf{A}_4$ nema podgrupu indeksa 2 (9.21), a za $n \neq 4$ $\mathbf{A}_n$ je prosta grupa. Stoga je $\mathbf{A}_n$ i jedina prava $(n-2)$-ko tranzitivna podgrupa.

Recimo još da je $\mathbf{A}_n$ primitivna grupa.

*(d) Ako je $k = n-1, n$, jedina $k$-tostruko tranzitivna grupa stepena $n$ je sama simetrična grupa.*

*(e) Izomorfna slika grupe $\mathbf{G}$ u $\mathbf{S}_G$ je regularna grupa permutacija (videti teoremu 9.30).*

**Lema 9.51** *(a) Ako je $p$ prost broj, tranzitivna podgrupa grupe $\mathbf{S}_p$ koja sadrži (bar) jednu transpoziciju jednaka je celoj grupi;*

*(b) Za svako $n$ dvostruko tranzitivna podgrupa grupe $\mathbf{S}_n$ koja sadrži (bar) jednu transpoziciju jednaka je celoj grupi.*

**Dokaz.** *(a)* Neka je $\mathbf{H}$ tranzitivna podgrupa grupe $\mathbf{S}_p$ koja sadrži transpoziciju $(0\ \ 1)$. Na skupu $\{0, 1, \dots, p-1\}$ definišimo relaciju $\sim$ sa: $i \sim j$ akko $(i\ \ j) \in H$. $\sim$ je relacija ekvivalencije:

refleksivnost i simetričnost su očigledni ($i \sim i \iff \imath \in H$), a ako je $i \sim j$ i $j \sim k$, tj. $(i\ \ j), (j\ \ k) \in H$, onda je i $(j\ \ k)(i\ \ j)(j\ \ k) = (i\ \ k) \in H$, pa je i $i \sim k$.

Konstatujmo dalje da sve klase ekvivalencije imaju isti broj elemenata. Posmatrajmo npr. $[0] = \{k \in \{0, 1, \dots, p-1\} \mid 0 \sim k\}$ i $[i]$. Kako je $\mathbf{H}$ tranzitivna grupa, postoji permutacija $\alpha \in H$ takva da je $0\alpha = i$. No tada je $\alpha|_{[0]}$ bijektivno preslikavanje skupa $[0]$ na skup $[i]$. Zaista:

$$k \in [0] \iff (0\ \ k) \in H \iff \alpha^{-1}(0\ \ k)\alpha \in H \iff (i\ \ k\alpha) \in H \iff k\alpha \in [i].$$

Kardinalnost (svake) klase ekvivalencije deli $p$, pa ili imamo $p$ klasa ekvivalencije sa po jednim elementom ili jednu klasu ekvivalencije sa $p$ elemenata. Prvi slučaj otpada jer je $|[0]| \geq 2$ $(1 \in [0])$, a drugi nam kaže da su svi elementi skupa $p = \{0, 1, \dots, p-1\}$ u relaciji, te su sve transpozicije u $H$ i $\mathbf{H} = \mathbf{S}_p$.

*(b)* Jasno. Ako je $\mathbf{H}$ dvostruko tranzitivna podgrupa grupe $\mathbf{S}_n$, $(0\ \ 1) \in H$ i $0\alpha = i$, $1\alpha = j$ za (neko) $\alpha \in H$, onda je $\alpha^{-1}(0\ \ 1)\alpha = (i\ \ j) \in H$.□

**Teorema 9.52** *Grupa $\mathbf{G}$ reda većeg od $n$ izomorfna je tranzitivnoj podgrupi grupe $\mathbf{S}_n$ ako i samo ako ima podgrupu indeksa $n$ čija nijedna podgrupa različita od jedinične nije normalna u $\mathbf{G}$.*

**Dokaz.** ($\Longleftarrow$) Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$ sa traženim svojstvima. Prema 9.34, preslikavanje $\Phi : a \longrightarrow \varphi_a \in S_K$, gde je $K$ skup desnih koseta podgrupe $\mathbf{H}$ ($K = \{Hg_0, \ldots, Hg_{n-1}\}$) i $(Hg_i)\varphi_a \stackrel{\text{def}}{=} H(g_i a)$, homomorfno je preslikavanje grupe $\mathbf{G}$ u grupu $\mathbf{S}_K$ sa jezgrom $\mathbf{Core}(\mathbf{H})$ ($\leq \mathbf{H}$). Po uslovu je $\mathbf{Ker}(\Phi) = \mathbf{E}$ pa je $\Phi$ bijektivno preslikavanje. Takođe, $\langle\{\varphi_a \mid a \in G\}, \cdot\rangle$ je tranzitivna podgrupa grupe $\mathbf{S}_K$ (npr. $(Hg_i)\varphi_{g_i^{-1}g_j} = Hg_ig_i^{-1}g_j = Hg_j$).

($\Longrightarrow$) Ako je pak $\mathbf{G}$ tranzitivna podgrupa grupe $\mathbf{S}_n$, onda je $\mathbf{H}_0 = \langle\{\alpha \in G \mid 0\alpha = 0\}, \circ\rangle$ njena podgrupa indeksa $n$. Jer, ako su $\alpha_i$, $i = 1, \ldots, n-1$, (proizvoljno izabrane permutacije iz $G$ koje preslikavaju 0 u, respektivno, $1, \ldots, n-1$, tada su $H_0$, $H_0\alpha_1, \ldots, H_0\alpha_{n-1}$ svi desni koseti podgrupe $\mathbf{H}_0$ (u $\mathbf{G}$) - $H_0\alpha_i = H_0\alpha_j$ za $i \neq j$ dalo bi $\alpha_i\alpha_j^{-1} \in H_0$, tj. $0(\alpha_i\alpha_j^{-1}) = 0$, odnosno $i = 0\alpha_i = 0\alpha_j = j$, a ako $\beta \notin H_0$ i $0\beta = k$, onda je $0(\alpha_k\beta^{-1}) = 0$ te je $H_0\alpha_k = H_0\beta$. S obzirom da je $|G| > n$, onda je i $|H_0| > 1$. Neka je $\imath \neq \alpha \in H_0$. Ako je $i\alpha = j$, $i \neq j$ (jasno, $i, j \neq 0$) i ako $\beta \in G$ preslikava $i$ u 0, tada je $0(\beta^{-1}\alpha\beta) = j\beta \neq 0$ i $\beta^{-1}\alpha\beta \notin H_0$; dakle, nijedna podgrupa grupe $\mathbf{H}_0$ različita od jedinične nije normalna u $\mathbf{G}$. Primetimo da ovo proizilazi i iz činjenice da su sve podgrupe $\mathbf{H}_i$, $i = 0, \ldots, n-1$, uzajamno konjugovane (ako je $i\beta = j$, onda je $\beta^{-1}\mathbf{H}_i\beta = \mathbf{H}_j$), a jasno, to su ujedno i podgrupe konjugovane sa $\mathbf{H}_0$.■

**Korolar 9.53** *Red $k$-tostruko tranzitivne grupe $\mathbf{G}$ stepena $n$ je $n \ldots (n-k+1) \cdot m$, gde je $m$ red jedne njene podgrupe koja ostavlja fiksnim $k$ elemenata i koja je ujedno i normalna podgrupa jedne podgrupe reda $k!\,m$.*

**Dokaz.** Prvi deo tvrđenja dokazujemo indukcijom po $k$.

Ako je $k = 1$, tj. ako je $\mathbf{G}$ tranzitivna podgrupa grupe $\mathbf{S}_n$, prema prethodnoj teoremi (i notaciji iz njenog dokaza) važi $|G| = |H_0| \cdot n$ (naravno, u opštem slučaju $\mathbf{H}_0$ može biti jedinična podgrupa - videti npr. 9.45($a$)).

Pretpostavimo dalje da je tvrđenje tačno za $k$ i neka je $\mathbf{G}$ $(k+1)$-struko tranzitivna podgrupa grupe $\mathbf{S}_n$. Upravo smo videli da je $\mathbf{H}_0 = \langle\{\alpha \in G \mid (n-1)\alpha = n-1\}, \circ\rangle$ podgrupa grupe $\mathbf{G}$ indeksa $n$. Pored toga ona je izomorfna $k$-tostrukoj podgrupi stepena $n-1$. Naime, očigledno je preslikavanje $\Psi : H_{n-1} \longrightarrow S_{n-1}$, gde je $(\alpha)\Psi \stackrel{\text{def}}{=} \alpha|_{n-1}$, izomorfizam, a ako su $(i_0, \ldots, i_k)$ i $(j_0, \ldots, j_k)$ bilo koje dve $k$-torke skupa $n-1$, s obzirom da u $G$ imamo permutaciju $\beta$ koja $i_r$ preslikava u $j_r$, $r = 0, \ldots, k$, i $n-1$ u $n-1$, to je $\beta$ u $H_{n-1}$ i $\beta|_{n-1}$ preslikava $i_r$ u $j_r$. Prema induktivnoj pretpostavci je $|H_{n-1}| = |(H_{n-1})\Psi| = (n-1)\ldots[(n-1)-k+1]\cdot m$, gde je $m$ red jedne podgrupe grupe $(\mathbf{H}_{n-1})\Psi$, recimo $\mathbf{K}$, koja ostavlja fiksnim (nekih) $k$ elemenata skupa $n-1$. No onda je $(\mathbf{K})\Psi^{-1}$ podgrupa grupe $\mathbf{H}_{n-1}$, dakle i grupe $\mathbf{G}$, koja ostavlja fiksnim $k+1$ elemenata i $|G| = n \cdot |H_{n-1}| = n \cdot (n-1)\ldots[n-(k+1)+1] \cdot m$.

Neka podgrupa $\mathbf{A}$ reda $m$ $k$-tostruko tranzitivne grupe $\mathbf{G}$ stepena $n$ ostavlja fiksnim $k$ elemenata, npr. $0, \ldots, k-1$, i neka je $\mathbf{B}$ podgrupa grupe $\mathbf{G}$ sa domenom $\{\alpha \in G \mid \alpha|_k \in S_k\}$. Naravno, $\mathbf{A}$ je podgrupa grupe $\mathbf{B}$, štaviše normalna; jer, ako je $\beta \in B$ i $\alpha \in A$, očigledno da i $\beta^{-1}\alpha\beta$ ostavlja fiksnim sve elemente iz $k$. Dalje je, za $\gamma, \delta \in B$: $A\gamma = A\delta$ akko $\gamma\delta^{-1} \in A$ akko $\gamma|_k = \delta|_k$, a pošto je $\mathbf{G}$ $k$-tostruko tranzitivna, za svaku permutaciju $\alpha$ iz $S_k$ postoji permutacija $\beta$ iz $B$ takva da je $\beta|_k = \alpha$; zaključujemo: $[\mathbf{B} : \mathbf{A}] = k!$ i $|B| = k! \cdot m$.□



## 10 Direktni i kartezijanski proizvodi grupa

Proizvodi grupa su (uz traženje podgrupa i homomorfnih slika) jedna od osnovnih i "najpopularnijih" metoda za dobijanje novih grupa od familije datih.

**Definicija 10.1** *Kartezijanski (ili kompletni direktni) proizvod neprazne familije grupa $\{\mathbf{G}_i \mid i \in I\}$ ($I \neq \emptyset$) je grupa sa domenom*

$$\prod_{i\in I} G_i \stackrel{\text{def}}{=} \{f \mid f : I \longrightarrow \bigcup_{i\in I} G_i \;\; i\;\forall i \in I \;\; (i)f \in G_i\}$$

*i operacijom $\cdot$ definisanom sa: $(i)(f \cdot g) = (i)f \cdot_i (i)g$, gde je $\cdot_i$ operacija grupe $\mathbf{G}_i$.*

*Dogovorno, kartezijanski proizvod prazne familije grupa je jedinična grupa (ovo je u skladu sa činjenicom da je $\emptyset^\emptyset = \{\emptyset\}$).*

Jasno, element $e$ za koji važi $\forall i \in I \;\; (i)e = e_i$ (= jedinični element grupe $G_i$) jedinični je element kartezijanskog proizvoda, a $(i)f^{-1} = ((i)f)^{-1}$.

Iz praktičnih razloga ubuduće ćemo indeksni skup $I$ ili indeks $i$ (ili oboje), kad god to kontekst dozvoli, izostavljati.

Kartezijanski proizvod familije grupa $\{\mathbf{G}_i \mid i \in I\}$ obeležavaćemo sa $\prod^c_{i\in I} \mathbf{G}_i$ ili, shodno rečenom, jednostavnije sa $\prod^c_i \mathbf{G}_i$ ili, još jednostavnije, sa $\prod^c \mathbf{G}_i$.

Podgrupu grupe $\prod^c_{i\in I} \mathbf{G}_i$ sa domenom $\{f \in \prod_{i\in I} G_i \mid (i)f = e_i$ za skoro sve (sve sem konačno mnogo) indeksa $i \in I\}$ zovemo *direktnim proizvodom* familije grupa $\{\mathbf{G}_i \mid i \in I\}$, u oznaci $\prod_{i\in I} \mathbf{G}_i$ (koristi se, između ostalog, i $\prod^d_{i\in I} \mathbf{G}_i$).

Naravno, u slučaju kad je skup $I$ konačan kartezijanski i direktni proizvod se podudaraju. Tada ćemo najčešće koristiti i uobičajenu oznaku, npr. $\mathbf{G}_0 \times \mathbf{G}_1$ umesto $\prod_{i\in 2} \mathbf{G}_i$. U cilju pojednostavljenja notacije obeležavaćemo domen direktnog proizvoda sa $\prod^d_{i\in I} G_i$ ili samo sa (prema prethodnoj napomeni) $\prod^d G_i$. Opravdana je primedba da ovde imamo izvesnu nedoslednost u oznakama. S obzirom na domene podgrupa s pravom bi se moglo očekivati da se oznaka $\prod_{i\in I} \mathbf{G}_i$ koristi za kartezijanski proizvod. Ovo se neki put i čini, a onda se direktni proizvod označava sa $\prod^d_{i\in I} \mathbf{G}_i$ ili $\sum_{i\in I} \mathbf{G}_i$. No $\sum$ smo rezervisali za direktni proizvod (sumu) Abelovih grupa, i kako je za našu priču

interesantniji direktni proizvod ostajemo pri ("našoj") uobičajenoj i uveliko standardnoj notaciji.

Za $f \in \prod_{i\in I} G_i$ sa $S(f)$ ćemo označiti skup $\{i \in I \mid (i)f \neq e_i\}$. $S(f)$ zovemo *nosačem* (ili *potporom* – eng. *support*) elementa $f$. Prema tome je $\prod^d_{i\in I} G_i = \{f \in \prod_{i\in I} G_i \mid |S(f)| < \aleph_0\}$.

**Lema 10.2** *Neka se među (nepraznim) familijama grupa* $\{\mathbf{G}_i \mid i \in I\}$ *i* $\{\mathbf{H}_j \mid j \in J\}$ *može uspostaviti uzajamno jednoznačna korespondencija takva da su korespondentne grupe izomorfne. Tada važi:*

$$\prod^c_{i\in I} \mathbf{G}_i \cong \prod^c_{j\in J} \mathbf{H}_j \quad i \quad \prod_{i\in I} \mathbf{G}_i \cong \prod_{j\in J} \mathbf{H}_j.$$

**Dokaz.** Neka je $\varphi$ biunivoko preslikavanje skupa $J$ na skup $I$ takvo da su grupe $\mathbf{H}_j$ i $\mathbf{G}_{(j)\varphi}$ izomorfne i neka je $\psi_{(j)\varphi}$ izomorfno preslikavanje grupe $\mathbf{G}_{(j)\varphi}$ na grupu $\mathbf{H}_j$. Onda je preslikavanje $\Phi : \prod_{i\in I} G_i \longrightarrow \prod_{j\in J} H_j$ dato sa (za $f \in \prod_{i\in I} G_i$):

$$(j)((f)\Phi) \stackrel{\text{def}}{=} (((j)\varphi)f)\psi_{(j)\varphi}$$

izomorfno preslikavanje grupe $\prod^c_{i\in I} \mathbf{G}_i$ na grupe $\prod^c_{j\in J} \mathbf{H}_j$, a njegova restrikcija na skup $\prod^d_{i\in I} G_i$ je izomorfno preslikavanje grupe $\prod_{i\in I} \mathbf{G}_i$ na grupu $\prod_{j\in J} \mathbf{H}_j$. Proverićemo samo svojstvo homomorfnosti.

Neka je $f, g \in \prod_{i\in I} G_i$. Tada je (za svako $j \in J$):

$$(j)((f \cdot g)\Phi) = (((j)\varphi)(f \cdot g))\psi_{(j)\varphi} = (((j)\varphi)f \cdot_{(j)\varphi} ((j)\varphi)g)\psi_{(j)\varphi} =$$

$$(((j)\varphi)f)\psi_{(j)\varphi} \cdot_j (((j)\varphi)g)\psi_{(j)\varphi} = (j)((f)\Phi) \cdot_j (j)((g)\Phi) = (j)((f)\Phi \cdot (g)\Phi)$$

pa je $(f \cdot g)\Phi = (f)\Phi \cdot (g)\Phi$ (jasno, $\cdot_{(j)\varphi}$ i $\cdot_j$ su operacije u, respektivno, grupama $\mathbf{G}_{(j)\varphi}$ i $\mathbf{H}_j$ a za operaciju grupa $\prod^c_{i\in I} \mathbf{G}_i$ i $\prod^c_{j\in J} \mathbf{H}_j$ smo koristili isti znak – $\cdot$).□

Data lema nam dozvoljava da za skup indeksa uvek uzmemo neki dobro uređen skup. Naša metateorija, ne zaboravimo, uključuje aksiomu izbora – uostalom ona nam i garantuje da je skup $\prod_{i\in I} G_i$ $(I \neq \emptyset)$ neprazan; njenu primenu nismo ni dosad naglašavali (sem u 4.38 – Zornova lema je jedan njen ekvivalent) niti ćemo to i ubuduće činiti. Za dobro uređen skup (indeksa), kad nam takav zatreba, obično se uzima kardinal (ili, još šire, ordinal) u smislu von Neumanove definicije (shodno uobičajenoj notaciji kardinale obeležavamo grčkim slovima iz sredine alfabeta – $\lambda$, $\mu$, $\nu$, ..., a ordinale grčkim slovima sa početka alfabeta – $\alpha$, $\beta$, $\gamma$, ...). U takvom slučaju često se element $f$ skupa $\prod_{\alpha\in\lambda} G_\alpha$ predstavlja $\lambda$-nizom $\langle (\alpha)f \rangle_{\alpha\in\lambda}$.

**Lema 10.3** (*a*) *Grupe* $\prod^c_{i\in I} \mathbf{G}_i$ *i* $\prod_{i\in I} \mathbf{G}_i$ *su Abelove akko je* $\mathbf{G}_i$ *Abelova grupa za svako* $i$ *iz* $I$;



(*b*) *Ako je* $\mathbf{H}_i \leq \mathbf{G}_i$ *za svako* $i$ *iz* $I$, *tada je* $\prod^c_{i\in I} \mathbf{H}_i \leq \prod^c_{i\in I} \mathbf{G}_i$ *i* $\prod_{i\in I} \mathbf{H}_i \leq \prod_{i\in I} \mathbf{G}_i$. *Posebno, ako je za svaki indeks* $i$ $\mathbf{H}_i \lhd \mathbf{G}_i$, $\prod^c_{i\in I} \mathbf{H}_i$ *i* $\prod_{i\in I} \mathbf{H}_i$ *su normalne podgrupe, respektivno, grupa* $\prod^c_{i\in I} \mathbf{G}_i$ *i* $\prod_{i\in I} \mathbf{G}_i$ *i važi:*

$$\prod^c_{i\in I} \mathbf{G}_i / \prod^c_{i\in I} \mathbf{H}_i \cong \prod^c_{i\in I} \mathbf{G}_i/\mathbf{H}_i, \quad \prod_{i\in I} \mathbf{G}_i / \prod_{i\in I} \mathbf{H}_i \cong \prod_{i\in I} \mathbf{G}_i/\mathbf{H}_i;$$

(*c*) *Ako je* $\mu$ *beskonačni kardinal manji od kardinala* $\lambda$, *tada je* $\{f \in \prod_{\alpha\in\lambda} G_\alpha \mid |S(f)| < \mu\}$ *domen normalne podgrupe grupe* $\prod^c_{\alpha\in\lambda} \mathbf{G}_\alpha$.
*Direktni proizvod je normalna podgrupa kartezijanskog proizvoda;*

(*d*) $\mathbf{Z}(\prod^c_{i\in I} \mathbf{G}_i) = \prod^c_{i\in I} \mathbf{Z}(\mathbf{G}_i)$, $\quad \mathbf{Z}(\prod_{i\in I} \mathbf{G}_i) = \prod_{i\in I} \mathbf{Z}(\mathbf{G}_i)$;

(*e*) $(\prod^c_{i\in I} \mathbf{G}_i)' \leq \prod^c_{i\in I} \mathbf{G}'_i$, $\quad (\prod_{i\in I} \mathbf{G}_i)' = \prod_{i\in I} \mathbf{G}'_i$.

**Dokaz.** (*b*) Neka je $\mathbf{H}_i \lhd \mathbf{G}_i$ za svako $i \in I$. Lako se proverava da je $\prod^c_{i\in I} \mathbf{H}_i \lhd \prod^c_{i\in I} \mathbf{G}_i$, a preslikavanje $\varphi : \prod_{i\in I} G_i / \prod_{i\in I} H_i \longrightarrow \prod_{i\in I} G_i/H_i$ dato sa (za $f \in \prod_{i\in I} G_i$): $(f \prod_{i\in I} H_i)\varphi = \overline{f}$, gde je $(i)\overline{f} \stackrel{\text{def}}{=} (i)fH_i$, izomorfno je preslikavanje grupe $\prod^c_{i\in I} \mathbf{G}_i / \prod^c_{i\in I} \mathbf{H}_i$ na grupu $\prod^c_{i\in I} \mathbf{G}_i/\mathbf{H}_i$.

Od ostalih tačaka (*e*) je nešto manje trivijalna.

(*e*) Inkluzija $\subseteq$ u oba slučaja odmah sledi, jer ako je $g = f_1^{-1} \dots f_k^{-1} f_1 \dots f_k$ element izvodne grupe $\prod^c_{i\in I} \mathbf{G}_i$ (videti lemu 5.27), onda je

$$(i)g = (i)f_1^{-1} \dots (i)f_k^{-1} (i)f_1 \dots (i)f_k = ((i)f_1)^{-1} \dots ((i)f_k)^{-1} (i)f_1 \dots (i)f_k \in G'_i.$$

Dokažimo sada inkluziju $\supseteq$ za direktne proizvode. Dovoljno je samo pokazati da je za (proizvoljne) grupe $\mathbf{A}$ i $\mathbf{B}$, $\mathbf{A}' \times \mathbf{B}' = (\mathbf{A} \times \mathbf{B})'$ (ostalo daje indukcija i činjenica da su nosači elemenata konačni).

Neka je skupovni indeks $2 = \{0, 1\}$ $(\mathbf{A} = \mathbf{G}_0,\ \mathbf{B} = \mathbf{G}_1)$, $f \in A' \times B'$ i

$$(0)f = a_1^{-1} \dots a_k^{-1}\, a_1 \dots a_k, \quad a_i \in A$$

i

$$(1)f = b_1^{-1} \dots b_l^{-1}\, b_1 \dots b_l, \quad b_j \in B.$$

Pretpostavimo da je $k$ veće od $l$. Tada je

$$f = g_1^{-1} \dots g_k^{-1}\, g_1 \dots g_k \in (A \times B)',$$

gde je $(0)g_i = a_i$ za $1 \leq i \leq k$ i $(1)g_j = \begin{cases} b_j & 1 \leq j \leq l \\ e_B & l < j \leq k. \end{cases}$

$(\prod^c_{i\in I} \mathbf{G}_i)'$ može biti prava podgrupa grupe $\prod^c_{i\in I} \mathbf{G}'_i$.□

**Definicija 10.4** *Neka je* $f$ *element neke od grupa* $\prod^c_{i\in I} \mathbf{G}_i$, $\prod_{i\in I} \mathbf{G}_i$. $(i)f$ *zovemo komponentom elementa* $f$ *u grupi* $\mathbf{G}_i$ *(u upotrebi je i termin projekcija).*

*Ako je* $\mathbf{H}$ *podgrupa neke od grupa* $\prod^c_{i\in I}\mathbf{G}_i$, $\prod_{i\in I}\mathbf{G}_i$, *tada je podgrupa grupe* $\mathbf{G}_i$ *sa domenom* $\{a \in G_i \mid a$ *je komponenta nekog elementa iz* $H\}$ *tzv. komponenta podgrupe* $\mathbf{H}$ *u grupi* $\mathbf{G}_i$ *(ili projekcija podgrupe* $\mathbf{H}$ *na faktor* $\mathbf{G}_i$*). Neki put ćemo tu podgrupu, u oznaci* $\mathbf{H}^i$, *zvati i-tom komponentom podgrupe* $\mathbf{H}$.

**Lema 10.5** *Ako je* $\mathbf{H}$ *podgrupa grupe* $\prod^c_{i\in I}\mathbf{G}_i$ $(\prod_{i\in I}\mathbf{G}_i)$, *onda je* $i$ *podgrupa kartezijanskog (direktnog) proizvoda svojih komponenti.*

**Dokaz.** Dajemo samo primer direktnog proizvoda sa podgrupom koja je prava podgrupa direktnog proizvoda svojih komponenti.

Kleinova grupa sa elementima $e, a, b, c$ je direktni proizvod cikličnih grupa $\mathbf{A} = \langle a\rangle$ i $\mathbf{B} = \langle b\rangle$ a komponente njene podgrupe $\mathbf{C} = \langle c\rangle$ su opet $\mathbf{A}$ i $\mathbf{B}$.

Ovo je tek jedan od slučajeva klase "istotipnih" primera u kojima je podgrupa direktnog proizvoda prava podgrupa svojih projekcija. Naime, ako je (indeksni) skup $I$ konačne kardinalnosti veće od 1 i ako su sve grupe $\mathbf{G}_i = \langle\{g^i_\alpha \mid \alpha \in \lambda\}, \cdot_i\rangle$, $i \in I$, kopije iste nejedinične grupe $\mathbf{G}$ (sa domenom $\{g_\alpha \mid \alpha \in \lambda\}$), tada je podgrupa direktnog proizvoda $\prod_{i\in I}\mathbf{G}_i$ sa domenom $\{h_\alpha \mid \alpha \in \lambda\}$, gde je, za $\alpha \in \lambda$ i $i \in I$, $(i)h_\alpha \stackrel{\text{def}}{=} g^i_\alpha$, prava podgrupa direktnog proizvoda svojih komponenti (koji je baš cela grupa – $\prod_{i\in I}\mathbf{G}_i$).□

Primeri poput ovih iz prethodnog dokaza inspirali su sledeću definiciju.

**Definicija 10.6** *Podgrupa* $\mathbf{H}$ *direktnog (kartezijanskog) proizvoda* $\prod_{i\in I}\mathbf{G}_i$ $(\prod^c_{i\in I}\mathbf{G}_i)$ *je poddirektni (podkartezijanski) proizvod (eng. subdirect product) familije grupa* $\{\mathbf{G}_i \mid i \in I\}$ *akko je* $\mathbf{H}^i = \mathbf{G}_i$ *za svako* $i$ *iz* $I$.

**Napomena.** Reč o terminologiji. U univerzalnoj algebri se, kada je reč o direktnom proizvodu algebri, upravo smatra onim što je kod grupa kartezijanski proizvod (videti npr. [30], [57]), pa se, saglasno tome, i poddirektnim proizvodom smatra ono što mi nazivamo *podkartezijanskim proizvodom*. No, postojanje na izvestan način "simpatičnog" jediničnog elementa omogućava (u teoriji grupa) definiciju direktnog proizvoda grupa (koji je obično i od većeg interesa), a to nas primorava i da pravimo razliku kada je o odgovarajućim podgrupama ovih proizvoda reč.

Dajemo još jedan primer poddirektnog proizvoda koji se razlikuje od već navedenih. Podgrupa $\mathbf{B}$ grupe $\mathbf{A} = \mathbf{Z}\times\mathbf{Z}$ sa domenom $\{(m,n) \mid m \equiv n\ (mod\ 4)\}$ prava je podgrupa grupe $\mathbf{A}$ $((2,0) \notin B)$ i poddirektni je proizvod: za svako $m \in Z$ je $(m, m+4) \in B$.

**Lema 10.7** *Neka je dat direktni proizvod* $\mathbf{G} = \prod_{i\in I}\mathbf{G}_i$. *Označimo sa* $\widehat{\mathbf{G}}_j$ *njegovu podgrupu sa domenom* $\{f \in \prod_{i\in I}G_i \mid (i)f = e_i$ *za svako* $i \neq j\}$. *Tada važi (za svako* $j$ *iz* $I$*):* $\widehat{\mathbf{G}}_j$ *je normalna podgrupa grupe* $\mathbf{G}$ *izomorfna sa* $\mathbf{G}_j$; *ako je* $j \neq k$, *onda je* $\widehat{\mathbf{G}}_j \cap \widehat{\mathbf{G}}_k = \mathbf{E}$; *grupa* $\mathbf{G}$ *je generisana skupom* $\bigcup_{i\in I}\widehat{G}_i$.



Prethodna lema nas navodi da uvedemo definiciju unutrašnjeg direktnog proizvoda.

**Definicija 10.8** *Grupa* $\mathbf{G}$ *je unutrašnji direktni proizvod familije svojih podgrupa* $\{\mathbf{G}_i \mid i \in I\}$ *akko su ispunjeni sledeći uslovi:*

$(a)$ $\mathbf{G} = \langle\bigcup_{i\in I}G_i\rangle$;

$(b)$ $\forall j \in I$ $\mathbf{G}_j \lhd \mathbf{G}$

$i$

$(c)$ $\forall j \in I$ $\mathbf{G}_j \cap \langle\bigcup_{i\in I\setminus\{j\}}G_i\rangle = \mathbf{E}$.

Iz 10.7 sledi da je $\mathbf{G} = \prod_{i\in I}\mathbf{G}_i$ unutrašnji direktni proizvod familije podgrupa $\{\widehat{\mathbf{G}_i} \mid i \in I\}$.

**Lema 10.9** *Sledeći uslovi su ekvivalentni za datu grupu* $\mathbf{G}$ *i nepraznu familiju njenih podgrupa* $\{\mathbf{G}_i \mid i \in I\}$:

(1) $\mathbf{G}$ *je unutrašnji direktni proizvod familije* $\{\mathbf{G}_i \mid i \in I\}$.

(2) *Važi:*

$(i)$ *elementi različitih podgrupa familije* $\{\mathbf{G}_i \mid i \in I\}$ *uzajamno su permutabilni*

$i$

$(ii)$ *svaki element iz* $G$ *različit od* $e$ *(ukoliko takav postoji) može se na jedinstven način, ne uzimajući u obzir poredak elemenata, predstaviti kao (konačan) proizvod elemenata različitih od* $e$ *izabranih iz podgrupa* $\mathbf{G}_i$, $i \in I$ *(podrazumevamo da se iz svake podgrupe* $\mathbf{G}_i$ *u ovom proizvodu javlja najviše jedan element).*

**Dokaz.** (1) $\Longrightarrow$ (2). Neka je $j \neq k$ i $a \in G_j$, $b \in G_k$. Zbog normalnosti podgrupa $\mathbf{G}_j$, $\mathbf{G}_k$ i $\mathbf{G}_j \cap \mathbf{G}_k = \mathbf{E}$ imamo $a^{-1}b^{-1}ab \in G_j \cap G_k = \{e\}$, tj. $ab = ba$. Dalje, kako je $\mathbf{G} = \langle\bigcup_{i\in I}G_i\rangle$, nejedinični element $g$ (pretpostavljamo da takav postoji) jednak je nekom proizvodu nejediničnih elemenata iz $\bigcup_{i\in I}G_i$. S obzirom na permutabilnost elemenata iz različitih podgrupa zahtevamo da se u proizvodu javlja po najviše jedan element iz iste podgrupe. Ako je pak $g = a_1\ldots a_m = b_1\ldots b_n$, $a_r \in G_{i_r}$, $b_s \in G_{j_s}$, $i_r, j_s \in I$, $a_r, b_s \neq e$ i, recimo, $i_1 \notin \{j_1,\ldots,j_n\}$, sledi $a_1 \in G_{i_1} \cap \langle\bigcup_{i\in I\setminus\{i_1\}}G_i\rangle = \{e\}$, kontradikcija; odatle proizilazi jednakost skupova $\{i_1,\ldots,i_m\}$ i $\{j_1,\ldots,j_n\}$, a analognim zaključivanjem izvodimo i da su elementi iz istih podgrupa jednaki.

(2) $\Longrightarrow$ (1). $(ii)$ samo implicira $(a)$ i $(c)$ a uz saradnju sa $(i)$ i tačku $(b)$ definicije 10.8.□

Lako se uviđa i iz datog dokaza da kada je skup indeksa $I$ ordinal $\alpha$ ili uopšte neki dobro uređen skup (što, već smo videli, možemo uvek pretpostaviti), tačka $(c)$ iz 10.8 može se zameniti sa prividno slabijim zahtevom $(c')$: $\forall\beta \in \alpha$ $\mathbf{G}_\beta \cap \langle\bigcup_{\gamma\in\beta}\mathbf{G}_\gamma\rangle = \mathbf{E}$.

Uočimo još da ako je $g = a_1 \cdot \ldots \cdot a_n$ element direktnog proizvoda $\prod_{i\in I} \mathbf{G}_i$, gde su $a_k$, $k = 1, \ldots, n$, nejedinični elementi konačnih redova iz različitih (pod)grupa, onda je

$$red(g) = NZS(red(a_1), \ldots, red(a_n));$$

ranije smo već dobili relaciju $\leq$, a $\geq$ sledi zbog $2(ii)$.

**Lema 10.10** *Ako je* $\mathbf{G}$ *unutrašnji direktni proizvod familije podgrupa* $\{\mathbf{G}_i \mid i \in I\}$, *tada je* $\mathbf{G} \cong \prod_{i\in I} \mathbf{G}_i$.

**Dokaz.** Definišimo preslikavanje $\varphi : \prod^d_{i\in I} G_i \longrightarrow G$ na sledeći način: ako je $f \in \prod^d_{i\in I} G_i$ i $S(f) = \{i_1, \ldots, i_n\}$, onda je $(f)\varphi \stackrel{\text{def}}{=} (i_1)f \ldots (i_n)f$. Dobra definisanost i bijektivnost preslikavanja su očigledni, a polazeći od relacije

$$S(f \cdot g) = (S(f) \cup S(g)) \setminus \{i \in S(f) \cap S(g) \mid (i)f = ((i)g)^{-1}\}$$

lako se proverava da je to i homomorfno preslikavanje grupe $\prod_{i\in I} \mathbf{G}_i$ u grupu $\mathbf{G}$.□

Gornja lema i konstatacija uz 10.8 oslobađaju nas briga oko uvođenja oznake za unutrašnji direktni proizvod. Jednostavno ostajemo pri već datoj za direktni proizvod kome se onda neki put dodeljuje i atribut spoljašnji (s napomenom da ćemo u slučaju Abelovih grupa koristiti aditivnu notaciju). Iz teksta će već biti jasno o kojem je proizvodu reč. Pridev unutrašnji nećemo bez velike potrebe ni koristiti. Pojam komponente (projekcije) iz 10.4 možemo, uz jasnu modifikaciju, zadržati i kod unutrašnjeg direktnog proizvoda (naravno, skoro sve komponente svakog elementa su jedinični element. Tako je projekcija nejediničnog elementa $g = g_1 \ldots g_k$ ($e \neq g_r \in G_{i_r}$, $r = 1, \ldots, k$) u grupu $\mathbf{G}_i$ $g_r$ ako je $i = i_r$ za neko $r \in \{1, \ldots, k\}$, inače je $e$. Jedinični element, treba li i to reći, jednak je svim svojim komponentama. Definicija projekcije podgrupe grupe $\mathbf{G}$ se analogno prenosi kao i pojam poddirektnog proizvoda.

**Lema 10.11** *Ako je* $\mathbf{G}$ *direktni proizvod familije podgrupa* $\{\mathbf{G}_i \mid i \in I\}$, *tada je za svako* $j$ *iz* $I$:

$$\mathbf{G}_j \cong \mathbf{G}/\langle \bigcup_{i\in I\setminus\{j\}} G_i \rangle = \mathbf{G}/\prod_{i\in I\setminus\{j\}} \mathbf{G}_i.$$

**Dokaz.** Preslikavanje $\varphi : G \longrightarrow G_j$ koje svakom elementu dodeljuje njegovu projekciju u $\mathbf{G}_j$ homomorfno je i surjektivno preslikavanje sa jezgrom $\langle \bigcup_{i\in I\setminus\{j\}} G_i \rangle$. Naravno, to jezgro je (unutrašnji) direktni proizvod familije podgrupa $\{\mathbf{G}_i \mid i \in I \setminus \{j\}\}$.□

Napomenimo da je u razlaganju grupe u direktni proizvod, recimo, dva faktora pri čemu smo jedan fiksirali, drugi generalno određen samo do na izomorfizam; npr. u slučaju Kleinove grupe $\mathbf{K}$ imamo (sa oznakama iz 10.5): $\mathbf{K} = \mathbf{A} \times \mathbf{B} = \mathbf{A} \times \mathbf{C}$.



**Lema 10.12** *Neka je* $\mathbf{G}$ *direktni proizvod familije podgrupa* $\{\mathbf{G}_i \mid i \in I\}$.

(*a*) *Ako je, za* $i \in I$, $\mathbf{G}_i$ *direktni proizvod familije svojih podgrupa* $\{\mathbf{H}_{ij} \mid j \in J_i\}$, *onda je* $\mathbf{G}$ *direktni proizvod familije podgrupa* $\{\mathbf{H}_{ij} \mid i \in I, j \in J_i\}$. *Dekompoziciju* $\prod_{i,j} \mathbf{H}_{ij}$ *zovemo produženjem ili proširenjem dekompozicije* $\prod_i \mathbf{G}_i$ *(u engleskoj literaturi koristi se izraz refinement).*

(*b*) *Neka je* $\{I_j \mid j \in J\}$ *particija skupa* $I$. *Tada je* $\mathbf{G}$ *direktan proizvod familije podgrupa* $\{\prod_{i\in I_j} \mathbf{G}_i \mid j \in J\}$.

**Dokaz.** Trivijalan. Ipak recimo, uputnije je dokazivati tačke $(i)$ i $(ii)$ uslova (2) iz leme 10.9.□

**Lema 10.13** *Neka je* $\mathbf{G}$ *direktni proizvod familije podgrupa* $\{\mathbf{G}_i \mid i \in I\}$ *i neka je* $\varphi$ *izomorfno preslikavanje grupe* $\mathbf{G}$ *na grupu* $\mathbf{H}$. *Tada je* $\mathbf{H}$ *direktni proizvod familije podgrupa* $\{(\mathbf{G}_i)\varphi \mid i \in I\}$.

**Dokaz.** Surjektivni homomorfizam očuvava svojstvo normalnosti podgrupa (videti teoremu 8.7) te je $(\mathbf{G}_i)\varphi \lhd \mathbf{H}$ za svako $i \in I$. Kako je $\mathbf{G} = \langle \bigcup_{i\in I} G_i \rangle$ to je i $\mathbf{H} = \langle (\bigcup_{i\in I} G_i)\varphi \rangle = \langle \bigcup_{i\in I} (G_i)\varphi \rangle$, a $\mathbf{G}_j \cap \langle \bigcup_{i\in I\setminus\{j\}} G_i \rangle = \mathbf{E}$ implicira, zbog injektivnosti preslikavanja $\varphi$, $(\mathbf{G}_j)\varphi \cap \langle (\bigcup_{i\in I\setminus\{j\}} G_i)\varphi \rangle = \mathbf{E}$.□

**Lema 10.14** *Neka je* $\{\mathbf{N}_i \mid i \in I\}$ *familija normalnih podgrupa grupe* $\mathbf{G}$ *i neka je* $\bigcap_{i\in I} \mathbf{N}_i = \mathbf{N}$. *Tada je faktor grupa* $\mathbf{G}/\mathbf{N}$ *izomorfna nekoj podgrupi grupe* $\prod^c_{i\in I} \mathbf{G}/\mathbf{N}_i$.

**Dokaz.** Preslikavanje $\varphi : G \longrightarrow \prod_{i\in I} G/N_i$, gde je (za $a \in G$) $(a)\varphi = f_a$ i $(i)f_a \stackrel{\text{def}}{=} aN_i$, homomorfno je preslikavanje grupe $\mathbf{G}$ u kartezijanski proizvod $\prod^c_{i\in I} \mathbf{G}/\mathbf{N}_i$. Odista, $(i)f_{ab} = abN_i = aN_i\, bN_i = (i)f_a\,(i)f_b = (i)(f_a \circ f_b)$; dakle $f_{ab} = f_a \circ f_b$, odnosno $(ab)\varphi = (a)\varphi \circ (b)\varphi$ (ostalo je gotovo očigledno).

Jezgro ovog homomorfizma je baš $\mathbf{N}$, jer:

$$a \in Ker(\varphi) \Longleftrightarrow \forall i \in I\ aN_i = N_i \Longleftrightarrow \forall i \in I\ a \in N_i \Longleftrightarrow a \in \bigcap_{i\in I} N_i.$$□

U vezi ove leme primetimo još da faktor grupa $\mathbf{G}/\mathbf{N}$ ne mora, u opštem, biti izomorfna i nekoj podgrupi direktnog proizvoda $\prod_{i\in I} \mathbf{G}/\mathbf{N}_i$. Tako na primer za aditivnu grupu celih brojeva $\mathbf{Z}$ i familiju njenih podgrupa $\{n\mathbf{Z} \mid n \geq 1\}$ (videti napomenu uz 3.17) imamo $\bigcap_{n\in\omega\setminus\{0\}} n\mathbf{Z} = \mathbf{O}$ i $\mathbf{Z}/\mathbf{O} \cong \mathbf{Z}$, dok je $\prod_{n\in\omega\setminus\{0\}} \mathbf{Z}/n\mathbf{Z}$ periodična grupa. U svakom slučaju važi

**Korolar 10.15** *Ako su* $\mathbf{H}_1, \ldots, \mathbf{H}_n$ *normalne podgrupe grupe* $\mathbf{G}$ *i ako je* $\mathbf{H} = \bigcap^n_{i=1} \mathbf{H}_i$, *tada je grupa* $\mathbf{G}/\mathbf{H}$ *izomorfna podgrupi grupe* $\mathbf{G}/\mathbf{H}_1 \times \cdots \times \mathbf{G}/\mathbf{H}_n$.

**Dokaz.** Kopija dokaza prethodne leme.□

**Lema 10.16** *Ako je* $\mathbf{A}$ *normalna podgrupa grupe* $\mathbf{G}$ *i ako je faktor grupa* $\mathbf{G/A}$ *direktni proizvod* $\prod_{i\in I}(\mathbf{B}_i/\mathbf{A})$, *gde je, za svako* $i \in I$, $\mathbf{B}_i = \mathbf{A} \times \mathbf{C}_i$ *i* $\mathbf{C}_i \lhd \mathbf{G}$, *tada je* $\mathbf{G} = \mathbf{A} \times \prod_{i\in I} \mathbf{C}_i$.

**Dokaz.** Jasno, grupa $\mathbf{G}$ je generisana skupom $A \cup \bigcup_{i\in I} C_i$. Elementi iz različitih podgrupa $\mathbf{C}_i$, $\mathbf{C}_j$ $(i \neq j)$ su uzajamno permutabilni; za $c_i \in C_i$, $c_j \in C_j$ je $c_i^{-1}c_j^{-1}c_ic_j \in C_i \cap C_j = \{e\}$. Naime, $(e \neq)\ d \in C_i \cap C_j$ bi dalo: $(A \neq)\ dA \in B_i/A \cap B_j/A = \{A\}$, kontradikcija. S obzirom na rečeno imamo i $\langle \bigcup_{i\in I} C_i\rangle = \prod_{i\in I} \mathbf{C}_i$. Konačno, ako je $a = c_{i_1} \cdot \ldots \cdot c_{i_k}$, gde je $a \in A$, $c_{i_j} \in C_{i_j}$ i indeksi $i_1, \ldots, i_k$ su različiti, sledi: $A = c_{i_1}A \cdot \ldots \cdot c_{i_k}A$, pa je za svako $j$, $1 \leq j \leq k$, $c_{i_j} \in A$, odnosno, $c_{i_j} = e$. Prema tome je $\mathbf{A} \cap \prod_{i\in I} \mathbf{C}_i = \mathbf{O}$ i $\mathbf{G} = \mathbf{A} \times \prod_{i\in I} \mathbf{C}_i$.□

**Lema 10.17** $(a)$ *Neka je* $\mathbf{H}$ *podgrupa grupe* $\mathbf{G} = \mathbf{A} \times \mathbf{B}$ *takva da je* $\mathbf{A} \times \mathbf{E} \leq \mathbf{H}$. *Tada je* $\mathbf{H} = \mathbf{A} \times (\mathbf{H})\pi_B$, *gde je* $\pi_B$ *projekcija grupe* $\mathbf{G}$ *na grupu* $\mathbf{B}$.

*Posebno, ako je grupa* $\mathbf{G}$ *(unutrašnji) direktni proizvod svojih (normalnih) podgrupa* $\mathbf{A}$ *i* $\mathbf{B}$ *i ako je* $\mathbf{H}$ *njena podgrupa takva da je* $\mathbf{A} \leq \mathbf{H}$, *onda je* $\mathbf{H}$ *(unutrašnji) direktni proizvod podgrupa* $\mathbf{A}$ *i* $\mathbf{H} \cap \mathbf{B}$.

$(b)$ *Neka je* $\mathbf{G}$ *podgrupa grupe* $(\mathbf{B/A}) \times \mathbf{C}$ *i neka postoji podgrupa* $\mathbf{B}_1$ *grupe* $\mathbf{B}$ *koja sadrži* $\mathbf{A}$ *i takva je da je* $(\mathbf{B}_1/\mathbf{A}) \times \mathbf{E} \leq \mathbf{G}$. *Tada postoji podgrupa* $\mathbf{D}$ *grupe* $\mathbf{B} \times \mathbf{C}$ *takva da je* $\mathbf{D}/(\mathbf{A} \times \mathbf{E}) \cong \mathbf{G}$.

**Dokaz.** $(a)$ Inkluzija $\leq$ je očigledna. S druge strane, neka je $a \in A$ i $b \in (H)\pi_B$. Onda je $(a_1, b) \in H$ za neko $a_1$ iz $A$. No zbog $(a_1^{-1}, e) \in H$ sledi: $(e, b) = (a_1^{-1}, e) \cdot (a_1, b) \in H$, a onda i $(a, b) = (a, e) \cdot (e, b) \in H$.

$(b)$ Neka je $D = \{(b, c) \mid (bA, c) \in G\}$. Lako se proverava da je $D$ domen podgrupe grupe $\mathbf{B} \times \mathbf{C}$ ($D$ je neprazan skup jer je, zbog uslova zadatka, barem $(e, e) \in D$). Neka je, dalje, $\varphi$ preslikavanje faktor grupe $\mathbf{D}/(\mathbf{A} \times \mathbf{E})$ u grupu $\mathbf{G}$ dato sa $((b, c)(A \times E))\varphi = (bA, c)$. $\varphi$ je dobro definisano, jer ako je $(b, c)(A \times E) = (b_1, c_1)(A \times E)$, onda je $b_1^{-1}b \in A$, $c_1^{-1}c \in E$, pa je $bA = b_1A$ i $c = c_1$. Kada se krene istim putem unazad pokazuje se injektivnost preslikavanja $\varphi$. I očigledno, $\varphi$ je surjektivno i homomorfno preslikavanje.□

**Korolar 10.18** $\mathbf{Fr}(\prod^{c}_{i\in I} \mathbf{G}_i) \leq \prod^{c}_{i\in I} \mathbf{Fr}(\mathbf{G}_i)$; $\mathbf{Fr}(\prod_{i\in I} \mathbf{G}_i) \leq \prod_{i\in I} \mathbf{Fr}(\mathbf{G}_i)$.

**Dokaz.** U osnovi je isti za oba proizvoda. Recimo, ako je $\mathbf{H}_i$ maksimalna podgrupa grupe $\mathbf{G}_i$, onda je, prema prethodnoj lemi, $\mathbf{H}_i \times \prod_{i\neq j\in I} \mathbf{G}_j$ maksimalna podgrupa grupe $\prod_{k\in I} \mathbf{G}_k$, pa je $\mathbf{Fr}(\prod_{i\in I} \mathbf{G}_i) \leq \mathbf{Fr}(\mathbf{G}_i) \times \prod_{i\neq j\in I} \mathbf{G}_j$ i, generalno, $\mathbf{Fr}(\prod_{i\in I} \mathbf{G}_i) \leq \prod_{i\in I} \mathbf{Fr}(\mathbf{G}_i)$.

U vezi ovog tvrđenja videti i 49.27.□

**Lema 10.19** *Podgrupa* $\mathbf{H}$ *podgrupe* $\mathbf{A} \times \mathbf{B}$ *(grupe* $\mathbf{G}$*) poddirektan je proizvod podgrupa* $\mathbf{A}$ *i* $\mathbf{B}$ *akko su za neke normalne podgrupe* $\mathbf{C}$ *i* $\mathbf{D}$ *grupa, respektivno,* $\mathbf{A}$ *i* $\mathbf{B}$, *faktor grupe* $\mathbf{A/C}$ *i* $\mathbf{B/D}$ *izomorfne i za neki izomorfizam* $\varphi \in Is(\mathbf{A/C}, \mathbf{B/D})$ *važi:* $(aC)\varphi = bD$ *akko* $ab \in H$.



**Dokaz.** $(\Longrightarrow)$ Neka je $\mathbf{H}$ poddirektan proizvod (pod)grupa $\mathbf{A}$ i $\mathbf{B}$ i neka je $\mathbf{C} = \mathbf{A} \cap \mathbf{H}$, $\mathbf{D} = \mathbf{B} \cap \mathbf{H}$, $c \in C$ i $a \in A$. Ako je, za $b \in B$, $ab \in H$, onda je $a^{-1}ca = (ab)^{-1}c(ab) \in A \cap H = C$ i $\mathbf{C}$ je normalna podgrupa grupe $\mathbf{A}$. Isto tako je $\mathbf{D}$ normalna podgrupa grupe $\mathbf{B}$. Definišimo, dalje, preslikavanje $\varphi : A/C \longrightarrow B/D$ sa: $(aC)\varphi = bD$ akko $ab \in H$. $\varphi$ je dobro definisano; ako je, za $a_1, a_2 \in A$ i $b_1, b_2 \in B$, $a_1C = a_2C$ i $a_1b_1, a_2b_2 \in H$, tada iz $(a_1b_1)^{-1}a_2b_2 = a_1^{-1}a_2 \cdot b_1^{-1}b_2 \in H$ sledi $b_1^{-1}b_2 \in B \cap H = D$ (jer $a_1^{-1}a_2 \in C$), tj. $b_1D = b_2D$. Analogno se pokazuje da je $\varphi$ injektivno, a očigledno je i surjektivno. Konačno, ako je $(a_1C)\varphi = b_1D$, $(a_2C)\varphi = b_2D$, odnosno, $a_1b_1, a_2b_2 \in H$, onda je $a_1b_1 \cdot a_2b_2 = a_1a_2 \cdot b_1b_2 \in H$ i $(a_1C \cdot a_2C)\varphi = (a_1a_2C)\varphi = b_1b_2D = b_1D \cdot b_2D = (a_1C)\varphi \cdot (a_2C)\varphi$. Prema tome, $\varphi \in Is(\mathbf{A/C}, \mathbf{B/D})$.

$(\Longleftarrow)$ Trivijalno. Primetimo samo da je $CD \subseteq H$ i $\mathbf{A} \cap \mathbf{H} = \mathbf{C}$, $\mathbf{B} \cap \mathbf{H} = \mathbf{D}$. Jer ako je $h \in A \cap H$, onda je $he \in H$ i $(hC)\varphi = D$, te je $hC = C$, tj. $h \in C$. Za $c \in C$ je $(cC)\varphi = (C)\varphi = D = eD$ i stoga $ce = c \in H$.□

**Lema 10.20** *Neka je grupa* $\mathbf{G}$ *direktni proizvod svojih podgrupa* $\mathbf{A}_i$, $i \in I$, *i neka je* $\mathbf{Fr(G)} \cap \mathbf{A}_{i_0} < \mathbf{Fr}(\mathbf{A}_{i_0})$ *za neko* $i_0 \in I$. *Tada postoji normalna podgrupa* $\mathbf{B}$ *grupe* $\mathbf{A}_{i_0}$ *takva da je* $\mathbf{A}_{i_0}/\mathbf{B}$ *beskonačna prosta grupa bez maksimalnih podgrupa.*

**Dokaz.** Grupu $\mathbf{A}_{i_0}$ označimo kraće sa $\mathbf{A}$, $\mathbf{C}$ će biti $\prod_{i\in I\setminus\{i_0\}} \mathbf{A}_i$. Neka je $\mathbf{M}$ maksimalna podgrupa grupe $\mathbf{G}$ takva da $\mathbf{M} \cap \mathbf{A}$ ne sadrži $\mathbf{Fr(A)}$ (njenu egzistenciju garantuje uslov $\mathbf{Fr(G)} \cap \mathbf{A} < \mathbf{Fr(A)}$). Prema tome, $\mathbf{M} \cap \mathbf{A}$ je prava ali sigurno ne i maksimalna podgrupa grupe $\mathbf{A}$. Pretpostavimo prvo da $\mathbf{M}$ nije poddirektni proizvod podgrupa $\mathbf{A}$ i $\mathbf{C}$. Ako su $\pi_1$ i $\pi_2$ projekcije grupe $\mathbf{A} \times \mathbf{C}$ na, respektivno, $\mathbf{A}$ i $\mathbf{C}$ ($(ac)\pi_1 \stackrel{\text{def}}{=} a$, $(ac)\pi_2 \stackrel{\text{def}}{=} c$) i $(\mathbf{M})\pi_1 = \mathbf{M}_1$, $(\mathbf{M})\pi_2 = \mathbf{M}_2$, onda je $\mathbf{M} \leq \mathbf{M}_1 \times \mathbf{M}_2 < \mathbf{A} \times \mathbf{C}$, te je, s obzirom na maksimalnost podgrupe $\mathbf{M}$, $\mathbf{M} = \mathbf{M}_1 \times \mathbf{M}_2$. Prema rečenom je, za neku pravu podgrupu $\mathbf{H}$ grupe $\mathbf{A}$: $\mathbf{M} \cap \mathbf{A} = \mathbf{M}_1 < \mathbf{H} < \mathbf{A}$ i, odatle, $\mathbf{M} = \mathbf{M}_1 \times \mathbf{M}_2 < \mathbf{H} \times \mathbf{M}_2 < \mathbf{A} \times \mathbf{C}$, kontradikcija. Opet, prema prethodnoj lemi, ako je $\mathbf{M}$ poddirektni proizvod, onda su $\mathbf{B} = \mathbf{A} \cap \mathbf{M}$ i $\mathbf{D} = \mathbf{C} \cap \mathbf{M}$ normalne podgrupe, respektivno, grupa $\mathbf{A}$ i $\mathbf{C}$, grupe $\mathbf{A/B}$ i $\mathbf{C/D}$ su izomorfne i jedan izomorfizam – $\varphi$ – je dat sa: $(aB)\varphi = cD$ akko $ac \in M$. $\mathbf{A/B}$ je prosta grupa. Jer neka je $\mathbf{K/B}$ njena netrivijalna normalna podgrupa i $(\mathbf{K/B})\varphi = \mathbf{L/C}$. Onda su $\mathbf{A/K}$ i $\mathbf{C/L}$ izomorfne grupe; jedan izomorfizam $(\overline{\varphi})$ je kompozicija izomorfnih preslikavanja:

$$A/K \longrightarrow (A/B)/(K/B) \xrightarrow{\psi} (C/D)/(L/D) \longrightarrow C/L,$$

gde je $\psi$ indukovano sa $\varphi$: $((aB)\,K/B)\psi \stackrel{\text{def}}{=} ((aB)\varphi)\,L/D$, a u ostalim slučajevima se radi o kanoničkim preslikavanjima (npr. $aK \longrightarrow (aB)\,K/B$). Ako je $(aB)\varphi = cD$, onda je $(aK)\overline{\varphi} = bL$ $(aK \longrightarrow (aB)\,K/B \longrightarrow (aB)\varphi\,L/D = cD\,L/D \longrightarrow cL)$, te je (ponovo prema prethodnoj lemi) $\mathbf{M}$ prava podgrupa

prave podgrupe $\mathbf{N}$ sa domenom $\{ac \mid a \in A, c \in C, (aB)\overline{\varphi} = cD\}$, koja je i poddirektni proizvod pogrupa $\mathbf{A}$ i $\mathbf{C}$), a $\mathbf{A} \cap \mathbf{N} = \mathbf{K}$, $\mathbf{C} \cap \mathbf{N} = \mathbf{L}$, kontradikcija. Grupa $\mathbf{A/B}$ je i bez maksimalnih podgrupa; ako bi ih bilo, imali bismo $\mathbf{Fr(A/B)} = \overline{\mathbf{E}}$ (5.25) i stoga, prema 8.7, $\mathbf{Fr(A)} \leq \mathbf{B} = \mathbf{A} \cap \mathbf{M}$, protivurečnost. $\mathbf{A/B}$ je, dakle, i beskonačna grupa.□

**Korolar 10.21** *Grupa* $\mathbf{G}$ *ima svojstvo* $\mathcal{P}$ *rezidualno akko je izomorfna podkartezijanskom proizvodu kartezijanskog proizvoda grupa sa svojstvom* $\mathcal{P}$.

**Dokaz**. Neka grupa $\mathbf{G}$ ima svojstvo $\mathcal{P}$ rezidualno i neka je $\mathbf{N} = \bigcap_{g \in G \setminus \{e\}} \mathbf{N}_g$, gde je, za $g \in G \setminus \{e\}$, $\mathbf{N}_g$ normalna podgrupa grupe $\mathbf{G}$ takva da $\mathbf{G/N}_g$ ima svojstvo $P$ i $g \notin N_g$. No tada je $\mathbf{N} = \mathbf{E}$ i $\mathbf{G} \cong \mathbf{G/N}$, dok je grupa $\mathbf{G/N}$ izomorfna podgrupi kartezijanskog proizvoda $\prod^c_{g \in G \setminus \{e\}} \mathbf{G/N}_g$.

Pretpostavimo sada da je $\mathbf{G}$ podgrupa kartezijanskog proizvoda familije grupa sa svojstvom $\mathcal{P}$, $\{\mathbf{G}_i \mid i \in I\}$, takva da je $\mathbf{G}^i = \mathbf{G}_i$ za svako $i \in I$. Neka je $\pi_i$ projekcija grupe $\mathbf{G}$ u grupu $\mathbf{G}_i$. Onda je, jasno, $\bigcap_{i \in I} \mathbf{Ker}(\pi_i) = \mathbf{E}$, pa ako je $g$ nejedinični element grupe $\mathbf{G}$, tada $g \notin Ker(\pi_j)$ za neko $j \in I$, dok je $\mathbf{G/Ker}(\pi_j) \cong \mathbf{G}_j$ (s obzirom da je $\mathbf{G}$ podkartezijanski proizvod).□

**Lema 10.22** *Kartezijanski (direktni) proizvod konačno rezidualnih grupa je konačno rezidualna grupa.*

**Dokaz**. Neka je svaka od grupa $\mathbf{G}_i$, $i \in I$, konačno rezidualna i neka je $f$ nejedinični element grupe $\mathbf{G} = \prod^c_{i \in I} \mathbf{G}_i$. Ako je, za $j \in I$, $(j)f \neq e_j$ i $\mathbf{N}_j$ normalna podgrupa grupe $\mathbf{G}_j$ takva da je $\mathbf{G}_j/\mathbf{N}_j$ konačna grupa i $(j)f \notin N_j$, onda je $\mathbf{N} = \prod^c_{i \in I \setminus \{j\}} \mathbf{G}_i \times \mathbf{N}_j$ normalna podgrupa grupe $\mathbf{G}$ koja ne sadrži element $f$ i čija je faktor grupa konačna: $\mathbf{G/N} \cong \mathbf{G}_j/\mathbf{N}_j$ - 10.3($b$).□

**Definicija 10.23** *Grupa* $\mathbf{G}$ *je razloživa (u direktni proizvod) akko je direktni proizvod netrivijalnih normalnih podgrupa (uvek je, trivijalno,* $\mathbf{G} = \mathbf{G} \times \mathbf{E}$*).*

*Grupa* $\mathbf{G}$ *je potpuno razloživa akko se svaka njena normalna podgrupa javlja kao direktni faktor u nekom razlaganju grupe* $\mathbf{G}$ *u direktni proizvod.*

**Primer 10.24** ($a$) *Svaka prosta grupa je nerazloživa.*

($b$) *Grupa kvaterniona je nerazloživa.*

($c$) *Aditivne grupe celih i racionalnih brojeva su nerazložive.*

($d$) *Za prost broj $p$ ciklična grupa $\mathbf{C}_{p^n}$ nije razloživa.*

($e$) *Prüferova grupa $\mathbf{p}^\infty$ nije razloživa.*

Primetimo da su grupe iz tačaka ($b$), ($c$), ($d$) i ($e$) sa svojstvom da bilo koje dve netrivijalne podgrupe imaju netrivijalni presek (videti 5.7($a$) i 7.10($d$)); posebno, u slučaju tačaka ($d$) i ($e$) podgrupe datih grupa su linearno uređene.



($e$) *Aditivna grupa kompleksnih brojeva je direktna suma svojih podgrupa* $\mathbf{Re}$ *i* $\langle iRe, + \rangle$, *$i$ - imaginarna jedinica.*

Kasnije ćemo pokazati da su aditivne grupe realnih i kompleksnih brojeva izomorfne; prema tome grupa može biti izomorfna svom netrivijalnom direktnom faktoru (čitaoca upućenog bar donekle u teoriju polja podsećamo da polja realnih i kompleksnih brojeva nisu izomorfna – lako se pokazuje da bi pretpostavljeni izomorfizam morao preslikati 0 u 0, 1 u 1 i -1 u -1, ali u polju kompleksnih brojeva jednačina $x^2 + 1 = 0$ ima rešenje dok ga u polju realnih brojeva nema).

($f$) $\langle Ra \setminus \{0\}, \cdot \rangle = \langle Ra^+, \cdot \rangle \times \langle \{1, -1\}, \cdot \rangle$,
$\langle Re \setminus \{0\}, \cdot \rangle = \langle Re^+, \cdot \rangle \times \langle \{1, -1\}, \cdot \rangle$.
$\langle C \setminus \{0\}, \cdot \rangle = \langle Re^+, \cdot \rangle \times \langle \{z \in C \mid |z| = 1\}, \cdot \rangle$ *(gde je $C$ skup kompleksnih brojeva, $Re^+$ skup pozitivnih realnih brojeva i $|z|$ moduo kompleksnog broja $z$).*

($g$) *Neka je $m > 1$ i $n = p_1^{k_1} \dots p_m^{k_m}$, gde su, za $i = 1, \dots, m$, $p_i$ različiti prosti a $k_i$ pozitivni prirodni brojevi. Tada je*

$$\mathbf{Z}_n = \langle \frac{n}{p_1^{k_1}} \rangle \oplus \cdots \oplus \langle \frac{n}{p_m^{k_m}} \rangle.$$

**Dokaz**. U pitanju je direktna suma Abelovih grupa pa shodno tome koristimo aditivnu notaciju, a praksa je da se za konačnu direktnu sumu koristi $\oplus$. O ovome će još biti reči u poglavlju o Abelovim grupama. U svakom slučaju, kada su u pitanju podgrupe Abelove grupe, nastojaćemo da iz konteksta uvek bude jasno da li je reč o "običnoj" ili direktnoj sumi.

Element $a_i = \frac{n}{p_i^{k_i}}$ je reda $p_i^{k_i}$, a $\langle a_i \rangle \cap \langle \{a_j \mid j \neq i\} \rangle = \mathbf{O}$, jer su redovi elemenata grupe $\langle \{a_j \mid j \neq i\} \rangle$ uzajamno prosti sa $p_i$ (videti 2.7($d$)). Direktna suma

$$\langle a_1 \rangle + \cdots + \langle a_m \rangle$$

je reda $p_1^{k_1} \dots p_m^{k_m}$, dakle jednaka je celoj grupi $\mathbf{Z}_n$.

Ilustrujmo ovo i "konkretnim" primerom. Tako je npr.

$$\mathbf{Z}_{360} = \langle 45 \rangle + \langle 40 \rangle + \langle 72 \rangle.$$

Direktni sumandi su reda, respektivno, 8, 9 i 5, a recimo,

$$150 = 6 \cdot 45 +_{360} 6 \cdot 40, \quad 149 = 45 +_{360} 8 \cdot 40 +_{360} 2 \cdot 72.$$

Čitaocu ostavljamo kao vežbu iznalaženje algoritma za izračunavanje "koeficijenata" za elemente grupe; dakle, za dato $m \in 360$ treba odrediti $x \in 8$, $y \in 9$ i $z \in 5$ tako da je $m = x \cdot 45 +_{360} y \cdot 40 +_{360} z \cdot 72$ (jedno takvo rešenje koristi homomorfno preslikavanje grupe $\mathbf{Z}$ na grupu $\mathbf{Z}_{360}$).

(*h*) $\langle Ra^+, \cdot\rangle = \prod_{p\in P}\langle p\rangle$, *gde je* $P$ *skup prostih brojeva.*

**Dokaz.** Jasno; $P$ je generatorni skup grupe $\langle Ra^+, \cdot\rangle$ (svaki racionalan broj je proizvod stepena prostih brojeva) a $\langle p\rangle \cap \langle P\setminus\{p\}\rangle = \mathbf{E}$.

S obzirom na (*f*) imamo $\langle Ra\setminus\{0\}, \cdot\rangle = \langle\{1,-1\}, \cdot\rangle \times \prod_{p\in P}\langle p\rangle$.

(*i*) $\mathbf{D}_{2(2n+1)} = \mathbf{D}_{2n+1} \times \mathbf{C}_2$ *za svako* $n$ *veće od* 1.

**Dokaz.** Dijedarska grupa $\mathbf{D}_{4n+2}$ (stepena $2(2n+1)$) generisana je elementima $\rho_{\frac{2\pi}{4n+2}} (= \rho)$ i $\sigma_y (= \sigma)$ i određena relacijama $\rho^{4n+2} = \sigma^2 = \imath$ i $\rho\sigma = \sigma\rho^{4n+1}$ (videti 3.4(*e*)). Podgrupe

$\mathbf{H} = \langle\rho^{2n+1}\rangle = \langle\{\imath, \rho^{2n+1}\}, \circ\rangle$

i

$\mathbf{K} = \langle\rho^2, \sigma\rangle = \langle\{\imath, \rho^2, \rho^{2\cdot 2}, \ldots, \rho^{2\cdot 2n}, \sigma, \sigma\rho^2, \sigma\rho^4, \ldots, \sigma\rho^{4n}\}, \circ\rangle$

su normalne jer je:

$$\sigma\rho^{2n+1}\sigma = \sigma^2\rho^{(2n+1)(4n+1)} = \rho^{2n+1}$$

i za $1 \le k \le 2n$

$$\rho^{2k}\sigma = \sigma\rho^{2k(4n+1)} = \sigma\rho^{4n-2(k-1)}$$

(koristili smo: $(2n+1)(4n+1) \equiv (2n+1)\,(mod\,(4n+2))$ i $2k(4n+1) \equiv 4n-2(k-1)(mod(4n+2))$). S obzirom da je $\mathbf{H}\cap\mathbf{K} = \mathbf{E}$, sledi $\mathbf{D}_{4n+2} = \mathbf{H}\times\mathbf{K}$. No $\mathbf{K}$ je, zapravo, dijedarska grupa $\mathbf{D}_{2n+1}$, pošto je $(\rho^2)$ reda $2n+1$ i (prema gore navedenom)

$$\rho^2\sigma = \sigma\rho^{4n} = \sigma(\rho^2)^{2n} = \sigma(\rho^2)^{-1}.$$

Primetimo još da grupa $\mathbf{D}_{2\cdot 2n}$ nije izomorfna sa direktnim proizvodom $\mathbf{D}_{2n} \times \mathbf{C}_2$. U grupi $\mathbf{D}_{4n}$ imamo element reda $4n$, dok je red ma kog elementa grupe $\mathbf{D}_{2n} \times \mathbf{C}_2$ manji od ili jednak $2n$.□

**Lema 10.25** *Neka je* $\mathbf{G}$ *konačna grupa i neka su* $\mathbf{H}$ *i* $\mathbf{K}$ *njene normalne podgrupe takve da* $|H|\cdot|K| = |G|$. *Tada su uslovi* (1) $\mathbf{H}\cap\mathbf{K} = \mathbf{E}$ *i* (2) $HK = G$ *ekvivalentni i ako su ispunjeni, onda je* $\mathbf{G} = \mathbf{H}\times\mathbf{K}$.

**Dokaz.** Setimo se samo jednakosti (za zaboravne – videti 3.21(*a*)):

$$|HK| = \frac{|H|\cdot|K|}{|H\cap K|}.\square$$

**Korolar 10.26** *Za (svaki) prost broj* $p$ *postoje samo dve grupe reda* $p^2$ – $\mathbf{C}_{p^2}$ *i* $\mathbf{C}_p \times \mathbf{C}_p$.

**Dokaz.** Neka je $\mathbf{G}$ neciklična grupa reda $p^2$ (znamo već da je Abelova – 8.20). Svaki nejedinični element je, prema tome, reda $p$. Neka su $a$ i $b$ nejedinični elementi takvi da $b \notin \langle a\rangle$. Onda je $|\langle a\rangle|\cdot|\langle b\rangle| = |G|$ i $\langle a\rangle \cap \langle b\rangle = \mathbf{E}$ te je $\mathbf{G} = \langle a\rangle \times \langle b\rangle$.

Konstatujmo na kraju da za $n > 1$ grupe $\mathbf{C}_{n^2}$ i $\mathbf{C}_n \times \mathbf{C}_n$ nisu izomorfne – red (ma kog) elementa grupe $\mathbf{C}_n \times \mathbf{C}_n$ deli $n$.□



**Lema 10.27** *Neka je grupa* $\mathbf{G}$ *direktni proizvod karakterističnih podgrupa* $\mathbf{A}$ *i* $\mathbf{B}$. *Tada je:*

$$\mathbf{Aut(G)} \cong \mathbf{Aut(A)} \times \mathbf{Aut(B)}.$$

**Dokaz.** Tvrdimo: preslikavanje $\Phi : Aut(\mathbf{G}) \longrightarrow Aut(\mathbf{A}) \times Aut(\mathbf{B})$ definisano sa $(\varphi)\Phi = (\varphi|_A, \varphi|_B)$ izomorfizam je grupa $\mathbf{Aut(G)}$ i $\mathbf{Aut(A)} \times \mathbf{Aut(B)}$ (elemente grupe $\mathbf{Aut(A)} \times \mathbf{Aut(B)}$ predstavljamo ovde kao uređene parove – videti komentar uz 10.2; ubuduće ovakav način predstavljanja elemenata proizvoda nećemo više posebno obrazlagati). Svojstvo homomorfnosti preslikavanja $\Phi$ sledi iz $(\varphi\circ\psi)|_A = \varphi|_A \circ \psi|_A$ $(\varphi, \psi \in Aut(\mathbf{G}))$. Pokažimo još surjektivnost preslikavanja $\Phi$ (injektivnost je očigledna). Neka je $(\psi, \theta) \in Aut(\mathbf{A}) \times Aut(\mathbf{B})$. Definišimo preslikavanje $\varphi : G \longrightarrow G$ sa: $(ab)\varphi = (a)\psi\,(b)\theta$. Zbog jedinstvenosti komponenti u razlaganju elementa $(g = ab)$ $\varphi$ je dobro definisano. Iz istog razloga kao i zbog injektivnosti preslikavanja $\psi, \theta$, $\varphi$ je injektivno. Surjektivnost je takođe očigledna. $\varphi$ je konačno i homomorfno preslikavanje:

$$((ab)\,(a_1b_1))\varphi = ((aa_1)\,(bb_1))\varphi = (aa_1)\psi\,(bb_1)\theta =$$

$$(a)\psi\,(a_1)\psi\,(b)\theta\,(b_1)\theta = ((a)\psi\,(b)\theta)\,((a_1)\psi\,(b_1)\theta) = (ab)\varphi\,(a_1b_1)\varphi$$

(koristili smo uzajamnu permutabilnost elemenata podgrupa $\mathbf{A}$ i $\mathbf{B}$).□

**Korolar 10.28** *Neka je periodična grupa* $\mathbf{G}$ *direktni proizvod svojih podgrupa* $\mathbf{A}$ *i* $\mathbf{B}$ *pri čemu je ispunjeno:* $\forall a \in A\,\forall b \in B\ \ (red(a), red(b)) = 1$. *Tada je*

$$\mathbf{Aut(G)} \cong \mathbf{Aut(A)} \times \mathbf{Aut(B)}.$$

**Dokaz.** Podgrupe $\mathbf{A}$ i $\mathbf{B}$ su karakteristične. Zaista, neka je $\varphi \in Aut(\mathbf{G})$ i $a \in A$. Tada je i $(a)\varphi \in A$; jer $a$ i $(a)\varphi$ su istog reda, pa $(a)\varphi = a_1b_1$, $a_1 \in A$, $b_1 \in B$, implicira, s obzirom na uslove, $red(a) = red(a_1)\,red(b_1)$, odakle $red(b_1) = 1$, tj. $b_1 = e$.□

**Lema 10.29** (*a*) *Normalna podgrupa potpuno razložive grupe je potpuno razloživa;*

(*b*) *Homomorfna slika potpuno razložive grupe je potpuno razloživa grupa;*

**Dokaz.** (*a*) Neka je $\mathbf{G}$ potpuno razloživa grupa, $\mathbf{A}$ njena normalna podgrupa i $\mathbf{B} \lhd \mathbf{A}$. Onda je $\mathbf{B}$ normalna podgrupa i grupe $\mathbf{G}$ (jer je $\mathbf{G} = \mathbf{A}\times\mathbf{C}$ za neku podgrupu $\mathbf{C}$, pa za $g = ac$ imamo $g^{-1}\mathbf{B}g = c^{-1}a^{-1}\mathbf{B}ac = c^{-1}\mathbf{B}c = \mathbf{B}$ – elementi podgrupa $\mathbf{B}$ i $\mathbf{C}$ su uzajamno permutabilni). Stoga je, za neku podgrupu $\mathbf{D}$, $\mathbf{G} = \mathbf{B}\times\mathbf{D}$. Ali tada je $\mathbf{A} = \mathbf{B}\times(\mathbf{A}\cap\mathbf{D})$ (10.17).

(*b*) Prema komentaru uz 8.1 dovoljno je posmatrati faktor grupe potpuno razložive grupe ($\mathbf{G}$). Ali ako je $\mathbf{A} \lhd \mathbf{G}$ i $\mathbf{G} = \mathbf{A}\times\mathbf{B}$, tada je $\mathbf{G}/\mathbf{A} \cong \mathbf{B}$ (videti

10.12) i kako je, prema prethodnoj tački, $\mathbf{B}$ potpuno razloživa to je i $\mathbf{G}/\mathbf{A}$ potpuno razloživa grupa.□

Analogno tvrđenje za razložive grupe, naravno, ne važi. Tako je npr. aditivna grupa kompleksnih brojeva razloživa ali ne i aditivna grupa racionalnih brojeva. Ili, recimo, ako je $\mathbf{H}$ prosta nejedinična grupa, $\mathbf{K}$ ma kakva nejedinična grupa i $\mathbf{G}$ spoljašnji direktni proizvod grupa $\mathbf{H}$ i $\mathbf{K}$, tada je $\mathbf{G}$ razloživa grupa ($\mathbf{G} = \widehat{\mathbf{H}} \times \widehat{\mathbf{K}}$ – videti 10.8), a $\mathbf{G}/\widehat{\mathbf{K}}$ nije.

**Teorema 10.30** *Sledeći uslovi su ekvivalentni za grupu* $\mathbf{G}$*:*

($a$) $\mathbf{G}$ *je potpuno razloživa grupa;*

($b$) $\mathbf{G}$ *je direktni proizvod familije normalnih, prostih podgrupa;*

($c$) $\mathbf{G}$ *je generisana unijom domena familije normalnih, prostih podgrupa.*

**Dokaz.** ($c$) $\Longrightarrow$ ($a$). Neka je $\mathbf{G} = \langle \bigcup_{i\in I} G_i \rangle$, gde su $\mathbf{G}_i$, $i \in I$, proste, normalne podgrupe (prema tome je, za $i \neq j$, $\mathbf{G}_i \cap \mathbf{G}_j = \mathbf{E}$ i $\langle G_i \cup G_j \rangle = \mathbf{G}_i \times \mathbf{G}_j$; uzimamo, jasno, $|I| > 1$) i neka je $\mathbf{H} \lhd \mathbf{G}$. Posmatrajmo parcijalno uređen skup $\langle \mathcal{F}, \subseteq \rangle$, gde je $\mathcal{F} = \{J \subseteq I \mid$ podgrupa generisana skupom $H \cup \bigcup_{i\in J} G_i$ je (unutrašnji) direktni proizvod $\mathbf{H} \times \prod_{i\in J} \mathbf{G}_i\}$. $\mathcal{F}$ je neprazan skup jer je, u svakom slučaju, $\emptyset \in \mathcal{F}$. Osim toga unija ma kog lanca elemenata iz $\mathcal{F}$ je opet u $\mathcal{F}$ (ako je $\forall \alpha, \beta\ (< \gamma)$ $J_\alpha \subseteq J_\beta$, $J_\alpha, J_\beta \in \mathcal{F}$, i $J = \cup_{\alpha<\gamma} J_\alpha$, onda je $\langle H \cup \bigcup_{i\in J} G_i \rangle = \mathbf{H} \times \prod_{i\in J} \mathbf{G}_i$ – lako se proverava da su ispunjeni zahtevi tačaka ($i$) i ($ii$) uslova (2) u 10.9; naravno, razmatramo samo slučaj kada je $\gamma$ granični ordinal), te u $\mathcal{F}$ postoji maksimalni element, recimo, $M$. No onda je $\mathbf{G} = \mathbf{H} \times \prod_{i\in M} G_i$; u suprotnom bismo, naime, imali $\mathbf{G}_k \not\leq \mathbf{H} \times \prod_{i\in M} \mathbf{G}_i$ za neko $k \in I \setminus M$, tj. $\mathbf{G}_k \cap (\mathbf{H} \times \prod_{i\in M} \mathbf{G}_i) = \mathbf{E}$ i stoga $M \cup \{k\} \in \mathcal{F}$, kontradikcija.

($c$) $\Longrightarrow$ ($b$). Kao u prethodnom slučaju – uzeti $\mathbf{H} = \mathbf{E}$.

($b$) $\Longrightarrow$ ($c$). Vrlo trivijalno.

($a$) $\Longrightarrow$ ($c$). Neka je $\mathbf{H}$ podgrupa generisana svim prostim, normalnim podgrupama potpuno razložive grupe $\mathbf{G}$ i pretpostavimo da je $\mathbf{H}$ prava podgrupa. Za dato $g \in G \setminus H$ prema lemi Zorna postoji maksimalna normalna podgrupa $\mathbf{M}$ grupe $\mathbf{G}$ takva da je $\mathbf{H} \leq \mathbf{M}$ i $g \notin M$. Ako je $\mathbf{G}/\mathbf{M}$ prosta grupa i $\mathbf{G} = \mathbf{M} \times \mathbf{K}$, onda je $\mathbf{K}$ ($\cong \mathbf{G}/\mathbf{M}$) prosta grupa i $\mathbf{H} \cap \mathbf{K} = \mathbf{E}$, kontradikcija. Ako je pak $\mathbf{A}/\mathbf{M}$ netrivijalna normalna podgrupa grupe $\mathbf{G}/\mathbf{M}$, tada je $\mathbf{G}/\mathbf{M} = \mathbf{A}/\mathbf{M} \times \mathbf{B}/\mathbf{M}$ za neku normalnu podgrupu $\mathbf{B}$ (pošto je i $\mathbf{G}/\mathbf{M}$ potpuno razloživa grupa). Ali sada je, s obzirom na izbor podgrupe $\mathbf{M}$, $g \in A \cap B = M$ i opet kontradikcija.■

**Korolar 10.31** *Neka je* $\mathbf{G} = \prod_{i\in I} \mathbf{H}_i$*, gde su* $\mathbf{H}_i$*,* $i \in I$*, proste (normalne) podgrupe. Ako je* $\mathbf{Z}(\mathbf{G}) = \mathbf{E}$*, onda su to i jedine minimalne normalne podgrupe grupe* $\mathbf{G}$ *i svaka normalna podgrupa grupe* $\mathbf{G}$ *je direktan proizvod neke podfamilije (podgrupa) familije* $\{\mathbf{H}_i \mid i \in I\}$.



**Dokaz.** Jasno, svaka podgrupa $\mathbf{H}_i$, $i \in I$, je minimalna normalna podgrupa grupe $\mathbf{G}$. Pretpostavimo da je i $\mathbf{K}$ ($\neq \mathbf{H}_i$ za svako $i \in I$) minimalna normalna podgrupa grupe $\mathbf{G}$. No onda je, za svako $i \in I$, $\mathbf{H}_i \cap \mathbf{K} = \mathbf{E}$, pa $\mathbf{H}_i \leq \mathbf{C}(\mathbf{K})$ i stoga $\mathbf{C}(\mathbf{K}) = \mathbf{G}$, tj. $\mathbf{K} \leq \mathbf{Z}(\mathbf{G})$, kontradiktorno uslovu da je $\mathbf{G}$ bez centra. Neka je, dalje, $\mathbf{N}$ normalna podgrupa grupe $\mathbf{G}$ i neka je $\{\mathbf{H}_j \mid i \in J\ (\subseteq I)\}$ familija svih minimalnih normalnih podgrupa grupe $\mathbf{G}$ sadržanih u $\mathbf{N}$ (ako je $\mathbf{N}$ nejedinična grupa, tada je, upravo smo videli, $J$ neprazan skup). Ako je $\mathbf{L}_1 = \prod_{i\in J} \mathbf{H}_i$ i $\mathbf{L}_2 = \prod_{i\in I\setminus J} \mathbf{H}_i$ (za $I = J$ nema se šta dokazivati), tada je $\mathbf{N} = \mathbf{L}_1 \times (\mathbf{N} \cap \mathbf{L}_2)$ (10.17). $\mathbf{N} \cap \mathbf{L}_2$ je normalna podgrupa grupe $\mathbf{L}_2$, čije su jedine normalne podgrupe $\mathbf{H}_i$, $i \in I \setminus J$, te bi $\mathbf{N} \cap \mathbf{L}_2 \neq \mathbf{E}$ impliciralo da je neka od podgrupa $\mathbf{H}_i$, $i \in I \setminus J$, podgrupa grupe $\mathbf{N}$, kontradikcija.□

**Napomena.** Uslov $\mathbf{Z}(\mathbf{G}) = \mathbf{E}$ se ne može eleminisati iz prethodnog tvrđenja (najprostiji kontraprimer nudi Kleinova grupa).

**Korolar 10.32** *Ako je grupa* $\mathbf{G}$ *direktni proizvod neabelovih prostih grupa i ako je* $\mathbf{N}$ *njena normalna podgrupa, onda je* $\mathbf{G} = \mathbf{N} \times \mathbf{C}(\mathbf{N})$.

**Korolar 10.33** *Neka je* $\mathbf{G}$ *Abelova grupa čiji su svi nenula elementi prostog reda* $p$*, tzv. elementarna Abelova* $p$*-grupa. Tada je* $\mathbf{G}$ *potpuno razloživa grupa – direktna suma cikličnih grupa reda* $p$.

**Napomena.** Dokaz prethodnog korolara se lako daje i uz elementarno poznavanje linearne algebre. Takva grupa se jednostavno posmatra kao vektorski prostor nad poljem $\langle Z_p, +_p, \cdot_p \rangle$, a svaki vektorski prostor, poznato je, ima bazu.

Recimo još da je prema tom korolaru kartezijanski proizvod $\prod^c_{\alpha<\lambda} G_\alpha$, gde je $\lambda$ beskonačan kardinal i $\mathbf{G}_\alpha$ ciklična grupa prostog reda $p$ za svako $\alpha < \lambda$, direktna suma $2^\lambda$ cikličnih grupa reda $p$.

**Korolar 10.34** ($a$) *Elementarna Abelova* $p$*-grupa je karakteristično prosta;*

($b$) *Konačna Abelova grupa je karakteristično prosta akko je elementarna.*

($c$) *Direktni proizvod prostih i uzajamno izomorfnih grupa je karakteristično prosta grupa.*

**Dokaz.** ($a$) Neka je $\mathbf{A}$ elementarna Abelova $p$-grupa i $\mathbf{B}$ njena nenula karakteristična podgrupa. $\mathbf{A}$ je, gledaćemo tako, vektorski prostor nad poljem $\langle Z_p, +_p, \cdot_p \rangle$. Ako $0 \neq a \in A$ i $0 \neq b \in B$, onda, budući da je svaki nenula element element neke baze, postoji inverzibilna linearna transformacija (našeg vektorskog prostora) $\varphi$ koja preslikava $b$ u $a$. Posebno, $\varphi$ je automorfizam grupe $\mathbf{A}$, pa kako je $\mathbf{B}$ karakteristična podgrupa, sledi $a \in B$, tj. $\mathbf{B} = \mathbf{A}$.

($b$) Neka je $\mathbf{A}$ konačna, karakteristično prosta Abelova grupa i neka prost broj $p$ deli njen red. Tada je $B = \{b \in A \mid b^p = e\}$ domen nejedinične karakteristične podgrupe, te je $B = A$.

($c$) Ako su grupe Abelove pozivamo se na tačku ($a$), u suprotnom na 10.31. Jer, ako je $\mathbf{N}$ netrivijalna normalna podgrupa grupe $\mathbf{G}$ koja je pak direktni proizvod familije neabelovih, prostih i uzajamno izomorfnih podgrupa $\{\mathbf{H}_i \mid i \in I\}$, onda je $\mathbf{N} = \prod_{i\in J} \mathbf{H}_i$ za neki pravi (neprazan) podskup $J$ skupa $I$. Fiksirajmo jedan indeks, $j_0$, iz $J$ i jedan, $i_0$, iz $I \setminus J$. Ako je $\varphi_{j_0 i_0}$ izomorfno preslikavanje podgrupe $\mathbf{H}_{j_0}$ na $\mathbf{H}_{i_0}$ (dakle, $\varphi_{j_0 i_0}^{-1} \in Aut(\mathbf{H}_{i_0}, \mathbf{H}_{j_0})$), tada je preslikavanje $\varphi : H_{j_0} H_{i_0} \longrightarrow H_{j_0} H_{i_0}$ dato sa $(h_{j_0} h_{i_0})\varphi = (h_{j_0})\varphi_{j_0 i_0}(h_{i_0})\varphi_{j_0 i_0}^{-1}$ automorfizam (podgrupe) $\mathbf{H}_{j_0} \times \mathbf{H}_{i_0}$, koji opet determiniše automorfizam $\overline{\varphi}$ grupe $\mathbf{G}$ čija je restrikcija nad $\prod^d_{i\in I\setminus\{i_0,j_0\}} H_i$ identično preslikavanje i za koji važi $\mathbf{N} \not\leq (\mathbf{N})\overline{\varphi}$.□

**Napomena**. Uslov konačnosti se ne može eleminisati iz tačke ($b$) (kada je u pitanju pravac $\Longrightarrow$) - podsećamo se: aditivna grupa svakog polja je karakteristično prosta.

**Korolar 10.35** *Frattijeva podgrupa elementarne Abelove p-grupe je jedinična grupa.*

**Dokaz**. Ako je $\mathbf{G} = \sum_{i\in I} \mathbf{H}_i$, gde je, za svako $i \in I$, $\mathbf{H}_i$ ciklična grupa reda $p$, tada je $\{\mathbf{G}_j \mid j \in I\}$, gde je $\mathbf{G}_j = \sum_{i\in I\setminus\{j\}} \mathbf{H}_i$, familija maksimalnih podgrupa grupe $\mathbf{G}$ i, očigledno, $\mathbf{Fr}(\mathbf{G}) = \bigcap_{j\in I} \mathbf{G}_j = \mathbf{E}$.□

**Korolar 10.36** *Grupa bez netrivijalnih automorfizama ima najviše dva elementa.*

**Dokaz**. Neka je identično preslikavanje jedini automorfizam grupe $\mathbf{G}$. Kako je $\mathbf{G}/\mathbf{Z}(\mathbf{G}) \cong \mathbf{Inn}(\mathbf{G}) \leq \mathbf{Aut}(\mathbf{G})$, to je $\mathbf{G} = \mathbf{Z}(\mathbf{G})$, tj. $\mathbf{G}$ je Abelova grupa. Ako bi postojao bar jedan element reda većeg od 2, onda bi preslikavanje $\varphi : G \longrightarrow G$, gde je $(g)\varphi = g^{-1}$, bilo netrivijalni automorfizam (2.16). Ako su pak svi elementi reda 2, grupa $\mathbf{G}$ bi bila, u slučaju da ima više od dva elementa, direktni proizvod više cikličnih grupa reda 2, recimo $\mathbf{G} = \prod_{i\in I} \langle a_i\rangle$ ($|I| \geq 2$), pa bi svaka netrivijalna permutacija skupa $I$ određivala netrivijalni automorfizam grupe $\mathbf{G}$.□

**Korolar 10.37** *Ne postoji grupa čija bi grupa automorfizama bila ciklična grupa neparnog reda većeg od* 1.

**Dokaz**. Već smo videli da grupe automorfizama neabelovih grupa nisu ciklične grupe (8.22).

Ako je $\mathbf{G}$ Abelova grupa sa bar jednim elementom koji nije reda 2, tada je njen automorfizam koji svakom elementu "dodeljuje" njemu inverzni reda



2. Ako su svi elementi grupe $\mathbf{G}$ reda 2, $\mathbf{G}$ je direktni proizvod cikličnih grupa reda 2. Ako je $\mathbf{G}$ reda 2, njena grupa automorfizama je jedinična grupa. Ako je $\mathbf{G} = \langle a\rangle \times \langle b\rangle \times \mathbf{H}$, gde je $\mathbf{H}$ ili jedinična podgrupa ili direktni proizvod cikličnih podgrupa (reda 2), onda je grupa automorfizama Kleinove podgrupe $\langle a\rangle \times \langle b\rangle$ - simetrična grupa $\mathbf{S}_3$, tj. njena izomorfna slika, podgrupa grupe $\mathbf{Aut}(\mathbf{G})$.□

**Korolar 10.38** *Direktni proizvod potpuno razloživih grupa je potpuno razloživa grupa.*

Nešto od dokaza poslednje teoreme ($(c) \Longrightarrow (a)$), zapravo nešto opštiji slučaj, imamo u narednom tvrđenju.

**Lema 10.39** *Neka je* $\mathbf{H}$ *podgrupa i* $\mathcal{S}$ *familija podgrupa grupe* $\mathbf{G}$. *Tada postoji maksimalna podfamilija* $\mathcal{M}$ *familije* $\mathcal{S}$ *takva da je* $\langle H, \bigcup\mathcal{M}\rangle = \mathbf{H} \times \prod_{\mathbf{A}\in\mathcal{M}} \mathbf{A}$.

**Dokaz**. Neka je $\Upsilon = \{\mathcal{K} \subseteq \mathcal{S} \mid \langle H, \bigcup\mathcal{K}\rangle = \mathbf{H} \times \prod_{\mathbf{A}\in\mathcal{K}} \mathbf{A}\}$ (u pitanju je neprazan skup jer je svakako $\emptyset \in \Upsilon$) i neka je $\{\mathcal{S}_\alpha \mid \alpha < \gamma\}$, $\gamma$ granični ordinal, jedan lanac parcijalno uređenog skupa $\langle\Upsilon, \subseteq\rangle$ (za $\alpha < \beta$ je $\mathcal{S}_\alpha \subseteq \mathcal{S}_\beta$). Proveravamo: $\langle H, \bigcup_{\alpha<\gamma} \mathcal{S}_\alpha\rangle = \mathbf{H} \times \prod_{\mathbf{A}\in\bigcup_{\alpha<\gamma}\mathcal{S}_\alpha} \mathbf{A}$, tj. važenje tačaka ($i$) i ($ii$) uslova (2) iz leme 10.9. Očigledna je uzajamna permutabilnost elemenata iz različitih podgrupa $\mathbf{A}$, $\mathbf{B}$ koje pripadaju nekim od familija $\mathcal{S}_\alpha$, $\alpha < \gamma$, kao i permutabilnost elemenata ovih podgrupa sa elementima grupe $\mathbf{H}$; bilo koji konačan skup elemenata iz $\bigcup\{A \mid A \in \bigcup_{\alpha<\gamma} \mathcal{S}_\alpha\}$ sadržan je u $\{A \mid A \in \bigcup_{\alpha<\beta} \mathcal{S}_\alpha\}$ za neki ordinal $\beta$ manji od $\gamma$. Isto tako, ako je $h_1 a_1 \dots a_m = h_2 b_1 \dots b_n$, $h_1, h_2 \in H$, $a_i, b_j \in \bigcup\{A \mid A \in \bigcup_{\alpha<\beta(<\gamma)} \mathcal{S}_\alpha\}$ i ako su $a_1, \dots, a_m$, $b_1, \dots, b_n$ nejedinični elementi različitih podgrupa, onda iz $h_2^{-1} h_1 = b_1 \dots b_n a_m^{-1} \dots a_1^{-1} \in H \cap \prod^d_{\mathbf{A}\in\bigcup_{\alpha<\beta}\mathcal{S}_\alpha} A = \{e\}$ sledi $h_1 = h_2$, a pretpostavka da je npr. $a_1$ različito od svakog $b_j$, $j = 1, \dots, n$, jednako vodi u kontradikciju. Konačno, lema Zorna nam garantuje egzistenciju maksimalne podfamilije familije $\mathcal{S}$ sa traženim svojstvom (ako je $\gamma$ nasledni ordinal imamo još trivijalniji slučaj).□

**Korolar 10.40** *Ako je grupa* $\mathbf{G}$ *karakteristično prosta a* $\mathbf{H}$ *jedna njena minimalna normalna podgrupa, onda je* $\mathbf{H}$ *prosta grupa i* $\mathbf{G}$ *je direktan proizvod podgrupa izomorfnih sa* $\mathbf{H}$.

**Dokaz**. Pretpostavimo odmah da je $\mathbf{H}$ prava podgrupa i neka je $\mathcal{S} = \{(\mathbf{H})\varphi \mid \varphi \in Aut(\mathbf{G})\}$. Svaka podgrupa iz $\mathcal{S}$ je minimalna normalna (dakle nejedinična), te je presek bilo koje dve različite podgrupe iz $\mathcal{S}$ jedinična podgrupa. Prema prethodnoj lemi postoji maksimalna podfamilija $\mathcal{M}$ familije $\mathcal{S}$ takva da je $\mathbf{N} = \langle\bigcup\mathcal{M}\rangle = \prod_{\mathbf{K}\in\mathcal{M}} \mathbf{K}$. Ako bi $\mathbf{N}$ bila prava podgrupa grupe $\mathbf{G}$, onda bi za neki automorfizam $\psi$ grupe $\mathbf{G}$ bilo: $(\mathbf{H})\psi \not\leq \mathbf{N}$ (inače bi $\mathbf{N}$ bila

karakteristična podgrupa) i, s obzirom da je $(\mathbf{H})\psi$ minimalna normalna podgrupa, $(\mathbf{H})\psi \cap \mathbf{N} = \mathbf{E}$. No tada je $\langle (H)\psi, N\rangle = (\mathbf{H})\psi \times \mathbf{N}$, kontradiktorno sa maksimalnošću familije $\mathcal{M}$. Naravno, možemo pretpostaviti da je jedan od direktnih faktora grupe baš podgrupa $\mathbf{H}$. Pretpostavimo još da $\mathbf{H}$ nije prosta. Ali onda je njena netrivijalna normalna podgrupa (kao normalna podgrupa direktnog faktora) normalna podgrupa i grupe $\mathbf{G}$, kontradikcija.□

**Korolar 10.41** *Ako je $\mathcal{I} = \{\mathbf{H}_i \mid i \in I\}$ familija minimalnih normalnih podgrupa grupe $\mathbf{G}$, onda je podgrupa $\mathbf{K} = \langle \bigcup_{i\in I} H_i\rangle$ direktan proizvod podgrupa neke podfamilije $\mathcal{J}$ familije $\mathcal{I}$.*

**Dokaz.** Neka je $\mathcal{J} = \{\mathbf{H}_i \mid i \in J\}$ maksimalna podfamilija familije $\mathcal{I}$ takva da je $\mathbf{L} = \langle \bigcup_{i\in J} H_i\rangle = \prod_{i\in J} \mathbf{H}_i$. Jasno, $\mathbf{L}$ i $\mathbf{K}$ su normalne podgrupe grupe $\mathbf{G}$ (i $\mathbf{L} \leq \mathbf{K}$). Ako bi $\mathbf{L}$ bila prava podgrupa grupe $\mathbf{K}$, onda bi za neko $i \in I$ imali $\mathbf{H}_i \not\leq \mathbf{L}$ i $\langle H_i, L\rangle = \mathbf{H}_i \times \mathbf{L}$, kontradiktorno izboru podfamilije $\mathcal{J}$.□

**Korolar 10.42** *Ako je $\mathbf{H}$ minimalna normalna podgrupa grupe $\mathbf{G}$ i $\mathbf{K}$ minimalna normalna podgrupa grupe $\mathbf{H}$, tada je $\mathbf{K}$ prosta grupa, a $\mathbf{H}$ je direktni proizvod konjugata (u grupi $\mathbf{G}$) podgrupe $\mathbf{K}$.*

**Dokaz.** $\mathbf{H}$ nema netrivijalnih karakterističnih podgrupa (4.34) te je, prema prethodnom korolaru, $\mathbf{K}$ prosta grupa a $\mathbf{H}$ direktni proizvod familije podgrupa izomorfnih sa $\mathbf{K}$. Preostaje jedino da se pokaže da izomorfne kopije podgrupe $\mathbf{K}$ možemo izabrati baš iz familije podgrupa konjugovanih sa $\mathbf{K}$; obeležimo tu familiju sa $\mathcal{S}$. Prema prethodnoj teoremi je $\mathbf{N} = \langle \bigcup \mathcal{S}\rangle$ direktni proizvod prostih podgrupa, konjugata podgrupe $\mathbf{K}$, i kako je to normalna podgrupa grupe $\mathbf{G}$, važi $\mathbf{H} = \mathbf{N}$.□

**Korolar 10.43** *Minimalna normalna podgrupa konačne grupe je direktni proizvod prostih podgrupa.*

**Lema 10.44** *Sledeći uslovi su ekvivalentni za grupu $\mathbf{G}$:*

*(a) $\mathbf{G}$ je (do na izomorfizam) kartezijanski proizvod familije grupa $\{\mathbf{G}_i \mid i \in I\}$;*

*(b) Postoje homomorfizmi $\pi_i \in Hom(\mathbf{G}, \mathbf{G}_i)$, $i \in I$, za koje važi:*

$$\bigcap_{i\in I} \mathbf{Ker}(\pi_i) = \mathbf{E},$$

*i ako je $\mathbf{H}$ (ma kakva) grupa i $\varphi_i \in Hom(\mathbf{H}, \mathbf{G}_i)$ (za svako $i \in I$), onda postoji jedinstven homomorfizam $\varphi \in Hom(\mathbf{H}, \mathbf{G})$ takav da je $\varphi\pi_i = \varphi_i$ za svako $i \in I$.*

**Dokaz.** $(a) \Longrightarrow (b)$. Neka je $\mathbf{G} = \prod^c_{i\in I} \mathbf{G}_i$ i $\pi_i : G \longrightarrow G_i$ projekcija grupe $\mathbf{G}$ na $\mathbf{G}_i$, dakle $(f)\pi_i = (i)f$ (ovo preslikavanje neki put zovemo i *prirodnim*



*ili kanoničkim homomorfizmom*). Trivijalno, $\bigcap_{i\in I} \mathbf{Ker}(\pi_i) = \mathbf{E}$. Ako se, opet, neka grupa $\mathbf{H}$ homomorfno preslikava u svaku od grupa $\mathbf{G}_i$, pri čemu su $\varphi_i$ odgovarajući homomorfizmi, onda preslikavanje $\varphi : H \longrightarrow G$ definisano sa $(i)((a)\varphi) = (a)\varphi_i$ $(a \in H)$ ispunjava uslove tačke $(b)$. Jer, $\varphi$ je homomorfizam:

$$(i)((ab)\varphi) = (ab)\varphi_i = (a)\varphi_i(b)\varphi_i = (i)((a)\varphi)(i)((b)\varphi) = (i)((a)\varphi(b)\varphi),$$

znači $(ab)\varphi = (a)\varphi(b)\varphi$; dalje je $(a)(\varphi\pi_i) = ((a)\varphi)\pi_i = (i)((a)\varphi) = (a)\varphi_i$, pa je $\varphi\pi_i = \varphi_i$ za svako $i \in I$; konačno, ako je i $\psi \in Hom(\mathbf{H}, \mathbf{G})$ i $\psi\pi_i = \varphi_i$ za svako $i \in I$, tada iz $(i)((a)\psi) = (a)\varphi_i$ (za svako $a \in H$ i svako $i \in I$) sledi $(i)((a)\psi) = (i)((a)\varphi)$, tj. $(a)\psi = (a)\varphi$, te je $\psi = \varphi$.

$(b) \Longrightarrow (a)$. Pretpostavimo da važi $(b)$. Neka je $\mathbf{H} = \prod^c_{i\in I} \mathbf{G}_i$ i $\varphi_i$ projekcija grupe $\mathbf{H}$ na $\mathbf{G}_i$ za svako $i \in I$. Tada je, za jedinstveno $\varphi \in Hom(\prod^c_{i\in I} \mathbf{G}_i, \mathbf{G})$, $\forall i \in I$ $\varphi\pi_i = \varphi_i$. Iz prvog dela dokaza sledi pak egzistencija homomorfizma $\pi \in Hom(\mathbf{G}, \prod^c_{i\in I} \mathbf{G}_i)$ takvog da je $\pi\varphi_i = \pi_i$ za svako $i \in I$. Iz datih relacija se dobija $\varphi\pi\varphi_i = \varphi\pi_i = \varphi_i$; prema tome je, za svako $f \in \prod_{i\in I} G_i$ i svako $i \in I$, $(f)((\varphi\pi)\varphi_i) = (f)\varphi_i = (i)f$, odnosno $(i)((f)(\varphi\pi)) = (i)f$. Znači, $(f)(\varphi\pi) = f$ pa je $\varphi\pi = \imath_H$ – identično preslikavanje skupa $H = \prod_{i\in I} G_i$. Osim toga imamo i $\pi\varphi\pi_i = \pi\varphi_i = \pi_i$ te je, za svako $g \in G$ i svako $i \in I$, $((g)(\pi\varphi))\pi_i = (g)\pi_i$. Odatle: $(g)(\pi\varphi)\cdot g^{-1} = e$, tj. $(g)(\pi\varphi) = g$. Zaključujemo: kako je $\pi\varphi = \imath_G$, $\varphi$ i $\pi$ su bijektivna preslikavanja i $\mathbf{G} \cong \prod^c_{i\in I} \mathbf{G}_i$.□

**Primer 10.45** *(a) Konačan (direktan) proizvod konačnih cikličnih grupa je ciklična grupa akko su redovi svake dve ciklične grupe uzajamno prosti.*

**Dokaz.** Dovoljno je posmatrati proizvod dve ciklične grupe. Kao i obično radimo sa "prototipovima" cikličnih grupa. Ako su $m$ i $n$ uzajamno prosti brojevi, onda je u grupi $\mathbf{Z}_m + \mathbf{Z}_n$ element $(1,1) = (1,0)+(0,1)$ reda $NZS(m,n) = mn$, pa je $\mathbf{Z}_m + \mathbf{Z}_n \cong \mathbf{Z}_{mn}$. S druge strane, ako je $(m,n) = k > 1$ i $m = kr$, $n = kt$, onda za bilo koji element $(a,b)$ grupe $\mathbf{Z}_m + \mathbf{Z}_n$ imamo:

$$krt(a,b) = krt(a,0)+krt(0,b) = (krta-[\frac{krta}{m}]m,0)+(0,krtb-[\frac{krtb}{n}]n) = (0,0),$$

te grupa $\mathbf{Z}_m + \mathbf{Z}_n$ nije ciklična.

*(b) Za $n \geq 3$ važi $\mathbf{Aut}(\mathbf{Z}_{2^n}) \cong \mathbf{Z}_2 \times \mathbf{Z}_{2^{n-2}}$; $\mathbf{Aut}(\mathbf{Z}_4) \cong \mathbf{Z}_2$.*

**Dokaz.** Neka je $n > 3$. Već znamo da je $\mathbf{Aut}(\mathbf{Z}_{2^n})$ grupa reda $2^{n-1}$, izomorfna grupi $\langle\{a \in 2^n \mid (a,2) = 1\}, \cdot_{2^n}\rangle$ sa kojom nadalje radimo (videti dokaz tačke $(g)$ primera 3.4 i lemu 8.24). $2^n-1$ je element reda 2, a 3 je element reda $2^{n-2}$; lako se proverava indukcijom da je, za $n \geq 3$, $3^{2^{n-2}} \equiv 1 \pmod{2^n}$, međutim za $k < n-2$ i $n > 3$ ne važi $3^{2^k} \equiv 1 \pmod{2^n}$ (ta bi relacija, uz uslov $k > 1$, implicirala $4|(3^{2^{k-1}}+1)$). Dalje, $2^n - 1 \notin \langle 3\rangle$; jer kako je $2^n - 1$ reda 2, iz pretpostavke $2^n - 1 \in \langle 3\rangle$ sledilo bi $2^n - 1 = 3^{2^{n-3}} - [\frac{3^{2^{n-3}}}{2^n}]2^n$ (ciklična

grupa parnog reda sadrži samo jedan element reda 2), a odatle $2^n|(3^{2^{n-3}}+1)$, što je već očigledno nemoguće. Zaključujemo: prema 10.25 – $\langle\{a \in 2^n \mid (a,2)=1\}, \cdot_{2^n}\rangle$ je direktan proizvod cikličnih podgrupa $\langle 2^n-1\rangle$ i $\langle 3\rangle$, redova, respektivno, 2 i $2^{n-2}$.

Gornje razmatranje obuhvata i slučaj $n=3$, te je

$$\mathbf{Aut}(\mathbf{Z}_8) \cong \langle\{1,3,5,7\}, \cdot_8\rangle = \langle 7\rangle \times \langle 3\rangle \quad \textit{(Kleinova grupa).}$$

(*c*) *Neka su* $m_1,\ldots,m_r$ *uzajamno prosti brojevi. Tada je*

$$\langle\{k \in m_1\ldots m_r \mid (k, m_1\ldots m_r)=1\}, \cdot_{m_1\ldots m_r}\rangle \cong$$

$$\langle\{k \in m_1 \mid (k,m_1)=1\}, \cdot_{m_1}\rangle \times\cdots\times \langle\{k \in m_r \mid (k,m_r)=1\}, \cdot_{m_r}\rangle.$$

**Dokaz**. Direktna posledica tačke (*a*) i 2.10(*e*), 8.24 i 10.28.

(*d*) $\mathbf{End}(\underbrace{\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}}_{n-puta}) \cong \mathbf{M}_n(\mathbf{Z})$, *gde je* $\mathbf{M}_n(\mathbf{Z})$ *polugrupa (sa jedinicom) kvadratnih matrica formata* $n\times n$ *čiji su elementi celi brojevi – elementi prstena celih brojeva (operacija je, jasno, matrično množenje).*

**Dokaz**. Generatorni elementi grupe $\underbrace{\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}}_{n-puta}$ su

$$(1,0,\ldots,0), (0,1,\ldots,0),\ldots,(0,0,\ldots,1).$$

Naravno, $A = \{(1,0,\ldots,0),\ldots,(0,0,\ldots,1)\}$ nije jedini generatorni skup (inače, čitalac iole upućen u teoriju modula zna da se ovde radi o slobodnom modulu nad prstenom celih brojeva). Svaki endomorfizam date grupe određen je, jasno, slikama generatornih elemenata. S druge strane, svako se preslikavanje $\varphi : A \longrightarrow Z\oplus\cdots\oplus Z$ može proširiti do endomorfizma. Ako je $(1,0,\ldots,0)\varphi = (a_{11},a_{12},\ldots,a_{1n})$, $\ldots$, $(0,0,\ldots,1)\varphi = (a_{n1},a_{n2},\ldots,a_{nn})$, onda je preslikavanje $\Phi : Z\oplus\cdots\oplus Z \longrightarrow Z\oplus\cdots\oplus Z$ dato sa

$$(b_1,\ldots,b_n)\Phi = (b_1a_{11}+b_2a_{21}+\cdots+b_na_{n1},\ldots,b_1a_{1n}+b_2a_{2n}+\cdots+b_na_{nn})$$

endomorfizam grupe i $\Phi|_A = \varphi$ (proveru detalja ostavljamo za vežbu). Pridružimo endomorfizmu $\Phi$ matricu

$$M_\Phi = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix}.$$

Preostaje nam samo da proverimo da je $M_{\Phi\Psi} = M_\Phi M_\Psi$ za $\Phi,\Psi \in End(\mathbf{Z}\oplus\cdots\oplus\mathbf{Z})$.



Neka je $\Phi$ gore dato preslikavanje i

$$(1,0,\ldots,0)\Psi = (b_{11},b_{12},\ldots,b_{1n})$$

$$(0,1,\ldots,0)\Psi = (b_{21},b_{22},\ldots,b_{2n})$$

$$\vdots$$

$$(0,0,\ldots,1)\Psi = (b_{n1},b_{n2},\ldots,b_{nn}).$$

Tada je

$$(1,0,\ldots,0)\Phi\Psi = (a_{11},a_{12},\ldots,a_{1n})\Psi =$$

$$(a_{11}b_{11}+a_{12}b_{21}+\cdots+a_{1n}b_{n1},\ \ldots,\ a_{11}b_{1n}+a_{12}b_{2n}+\cdots+a_{1n}b_{nn})$$

$$\vdots$$

$$(0,0,\ldots,1)\Phi\Psi = (a_{n1},a_{n2},\ldots,a_{nn})\Psi =$$

$$(a_{n1}b_{11}+a_{n2}b_{21}+\cdots+a_{nn}b_{n1},\ \ldots,\ a_{n1}b_{1n}+a_{n2}b_{2n}+\cdots+a_{nn}b_{nn}),$$

te je

$$M_{\Phi\Psi} = M_\Phi M_\Psi =$$

$$\begin{bmatrix} a_{11}b_{11}+a_{12}b_{21}+\cdots+a_{1n}b_{n1} & \ldots & a_{11}b_{1n}+a_{12}b_{2n}+\cdots+a_{1n}b_{nn} \\ \vdots & \ddots & \vdots \\ a_{n1}b_{11}+a_{n2}b_{21}+\cdots+a_{nn}b_{n1} & \ldots & a_{n1}b_{1n}+a_{n2}b_{2n}+\cdots+a_{nn}b_{nn} \end{bmatrix}$$

(skrećemo pažnju onima koji su upoznati sa matričnim računom da mi elemente pišemo sa leve strane funkcije, pa shodno tome, i komponente slika generatornih elemenata slažemo po vrstama a ne po kolonama, kako se uglavnom radi).

(*e*) $\mathbf{Aut}(\underbrace{\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}}_{n-puta}) \cong \mathbf{GL}_n(\mathbf{Z})$, *gde je* $\mathbf{GL}_n(\mathbf{Z})$ *grupa čiji je domen skup inverzibilnih matrica polugrupe* $\mathbf{M}_n(\mathbf{Z})$.

**Dokaz**. Obeležimo u cilju pojednostavljenja notacije generatorne elemente grupe $\underbrace{\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}}_{n-puta}$ date u dokazu prethodne tačke sa, respektivno (imajući u vidu njihov redosled), $\mathbf{a}_1$, $\ldots$, $\mathbf{a}_n$, a nula element $((0,0,\ldots,0))$ sa $\mathbf{0}$. Ako je $\Phi$ automorfizam "naše" grupe, onda su elementi $(\mathbf{a}_1)\Phi,\ldots,(\mathbf{a}_n)\Phi$ linearno nezavisni, tj. važi:

$$m_1(\mathbf{a}_1)\Phi+\cdots+m_n(\mathbf{a}_n)\Phi = \mathbf{0},\ m_i \in Z \text{ akko } m_1=\cdots=m_n=0$$

(jer, $m_1(\mathbf{a}_1)\Phi+\cdots+m_n(\mathbf{a}_n)\Phi = (m_1\mathbf{a}_1+\cdots+m_n\mathbf{a}_n)\Phi = \mathbf{0}$ akko $m_1\mathbf{a}_1+\cdots+m_n\mathbf{a}_n = \mathbf{0}$ akko $m_1=\cdots=m_n=0$). Stoga su u matrici $M_\Phi$ vektori vrste linearno nezavisni ($rang(M_\Phi)=n$) pa je ona inverzibilna. Kako je za identični

automorfizam ($\imath$) $M_\imath = I$ – jedinična matrica i $I = M_{\Phi\Phi^{-1}} = M_\Phi M_{\Phi^{-1}}$, to je $M_\Phi^{-1} = M_{\Phi^{-1}} \in M_n(\mathbf{Z})$.

S druge strane ako je matrica

$$M = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \in M_n(\mathbf{Z})$$

inverzibilna u $M_n(\mathbf{Z})$ (dakle, i $M^{-1} \in M_n(\mathbf{Z})$), onda je preslikavanje $\Phi_M$ (domena grupe u sebe) dato sa:

$$(\mathbf{a}_i)\Phi = a_{i1}\mathbf{a}_1 + \dots + a_{in}\mathbf{a}_n, \quad i = 1, \dots, n,$$

automorfizam. Zaista, $\Phi$ je injektivno, jer ako je $\mathbf{b} = (x_1, \dots, x_n)$, $\mathbf{c} = (y_1, \dots, y_n)$ i $(\mathbf{b})\Phi_M = (\mathbf{c})\Phi_M$, tada je i $BM = CM$, gde su $B$ i $C$, respektivno, matrice $[x_1, \dots, x_n]$, $[y_1, \dots, y_n]$, a odatle $B = (BM)M^{-1} = (CM)M^{-1} = C$, dakle i $\mathbf{b} = \mathbf{c}$. $\Phi$ je surjektivno zbog $(BM^{-1})M = B$. Svojstvo homomorfnosti se takođe lako proverava.

($f$)

$$\mathbf{End}(\underbrace{\mathbf{Z}_m \oplus \dots \oplus \mathbf{Z}_m}_{n-puta}) \cong \mathbf{M}_n(\mathbf{Z}_m);$$

$$\mathbf{Aut}(\underbrace{\mathbf{Z}_m \oplus \dots \oplus \mathbf{Z}_m}_{n-puta}) \cong \mathbf{GL}_n(\mathbf{Z}_m).$$

**Dokaz.** Analogan je dokazu prethodnih tačaka ($d$) i ($e$). Dodajmo samo da se umesto $\mathbf{M}_n(\mathbf{Z}_m)$, $\mathbf{GL}_n(\mathbf{Z}_m)$ piše i $\mathbf{M}_n(m)$, $\mathbf{GL}_n(m)$, jer su elementi matrica prirodni brojevi manji od $m$, a sabiranje i množenje elemenata je po modulu $m$, dakle kako već nalažu operacije u prstenu $\langle m, +_m, \cdot_m \rangle$ (za koji ovde iznimno koristimo oznaku inače rezervisa za cikličnu grupu $\langle m, +_m \rangle$ – $\mathbf{Z}_m$).

($g$)

$$\mathbf{End}(\underbrace{\mathbf{Ra} \oplus \dots \oplus \mathbf{Ra}}_{n-puta}) \cong \mathbf{M}_n(\mathbf{Ra});$$

$$\mathbf{Aut}(\underbrace{\mathbf{Ra} \oplus \dots \oplus \mathbf{Ra}}_{n-puta}) \cong \mathbf{GL}_n(\mathbf{Ra}).$$

**Dokaz.** Primetimo prvo da je svaki endomorfizam ponovo određen slikama elemenata $\mathbf{a}_1 = (1, 0, \dots, 0), \dots, \mathbf{a}_n = (0, 0, \dots, 1)$ (premda oni ne generišu datu grupu). Jer, ako je $\mathbf{a} = (\frac{p_1}{q_1}, \dots, \frac{p_n}{q_n})$, $p_i \in Z$, $q_i \in \omega \setminus \{0\}$, $q = NZS(q_1, \dots, q_n)$ i $q = q_i r_i$ za $i = 1, \dots, n$, tada je $(q\mathbf{a})\Phi = (p_1 r_1, \dots, p_n r_n)\Phi$, pa je

$$q((\mathbf{a})\Phi) = p_1 r_1 (\mathbf{a}_1)\Phi + \dots + p_n r_n (\mathbf{a}_n)\Phi$$

i

$$(\mathbf{a})\Phi = \frac{p_1}{q_1}(\mathbf{a}_1)\Phi + \dots + \frac{p_n}{q_n}(\mathbf{a}_n)\Phi.$$



Svako preslikavanje skupa $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ u skup $\underbrace{Ra \oplus \dots \oplus Ra}_{n-puta}$ može se opet proširiti (na prirodan način) do endomorfizma grupe – dokaz je analogan dokazu tačke ($d$), a isto tako slede i provere navedenih relacija.

Podsetimo se da smo poseban slučaj ovog tvrđenja ($n = 1$) već imali ($2.10(f)$).

($h$) *Normalna podgrupa* $\mathbf{N}$ *grupe* $\mathbf{G}$ *je direktan faktor akko postoji endomorfizam* $\varphi$ *grupe* $\mathbf{G}$ *takav da je* $\varphi|_N = \imath_N$.

**Dokaz.** Pravac ($\Longrightarrow$) je trivijalan, a u drugom smeru imamo $\mathbf{G} = \mathbf{N} \times \mathbf{Ker}(\varphi)$.□

**Lema 10.46** *Za prost broj* $p$ *je*

$$|Aut(\underbrace{\mathbf{Z}_p \oplus \dots \oplus \mathbf{Z}_p}_{n-puta})| = |GL_n(\mathbf{Z}_p)| = (p^n - 1)(p^n - p)\dots(p^n - p^{n-1}).$$

**Dokaz.** Pozivamo se na elementarno poznavanje linearne algebre. Regularne matrice formata $n \times n$ sa elementima iz polja $\langle p, +_p, \cdot_p \rangle$ u jedan-jedan su korespondenciji sa regularnim linearnim transformacijama vektorskog prostora dimenzije $n$ nad tim poljem. Taj prostor ima $p^n = \overline{V}_n^p$ (= broj varijacija s ponavljanjem od $p$ elemenata $n$-klase) elemenata – za vektore možemo uzeti baš uređene $n$-torke sa elementima iz $p$. Fiksirajmo jednu bazu, npr. $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$. Znamo da je za regularnu linearnu transformaciju $T$ i $\{(\mathbf{v}_1)T, \dots, (\mathbf{v}_n)T\}$ baza. S druge strane, ako je $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ baza, postoji jedinstvena regularna transformacija $S$ koja preslikava $\mathbf{v}_i$ u $\mathbf{u}_i$ za svako $i = 1, \dots, n$. Stoga je broj regularnih linearnih transformacija jednak broju uređenih baza datog vektorskog prostora. Za prvi element baze možemo uzeti bilo koji nenula vektor; imamo, dakle, na raspolaganju $p^n - 1$ elemenata. Ako smo izabrali $\mathbf{w}_1$, on generiše podprostor sa $p$ elemenata (članovi tog podprostora su $k\mathbf{w}_1$, $k \in p$), pa za drugi element baze možemo uzeti bilo koji od preostalih vektora, a tih je $p^n - p$. Kada smo već izabrali prvih $i$ elemenata baze $\mathbf{w}_1, \dots, \mathbf{w}_i$, za $i+1$-vi možemo uzeti bilo koji od vektora koji nije u podprostoru generisanom skupom izabranih. Taj podprostor ima $p^i$ elemenata (jer upravo je toliko različitih linearnih kombinacija $k_1\mathbf{w}_1 + \dots + k_i\mathbf{w}_i$, $k_j \in p$), prema tome na raspolaganju nam je $p^n - p^i$ vektora. Konačno, za poslednji element baze preostaće $p^n - p^{n-1}$ "kandidata", te uređenih baza imamo $\prod_{j=0}^{n-1}(p^n - p^j)$.□

**Lema 10.47** *Ako je* $n = 2^{k_0} p_1^{k_1} \dots p_{r-1}^{k_{r-1}}$, *gde su* $p_1, \dots, p_{r-1}$ *različiti neparni prosti brojevi,* $r \geq 0$, $k_0 \geq 0$, $k_i \geq 1$ *za* $i = 1, \dots, r-1$, *tada je*

$$\mathbf{Aut}(\mathbf{Z}_n) \cong \mathbf{H}_2 \times \mathbf{Z}_{p_1^{k_1-1}(p_1-1)} \times \dots \times \mathbf{Z}_{p_{r-1}^{k_{r-1}-1}(p_{r-1}-1)},$$

*gde je*

$$\mathbf{H}_2 = \begin{cases} \mathbf{E} & k_0 = 0 \\ \mathbf{Z}_{2^{k_0-1}} & k_0 = 1, 2 \\ \mathbf{Z}_2 \times \mathbf{Z}_{2^{k_0-2}} & k_0 \geq 3. \end{cases}$$

**Dokaz**. Primetimo samo: ako je $r = 1$, onda je $n = 2^{k_0}$. Ostalo je dokazano: 8.26, 10.45($b$), 10.24($g$) i 10.27 (ili, po izboru, 10.28).□

Konstatujmo ovom prilikom i sledeće. Direktni proizvod je podgrupa kartezijanskog proizvoda. Analogno, mogli smo posmatrati i ovakve podgrupe: neka je, za svako $i \in I$, $\mathbf{H}_i < \mathbf{G}_i$; onda je $\{f \in \prod_{i\in I} G_i \mid |\{i \mid (i)f \notin H_i\}| < \aleph_0\}$ domen podgrupe kartezijanskog proizvoda – slučaj: $\mathbf{H}_i = \mathbf{E}$ za svako $i \in I$ daje upravo direktan proizvod. Naravno, i tu su nam na raspolaganju dalje varijacije. Recimo za kardinal $\mu$, $\aleph_0 < \mu < \lambda$ imamo podgrupu kartezijanskog proizvoda $\prod^{c}_{i\in I} \mathbf{G}_i$, $|I| = \lambda$, sa domenom $\{f \in \prod_{i\in I} G_i \mid |\{i \mid (i)f \notin H_i\}| < \mu\}$. Tema se proširuje razmatranjem u kakvoj su relaciji svojstva tako dobijenih podgrupa kartezijanskog proizvoda sa svojstvima podgrupa $\mathbf{H}_i$, $i \in I$.

Dajemo na kraju i ovu interesantnu teoremu.

**Teorema 10.48** *Postoji kontinuum mnogo neizomorfnih grupa generisanih sa dva elementa.*

**Dokaz**. Neka je $\xi$ strogo rastući beskonačni niz neparnih brojeva: $u_1 < u_2 < \cdots < u_n < \cdots$, gde je $u_1 \geq 5$, i neka je $\mathbf{H}_\xi = \mathbf{A}_{u_1} \times \mathbf{A}_{u_2} \times \cdots \times \mathbf{A}_{u_n} \times \cdots$, gde je $\mathbf{A}_{u_k}$ grupa parnih permutacija skupa $D_k = \{0_k, 1_k, \ldots, (u_k - 1)_k\}$ (dakle, alternativna grupa stepena $u_k$). Prema 9.18($a$), $\mathbf{A}_{u_k}$ je generisana permutacijama $\alpha_k = (0_k \ \ 1_k \ldots (u_k - 1)_k)$ i $\beta_k = (0_k \ \ 1_k \ \ 2_k)$. Grupu $\mathbf{H}_\xi$ možemo, jasno, tretirati kao podgrupu grupe $\mathbf{S}_{A_\xi}$, gde je $A_\xi = \bigcup_{k=1}^{\infty} D_k$. Pokazaćemo prvo da je ona sadržana u podgrupi $\mathbf{G}_\xi$ (grupe $\mathbf{S}_{A_\xi}$ generisanoj elementima $\alpha = (0_1 \ 1_1 \ \ldots (u_1-1)_1)(0_2 \ 1_2 \ldots (u_2-1)_2)\ldots(0_n \ 1_n \ldots (u_n - 1)_n)\ldots$ i $\beta = (0_1 \ 1_1 \ 2_1)(0_2 \ 1_2 \ 2_2)\ldots(0_n \ 1_n \ 2_n)\ldots$; pisaćemo nedovoljno korektno ali dovoljno jasno: $\alpha = \alpha_1\alpha_2\ldots\alpha_n\ldots$, $\beta = \beta_1\beta_2\ldots\beta_n\ldots$ (naravno, na desnoj strani nisu proizvodi, samo smo rekli da je $\alpha|_{D_k} = \alpha_k$ za svako $k$). Uočimo da su, za $n > m$, elementi $\alpha_n^{-(u_m-2)} \circ \beta \circ \alpha^{u_m-2}$ i $\beta$ permutabilni. Zaista, ako je $\gamma = (0_1 \ 1_1 \ 2_1)\ldots(0_{n-1} \ 1_{n-1} \ 2_{n-1})(0_{n+1} \ 1_{n+1} \ 2_{n+1})\ldots$, pa dakle, $\beta = \beta_n \circ \gamma$, onda su $\alpha_n$ i $\gamma$ uzajamno komutativni (kao disjunktne permutacije), a prema 9.3 i 9.8 je (zbog $u_n - (u_m - 2) \geq 4$): $\alpha_n^{-(u_m-2)} \circ \beta \circ \alpha^{u_m-2} = ((u_m-2)_n \ (u_m-1)_n \ (u_m)_n) \circ \gamma$; stoga je $(\alpha_n^{-(u_m-2)} \circ \beta \circ \alpha_n^{u_m-2}) \circ \beta = ((u_m-2)_n \ (u_m-1)_n \ (u_m)_n)(0_n \ 1_n \ 2_n) \circ \gamma^2 = (0_n \ 1_n \ 2_n)\gamma \circ ((u_m - 2)_n \ (u_m-1)_n \ (u_m)_n)\gamma = \beta \circ (\alpha_n^{-(u_m-2)} \circ \beta \circ \alpha^{u_m-2})$. Odatle sledi da komutator $\gamma_m = [\alpha^{-(u_m-2)} \circ \beta \circ \alpha^{u_m-2}, \beta]$ ostavlja fiksnim sve elemente skupa $\bigcup_{n>m} D_n$, dok sigurno "premešta" elemente skupa $D_m$ i moguće neke iz $D_k$,



za $k < m$. Jer, u grupi $\mathbf{A}_{u_m-2}$ je $((u_m-2)_m \ (u_m-1)_m \ 0_m) \circ (0_m \ 1_m \ 2_m) \neq (0_m \ 1_m \ 2_m) \circ ((u_m-2)_m \ (u_m-1)_m \ 0_m)$; koristili smo i očigledno: $\alpha^{u_m-2} = \alpha_1^{u_m-2}\alpha_2^{u_m-2}\ldots\alpha_n^{u_m-2}\ldots$ i, uopšte:

$$[\alpha^{-(u_m-2)} \circ \beta \circ \alpha^{u_m-2}, \beta] =$$

$$[\alpha_1^{-(u_m-2)} \circ \beta_1 \circ \alpha_1^{u_m-2}, \beta_1]\ldots[\alpha_m^{u_m-2} \circ \beta_m \circ \alpha_m^{u_m-2}, \beta_m]$$

$$[\alpha_{m+1}^{-(u_m-2)} \circ \beta_{m+1} \circ \alpha_{m+1}^{u_m-2}, \beta_{m+1}]\ldots.$$

Stoga su $\gamma_m$ kao i svi njegovi konjugati u $\mathbf{G}_\xi$ u podgrupi $\mathbf{A}_{u_1} \times \cdots \times \mathbf{A}_{u_m}$, znači i normalna podgrupa generisana tim elementima, $\mathbf{N}$, je sadržana u njoj. Komponenta grupe $\mathbf{N}$ u $\mathbf{A}_{u_m}$ je nejedinična normalna podgrupa, pa je, s obzirom da je $\mathbf{A}_{u_m}$ prosta grupa, baš $\mathbf{A}_{u_m}$. Proizilazi da je $\mathbf{A}_{u_1}$ normalna podgrupa grupe $\mathbf{G}_\xi$ (generisana elementom $\gamma_1$), a ako pretpostavimo da su $\mathbf{A}_{u_1}, \ldots, \mathbf{A}_{u_{m-1}}$ normalne podgrupe grupe $\mathbf{G}_\xi$, onda je to i $\mathbf{A}_{u_m}$. Ako je $\delta_m \in A_{u_m}$, tada postoje elementi $\delta_i$ podgrupa $\mathbf{A}_{u_i}$, $i = 1, \ldots, m-1$, i element $\theta$ iz $\mathbf{N}$ takvi da je $\theta = \delta_1 \circ \cdots \circ \delta_{m-1} \circ \delta_m$, te $\delta_m = (\delta_1 \circ \cdots \circ \delta_{m-1})^{-1} \circ \theta \in G_\xi$; isto tako je, za $\varphi \in G_\xi$, $\varphi^{-1} \circ \delta_m \circ \varphi$ komponenta elementa $\varphi^{-1} \circ \theta \circ \varphi$ ($\in N$), i $\varphi^{-1} \circ \delta_m \circ \varphi \in A_{u_m}$. Prema tome je $\mathbf{H}_\xi$ normalna podgrupa grupe $\mathbf{G}_\xi$.

Neka je sada $\mathbf{N}$ konačna normalna podgrupa grupe $\mathbf{G}_\xi$. Za svako $\varphi$ iz $\mathbf{N}$ i svako $m$ postoji permutacija $\varphi_m$ iz $\mathbf{A}_{u_m}$ takva da je $\varphi|_{D_m} = \varphi_m$ ($\varphi$ je proizvod stepena elemenata $\alpha$ i $\beta$, a za svako $m$ su $\alpha^m|_{D_m}$ i $\beta^m|_{D_m}$ permutacije iz $\mathbf{A}_{u_m}$). Skup komponenata elemenata iz $\mathbf{N}$ je domen normalne podgrupe proste grupe $\mathbf{A}_{u_m}$; u pitanju je, znači, ili jedinična podgrupa ili cela grupa. Činjenica da je $\mathbf{N}$ konačna grupa implicira da je $\mathbf{N} \leq \mathbf{A}_{u_1} \times \cdots \times \mathbf{A}_{u_k}$ za neko $k$, pri čemu je $\mathbf{A}_{u_k} = \mathbf{N}^k$ – komponenta podgrupe $\mathbf{N}$ u $\mathbf{A}_{u_k}$. Ako je $\mathbf{N}$ izomorfna nekoj alternativnoj grupi $\mathbf{A}_r$, onda je, pošto je u pitanju prosta grupa, jednaka svojoj komponenti u $\mathbf{A}_{u_k}$. Zbog toga grupa $\mathbf{G}_\xi$ sadrži podgrupu izomorfnu alternativnoj podgrupi $\mathbf{A}_r$ akko je $r$ član niza $\xi$.

Zaključujemo konačno: rastućih beskonačnih nizova neparnih brojeva većih od 3 ima kontinuum mnogo i svaka dva takva različita niza $\xi$ i $\eta$ određuju neizomorfne grupe $\mathbf{G}_\xi$ i $\mathbf{G}_\eta$ generisane sa dva elementa.■

**Korolar 10.49** *Ne postoji prebrojiva grupa u koju bi se mogle utopiti sve prebrojive grupe.*

**Dokaz**. Već grupa generisanih sa dva elementa ima kontinuum mnogo, dok je u svakoj prebrojivoj grupi najviše prebrojivo mnogo podgrupa generisanih sa dva elementa (videti i 28.18).□

# 11 Centralno izomorfne dekompozicije

U daljem ispitivanju svojstava direktnog proizvoda koristićemo sledeće oznake:

ako je $\mathbf{G}$ direktni proizvod familije podgrupa $\{\mathbf{G}_i \mid i \in I\}$, onda je $\overline{\mathbf{G}}_i \stackrel{\text{def}}{=} \langle \bigcup_{j\in I\setminus\{i\}} G_j\rangle = \prod_{j\in I\setminus\{i\}} \mathbf{G}_j$. Jasno, $\mathbf{G} = \mathbf{G}_i \times \overline{\mathbf{G}}_i$. Za podgrupu $\mathbf{A}$ grupe $\mathbf{G}$ je $\mathbf{A}^{\overline{i}}$ njena komponenta u $\overline{\mathbf{G}}_i$.

**Lema 11.1** *Neka je $\mathbf{A}$ podgrupa grupe $\mathbf{G}$, koja je direktni proizvod familije podgrupa $\{\mathbf{G}_i \mid i \in I\}$. Tada važi:*

*(a) Ako je $\mathbf{A}^i = \mathbf{A} \cap \mathbf{G}_i$ ($\mathbf{A}^i$ je, podsetimo se, komponenta ili projekcija podgrupe $\mathbf{A}$ u $\mathbf{G}_i$), onda je komponenta od $\mathbf{A}$ u $\overline{\mathbf{G}}_i$ takođe presek tih podgrupa ($\mathbf{A} \cap \overline{\mathbf{G}}_i$) i $\mathbf{A}$ je direktni proizvod svojih komponenti u $\mathbf{G}_i$ i $\overline{\mathbf{G}}_i$.*

*Posebno, ako je $\mathbf{G} = \mathbf{G}_0 \times \mathbf{G}_1$ i $\mathbf{A}^0 = \mathbf{A} \cap \mathbf{G}_0$, tada je $\mathbf{A}^1 = \mathbf{A} \cap \mathbf{G}_1$ i $\mathbf{A} = \mathbf{A}^0 \times \mathbf{A}^1$. Odatle, ako je $\mathbf{G}_0 \le \mathbf{A}$, onda je $\mathbf{A} = \mathbf{G}_0 \times (\mathbf{A} \cap \mathbf{G}_1)$;*

*(b) $\mathbf{A}^i = \mathbf{G}_i \cap \mathbf{A}\,\overline{\mathbf{G}}_i$;*

*(c) Ako je $\mathbf{B} \le \mathbf{A}$, onda je $\mathbf{B}^i \le \mathbf{A}^i$ za svako $i \in I$;*

*(d) $\mathbf{A}^i = \mathbf{E}$ akko $\mathbf{A} \le \overline{\mathbf{G}}_i$, $\mathbf{A} = \mathbf{A}^i$ akko $\mathbf{A} \le \mathbf{G}_i$, $(\mathbf{A}^i)^i = \mathbf{A}^i$;*

*(e) $(\mathbf{A}^{\overline{i}})^i = (\mathbf{A}^i)^{\overline{i}} = \mathbf{E}$;*

*(f) Ako je $\mathbf{A} = \langle \bigcup_{k\in K} A_k\rangle$, tada je $\mathbf{A}^i = \langle \bigcup_{k\in K} A_k^i\rangle$ za svako $i \in I$;*

*(g) Neka je $J$ pravi neprazni podskup skupa (indeksa) $I$ i neka je $\mathbf{H}_0 = \prod_{j\in J} \mathbf{G}_j$, $\mathbf{H}_1 = \prod_{i\in I\setminus J} \mathbf{G}_i$. Ako je $\mathbf{A}^n$ projekcija od $\mathbf{A}$ na $\mathbf{H}_n$, $n = 0, 1$, onda je $\mathbf{A}^0 \le \langle \bigcup_{j\in J} A^j\rangle = \prod_{j\in J} \mathbf{A}^j$, $\mathbf{A}^1 = \prod_{i\in I\setminus J} \mathbf{A}^i$;*

*(h) Ako je $\mathbf{B} \le \mathbf{A}^i$ ($\mathbf{B} \lhd \mathbf{A}^i$), onda postoji podgrupa (normalna podgrupa) $\mathbf{C}$ grupe $\mathbf{A}$ takva da je $\mathbf{C}^i = \mathbf{B}$.*

**Dokaz.** *(a)* Neka je $\mathbf{G} = \mathbf{G}_0 \times \mathbf{G}_1$ i $\mathbf{A}^0 = \mathbf{A} \cap \mathbf{G}_0$. Uvek, naravno, imamo $\mathbf{A} \cap \mathbf{G}_1 \le \mathbf{A}^1$. Opet, ako je $c \in A^1$, onda je, za neko $a \in A$, $a = bc$, gde je $b \in G_0$. Odatle je $b \in A^0 = A \cap G_0$, pa je $c = b^{-1}a \in A$. Sada trivijalno sledi i $\mathbf{A} = \mathbf{A}^0 \times \mathbf{A}^1$.

*(b)* Neka je $g_i \in A^i$. Onda je, za neko $a \in A$, $a = g_i g_{j_1} \cdots g_{j_n} = g_i \overline{g}_i$, gde je $\overline{g}_i = g_{j_1} \cdots g_{j_n}$, $n \ge 0$ (shodno uobičajenoj praksi u algebri slučaj $n = 0$ zapravo znači da elementa $\overline{g}_i$ "nemamo", drugim rečima, u tom slučaju podrazumevamo da je $\overline{g}_i = e$). Sada je direktno $g_i = a\,\overline{g_i}^{-1} \in G_i \cap A\,\overline{G}_i$. Još je očiglednija inkluzija u suprotnom pravcu.

*(f)* Zbog $\mathbf{A}_k \le \mathbf{A}_k^i\,\overline{\mathbf{G}}_i$ je $\mathbf{A} \le \langle \bigcup_{k\in K} A_k^i\,\overline{G}_i\rangle = \langle \bigcup A_k^i\rangle\,\overline{\mathbf{G}}_i$ (uopšte važi: ako je data familija podgrupa $\{\mathbf{C}_t \mid t \in T\}$ i ako je $\mathbf{D}$ normalna podgrupa, onda je $\langle \bigcup_{t\in T} C_t D\rangle = \langle \bigcup_{t\in T} C_t\rangle\mathbf{D}$ – laki dokaz ostavljamo za vežbu; u našem slučaju imamo i više od toga: elementi podgrupa $\mathbf{A}_k^i$, $k \in K$, permutabilni su sa elementima iz $\overline{\mathbf{G}}_i$). Prema tome je $\mathbf{A}^i \le (\langle \bigcup_{k\in K} A_k^i\rangle\overline{\mathbf{G}}_i)^i = \langle \bigcup_{k\in K} A_k^i\rangle$. Obrat je trivijalan.

*(h)* Neka je $\mathbf{C} = \mathbf{A} \cap \mathbf{B}\overline{\mathbf{G}}_i$ ($\le \mathbf{A}$). Ako je $\mathbf{B}$ normalna podgrupa grupe $\mathbf{A}$, onda je i $\mathbf{C}$ normalna podgrupa. Jer, recimo, neka je $b\,\overline{g}_i \in A \cap B\overline{G}_i = C$,



$b \in B$, $\overline{g}_i \in \overline{G}_i$ i neka je $a = a_i\overline{a}_i \in A$, $a_i \in A^i$, $\overline{a}_i \in A^{\overline{i}}$. Tada je $a^{-1}b\overline{g}_i a = a_i^{-1}ba_i \cdot \overline{a}_i^{-1}\overline{g}_i\overline{a}_i \in A \cap B\overline{G}_i = C$. Dalje je, prema *(b)*:

$$\mathbf{C}^i = \mathbf{G}_i \cap (\mathbf{A} \cap \mathbf{B}\overline{\mathbf{G}}_i)\overline{\mathbf{G}}_i = \mathbf{G}_i \cap (\mathbf{A}\overline{\mathbf{G}}_i \cap \mathbf{B}\overline{\mathbf{G}}_i) =$$

$$(\mathbf{G}_i \cap \mathbf{A}\overline{\mathbf{G}}_i) \cap \mathbf{B}\overline{\mathbf{G}}_i = \mathbf{A}^i \cap \mathbf{B}\overline{\mathbf{G}}_i = \mathbf{B}.$$

Relacija $\mathbf{A}\overline{\mathbf{G}}_i \cap \mathbf{B}\overline{\mathbf{G}}_i \le (\mathbf{A} \cap \mathbf{B}\overline{\mathbf{G}}_i)\overline{\mathbf{G}}_i$ se, kao uostalom i poslednja jednakost, direktno proverava. Neko će se radije pozvati na sledeće (opštije) činjenice:

*ako je normalna podgrupa $\mathbf{N}$ sadržana u podgrupi $\mathbf{K}$, tada je, za svaku podgrupu $\mathbf{H}$, $(\mathbf{H} \cap \mathbf{K})\mathbf{N} = \mathbf{H}\mathbf{N} \cap \mathbf{K}$;*

*ako je podgrupa $\mathbf{H}$ saržana u podgrupi $\mathbf{K}$ i ako je $\mathbf{N}$ normalna podgrupa, tada je $\mathbf{K} \cap \mathbf{H}\mathbf{N} = \mathbf{H}(\mathbf{K} \cap \mathbf{N})$.*

i uopšte (Dedekindovo pravilo):

*ako su $\mathbf{H}$, $\mathbf{K}$ i $\mathbf{M}$ podgrupe grupe $\mathbf{G}$ i $\mathbf{H} \le \mathbf{K}$, tada je $K \cap (HM) = H(K \cap M)$.*□

**Lema 11.2** *Ako je svaki opadajući niz direktnih faktora grupe $\mathbf{G}$ konačan, grupa $\mathbf{G}$ se ne može razložiti u direktni proizvod beskonačne familije (netrivijalnih) podgrupa i za svaku dekompoziciju postoji produženje čiji su svi faktori nerazloživi.*

**Dokaz.** Neka je ispunjen uslov leme i neka je $\mathbf{G} = \prod_{\alpha<\lambda} \mathbf{G}_\alpha$, $\lambda \ge \aleph_0$. No onda podgrupe $\mathbf{H}_n = \prod_{n<\alpha<\lambda} \mathbf{G}_\alpha$, $n \in \omega$, obrazuju beskonačni opadajući lanac (direktnih faktora grupe $\mathbf{G}$): $\mathbf{H}_0 > \mathbf{H}_1 > \cdots > \mathbf{H}_n \ge \cdots$, kontradikcija.

Ako je pak $\mathbf{G} = \mathbf{G}_0 \times \mathbf{G}_1 \times \cdots \times \mathbf{G}_n$ , gde podgrupa $\mathbf{G}_0$ nije razloživa u direktan proizvod nerazloživih faktora, tada je $\mathbf{G}_0 = \mathbf{G}_{00} \times \mathbf{G}_{01}$, gde bar jedna od grupa $\mathbf{G}_{0i}$, $i = 0, 1$, nije razloživa u proizvod nerazloživih faktora. Iteracijom postupka (uzimajući npr. da je $\mathbf{G}_{00}$ nerazloživa u proizvod nerazloživih faktora itd.) dolazimo opet do dekompozicije grupe $\mathbf{G}$ sa beskonačno mnogo faktora.□

**Teorema 11.3** *Dekompozicije $\prod_{i\in I} \mathbf{A}_i$ i $\prod_{j\in J} \mathbf{B}_j$ grupe $\mathbf{G}$ imaju zajedničko produženje (videti 10.12) ako i samo ako za svako $i' \in I$ i za svako $j' \in J$ važi: $((\mathbf{G}^{\overline{i'}})^{j'})^{i'} = \mathbf{E}$, gde je $\mathbf{G}^{\overline{i'}}$ projekcija grupe $\mathbf{G}$ na faktor $\prod_{i\in I\setminus\{i'\}} \mathbf{A}_i$, dakle, upravo i njemu jednaka (a dalje je, analogno, $(\mathbf{G}^{\overline{i'}})^{j'}$ komponenta od $\mathbf{G}^{\overline{i'}}$ u $\mathbf{B}_{j'}$ i $((\mathbf{G}^{\overline{i'}})^{j'})^{i'}$ komponenta od $(\mathbf{G}^{\overline{i'}})^{j'}$ u $\mathbf{A}_{i'}$).*

**Dokaz.** Neka dekompozicije $\prod_{i\in I} \mathbf{A}_i$ i $\prod_{j\in J} \mathbf{B}_j$ imaju zajedničko produženje $\prod_{k\in K} \mathbf{C}_k$. Jasno, $\forall k \in K\,\exists i \in I\,\exists j \in J$ $\mathbf{C}_k \le \mathbf{A}_i \cap \mathbf{B}_j$ i stoga je grupa $\mathbf{G}$ generisana skupom $\bigcup_{i,j} A_i \cap B_j$ (podrazumevamo da je unija po svim indeksima $i$ iz $I$ i $j$ iz $J$). No kako je $\mathbf{A}_i \cap \mathbf{B}_j \lhd \mathbf{G}$ i $(\mathbf{A}_i \cap \mathbf{B}_j) \cap \langle \bigcup_{(i',j')\neq(i,j)} A_{i'} \cap$

$B_{j'}) = \mathbf{E}$, proizilazi da je, zapravo, $\mathbf{G} = \prod_{i,j}(\mathbf{A}_i \cap \mathbf{B}_j)$, pa je $\mathbf{A}_i = \prod_j(\mathbf{A}_i \cap \mathbf{B}_j)$, $\mathbf{B}_j = \prod_i(\mathbf{A}_i \cap \mathbf{B}_j)$ (imamo u vidu: za dato $i \in I$ je $\mathbf{A}_i = \prod_{k \in K_i} \mathbf{C}_k$, $K_i \subseteq K$, i pošto za svako $k \in K_i$ postoji $j_k \in J$ takvo da je $\mathbf{C}_k \leq \mathbf{B}_{j_k}$, odnosno $\mathbf{C}_k \leq \mathbf{A}_i \cap \mathbf{B}_{j_k}$, sledi $\mathbf{A}_i \leq \prod_j(\mathbf{A}_i \cap \mathbf{B}_j)$ - naravno, ne isključujemo mogućnost da su neki od faktora $\mathbf{A}_i \cap \mathbf{B}_j$, $j \in J$, trivijalna podgrupa). Sada izvodimo:

$$\mathbf{G}^{\overline{i'}} = \overline{\mathbf{A}}_{i'} = \prod_{i \neq i'} \mathbf{A}_i = \prod_{i \neq i'}(\prod_j(\mathbf{A}_i \cap \mathbf{B}_j))$$

i

$$\overline{\mathbf{A}}_{i'}^{j'} = (\prod_{i \neq i'} \mathbf{A}_i)^{j'} = (\prod_{i \neq i'}(\prod_j(\mathbf{A}_i \cap \mathbf{B}_j)))^{j'} =$$

$$\langle \bigcup_{i \neq i'}(\prod_j^d A_i \cap B_j)^{j'} \rangle = \langle \bigcup_{i \neq i'}\langle \bigcup_j (A_i \cap B_j)^{j'} \rangle \rangle$$

(dvostruka primena tačke $(e)$ leme 11.1). Očigledno je

$$(A_i \cap B_j)^{j'} = \begin{cases} E & j \neq j' \\ A_i \cap B_j & j = j' \end{cases},$$

te u nastavku imamo:

$$(\mathbf{G}^{\overline{i'}})^{j'} = \langle \bigcup_{i \neq i'}\langle A_i \cap B_{j'} \rangle \rangle = \langle \bigcup_{i \neq i'} A_i \cap B_{j'} \rangle,$$

i konačno

$$((\mathbf{G}^{\overline{i'}})^{j'})^{i'} = \langle \bigcup_{i \neq i'} A_i \cap B_j \rangle^{i'} = \langle \bigcup_{i \neq i'}(A_i \cap B_j)^{i'} \rangle = \mathbf{E}.$$

Neka je sada. za svako $i' \in I$ i svako $j' \in J$, $((\mathbf{G}^{\overline{i'}})^{j'})^{i'} = \mathbf{E}$. Onda je

$$\mathbf{A}_{i'} = \mathbf{G}^{i'} = (\prod_j \mathbf{B}_j)^{i'} = \langle \bigcup_j B_j^{i'} \rangle = \prod_j \mathbf{B}_j^{i'},$$

jer je

$$\mathbf{B}_{j'}^{i'} \cap \langle \bigcup_{j \neq j'} B_j^{i'} \rangle = \mathbf{B}_{j'}^{i'} \cap (\prod_{j \neq j'} \mathbf{B}_j)^{i'} = \mathbf{B}_{j'}^{i'} \cap \overline{\mathbf{B}}_{j'}^{i'} =$$

$$(\mathbf{A}_{i'} \cap \mathbf{B}_{j'}\overline{\mathbf{A}}_{i'}) \cap (\mathbf{A}_{i'} \cap \overline{\mathbf{B}}_{j'}\overline{\mathbf{A}}_{i'}) = \mathbf{A}_{i'} \cap (\mathbf{B}_{j'}\overline{\mathbf{A}}_{i'} \cap \overline{\mathbf{B}}_{j'}\overline{\mathbf{A}}_{i'}) =$$

(zbog modularnosti mreže normalnih podgrupa)

$$\mathbf{A}_{i'} \cap (\mathbf{B}_{j'} \cap \overline{\mathbf{B}}_{j'}\overline{\mathbf{A}}_{i'})\overline{\mathbf{A}}_{i'} = (\mathbf{B}_{j'} \cap \overline{\mathbf{B}}_{j'}\overline{\mathbf{A}}_{i'})^{i'} = (\overline{\mathbf{A}_{i'}}^{j'})^{i'} = ((\mathbf{G}^{\overline{i'}})^{j'})^{i'} = \mathbf{E}.$$

Stoga je

$$\prod_i(\prod_j \mathbf{B}_j^i) = \prod_{i,j} \mathbf{B}_j^i = \prod_j(\prod_i \mathbf{B}_j^i)$$

produženje dekompozicije $\prod_i \mathbf{A}_i$. No to je ujedno i produženje dekompozicije $\prod_j \mathbf{B}_j$. Prema lemi 10.5 je $\mathbf{B}_j \leq \prod_i \mathbf{B}_j^i = \mathbf{D}_j$, ali zapravo važi jednakost. Stroga inkluzija (za neko $j \in J$) dala bi

$$G = \prod_j^d B_j \subset \prod_j^d D_j = G.\blacksquare$$



**Lema 11.4** *Ako je* $\mathbf{G} = \prod_{i \in I} \mathbf{A}_i = \prod_{j \in J} \mathbf{B}_j$, *tada je za svako* $i \in I$ *i svako* $j \in J$:

$$((\mathbf{G}^{\overline{i}})^j)^i \leq \mathbf{Z}(\mathbf{A}_i) \leq \mathbf{Z}(\mathbf{G}).$$

**Dokaz.** U drugom delu dokaza prethodne teoreme pokazali smo: $((\mathbf{G}^{\overline{i}})^j)^i = \mathbf{B}_j^i \cap \overline{\mathbf{B}_j}^i$. Neka je $a = a_1a_2 \in A_i$, gde je $a_1 = a_{11}a_{12} \in B_j$, $a_{11} \in A_i$, $a_{12} \in \overline{A}_i$, $a_2 = a_{21}a_{22} \in \overline{B}_j$, $a_{21} \in A_i$, $a_{22} \in \overline{A}_i$, i neka je $c \in B_j^i \cap \overline{B}_j$. $c$ i $a_{11}$ su permutabilni, jer je $c$ $i$-ta komponenta nekog elementa $d$ iz $\overline{B}_j$ i kako su $a_1$ i $d$ permutabilni, to su i njihove $i$-te komponente permutabilne. Prema tome, element $c$ je permutabilan sa $a_1$, po analogiji i sa $a_2$, znači i sa $a$.□

**Lema 11.5** *Trivijalni endomorfizam (svaki element se preslikava u jedinični) je jedino homomorfno preslikavanje grupe* $\mathbf{G}$ *u* $\mathbf{Z}(\mathbf{G})$ *ako i samo ako je trivijalan homomorfizam jedino homomorfno preslikavanje grupe* $\mathbf{G}/\mathbf{G}'$ *u* $\mathbf{Z}(\mathbf{G})$.

**Dokaz.** Neka je trivijalni endomorfizam jedini element skupa $Hom(\mathbf{G}, \mathbf{Z}(\mathbf{G}))$. Ako bi postojao netrivijalni homomorfizam $\varphi : G/G' \longrightarrow Z(\mathbf{G})$ $((G/G')\varphi \neq E)$, onda bi kompozicija preslikavanja $G \longrightarrow G/G' \xrightarrow{\varphi} Z(\mathbf{G})$ dala netrivijalno homomorfno preslikavanje grupe $\mathbf{G}$ u $\mathbf{Z}(\mathbf{G})$ (naravno, podrazumevamo da je preslikavanje $G$ u $G/G'$ kanonički, dakle i surjektivni homomorfizam).

Pretpostavimo sada da je trivijalni homomorfizam jedino homomorfno preslikavanje grupe $\mathbf{G}/\mathbf{G}'$ u grupu $\mathbf{Z}(\mathbf{G})$. Ako je $\varphi$ homomorfno preslikavanje grupe $\mathbf{G}$ u $\mathbf{Z}(\mathbf{G})$, onda je $\mathbf{G}/\mathbf{Ker}(\varphi)$ $(\cong (\mathbf{G})\varphi \leq \mathbf{Z}(\mathbf{G}))$ Abelova grupa pa je $\mathbf{G}' \leq \mathbf{Ker}(\varphi)$. Ali tada imamo surjektivni homomorfizam $G/G' \longrightarrow G/Ker(\varphi) \longrightarrow (G)\varphi \leq Z(\mathbf{G})$, te mora biti $(G)\varphi = E$.□

Grupa za koju važi jedan od (ekvivalentnih) uslova prethodne leme zove se *F-grupa.*

**Korolar 11.6** $(a)$ *Svake dve direktne dekompozicije F-grupe imaju zajedničko produženje;*

$(b)$ *Ako je* $\mathbf{G}$ *grupa bez centra i ako je* $\mathbf{G} = \mathbf{G}'$, *onda svake dve direktne dekompozicije grupe* $\mathbf{G}$ *imaju zajedničko produženje.*

**Dokaz.** $(a)$ Neka je $\mathbf{G}$ $F$-grupa. Projekcije su homomorfna preslikavanja, a prema 11.2 je $((\mathbf{G}^{\overline{i}})^j)^i \leq \mathbf{Z}(\mathbf{G})$, pa mora biti $((\mathbf{G}^{\overline{i}})^j)^i = \mathbf{E}$. Ostaje još da se pozovemo na 11.1.

$(b)$ Prisetimo se samo da su uslovi $\mathbf{Z}(\mathbf{G}) = \mathbf{E}$ i $\mathbf{G} = \mathbf{G}'$ nezavisni (videti komentar uz 5.24).□

**Definicija 11.7** $(a)$ *Dve podgrupe* $\mathbf{A}$ *i* $\mathbf{B}$ *grupe* $\mathbf{G}$ *su centralno izomorfne akko su izomorfne i ako je za neko* $\varphi \in Is(\mathbf{A}, \mathbf{B})$ *ispunjeno:* $\forall a \in A$ $((a)\varphi)^{-1}a \in Z(\mathbf{G})$;

*(b) Dve direktne dekompozicije grupe* $\mathbf{G}$ *su centralno izomorfne akko se može uspostaviti uzajamno jednoznačna korespondencija između njihovih (direktnih) faktora takva da su odgovarajući faktori centralno izomorfni.*

Uočimo odmah u tački $(a)$: $a\,((a)\varphi)^{-1} = a\,((a)\varphi)^{-1}aa^{-1} = ((a)\varphi)^{-1}\,a$, pa su elementi $a$ i $((a)\varphi)^{-1}$ uzajamno permutabilni.

**Lema 11.8** *Ako je* $\mathbf{G} = \mathbf{A} \times \mathbf{C} = \mathbf{B} \times \mathbf{C}$, *tada su podgrupe* $\mathbf{A}$ *i* $\mathbf{B}$ *centralno izomorfne.*

**Dokaz.** Već znamo: $\mathbf{A} \cong \mathbf{G/C} \cong \mathbf{B}$. Neka su $\varphi_1 \in Is(\mathbf{A},\mathbf{G/C})$, $\varphi_2 \in Is(\mathbf{B},\mathbf{G/C})$ tzv. prirodni izomorfizmi (npr. za $a \in A$, $(a)\varphi_1 = aC$ - videti 10.12). $\varphi_1 \circ \varphi_2^{-1}$ je izomorfno preslikavanje grupe $\mathbf{A}$ na grupu $\mathbf{B}$ i $a$ i $(a)(\varphi_1 \circ \varphi_2^{-1})$ leže u istom kosetu podgrupe $\mathbf{C}$ $((a)(\varphi_1 \circ \varphi_2^{-1}) = b \iff (a)\varphi_1 = (b)\varphi_2 \iff aC = bC)$. Odatle je $((a)(\varphi_1 \circ \varphi_2^{-1}))^{-1}\,a = c \in C$. Kako je svaki element iz $C$ permutabilan i sa $a$ i sa $(a)(\varphi_1 \circ \varphi_2^{-1})^{-1}$, $c$ je u $Z(\mathbf{C})$, i jasno, $c$ je permutabilan sa svakim elementom iz $A$. Stoga je $c \in Z(\mathbf{G})$.□

**Korolar 11.9** *Neka je* $\mathbf{G} = \prod_{i\in I}\mathbf{A}_i = \prod_{i\in I}\mathbf{B}_i$ *i neka je* $\mathbf{G} = \mathbf{A}_{i'} \times \prod_{i\neq i'}\mathbf{B}_i$ *za svako* $i' \in I$ *(kažemo: podgrupa* $\mathbf{B}_{i'}$ *je zamenljiva ili nadoknadiva s podgrupom* $\mathbf{A}_{i'}$*). Tada su date dekompozicije grupe* $\mathbf{G}$ *centralno izomorfne.*

**Korolar 11.10** *Neka su* $\mathbf{A}$ *i* $\mathbf{B}$ *potpuno razložive, normalne podgrupe grupe* $\mathbf{G}$ *i neka je* $\mathbf{Z}(\mathbf{A}) = \mathbf{Z}(\mathbf{B}) = \mathbf{E}$. *Tada je i grupa* $\mathbf{AB}$ *potpuno razloživa i bez centra.*

**Dokaz.** Kako je $\mathbf{A} \cap \mathbf{B}$ normalna podgrupa grupe $\mathbf{A}$ (u stvari je $\mathbf{A} \cap \mathbf{B} \lhd \mathbf{G}$) i $\mathbf{A}$ potpuno razloživa grupa, to postoji dekompozicija grupe $\mathbf{A}$ oblika $\mathbf{A} = (\mathbf{A} \cap \mathbf{B}) \times \mathbf{C}$. Za $g \in G$, $u_g|_A$ je automorfizam grupe $\mathbf{A}$ ($u_g$ je unutrašnji automorfizam grupe $\mathbf{G}$ određen elementom $g$) i $\mathbf{A} = ((\mathbf{A} \cap \mathbf{B}) \times \mathbf{C})u_g = (\mathbf{A} \cap \mathbf{B}) \times g^{-1}\mathbf{C}g$. Proizilazi da su $\mathbf{C}$ i $g^{-1}\mathbf{C}g$ centralno izomorfne podgrupe grupe $\mathbf{A}$, no kako je $\mathbf{A}$ bez centra, one su baš jednake. Prema tome je i $\mathbf{C}$ normalna, potpuno razloživa i bez centra podgrupa grupe $\mathbf{G}$ (10.29), a iz $\mathbf{AB} = \mathbf{CB}$ i $\mathbf{C} \cap \mathbf{B} = \mathbf{E}$ sledi $\mathbf{AB} = \mathbf{C} \times \mathbf{B}$, te je i grupa $\mathbf{AB}$ potpuno razloživa i bez centra (10.30).□

**Korolar 11.11** *Svaka konačna grupa ima jedinstvenu maksimalnu potpuno razloživu normalnu podgrupu bez centra (dozvoljavamo mogućnost da je to baš cela grupa).*

Odgovor na pitanje o uslovima egzistencije centralno izomorfnih produženja datih dekompozicija grupe biće dat u narednim teoremama sa čijim dokazima započinjemo (dokaz spada u duže te ga čitalac može u prvom čitanju, a po volji i u svakom drugom, izostaviti).



Do daljnjega, preciznije do teoreme, pretpostavljamo: $\mathbf{G} = \mathbf{A}_1 \times \mathbf{A}_2 = \mathbf{B}_1 \times \mathbf{B}_2$, $\phi_1, \phi_2$ su projekcije grupe $\mathbf{G}$ na, respektivno, $\mathbf{A}_1, \mathbf{A}_2$, $\psi_1, \psi_2$ su projekcije na, respektivno, $\mathbf{B}_1, \mathbf{B}_2$.

**Lema 11.12** *Za svako* $g \in G$ *važi:*

$(a)$ $(g)\psi_1\phi_1\psi_2 = (g^{-1})\psi_1\phi_2\psi_2$;

$(b)$ $(g)\psi_2\phi_1\psi_1 = (g^{-1})\psi_2\phi_2\psi_1$;

$(c)$ $(g)\phi_1\psi_1\phi_2 = (g^{-1})\phi_1\psi_2\phi_2$;

$(d)$ $(g)\phi_2\psi_1\phi_1 = (g^{-1})\phi_2\psi_2\phi_1$.

**Dokaz.** $(a)$ Zbog $(g)\psi_1 = (g)\psi_1\phi_1 \cdot (g)\psi_1\phi_2$ imamo

$$(g)\psi_1\phi_1\psi_2 \cdot (g)\psi_2\phi_2\psi_2 = ((g)\psi_1\phi_1 \cdot (g)\psi_1\phi_2)\psi_2 = ((g)\psi_1)\psi_2 = e,$$

i odatle

$$(g)\psi_1\phi_1\psi_2 = ((g)\psi_1\phi_2\psi_2)^{-1} = (g^{-1})\psi_1\phi_2\psi_2.\square$$

**Korolar 11.13** *Za svaku podgrupu* $\mathbf{H}$ *grupe* $\mathbf{G}$ *važi:*

$(a)$ $(((\mathbf{H})\psi_1)\phi_1)\psi_2 = (((\mathbf{H})\psi_1)\phi_2)\psi_2$; *piše se i* $((\mathbf{H}^{\psi_1})^{\phi_1})^{\psi_2} = ((\mathbf{H}^{\psi_1})^{\phi_2})^{\psi_2}$;

$(b)$ $(((\mathbf{H})\psi_2)\phi_1)\psi_1 = (((\mathbf{H})\psi_2)\phi_2)\psi_1$;

$(c)$ $(((\mathbf{H})\phi_1)\psi_1)\phi_2 = (((\mathbf{H})\phi_1)\psi_2)\phi_2$;

$(d)$ $(((\mathbf{H})\phi_2)\psi_1)\phi_1 = (((\mathbf{H})\phi_2)\psi_2)\phi_1$.

**Korolar 11.14** *Ako je* $g \in A_1$, *tada je* $(g)\psi_1\phi_1\psi_2\phi_1 = (g)\psi_2\phi_1\psi_1\phi_1$.

**Dokaz.** Kako je $g = (g)\phi_1$, sledi prema poslednjoj lemi primenjujući je četiri puta:

$$(g)\psi_1\phi_1\psi_2\phi_1 = (g)\phi_1\psi_1\phi_1\psi_2\phi_1 = (g^{-1})\phi_1\psi_1\phi_2\psi_2\phi_1 =$$
$$(g)\phi_1\psi_2\phi_2\psi_2\phi_1 = (g^{-1})\phi_1\psi_2\phi_2\psi_1\phi_1 = (g)\phi_1\psi_2\phi_1\psi_1\phi_2 =$$
$$(g)\psi_2\phi_1\psi_1\phi_1.\square$$

**Definicija 11.15** $N_{11}^k \overset{\text{def}}{=} \{g \in A_1 \mid (g)(\psi_1\phi_1)^k = e\}$, $k = 1,2,\ldots$ $((\psi_1\phi_1)^k$ *je k-ti stepen preslikavanja* $\phi_1\psi_1$*);*

$$N_{12}^k \overset{\text{def}}{=} \{g \in A_1 \mid (g)(\psi_2\phi_1)^k = e\};$$
$$N_1^k \overset{\text{def}}{=} \{g \in A_1 \mid (g)(\psi_1\phi_1\psi_2\phi_1)^k = e\};$$
$$N_{21}^k \overset{\text{def}}{=} \{g \in A_2 \mid (g)(\psi_1\phi_2)^k = e\};$$
$$N_{22}^k \overset{\text{def}}{=} \{g \in A_2 \mid (g)(\psi_2\phi_2)^k = e\};$$
$$N_2^k \overset{\text{def}}{=} \{g \in A_2 \mid (g)(\psi_1\phi_2\psi_2\phi_2)^k = e\}.$$

*Analogno definišemo* $M_{1j}^k$, $M_1^k$, $j = 1,2,\ldots$, *s obzirom na direktni sumand* $\mathbf{B}_1$ *(tako je npr.* $M_{12}^k \overset{\text{def}}{=} \{g \in B_1 \mid (g)(\phi_2\psi_1)^k = e\}$*) i* $M_{2j}^k$, $M_2^k$, $j = 1,2,\ldots$, *s obzirom na direktni sumand* $\mathbf{B}_2$.

Jasno, adekvatna tvrđenja koja iznosimo u nekoliko narednih lema za $N_{11}^k$, $N_{12}^k$, $N_1^k$ važe, po simetriji stvari, i za ostale definisane skupove i mi ćemo ih kasnije jednostavno podrazumevati.

**Lema 11.16** *$N_{11}^k$, $N_{12}^k$, $N_1^k$, $k = 1,2,\ldots$, domeni su normalnih podgrupa grupe $\mathbf{A}_1$ i pritom je*

$$\mathbf{N}_{1j}^1 \leq \mathbf{N}_{1j}^2 \leq \cdots \leq \mathbf{N}_{1j}^k \leq \cdots, \quad j = 1,2;$$
$$\mathbf{N}_1^1 \leq \mathbf{N}_1^2 \leq \cdots \leq \mathbf{N}_1^k \leq \cdots;$$
$$\mathbf{N}_{1j}^k(\psi_j\phi_1)^k = \mathbf{E}, \quad j = 1,2;$$
$$\mathbf{N}_1^k(\psi_1\phi_1\psi_2\phi_1)^k = \mathbf{E};$$
$$\mathbf{N}_{1j}^k \leq \mathbf{N}_1^k, \quad j = 1,2.$$

**Dokaz**. Samo poslednja relacija zaslužuje pažnju.

Posmatrajmo slučaj $j = 1$ (dokaz je u osnovi isti za oba slučaja). Neka je $g \in N_{11}^k$, znači $(g)(\psi_1\phi_1)^k = e$. Tada je

$$(g)(\psi_1\phi_1\psi_2\phi_1)^k = (g)(\psi_1\phi_1)^k(\psi_2\phi_1)^k = e,$$

jer su, prema prethodnom korolaru, $\psi_1\phi_1$ i $\psi_2\phi_1$ permutabilna preslikavanja na skupu $A_1$.□.

**Lema 11.17** *Ako je $\mathbf{H}$ podgrupa grupe $\mathbf{A}_1$, tada je (za svako $k \geq 1$) $\mathbf{H}$ podgrupa grupe*

$$\langle (H)(\psi_1\phi_1)^k \cup (H)(\psi_1\phi_1)^{k-1}(\psi_2\phi_1) \cup \ldots \cup (H)(\psi_1\phi_1)(\psi_2\phi_1)^{k-1} \cup (H)(\psi_2\phi_1)^k \rangle.$$

**Dokaz**. Indukcijom po $k$.

Za $k = 1$ imamo: $\mathbf{H} \leq (\mathbf{H})\psi_1 \times (\mathbf{H})\psi_2$ pa je, prema tački $(f)$ leme 11.1,

$$(\mathbf{H})\phi_1 = \mathbf{H} \leq ((\mathbf{H})\psi_1 \times (\mathbf{H})\psi_2)\phi_1 = \langle (H)\psi_1\phi_1 \cup (H)\psi_2\phi_1 \rangle.$$

Pretpostavimo da je tvrđenje tačno za $k\,(\geq 1)$. Onda je

$$\begin{aligned}
\mathbf{H} &\leq \langle (H)(\psi_1\phi_1)^k \cup (H)(\psi_1\phi_1)^{k-1}(\psi_2\phi_1) \cup \ldots \\
&\qquad \ldots \cup (H)(\psi_1\phi_1)(\psi_2\phi_1)^{k-1} \cup (H)(\psi_2\phi_1)^k \rangle \\
&\leq \langle \langle (H)(\psi_1\phi_1)^k \cup (H)(\psi_1\phi_1)^{k-1}(\psi_2\phi_1) \cup \ldots \\
&\qquad \ldots \cup (H)(\psi_1\phi_1)(\psi_2\phi_1)^{k-1} \cup (H)(\psi_2\phi_1)^k \rangle \psi_1\phi_1 \cup \\
&\qquad \cup \langle (H)(\psi_1\phi_1)^k \cup (H)(\psi_1\phi_1)^{k-1}(\psi_2\phi_1) \cup \ldots \\
&\qquad \ldots \cup (H)(\psi_1\phi_1)(\psi_2\phi_1)^{k-1} \cup (H)(\psi_2\phi_1)^k \rangle \psi_2\phi_1 \rangle \\
&= \text{(prema tački } (e) \text{ leme 10.44 i korolaru 11.12)} \\
&\qquad \langle \langle (H)(\psi_1\phi_1)^{k+1} \cup (H)(\psi_1\phi_1)^k(\psi_2\phi_1) \cup \ldots \\
&\qquad \ldots \cup (H)(\psi_1\phi_1)^2(\psi_2\phi_1)^{k-1} \cup (H)(\psi_1\phi_1)(\psi_2\phi_1)^k \rangle \cup \\
&\qquad \cup \langle (H)(\psi_1\phi_1)^k(\psi_2\phi_1) \cup (H)(\psi_1\phi_1)^{k-1}(\psi_2\phi_1) \cup \ldots \\
&\qquad \ldots \cup (H)(\psi_1\phi_1)(\psi_2\phi_1)^k \cup (H)(\psi_2\phi_1)^{k+1} \rangle \rangle \\
&= \langle (H)(\psi_1\phi_1)^{k+1} \cup (H)(\psi_1\phi_1)^k(\psi_2\phi_1) \cup \ldots \\
&\qquad \ldots \cup (H)(\psi_1\phi_1)(\psi_2\phi_1)^k \cup (H)(\psi_2\phi_1)^{k+1} \rangle.
\end{aligned}$$

U poslednjem koraku smo koristili: $\langle\langle A\rangle \cup \langle B\rangle\rangle = \langle A \cup B\rangle$.□



**Lema 11.18** *Za sve pozitivne prirodne brojeve $k, l$ važi:*

$$\mathbf{N}_{11}^k \cap \mathbf{N}_{12}^l = \mathbf{E};$$
$$\mathbf{N}_{21}^k \cap \mathbf{N}_{22}^l = \mathbf{E};$$
$$\mathbf{M}_{11}^k \cap \mathbf{M}_{12}^l = \mathbf{E};$$
$$\mathbf{M}_{21}^k \cap \mathbf{M}_{22}^l = \mathbf{E}.$$

**Dokaz**. Neka je $g \in N_{11}^k \cap N_{12}^l$. Znači: $(g)(\psi_1\phi_1)^k = (g)(\psi_2\phi_1)^l = e$. Indukcijom po zbiru $k + l\,(\geq 2)$ zaključujemo da je $g = e$.

Ako je $k + l = 2$, tj. $k = l = 1$, tada je

$$g = (g)\phi_1 = (g)\psi_1\phi_1 \cdot (g)\psi_2\phi_1 = e \cdot e = e.$$

Pretpostavimo da je $\mathbf{N}_{11}^k \cap \mathbf{N}_{12}^l = \mathbf{E}$ za $k + l \leq r$ i razmotrimo slučaj kada je zbir $r + 1$ i $k > 1$. Neka je opet $g \in N_{11}^k \cap N_{12}^l$.

$$(g)(\psi_1\phi_1)^k = (g)(\psi_1\phi_1)(\psi_1\phi_1)^{k-1} = e$$

i

$$((g)(\psi_1\phi_1))(\psi_2\phi_1)^l = ((g)(\psi_2\phi_1)^l)(\psi_1\phi_1) = e$$

daju $(g)\psi_1\phi_1 \in N_{11}^{k-1} \cap N_{12}^l = E$, pa je $g = (g)\psi_2\phi_1$ (jer je $g = (g)\phi_1 = (g)\psi_1\phi_1 \cdot (g)\psi_2\phi_1$). Ali $(g)(\psi_2\phi_1)^l = (g)(\psi_2\phi_1)(\psi_2\phi_1)^{l-1} = e$, te za $l = 1$ imamo odmah $(g)\psi_2\phi_1 = e$, a ako je $l > 1$, onda je $g = (g)\psi_2\phi_1 \in N_{11}^k \cap N_{12}^{l-1}$ i po induktivnoj pretpostavci ponovo je $g = e$.□

**Lema 11.19** $\mathbf{N}_1^k = \mathbf{N}_{11}^k \times \mathbf{N}_{12}^k$ *za svaki pozitivan prirodan broj $k$.*

**Dokaz**. Indukcijom po $k$ dokazujemo relaciju $\leq$. Za $k = 1$ je, prema 11.15, $\mathbf{N}_1^1 \leq \langle (N_1^1)\psi_1\phi_1 \cup (N_1^1)\psi_2\phi_1 \rangle$, a kako je, po definiciji i 11.12, $(\mathbf{N}_1^1)\psi_1\phi_1\psi_2\phi_1 = (\mathbf{N}_1^1)\psi_2\phi_1\psi_1\phi_1 = \mathbf{E}$, to je $(\mathbf{N}_1^1)\psi_1\phi_1 \leq \mathbf{N}_{12}^1$ i $(\mathbf{N}_1^1)\psi_2\phi_1 \leq \mathbf{N}_{11}^1$; dakle, $\mathbf{N}_1^1 \leq \mathbf{N}_{11}^1\,\mathbf{N}_{12}^1$.

Pretpostavimo da je za $\mathbf{N}_1^k \leq \mathbf{N}_{11}^k\,\mathbf{N}_{12}^k$ za $k\,(\geq 1)$. Već znamo da je

$$\mathbf{N}_1^{k+1} \leq \langle (N_1^{k+1})(\psi_1\phi_1)^{k+1} \cup (N_1^{k+1})(\psi_1\phi_1)^k(\psi_2\phi_1) \cup \ldots$$
$$\cup (N_1^{k+1})(\psi_1\phi_1)(\psi_2\phi_1)^k \cup (N_1^{k+1})(\psi_2\phi_1)^{k+1} \rangle.$$

Zbog

$$(\mathbf{N}_1^{k+1})(\psi_1\phi_1)^{k+1}(\psi_2\phi_1)^{k+1} = (\mathbf{N}_1^{k+1})(\psi_1\phi_1\psi_2\phi_1)^{k+1} = \mathbf{E}$$

važi

$$(\mathbf{N}_1^{k+1})(\psi_1\phi_1)^{k+1} \leq \mathbf{N}_{12}^{k+1}.$$

Analogno: $(\mathbf{N}_1^{k+1})(\psi_2\phi_1)^{k+1}(\psi_1\phi_1)^{k+1} = \mathbf{E}$ i $(\mathbf{N}_1^{k+1})(\psi_2\phi_1)^{k+1} \leq \mathbf{N}_{11}^{k+1}$.

Dalje, iz

$$(\mathbf{N}_1^{k+1})(\psi_1\phi_1)^k(\psi_2\phi_1)(\psi_1\phi_1\psi_2\phi_1)^k = (\mathbf{N}_1^{k+1})(\psi_1\phi_1\psi_2\phi_1)^{k+1}(\psi_1\phi_1)^{k-1} = \mathbf{E}$$

sledi

$$(\mathbf{N}_1^{k+1})(\psi_1\phi_1)^k(\psi_2\phi_1) \leq \mathbf{N}_1^k \leq \mathbf{N}_{11}^k\,\mathbf{N}_{12}^k \leq \mathbf{N}_{11}^{k+1}\,\mathbf{N}_{12}^{k+1}.$$

Slično

$$(\mathbf{N}_1^{k+1})(\psi_1\phi_1)(\psi_2\phi_1)^k \leq \mathbf{N}_{11}^{k+1}\,\mathbf{N}_{12}^{k+1}.$$

Za $(\mathbf{N}_1^{k+1})(\psi_1\phi_1)^r(\psi_2\phi_1)^t$, $r+t=k+1$, $1<r,t$, imamo

$$(\mathbf{N}_1^{k+1})(\psi_1\phi_1)^r(\psi_2\phi_1)^t(\psi_1\phi_1\psi_2\phi_1)^{k-1} =$$

$$(\mathbf{N}_1^{k+1})(\psi_1\phi_1\psi_2\phi_1)^{k+1}(\psi_1\phi_1)^{r-2}(\psi_2\phi_1)^{t-2} = \mathbf{E},$$

dakle,

$$(\mathbf{N}_1^{k+1})(\psi_1\phi_1)^r(\psi_2\phi_1)^t \leq \mathbf{N}_1^{k-1} \leq \mathbf{N}_{11}^{k-1}\,\mathbf{N}_{12}^{k-1} \leq \mathbf{N}_{11}^{k+1}\,\mathbf{N}_{12}^{k+1}.$$

Lema 11.16 nam kaže da je upravo jednakost u pitanju, a prethodna da se radi o direktnom proizvodu.□

**Lema 11.20** $\mathbf{N}_1^k \times \mathbf{N}_2^k = \mathbf{M}_1^k \times \mathbf{M}_2^k$ *za svaki pozitivan prirodan broj* $k$.

**Dokaz**. Iz $(\mathbf{M}_1^k)(\phi_1\psi_1\phi_2\psi_1)^k = \mathbf{E}$ sledi (uzimajući u obzir lemu 11.12 i njen korolar)

$$((\mathbf{M}_1^k)\phi_1)(\psi_1\phi_1\psi_2\phi_1)^k = ((\mathbf{M}_1^k)\phi_1)(\psi_1\phi_2\psi_2\phi_1)^k =$$

$$((\mathbf{M}_1^k)\phi_1)(\psi_1\phi_2\psi_1\phi_1)^k = (\mathbf{M}_1^k)(\phi_1\psi_1\phi_2\psi_1)^k = \mathbf{E},$$

tj. $(\mathbf{M}_1^k)\phi_1 \leq \mathbf{N}_1^k$ (imamo u vidu i da je $(\mathbf{M}_1^k)\phi_1 \leq \mathbf{A}_1$); analogno, $(\mathbf{M}_1^k)\phi_2 \leq \mathbf{N}_2^k$. Stoga je $\mathbf{M}_1^k \leq (\mathbf{M}_1^k)\phi_1 \times (\mathbf{M}_1^k)\phi_2 \leq \mathbf{N}_1^k\,\mathbf{N}_2^k$.

Isto tako je i $\mathbf{M}_2^k \leq \mathbf{N}_1^k\,\mathbf{N}_2^k$, pa je $\mathbf{M}_1^k\,\mathbf{M}_2^k \leq \mathbf{N}_1^k\,\mathbf{N}_2^k = \mathbf{N}_1^k \times \mathbf{N}_2^k$.

Simetrija daje relaciju $\geq$.□

**Lema 11.21** *Za svaki pozitivan prirodan broj* $k$ *važi:*
$(\mathbf{N}_{12}^k)\psi_1 \leq \mathbf{M}_{12}^k$, $(\mathbf{N}_{21}^k)\psi_2 \leq \mathbf{M}_{21}^k$, $(\mathbf{N}_{11}^k)\psi_1 \leq \mathbf{M}_{11}$,
$(\mathbf{N}_{11}^k)\psi_2 \leq \mathbf{M}_{22}^k$, $(\mathbf{N}_{22}^k)\psi_1 \leq \mathbf{M}_{11}^k$, $(\mathbf{N}_{22}^k)\psi_2 \leq \mathbf{M}_{22}^k$.

**Dokaz**. $(\mathbf{N}_{12}^k)\psi_1 \leq \mathbf{B}_1$ i

$$((\mathbf{N}_{12}^k)\psi_1)(\phi_2\psi_1)^k = (\mathbf{N}_{12}^k)(\phi_1\psi_1)(\phi_2\psi_1)^k \text{ (jer je } \mathbf{N}_{12}^k \leq \mathbf{A}_1) =$$

$$(\mathbf{N}_{12}^k)(\phi_1\psi_1\phi_2\psi_1)(\phi_2\psi_1)^{k-1} = (\mathbf{N}_{12}^k)(\phi_1\psi_2\phi_2\psi_1)(\phi_2\psi_1)^{k-1} \text{ (zbog 11.12)} =$$

$$(\mathbf{N}_{12}^k)(\phi_1\psi_2)(\phi_2\psi_1)^k = (\mathbf{N}_{12}^k)\phi_1(\psi_2\phi_2\psi_1)(\phi_2\psi_1)^{k-1} =$$

$$(\mathbf{N}_{12}^k)(\phi_1\psi_2\phi_1)\psi_1(\phi_2\psi_1)^{k-1} = \cdots = (\mathbf{N}_{12}^k)\phi_1(\psi_2\phi_1)^k\psi_1 =$$

$$(\mathbf{N}_{12}^k)(\psi_2\phi_1)^k\psi_1 = (\mathbf{E})\psi_1 = \mathbf{E}.\square$$



**Lema 11.22** $\mathbf{N}_{12}^k \cap \mathbf{M}_{11}^k\,\mathbf{M}_2^k = \mathbf{E}$ *i* $\mathbf{N}_{11}^k \cap \mathbf{M}_1^k\,\mathbf{M}_2^k = \mathbf{E}$ *za svaki pozitivan prirodan broj* $k$.

**Dokaz**. Prema prethodnoj lemi je

$$(\mathbf{N}_{12}^k \cap \mathbf{M}_{11}^k\,\mathbf{M}_2^k)\psi_1 \leq (\mathbf{N}_{12}^k)\psi_1 \leq \mathbf{M}_{12}^k$$

a prema tački $(e)$ leme 11.1:

$$(\mathbf{N}_{12}^k \cap \mathbf{M}_{11}^k\,\mathbf{M}_2^k)\psi_1 \leq (\mathbf{M}_{11}^k\,\mathbf{M}_2^k)\psi_1 = \langle (M_{11}^k)\psi_1 \cup (M_2^k)\psi_1\rangle = \mathbf{M}_{11}^k.$$

Stoga je $(\mathbf{N}_{12}^k \cap \mathbf{M}_{11}^k\,\mathbf{M}_2^k)\psi_1 \leq \mathbf{M}_{12}^k \cap \mathbf{M}_{11}^k = \mathbf{E}$ (lema 11.18), te je $(\mathbf{N}_{12}^k \cap \mathbf{M}_{11}^k\,\mathbf{M}_2^k)\psi_1\phi_1 = \mathbf{E}$ i kako je $\mathbf{N}_{12}^k \cap \mathbf{M}_{11}^k\,\mathbf{M}_2^k \leq \mathbf{N}_{12}^k \leq \mathbf{A}_1$, dobijamo $\mathbf{N}_{12}^k \cap \mathbf{M}_{11}^k\,\mathbf{M}_2^k \leq \mathbf{N}_{11}^1$. Prema tome: $\mathbf{N}_{12}^k \cap \mathbf{M}_{11}^k\,\mathbf{M}_2^k \leq \mathbf{N}_{12}^k \cap \mathbf{N}_{11}^1 = \mathbf{E}$.

Analogno: $(\mathbf{N}_{11}^k \cap \mathbf{M}_1^k\,\mathbf{M}_{21}^k)\psi_2 \leq (\mathbf{N}_{11}^k)\psi_2 \leq \mathbf{M}_{22}^k$ i

$$(\mathbf{N}_{11}^k \cap \mathbf{M}_1^k\,\mathbf{M}_{21}^k)\psi_2 \leq (\mathbf{M}_1^k\,\mathbf{M}_{21}^k)\psi_2 = \langle (M_1^k)\psi_2 \cup (M_{21}^k)\psi_2\rangle = \mathbf{M}_{21}^k.$$

Dakle, $(\mathbf{N}_{11}^k \cap \mathbf{M}_1^k\,\mathbf{M}_{21}^k)\psi_2 \leq \mathbf{M}_{22}^k \cap \mathbf{M}_{21}^k = \mathbf{E}$ i $(\mathbf{N}_{11}^k \cap \mathbf{M}_1^k\,\mathbf{M}_{21}^k)\psi_2\phi_1 = \mathbf{E}$, znači $\mathbf{N}_{11}^k \cap \mathbf{M}_1^k\,\mathbf{M}_{21}^k \leq \mathbf{N}_{12}^1$, pa je $\mathbf{N}_{11}^k \cap \mathbf{M}_1^k\,\mathbf{M}_{21}^k \leq \mathbf{N}_{11}^k \cap \mathbf{N}_{12}^1 = \mathbf{E}$.□

**Lema 11.23** *Za svaki pozitivan prirodan broj* $k$ *važi:*
$\mathbf{M}_{12}^k \leq \langle N_{12}^k \cup M_{21}^k\rangle$, $\mathbf{M}_{11}^k \leq \langle N_{22}^k \cup M_2^k\rangle$, $\mathbf{M}_{22}^k \leq \langle N_{11}^k \cup M_{11}^k\rangle$.

**Dokaz**. Indukcijom po $k$.

Za $k=1$ je, po definiciji, $(\mathbf{M}_{12}^1)\phi_2\psi_1 = \mathbf{E}$. Prema tome je $(\mathbf{M}_{12}^1)\phi_2 \leq \mathbf{B}_2$, a zbog $(\mathbf{M}_{12}^1)\phi_2(\phi_1\psi_2) = (\mathbf{M}_{12}^1)(\phi_2\phi_1)\psi_2 = \mathbf{E}$ i $(\mathbf{M}_{12}^1)\phi_2 \leq \mathbf{M}_{21}^1$. Takođe imamo, prema analogonu leme 11.21, $(\mathbf{M}_{12}^1)\phi_1 \leq \mathbf{N}_{12}^1$, te izvodimo:

$$\mathbf{M}_{12}^1 \leq (\mathbf{M}_{12}^1)\phi_1 \times (\mathbf{M}_{12}^1)\phi_2 \leq \langle N_{12}^1 \cup M_{21}^1\rangle.$$

Pretpostavimo da je tvrđenje tačno za $k$ i pređimo na slučaj $k+1$. Prema 11.21 je $(\mathbf{M}_{12}^{k+1})\phi_1 \leq \mathbf{N}_{12}^{k+1}$, a po definiciji je

$$(\mathbf{M}_{12}^{k+1})(\phi_2\psi_1)^{k+1} = (\mathbf{M}_{12}^{k+1})\phi_2\psi_1(\phi_2\psi_1)^k = \mathbf{E},$$

što daje, s obzirom na induktivnu pretpostavku:

$$(\mathbf{M}_{12}^{k+1})\phi_2\psi_1 \leq \mathbf{M}_{12}^k \leq \langle N_{12}^k \cup M_{21}^k\rangle.$$

Slično: $(\mathbf{M}_{12}^{k+1})\phi_2\psi_2(\phi_1\psi_2)^k = (\mathbf{M}_{12}^{k+1})(\phi_2\psi_1)^{k+1} = \mathbf{E}$, a odatle $(\mathbf{M}_{12}^{k+1})\phi_2\psi_2 \leq \mathbf{M}_{21}^{k+1}$. Konačno, iz gore navedenog i $(\mathbf{M}_{12}^{k+1})\phi_2 \leq (\mathbf{M}_{12}^{k+1})\phi_2\psi_1 \times (\mathbf{M}_{12}^{k+1})\phi_2\psi_2$ sledi $(\mathbf{M}_{12}^{k+1})\phi_2 \leq \langle\langle N_{12}^k \cup M_{21}^k\rangle \cup M_{21}^{k+1}\rangle$, pa je

$$\mathbf{M}_{12}^{k+1} \leq (\mathbf{M}_{12}^{k+1})\phi_1 \times (\mathbf{M}_{12}^{k+1})\phi_2 \leq \langle N_{12}^{k+1} \cup M_{21}^{k+1}\rangle.$$

Pokazaćemo još da je $\mathbf{M}_{11} \leq \langle N_{22} \cup M_{22} \rangle$. Sledimo ideju prethodnog dokaza. $(\mathbf{M}_{11})\phi_1\psi_1 = \mathbf{E}$ implicira $(\mathbf{M}_{11})\phi_1 \leq \mathbf{B}_2$, a $(\mathbf{M}_{11})\phi_1(\phi_2\psi_2) = \mathbf{E}$ daje $(\mathbf{M}_{11})\phi_1 \leq \mathbf{M}_{22}$. Tu je, zbog

$$(\mathbf{M}_{11})\phi_2\psi_2\phi_2 = (\mathbf{M}_{11})\psi_1\phi_2\psi_2\phi_2 = (\mathbf{M}_{11})\psi_1\phi_1\psi_2\phi_2 =$$

$$(\mathbf{M}_{11})\psi_1\phi_1\psi_1\phi_2 = ((\mathbf{M}_{11})\phi_1\psi_1)\phi_2 = \mathbf{E},$$

i $(\mathbf{M}_{11})\phi_2 \leq \mathbf{N}_{22}$; dakle,

$$\mathbf{M}_{11} \leq (\mathbf{M}_{11})\phi_1 \times (\mathbf{M}_{11})\phi_2 \leq \langle N_{22} \cup M_{22} \rangle.\square$$

**Definicija 11.24** *Glavni niz grupe* $\mathbf{G}$ *je konačan niz podgrupa*

$$\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{i-1} > \mathbf{G}_i > \cdots > \mathbf{G}_n = \mathbf{E}$$

*gde je, za* $i = 1, \ldots, n$, $\mathbf{G}_i$ *maksimalna normalna podgrupa grupe* $\mathbf{G}$ *sadržana u* $\mathbf{G}_{i-1}$, *ukoliko takav postoji; u suprotnom kažemo da grupa* $\mathbf{G}$ *nema glavni niz.*

Definiciju glavnog niza ponovićemo u 46.12. Ovom prilikom samo navodimo (dokaz je dat u 46.13):

*Grupa* $\mathbf{G}$ *ima glavni niz ako i samo ako je svaki opadajući i svaki rastući lanac njenih normalnih podgrupa konačan.*

**Napomena.** U daljem tekstu, do teoreme, pretpostavljamo (uz već date) i sledeći uslov:

$(A)$ *za* $i = 1, 2$ *preslikavanja* $\phi_i\psi_1\phi_i\psi_2\phi_i$, $\psi_i\phi_1\psi_i\phi_2\psi_i$ *su homomorfna preslikavanje grupe* $\mathbf{G}$ *u (neku) normalnu podgrupu sa glavnim nizom.*

U cilju pojednostavljenja notacije stavljamo $\phi_1\psi_1\phi_1\psi_2\phi_1 = \eta$.

**Lema 11.25** *Grupe* $\mathbf{G}, (\mathbf{G})\eta, (\mathbf{G})\eta^2, \ldots$ *obrazuju opadajući niz normalnih podgrupa grupe* $\mathbf{G}$ *i za neko* $k_0$ *je*

$$(\mathbf{G})\eta^{k_0} = (\mathbf{G})\eta^{k_0+1} = \mathbf{G}\eta^{k_0+2} = \cdots.$$

*Ako je* $\mathbf{H} \leq (\mathbf{G})\eta^{k_0}$ *i* $(\mathbf{H})\eta = \mathbf{E}$, *onda je* $\mathbf{H} = \mathbf{E}$.

**Dokaz.** Jasno, $\mathbf{G} \geq (\mathbf{G})\eta \geq (\mathbf{G})\eta^2 \geq \cdots$.

Prema 11.4 je $(\mathbf{G})\psi_1\phi_1\psi_2 \leq \mathbf{Z}(\mathbf{G})$, a onda je i podgrupa $(\mathbf{G})\phi_1\psi_1\phi_1\psi_2\phi_1 = (\mathbf{G})\eta$ (pa sa njome i svaka njena podgrupa $(\mathbf{G})\eta^k$, $k \geq 1$) sadržana u centru grupe (imamo u vidu i 10.3$(d)$).

S obzirom na pretpostavku $(A)$ i Šrajerovu teoremu (46.4) opadajući niz $\mathbf{G} \geq (\mathbf{G})\eta \geq (\mathbf{G})\eta^2 \geq \cdots$ je konačan (podrazumevamo da se elementi niza ne ponavljaju), te je, počev od nekog $k_0$, $(\mathbf{G})\eta^{k_0} = (\mathbf{G})\eta^{k_0+1} = \cdots$.



Pretpostavimo da je $\mathbf{H}$ netrivijalna podgrupa grupe $(\mathbf{G})\eta^{k_0} = (\mathbf{G})\eta^{k_0+1} = ((\mathbf{G})\eta^{k_0})(\phi_1\psi_1\phi_1\psi_2)\phi_1$ i da je $(\mathbf{H})\eta = \mathbf{E}$. Prema 11.1$(g)$ postoji podgrupa $\mathbf{K}_1 \leq (\mathbf{G})\eta^{k_0}\phi_1\psi_1\phi_1\psi_2$ takva da je $(\mathbf{K}_1)\phi_1 = \mathbf{H}$. Konsekventno, postoji podgrupa $\mathbf{K}_2$ grupe $(\mathbf{G})\eta^{k_0}\phi_1\psi_1\phi_1$ takva da je $(\mathbf{K}_2)\psi_2 = \mathbf{K}_1$, podgrupa $\mathbf{K}_3$ grupe $(\mathbf{G})\eta^{k_0}\phi_1\psi_1$ takva da je $(\mathbf{K}_3)\phi_1 = \mathbf{K}_2$, podgrupa $\mathbf{K}_4$ grupe $(\mathbf{G})\eta^{k_0}\phi_1$ takva da je $(\mathbf{K}_4)\psi_1 = \mathbf{K}_3$ i, konačno, podgrupa $\mathbf{K}_5$ grupe $(\mathbf{G})\eta^{k_0}$ takva da je $(\mathbf{K}_5)\phi_1 = \mathbf{K}_4$. Odatle je

$$\mathbf{H} = (\mathbf{K}_1)\phi_1 = (\mathbf{K}_2)\psi_2\phi_1 = (\mathbf{K}_3)\phi_1\psi_2\phi_1 =$$

$$(\mathbf{K}_4)\psi_1\phi_1\psi_2\phi_1 = (\mathbf{K}_5)\phi_1\psi_1\phi_1\psi_2\phi_1 = (\mathbf{K}_5)\eta.$$

Sada je, prema 11.1$(f)$, $\langle H \cup K_5 \rangle\eta = \langle (H)\eta \cup (K_5)\eta \rangle = \langle K_5\eta \rangle = \mathbf{H}$ (jer je $(H)\eta = E$). Stoga je $\mathbf{H}$ prava podgrupa grupe $\mathbf{H}_1 = \langle H \cup K_5 \rangle$, koja je pak prava podgrupa grupe $(\mathbf{G})\eta$. Ponavljajući postupak dobili bismo redom podgrupe $\mathbf{H}_i$, $i = 2, 3, \ldots$, grupe $(\mathbf{G})\eta$ takve da je $H_1 \subset H_2 \subset H_3 \subset \ldots$, što je u protivurečnosti sa $(A)$.

Rezimiramo: iz $\mathbf{H} \leq (\mathbf{G})\eta^{k_0}$ i $(\mathbf{H})\eta = \mathbf{E}$ sledi $\mathbf{H} = \mathbf{E}.\square$

**Lema 11.26** $(a)$ $\mathbf{N}_1^{k_0} = \mathbf{N}_1^{k_0+1} = \mathbf{N}_1^{k_0+2} = \cdots$;

$(b)$ $\mathbf{N}_{1j}^{k_0} = \mathbf{N}_{1j}^{k_0+1} = \mathbf{N}_{1j}^{k_0+2} = \cdots$.

**Dokaz.** $(a)$ Za $r \geq 1$ imamo:

$$((\mathbf{N}_1^{k_0+r})\eta^{k_0+r-1})\eta = (\mathbf{N}_1^{k_0+r})\eta^{k_0+r} = (\mathbf{N}_1^{k_0+r})(\phi_1\psi_1\phi_1\psi_2\phi_1)^{k_0+r} =$$

$$(\mathbf{N}_1^{k_0+r})(\psi_1\phi_1\psi_2\phi_1)^{k_0+r} = \mathbf{E} \text{ (jer je } \mathbf{N}_1 \leq \mathbf{A}_1),$$

pa je prema prethodnoj lemi $(\mathbf{N}_1^{k_0+r})\eta^{k_0+r-1} = \mathbf{E}$. Jednako rezonujući dobijamo: $(\mathbf{N}_1^{k_0+r})\eta^{k_0+r-2} = \mathbf{E}$, ..., $(\mathbf{N}_1^{k_0+r})\eta^{k_0} = (\mathbf{N}_1^{k_0+r})(\psi_1\phi_1\psi_2\phi_1)^{k_0} = \mathbf{E}$; znači $\mathbf{N}_1^{k_0+r} \leq \mathbf{N}_1^{k_0}$, tj. $\mathbf{N}_1^{k_0+r} = \mathbf{N}_1^{k_0}$.

$(b)$ U 11.19 je pokazano: $\mathbf{N}_1^{k_0} = \mathbf{N}_{11}^{k_0} \times \mathbf{N}_{12}^{k_0}$, $\mathbf{N}_1^{k_0+r} = \mathbf{N}_{11}^{k_0+r} \times \mathbf{N}_{12}^{k_0+r}$, te je $\mathbf{N}_{11}^{k_0} \times \mathbf{N}_{12}^{k_0} = \mathbf{N}_{11}^{k_0+r} \times \mathbf{N}_{12}^{k_0+r}$, a odatle proizilazi, zbog $\mathbf{N}_{11}^{k_0} \leq \mathbf{N}_{11}^{k_0+r}$ i $\mathbf{N}_{12}^{k_0} \leq \mathbf{N}_{12}^{k_0+r}$:

$$\mathbf{N}_{11}^{k_0} = \mathbf{N}_{11}^{k_0+r}, \quad \mathbf{N}_{12}^{k_0} = \mathbf{N}_{12}^{k_0+r}.\square$$

Neka je

$$\mathbf{N}_1 = \bigcup_{k\geq 1} \mathbf{N}_1^k, \quad \mathbf{N}_{1j} = \bigcup_{k\geq 1} \mathbf{N}_{1j}^k, \quad j = 1, 2;$$
$$\mathbf{N}_2 = \bigcup_{k\geq 1} \mathbf{N}_2^k, \quad \mathbf{N}_{2j} = \bigcup_{k\geq 1} \mathbf{N}_{2j}^k, \quad j = 1, 2;$$
$$\mathbf{M}_i = \bigcup_{k\geq 1} \mathbf{M}_i^k, \quad \mathbf{M}_{ij} = \bigcup_{k\geq 1} \mathbf{M}_{ij}^k, \quad i = 1, 2;\ j = 1, 2.$$

**Lema 11.27** $\mathbf{N}_i = \mathbf{N}_{i1} \times \mathbf{N}_{i2}$, $\mathbf{M}_i = \mathbf{M}_{i1} \times \mathbf{M}_{i2}$, $i = 1, 2$;

$$\mathbf{N}_1 \times \mathbf{N}_2 = \mathbf{M}_1 \times \mathbf{M}_2;$$

$$\mathbf{N}_{11} \times \mathbf{N}_{12} \times \mathbf{N}_{21} \times \mathbf{N}_{22} = \mathbf{M}_{11} \times \mathbf{M}_{12} \times \mathbf{M}_{21} \times \mathbf{M}_{22}.$$

**Dokaz**. Direktna posledica prethodne i lema 11.19, 11.20.□

**Lema 11.28** *U dekompozicijama*

$$\mathbf{N}_{11} \times \mathbf{N}_{12} \times \mathbf{N}_{21} \times \mathbf{N}_{22} = \mathbf{M}_{11} \times \mathbf{M}_{12} \times \mathbf{M}_{21} \times \mathbf{M}_{22}$$

*uzajamno se nadoknađuju podgrupe* $\mathbf{N}_{11}$ *i* $\mathbf{M}_{22}$, $\mathbf{N}_{12}$ *i* $\mathbf{M}_{12}$, $\mathbf{N}_{22}$ *i* $\mathbf{M}_{11}$ *i* $\mathbf{N}_{21}$ *i* $\mathbf{M}_{21}$ *(videti* 11.9*).*

**Dokaz**. Prema 11.22 i 11.23 imamo: $\mathbf{N}_{12} \cap \mathbf{M}_{11}\mathbf{M}_2 = \mathbf{E}$, tj. $\mathbf{N}_{12} \cap (\mathbf{M}_{11} \times \mathbf{M}_{21} \times \mathbf{M}_{22}) = \mathbf{E}$ i $\mathbf{M}_{12} \leq \langle N_{12} \cup M_{21} \rangle$, pa je

$$\mathbf{N}_{12} \times \mathbf{M}_{11} \times \mathbf{M}_{21} \times \mathbf{M}_{22} = \mathbf{M}_{12} \times \mathbf{M}_{11} \times \mathbf{M}_{21} \times \mathbf{M}_{22}.$$

Ostali slučajevi se dokazuju analogno.□

**Lema 11.29** $\mathbf{N}_1 \cap (\mathbf{G})\eta^{k_0} = \mathbf{E}$.

**Dokaz**. $\mathbf{N}_1 = \bigcup_{k \geq 1} \mathbf{N}_1^k = \mathbf{N}_1^{k_0}$, stoga je

$$(\mathbf{N}_1 \cap (\mathbf{G})\eta^{k_0})\eta^{k_0} = (\mathbf{N}_1^{k_0} \cap (\mathbf{G})\eta^{k_0})\eta^{k_0} \leq (\mathbf{N}_1^{k_0})\eta^{k_0} = \mathbf{E},$$

a za dalje videti 11.25 i dokaz leme 11.26.□

**Lema 11.30** (*a*) $(\mathbf{G})\eta^{k_0} \cap (\mathbf{M}_1 \times \mathbf{B}_2) = \mathbf{E}$;
(*b*) $(\mathbf{G})\eta^{k_0} \cap (\mathbf{M}_2 \times \mathbf{B}_1) = \mathbf{E}$.

**Dokaz**. (*a*) Prema analogonu leme 11.26 je $\mathbf{M}_1 = \mathbf{M}_1^{k_0''}$ za neko $k_0''$. Dalje je:

$$(\mathbf{G})\eta^{k_0} \cap (\mathbf{M}_1 \times \mathbf{B}_2) \leq (\mathbf{G})\eta^{k_0} \leq \mathbf{A}_1$$

i

$$((\mathbf{G})\eta^{k_0} \cap (\mathbf{M}_1 \times \mathbf{B}_2))(\psi_1\phi_1\psi_2\phi_1)^{k_0''+1} \leq (\mathbf{M}_1^{k_0''} \times \mathbf{B}_2)(\psi_1\phi_1\psi_2\phi_1)^{k_0''+1} =$$

$$\langle (M_1^{k_0''})(\psi_1\phi_1\psi_2\phi_1)^{k_0''+1} \cup (B_2)(\psi_1\phi_1\psi_2\phi_1)^{k_0''+1} \rangle = \mathbf{E},$$

jer je, jasno, $(\mathbf{B}_2)\psi_1 = \mathbf{E}$ ali i

$$(\mathbf{M}_1^{k_0''})(\psi_1\phi_1\psi_2\phi_1)^{k_0''+1} = ((\mathbf{M}_1^{k_0''})\psi_1)(\phi_1\psi_2\phi_1)(\psi_1\phi_1\psi_2\phi_1)^{k_0''} =$$

$$(\mathbf{M}_1^{k_0''})(\phi_1\psi_2\phi_1\psi_1)^{k_0''}\phi_1\psi_2\phi_1 = (\mathbf{M}_1^{k_0''})(\phi_1\psi_1\phi_2\psi_1)^{k_0''}\phi_1\psi_2\phi_1 \text{ (videti 11.12)} =$$

$$(\mathbf{E})\phi_1\psi_2\phi_1 = \mathbf{E}.$$

Sledi $(\mathbf{G})\eta^{k_0} \cap (\mathbf{M}_1 \times \mathbf{B}_2) \leq \mathbf{N}_1^{k_0''} \leq \mathbf{N}_1$, te je $(\mathbf{G})\eta^{k_0} \cap (\mathbf{M}_1 \times \mathbf{B}_2) \leq \mathbf{N}_1 \cap (\mathbf{G})\eta^{k_0} = \mathbf{E}$.□



**Lema 11.31** (*a*) $\mathbf{A}_1 = \mathbf{N}_1 \times (\mathbf{G})\eta^{k_0}$, $\mathbf{A}_2 = \mathbf{N}_2 \times (\mathbf{G})(\phi_2\psi_1\phi_2\psi_2\phi_2)^{k_0'}$;
(*b*) $\mathbf{B}_1 = \mathbf{M}_1 \times (\mathbf{G})(\psi_1\phi_1\psi_1\phi_2\psi_1)^{k_0''}$, $\mathbf{B}_2 = \mathbf{M}_2 \times (\mathbf{G})(\psi_2\phi_1\psi_2\phi_2\psi_2)^{k_0'''}$.
*Uloga (prirodnih brojeva)* $k_0'$, $k_0''$, $k_0'''$ *za odgovarajuća preslikavanja adekvatna je ulozi broja* $k_0$ *za preslikavanje* $\eta$.

**Dokaz**. (*a*) Već znamo da su $\mathbf{N}_1$ i $(\mathbf{G})\eta^{k_0}$ normalne podgrupe grupe $\mathbf{A}_1$ (11.16 i 11.25) i da je $\mathbf{N}_1 \cap (\mathbf{G})\eta^{k_0} = \mathbf{E}$. Treba, dakle, samo pokazati: $\mathbf{A}_1 \leq \mathbf{N}_1 \times (\mathbf{G})\eta^{k_0}$.

Neka je $a_1 \in A_1$. Onda je $(a_1)\eta^{k_0} \in (G)\eta^{k_0} = ((G)\eta^{k_0})\eta^{k_0}$, pa je, za neko $g \in G$, $(a_1)\eta^{k_0} = ((g)\eta^{k_0})\eta^{k_0}$, tj. $(a_1 \cdot (g^{-1})\eta^{k_0})\eta^{k_0} = e$. Ali $a_1 \cdot (g^{-1})\eta^{k_0} \in A_1$ te je $(a_1 \cdot (g^{-1})\eta^{k_0})\eta^{k_0} = (a_1 \cdot (g^{-1})\eta^{k_0})(\phi_1\psi_1\phi_1\psi_2\phi_1)^{k_0} = (a \cdot (g^{-1})\eta^{k_0})(\psi_1\phi_1\psi_2\phi_1)^{k_0}$; dakle $a_1 \cdot (g^{-1})\eta^{k_0} \in N_1$.□

**Lema 11.32**
(*a*) $(\mathbf{G})(\psi_1\phi_1\psi_1\phi_2\psi_1)^{k_0''} \leq (\mathbf{G})(\phi_1\psi_1\phi_1\psi_2\phi_1)^{k_0} \cdot \mathbf{B}_2 \cap (\mathbf{G})(\phi_2\psi_1\phi_2\psi_2\phi_2)^{k_0'} \cdot \mathbf{B}_2$;
(*b*) $(\mathbf{G})(\psi_2\phi_1\psi_2\phi_2\psi_2)^{k_0'''} \leq (\mathbf{G})(\phi_1\psi_1\phi_1\psi_2\phi_2)^{k_0} \cdot \mathbf{B}_1 \cap (\mathbf{G})(\phi_2\psi_1\phi_2\psi_2\phi_2)^{k_0'} \cdot \mathbf{B}_1$;
(*c*) $(\mathbf{G})(\phi_1\psi_1\phi_1\psi_2\phi_1)^{k_0} \leq (\mathbf{G})(\psi_1\phi_1\psi_1\phi_2\psi_1)^{k_0''} \cdot \mathbf{A}_2 \cap (\mathbf{G})(\psi_2\phi_1\psi_2\phi_2\psi_2)^{k_0'''} \cdot \mathbf{A}_2$;
(*d*) $(\mathbf{G})(\phi_2\psi_1\phi_2\psi_2\phi_2)^{k_0'} \leq (\mathbf{G})(\psi_1\phi_1\psi_1\phi_2\psi_1)^{k_0''} \cdot \mathbf{A}_1 \cap (\mathbf{G})(\psi_2\phi_1\psi_2\phi_2\psi_2)^{k_0'''} \cdot \mathbf{A}_1$.

**Dokaz**. Proverimo samo prvi deo tačke (*a*):

$$(\mathbf{G})(\psi_1\phi_1\psi_1\phi_2\psi_1)^{k_0''} \leq (\mathbf{G})(\phi_1\psi_1\phi_1\psi_2\phi_1)^{k_0} \cdot \mathbf{B}_2.$$

Neka je

$$g \in (G)(\psi_1\phi_1\psi_1\phi_2\psi_1)^{k_0''} = (G)(\psi_1\phi_1\psi_1\phi_2\psi_1)^{k_0''+1} =$$

$$(G)(\psi_1\phi_1\psi_1\phi_2\psi_1)^{k_0''}(\psi_1\phi_1\psi_1\phi_2\psi_1).$$

Onda je za, neko $h \in (G)(\psi_1\phi_1\psi_1\phi_2\psi_1)^{k_0''}$,

$$g = (h)(\psi_1\phi_1\psi_1\phi_2\psi_1) = (h)(\phi_1\psi_1\phi_2\psi_1).$$

Neka je, dalje, $k = max\{k_0, k_0''\}$. Kako je

$$(\mathbf{G})(\psi_1\phi_1\psi_1\phi_2\psi_1)^{k_0''} = (\mathbf{G})(\psi_1\phi_1\psi_1\phi_2\psi_1)^{k} = (\mathbf{B}_1)(\phi_1\psi_1\phi_2\psi_1)^{k},$$

to je $h = (b_1)(\phi_1\psi_1\phi_2\psi_1)^k$ za neko $b_1 \in B_1$. Sada iz

$$(h)\phi_1 = (h)\phi_1\psi_1 \cdot (h)\phi_1\psi_2 = ((h)\phi_1\psi_1\phi_1 \cdot (h)\phi_1\psi_2\phi_2) \cdot (h)\phi_1\psi_2 =$$

$$(h)\phi_1\psi_1\phi_1 \cdot ((h)\phi_1\psi_1\phi_2\psi_1 \cdot (h)\phi_1\psi_1\phi_2\psi_2) \cdot (h)\phi_1\psi_2 =$$

$$(h)\phi_1\psi_1\phi_1 \cdot g \cdot (h)\phi_1\psi_1\phi_2\psi_2 \cdot (h)\phi_1\psi_2$$

sledi

$$g = ((h)\phi_1\psi_1\phi_1)^{-1} \cdot (h)\phi_1 \cdot ((h)\phi_1\psi_2)^{-1} \cdot ((h)\phi_1\psi_1\phi_2\psi_2)^{-1} =$$

$$(h^{-1})\phi_1\psi_1\phi_1\cdot(h)\phi_1\cdot(h^{-1})\phi_1\psi_2\cdot(h^{-1})\phi_1\psi_1\phi_2\psi_2.$$

Jasno, $(h^{-1})\phi_1\psi_2\cdot(h^{-1})\phi_1\psi_1\phi_2\psi_2 \in B_2$. Preostaje da se pokaže da su elementi $(h)\phi_1$ i $(h)\phi_1\psi_1\phi_1$ iz $A_1$ ujedno i elementi grupe $(\mathbf{G})\eta^{k_0}$.

$$(h)\phi_1 = (b_1)(\phi_1\psi_1\phi_2\psi_1)^k\phi_1 = ((b_1)\phi_1)(\psi_1\phi_2\psi_1\phi_1)^k =$$

$$((b_1)\phi_1)(\psi_1\phi_1\psi_2\phi_1)^k = (b)(\phi_1\psi_1\phi_1\psi_2\phi_1)^k \in (G)\eta^k = (G)\eta^{k_0};$$

Koristili smo (videti lemu 11.12): za $x \in G$ je

$$(x)\psi_1\phi_2\psi_1\phi_1 = ((x)\psi_1)^{-1}\phi_2\psi_2\phi_1 = (x^{-1})\psi_1\phi_2\psi_2\phi_1 = (x)\psi_1\phi_1\psi_2\phi_1.$$

$$(h)\phi_1\psi_1\phi_1 = (b_1)(\phi_1\psi_1\phi_2\psi_1)^k\phi_1\psi_1\phi_1 = ((b_1\phi_1)(\psi_1\phi_2\psi_1\phi_1)^k\psi_1\phi_1 =$$

$$((b_1)\phi_1)(\psi_1\phi_1\psi_2\phi_1)^k\psi_1\phi_1 \text{ (prema upravo navedenom)} =$$

$$((b_1)\phi_1\psi_1\phi_1)(\psi_2\phi_1\psi_1\phi_1)^k = ((b_1)\phi_1\psi_1\phi_1)(\psi_1\phi_1\psi_2\phi_1)^k \text{ (prema 11.14)} =$$

$$((b_1)\phi_1\psi_1)(\phi_1\psi_1\phi_1\psi_2\phi_1)^k \in (G)\eta^k = (G)\eta^{k_0}.\square$$

**Lema 11.33** *Među faktorima dekompozicija grupe* $\mathbf{G}$ $(= \mathbf{A}_1\times\mathbf{A}_2 = \mathbf{B}_1\times\mathbf{B}_2)$, *koje nam daju prethodni rezultati,*

$$\mathbf{N}_{11}\times\mathbf{N}_{12}\times(\mathbf{G})\eta^{k_0}\times\mathbf{N}_{21}\times\mathbf{N}_{22}\times(\mathbf{G})(\phi_2\psi_1\phi_2\psi_2\phi_2)^{k_0'}$$

*i*

$$\mathbf{M}_{11}\times\mathbf{M}_{12}\times(\mathbf{G})(\psi_1\phi_1\psi_1\phi_2\psi_1)^{k_0''}\times\mathbf{M}_{21}\times\mathbf{M}_{22}\times(\mathbf{G})(\psi_2\phi_1\psi_2\phi_2\psi_2)^{k_0'''}$$

*postoji uzajamno jednoznačna korespondencija takva da se korespondentni faktori mogu uzajamno zamenjivati (samim tim oni su i centralno izomorfni).*

**Dokaz**. Stavimo, u cilju pojednostavljenja notacije:

$$(\mathbf{G})\eta^{k_0} = \overline{\mathbf{A}}_1,\ (\mathbf{G})(\phi_2\psi_1\phi_2\psi_2\phi_2)^{k_0'} = \overline{\mathbf{A}}_2,$$

$$(\mathbf{G})(\psi_1\phi_1\psi_1\phi_2\psi_1)^{k_0''} = \overline{\mathbf{B}}_1,\ (\mathbf{G})(\psi_2\phi_1\psi_2\phi_2\psi_2)^{k_0'''} = \overline{\mathbf{B}}_2.$$

Prema lemi 11.28 u dekompozicijama

$$\mathbf{H} = \mathbf{N}_{11}\times\mathbf{N}_{12}\times\mathbf{N}_{21}\times\mathbf{N}_{22} = \mathbf{M}_{11}\times\mathbf{M}_{12}\times\mathbf{M}_{21}\times\mathbf{M}_{22},$$

uzajamno se nadoknađuju podgrupe $\mathbf{N}_{11}$ i $\mathbf{M}_{22}$, $\mathbf{N}_{12}$ i $\mathbf{M}_{12}$, $\mathbf{N}_{22}$ i $\mathbf{M}_{11}$, $\mathbf{N}_{21}$ i $\mathbf{M}_{21}$. Ovo, jasno, ostaje u važnosti i za date dekompozicije grupe $\mathbf{G}$; podsetimo se samo kako smo ih dobili:

$$\mathbf{G} = \mathbf{A}_1\times\mathbf{A}_2 = \mathbf{N}_1\times\overline{\mathbf{A}}_1\times\mathbf{N}_2\times\overline{\mathbf{A}}_2 \text{ (prema 11.31)} =$$

$$\mathbf{N}_{11}\times\mathbf{N}_{12}\times\overline{\mathbf{A}}_1\times\mathbf{N}_{21}\times\mathbf{N}_{22}\times\overline{\mathbf{A}}_2 \text{ (prema lemi 11.27)}$$



i analogno

$$\mathbf{G} = \mathbf{M}_{11}\times\mathbf{M}_{12}\times\overline{\mathbf{B}}_1\times\mathbf{M}_{21}\times\mathbf{M}_{22}\times\overline{\mathbf{B}}_2.$$

Pokažimo da se podgrupe $\overline{\mathbf{A}}_1$ i $\overline{\mathbf{B}}_1$ mogu takođe jedna drugom zameniti. Na osnovu poslednjih lema dobijamo redom:

$$\overline{\mathbf{B}}_1 \le \overline{\mathbf{A}}_1\cdot\mathbf{B}_2 = \overline{\mathbf{A}}_1\cdot(\overline{\mathbf{B}}_2\times\mathbf{M}_2) \le \overline{\mathbf{A}}_1\cdot(\overline{\mathbf{B}}_2\times\mathbf{H});$$

prema 11.30 je

$$\overline{\mathbf{A}}_1\cap(\mathbf{B}_2\times\mathbf{M}_1) = \mathbf{E},$$

i odatle

$$\overline{\mathbf{A}}_1\cap(\overline{\mathbf{B}}_2\times\mathbf{M}_2\times\mathbf{M}_1) = \overline{\mathbf{A}}_1\cap(\overline{\mathbf{B}}_2\times\mathbf{H}) = \mathbf{E},$$

pa je

$$\overline{\mathbf{B}}_1 \le \overline{\mathbf{A}}_1\times\overline{\mathbf{B}}_2\times\mathbf{H}.$$

Jednako tako se pokazuje da se i $\overline{\mathbf{A}}_2$ i $\overline{\mathbf{B}}_1$ mogu uzajamno zamenjivati; shodno tome se i $\overline{\mathbf{B}}_2$ može zameniti i sa $\overline{\mathbf{A}}_1$ i sa $\overline{\mathbf{A}}_2$.$\square$

**Teorema 11.34** *(Teorema Kuroša). Neka je* $\mathbf{G}$ *grupa sa svojstvom da svaka podgrupa njenog centra na koju se grupa može homomorfno preslikati ima glavni niz. Tada svake dve dekompozicije grupe* $\mathbf{G}$ *imaju centralno izomorfna produženja.*

**Dokaz**. Razmotrimo prvo slučaj konačnih dekompozicija, tj. pođimo od toga da $\mathbf{G}$ ima konačne dekompozicije sa, respektivno, $k$ i $r$ faktora. Indukcijom po zbiru $k+r$ pokazaćemo da se podgrupe prve dekompozicije (dekompozicije sa $k$ faktora) mogu razložiti u direktan proizvod od $r$ faktora a podgrupe druge dekompozicije u direktan proizvod od $k$ faktora (dopuštamo u oba slučaja mogućnost da su neki od faktora trivijalna podgrupa $\mathbf{E}$) tako da su dobijena proširenja centralno izomorfna i pri tome nikoja dva faktora podgrupe prve dekompozicije nisu u korespondenciji sa faktorima iste podgrupe druge dekompozicije.

Za $k+r=4$ ovo je već pokazano. Slučaj $k=1$, $r=3$ je trivijalan, a ako je $k=r=2$, onda polazeći od $\mathbf{G} = \mathbf{A}_1\times\mathbf{A}_2 = \mathbf{B}_1\times\mathbf{B}_2$ dobijamo, prema poslednjoj lemi (videti i dokaz leme 11.25) i činjenici da s obzirom na uslove teoreme pretpostavka $(A)$ važi:

$$((\mathbf{N}_{11}\times\overline{\mathbf{A}}_1)\times\mathbf{N}_{12})\times(\mathbf{N}_{21}\times(\mathbf{N}_{22}\times\overline{\mathbf{A}}_2)) =$$

$$(\mathbf{M}_{12}\times(\mathbf{M}_{11}\times\overline{\mathbf{B}}_1))\times(\mathbf{M}_{21}\times(\mathbf{M}_{22}\times\overline{\mathbf{B}}_2))$$

(zadržali smo poznatu notaciju). Korespondentni faktori koji ispunjavaju zahteve tvrđenja su: $\mathbf{N}_{11}\times\overline{\mathbf{A}}_1$ i $\mathbf{M}_{22}\times\overline{\mathbf{B}}_2$, $\mathbf{N}_{12}$ i $\mathbf{M}_{12}$, $\mathbf{N}_{21}$ i $\mathbf{M}_{21}$, $\mathbf{N}_{22}\times\overline{\mathbf{A}}_2$ i $\mathbf{M}_{11}\times\overline{\mathbf{B}}_1$.

Pretpostavimo da je tvrđenje tačno za svako $k_1 + r_1 < k + r$ $(> 4)$ (preciznije, da za svaku grupu koja ispunjava uslove teoreme i ima dekompozicije sa $k_1$, odnosno $r_1$ faktora važi tvrđenje iz prvog pasusa dokaza). Neka je

$$\mathbf{G} = \mathbf{A}_1 \times \cdots \times \mathbf{A}_{k-1} \times \mathbf{A}_k = \mathbf{B}_1 \times \cdots \times \mathbf{B}_r,$$

gde je $k > 2$. Stavimo $\mathbf{A}_{k-1} \times \mathbf{A}_k = \mathbf{A}^*_{k-1}$. Prema induktivnoj hipotezi postoje centralno izomorfna proširenja

$$(\mathbf{A}_{11} \times \cdots \times \mathbf{A}_{1r}) \times \cdots \times (\mathbf{A}^*_{k-1,1} \times \cdots \times \mathbf{A}^*_{k-1,r}) =$$

$$(\mathbf{B}_{11} \times \cdots \times \mathbf{B}_{1,k-1}) \times \cdots \times ((\mathbf{B}_{r1} \times \cdots \times \mathbf{B}_{r,k-1}) \qquad (1).$$

Recimo da su korespondentni faktori $\mathbf{A}_{ij}$ i $\mathbf{B}_{ji}$ za $i = 1, \ldots, k-2$ i $j = 1, \ldots, r$, i $\mathbf{A}^*_{k-1,j}$ i $\mathbf{B}_{j,k-1}$ za $j = 1, \ldots, r$.

Grupa $\mathbf{A}^*_{k-1} = \mathbf{A}_{k-1} \times \mathbf{A}_k = \mathbf{A}^*_{k-1,1} \times \cdots \times \mathbf{A}^*_{k-1,r}$ takođe ispunjava uslove teoreme: ako je $\mathbf{H}$ podgrupa (njenog) centra na koju se ona može homomorfno preslikati, onda se, jasno, na tu podgrupu može homomorfno preslikati i cela grupa $\mathbf{G}$. Kako je $2 + r < k + r$, date dekompozicije grupe $\mathbf{A}^*_{k-1}$ imaju (prema induktivnoj hipotezi) centralno izomorfna proširenja

$$(\mathbf{A}_{k-1,1} \times \cdots \times \mathbf{A}_{k-1,r}) \times (\mathbf{A}_{k,1} \times \cdots \times \mathbf{A}_{k,r}) =$$

$$(\mathbf{A}^*_{k-1,1,1} \times \mathbf{A}^*_{k-1,1,2}) \times \cdots \times (\mathbf{A}^*_{k-1,r,1} \times \mathbf{A}^*_{k-1,r,2}).$$

Neka su korespondentni faktori $\mathbf{A}^*_{k-1,j,1}$ i $\mathbf{A}_{k-1,j}$, $\mathbf{A}^*_{k-1,j,2}$ i $\mathbf{A}_{k,j}$ $(j = 1, \ldots, r)$. Pošto je (po učinjenoj pretpostavci) $\mathbf{A}^*_{k-1,j} \cong \mathbf{B}_{j,k-1}$, $j = 1, \ldots, r$, onda je $\mathbf{B}_{j,k-1} = \mathbf{B}_{j,k-1,1} \times \mathbf{B}_{j,k-1,2}$, gde je $\mathbf{B}_{j,k-1,i}$ izomorfna slika grupe $\mathbf{A}^*_{k-1,j,i}$, $i = 1, 2$, pa konstatujemo da su

$(\mathbf{A}_{11} \times \cdots \times \mathbf{A}_{1r}) \times (\mathbf{A}_{21} \times \cdots \times \mathbf{A}_{2r}) \times \cdots \times (\mathbf{A}_{k-1,1} \times \cdots \times \mathbf{A}_{k-1,r}) \times (\mathbf{A}_{k1} \times \cdots \times \mathbf{A}_{kr})$

i

$(\mathbf{B}_{11} \times \cdots \times \mathbf{B}_{1,k-1,1} \times \mathbf{B}_{1,k-1,2}) \times (\mathbf{B}_{21} \times \cdots \times \mathbf{B}_{2,k-1,1} \times \mathbf{B}_{2,k-1,2}) \times \cdots \times (\mathbf{B}_{r1} \times \cdots \times \mathbf{B}_{r,k-1,1} \times \mathbf{B}_{r,k-1,2})$

centralno izomorfna proširenja početnih dekompozicija. Korespondentni faktori su: $\mathbf{A}_{ij}$ i $\mathbf{B}_{ji}$ za $1 \leq i < k-1$ i $j = 1, \ldots, r$, i $\mathbf{A}_{k-1,j}$ i $\mathbf{B}_{j,k-1,1}$, $\mathbf{A}_{kj}$ i $\mathbf{B}_{j,k-1,2}$ za $j = 1, \ldots, r$.

Pritom smo imali u vidu sledeće:

*Ako su* $\mathbf{A}$, $\mathbf{B}$ *i* $\mathbf{C}$ *direktni faktori nekih dekompozicija i ako su* $\mathbf{A}$ *i* $\mathbf{B}$, $\mathbf{B}$ *i* $\mathbf{C}$ *centralno izomorfni, onda su i* $\mathbf{A}$ *i* $\mathbf{C}$ *centralno izomorfni.*

Uočimo još da smo u okviru dokaza posmatrali posebno centralna proširenja dekompozicija (direktnog faktora grupe $\mathbf{G}$) $\mathbf{A}^*_{k-1}$. No to ne menja ništa na stvari. Tako su npr. $\mathbf{A}^*_{k-1,j,1}$ i $\mathbf{A}_{k-1,j}$ centralno izomorfne podgrupe s obzirom na $\mathbf{A}^*_{k-1}$, ali onda i s obzirom na $\mathbf{G}$ jer je $\mathbf{Z}(\mathbf{A}^*_{k-1}) \leq \mathbf{Z}(\mathbf{G})$.

Preostaje slučaj kada su date dekompozicije sa proizvoljnim brojem faktora. Naredne dve leme ga, međutim, svode na upravo rešen slučaj konačnih dekompozicija.



**Lema 11.35** *Neka je* $\mathbf{G} = \prod_{i \in I} \mathbf{A}_i \times \prod_{k \in K} \mathbf{C}_k = \prod_{j \in J} \mathbf{B}_j \times \prod_{r \in R} \mathbf{D}_r$, *gde su* $\mathbf{C} = \prod_k \mathbf{C}_k$ *i* $\mathbf{D} = \prod_r \mathbf{D}_r$ *F-grupe (videti* 11.5*), i neka dekompozicije* $\prod_i \mathbf{A}_i \times \mathbf{C} = \prod_j \mathbf{B}_j \times \mathbf{D}$ *imaju centralno izomorfna proširenja; podrazumevamo da su odgovarajući indeksni skupovi* $I$, $J$, $K$, $R$ *proizvoljne kardinalnosti. Tada i date direktne dekompozicije imaju centralno izomorfna produženja.*

**Dokaz**. Neka su $\prod_{i'} \mathbf{A}'_{i'} \times \prod_{k'} \mathbf{C}'_{k'} = \prod_{j'} \mathbf{B}'_{j'} \times \prod_{r'} \mathbf{D}'_{r'}$ centralno izomorfna produženja dekompozicija $\prod_i \mathbf{A}_i \times \mathbf{C} = \prod_j \mathbf{B}_j \times \mathbf{D}$. Pošto je $\mathbf{C} = \prod_k \mathbf{C}_k = \prod_{k'} \mathbf{C}'_{k'}$ $F$-grupa, prema 11.6$(a)$ postoji zajedničko produženje datih dekompozicija $\prod_{k''} \mathbf{C}''_{k''}$. No onda su centralno izomorfne dekompozicije

$$\prod_{i'} \mathbf{A}'_{i'} \times \prod_{k''} \mathbf{C}''_{k''} = \prod_{j''} \mathbf{B}''_{j''} \times \prod_{r''} \mathbf{D}''_{r''},$$

gde su faktori $\mathbf{B}'_{j'}$, $\mathbf{D}'_{r'}$, koji su izomorfni sa faktorima $\mathbf{C}'_{k'}$, razloženi već kako nalažu dati izomorfizmi, s obzirom na razlaganje grupe $\mathbf{C}'_{j'}$ (videti 10.13).

Konačno, dekompozicije grupe $\mathbf{D}$, $\prod_r \mathbf{D}_r$ i $\prod_{r''} \mathbf{D}''_{r''}$, imaju zajedničko produženje $\prod_{r'''} \mathbf{D}'''_{r'''}$ (jer je i $\mathbf{D}$ $F$-grupa). No tada su dekompozicije

$$\prod_{i''} \mathbf{A}''_{i''} \times \prod_{k'''} \mathbf{C}'''_{k'''} = \prod_{j''} \mathbf{B}''_{j''} \times \prod_{r'''} \mathbf{D}'''_{r'''},$$

gde smo faktore $\mathbf{A}'_{i'}$ i $\mathbf{C}''_{k''}$ izomorfne sa $\mathbf{D}''_{r''}$ razložili kako već nalaže razlaganje faktora $\mathbf{D}''_{r''}$ (ponovo je u pitanju lema 10.13), centralno izomorfna produženja polaznih dekompozicija.□

**Lema 11.36** *Neka grupa* $\mathbf{G}$ *ispunjava uslove teoreme i neka je* $\prod_{i \in I} \mathbf{G}_i$ *jedna njena dekompozicija. Tada je* $\prod_{i \in I \setminus K} \mathbf{G}_i$ $F$*-grupa za neki konačan podskup* $K$ *skupa* $I$.

**Dokaz**. Naravno, interesantan je samo slučaj $|I| \geq \aleph_0$. Dokazujemo prvo:

U dekompoziciji $\prod_i \mathbf{G}_i$ postoji samo konačno mnogo faktora takvih da za svaki indeks $j$ (ma kojeg) beskonačnog podskupa $J$ skupa $I$ postoje netrivijalna homomorfna preslikavanja faktor grupe $\mathbf{G}_j/\mathbf{G}'_j$ u centar svake od njih.

Pretpostavimo suprotno. Onda postoji beskonačno prebrojiva familija direktnih faktora, $\{\mathbf{G}_{i_n} \mid n \in \omega\}$, takvih da se za neki beskonačno prebrojiv skup $J = \{j_0, j_1, \ldots\}$ i za sve prirodne brojeve $m, n$ faktor grupa $\mathbf{G}_{j_m}/\mathbf{G}'_{j_m}$ preslikava netrivijalno homomorfno u $\mathbf{Z}(\mathbf{G}_{i_n})$. Neka je $\varphi_n$ netrivijalno homomorfno preslikavanje grupe $\mathbf{G}_{j_n}/\mathbf{G}'_{j_n}$ u $\mathbf{Z}(\mathbf{G}_{i_n})$ $(\mathbf{E} \neq (\mathbf{G}_{j_n}/\mathbf{G}'_{j_n})\varphi_n \leq \mathbf{Z}(\mathbf{G}_{i_n}))$, pa definišimo preslikavanje $\varphi : \prod_n G_{j_n}/G'_{j_n} \longrightarrow \prod_n Z(\mathbf{G}_{i_n})$ (za $f \in \prod_n G_{j_n}/G'_{j_n}$) sa $(n)((f)\varphi) = ((n)f)\varphi_n$. Lako se proverava da je $\varphi$ homomorfno preslikavanje i da je

$$(\prod_n \mathbf{G}_{j_n}/\mathbf{G}'_{j_n})\varphi = \prod_n (\mathbf{G}_{j_n}/\mathbf{G}'_{j_n})\varphi_n \leq \prod_n \mathbf{Z}(\mathbf{G}_{i_n}).$$

Kako je

$$\prod_{j\in J}\mathbf{G}_j/(\prod_{j\in J}\mathbf{G}_j)' = \prod_{j\in J}\mathbf{G}_j/\prod_{j\in J}\mathbf{G}'_j \cong \prod_{j\in J}\mathbf{G}_j/\mathbf{G}'_j$$

(videti 10.3(*b*),(*e*)), to se i $\prod_{j\in J}\mathbf{G}_j/\prod_{j\in J}\mathbf{G}'_j$ homomorfno preslikava na grupu $\prod_n(\mathbf{G}_{j_n}/\mathbf{G}'_{j_n})\varphi_n$, a onda i

$$\mathbf{G}/\mathbf{G}' \cong \prod_{j\in J}\mathbf{G}_j/(\prod_{j\in J}\mathbf{G}_j)' \times \prod_{i\in I\setminus J}\mathbf{G}_i/(\prod_{i\in I\setminus J}\mathbf{G}_i)'.$$

Grupa $\prod_n(\mathbf{G}_{j_n}/\mathbf{G}'_{j_n})\varphi_n$, međutim, očigledno nema glavni niz, što je u suprotnosti sa uslovom leme (odnosno teoreme – videti takođe lemu 11.5 i njen dokaz).

Isključimo sada faktore o kojima govori prvi deo tvrđenja. Među preostalima postoji samo konačno mnogo takvih da se njihove faktor grupe po izvodnim podgrupama mogu netrivijalno homomorfno preslikati u centre nekih od faktora (naravno, opet imamo u vidu samo preostale faktore). Pretpostavka da ih ima beskonačno mnogo opet vodi u kontradikciju sa uslovom teoreme. Jer, ako bi elementi beskonačne familije $\{\mathbf{G}_{k_n} \mid n \in \omega\}$ imali to svojstvo, s obzirom da se u centar bilo kog od (preostalih) faktora može netrivijalno homomorfno preslikati samo konačno mnogo faktor grupa (preostalih direktnih faktora) po izvodnim grupama, to bi morala postojati i beskonačna familija $\{\mathbf{G}_{r_n} \mid n \in \omega\}$ takva da se za svako $m$ faktor grupa $\mathbf{G}_{k_m}/\mathbf{G}'_{k_m}$ preslikava netrivijalno homomorfno u centar neke grupe $\mathbf{G}_{r_n}$ (možemo pretpostaviti da se $\mathbf{G}_{k_m}/\mathbf{G}'_{k_m}$ preslikava netrivijalno baš u $\mathbf{Z}(\mathbf{G}_{r_m})$). Ali tada bi dobili, kao i u prethodnom slučaju, netrivijalno homomorfno preslikavanje faktor grupe $\mathbf{G}/\mathbf{G}'$ u podgrupu centra koja nema glavni niz.

Isključimo sada i ove faktore. Neka je $K$ skup indeksa svih faktora isključenih bilo u prvom bilo u drugom koraku (a takvih je bilo konačno mnogo) i neka je $L = I \setminus K$. Onda je $\prod_{i\in L}\mathbf{G}_i$ $F$-grupa. Naime, ako bi postojalo netrivijalno homomorfno preslikavanje grupe $\prod_{i\in L}\mathbf{G}_i/(\prod_{i\in L}\mathbf{G}_i)'$ u $\mathbf{Z}(\prod_{i\in L}\mathbf{G}_i) = \prod_{i\in L}\mathbf{Z}(\mathbf{G}_i)$, tada bismo imali i netrivijalno homomorfno preslikavanje grupe $\prod_{i\in L}\mathbf{G}_i/\mathbf{G}'_i$ u $\prod_{i\in L}\mathbf{Z}(\mathbf{G}_i)$, dakle i netrivijalno homomorfno preslikavanje nekog od faktora $\mathbf{G}_i/\mathbf{G}'_i$ u centar nekog od faktora $\mathbf{G}_j$ $(i, j \in L)$, kontradikcija.□

Poslednju implikaciju obrazlaže sledeća lema.

**Lema 11.37** *Neka je* $\varphi : \prod_{i\in M}^d A_i \longrightarrow \prod_{i\in M}^d B_i$ *netrivijalno homomorfno preslikavanje grupe* $\prod_{i\in M}\mathbf{A}_i$ *u* $\prod_{i\in M}\mathbf{B}_i$. *Onda za neke indekse* $i_r, j$ *iz* $M$ *postoji netrivijalno homomorfno preslikavanje grupe* $\mathbf{A}_{i_r}$ *u grupu* $\mathbf{B}_j$.

**Dokaz.** Neka je $e \neq f \in \prod_{i\in M}^d A_i$ i neka je $(f)\varphi \neq e$. Kako je u pitanju direktan proizvod, to je $f = f_{a_{i_1}} \dots f_{a_{i_m}}$, gde je

$$(i)f_{a_{i_k}} = \begin{cases} a_{i_k} \in A_{i_k} & i = i_k \\ e_i & \text{inače.} \end{cases}$$



Prema tome je $f_{a_{i_k}} \in \widehat{A_{i_k}}$ – videti lemu 10.7. Naravno, $(f_{a_{i_r}})\varphi \neq e$ za bar jedno $r$ $(1 \leq r \leq m)$; neka je npr. $(j)((f_{a_{i_r}})\varphi) \neq e_j$. Preslikavanje $\varphi_{i_r} : \widehat{A_{i_r}} \longrightarrow B_j$ definisano sa $\varphi_{i_r} = \varphi|_{\widehat{A_{i_r}}} \circ \pi_j$ ($\pi_j$ je projekcija grupe $\prod_{i\in M}\mathbf{B}_i$ u $\mathbf{B}_j$) očigledno je netrivijalno homomorfno preslikavanje grupe $\widehat{\mathbf{A}_{i_r}}$ $(\cong \mathbf{A}_{i_r})$ u grupu $\mathbf{B}_j$.□ ■

**Korolar 11.38** *Svake dve dekompozicije grupe* $\mathbf{G}$, *čiji centar ima glavni niz ili čija faktor grupa* $\mathbf{G}/\mathbf{G}'$ *ima glavni niz, imaju centralno izomorfna produženja.*

**Dokaz.** Primetimo samo da ako grupa ima glavni niz, onda i njene podgrupe i homomorfne slike imaju glavni niz (za dokaz videti 8.8). A ako se grupa $\mathbf{G}$ homomorfno preslikava na podgrupu $\mathbf{H}$ svog centra (neka je $\varphi$ homomorfizam), onda se na tu podgrupu homomorfno preslikava i faktor grupa $\mathbf{G}/\mathbf{G}'$ – videti dokaz leme 11.5 ili da ponovimo ukratko:

$$\mathbf{H} \cong \mathbf{G}/\mathbf{Ker}(\varphi) \cong (\mathbf{G}/\mathbf{G}')/(\mathbf{Ker}(\varphi)/\mathbf{G}');$$

$\mathbf{Ker}(\varphi) \geq \mathbf{G}'$ jer je $\mathbf{G}/\mathbf{Ker}(\varphi)$ Abelova grupa.□

**Korolar 11.39** *(Teorema Krull-Schmidta). Ako grupa ima glavni niz, tada su svake dve dekompozicije sa nerazloživim faktorima centralno izomorfne.*

**Napomena.** A. G. Kuroš je, treba reći, dokaz svoje teoreme postavio na mnogo širu platformu ([92]). On je prvo dokazao adekvatno tvrđenje za kompletno modularne mreže pa se teorema za grupe javlja kao (gotovo direktna) posledica tog analogona. Naravno, može se postaviti pitanje zašto i mi nismo sledili taj put, tim pre što je pojam mreže već uveden (videti 5.26, 5.27). Pa, osnovni razlog je da, svejedno, ne bismo bili pošteđeni izvođenja brojnih lema, a cilj nam je prvenstveno da se upoznamo sa grupama. Ovako bi se moglo desiti da čitalac prolazaći kroz brojne "mrežne" dokaze zaboravi na tu "poentu".

## 12 Poludirektni proizvodi

Poludirektni proizvod je prirodno uopštenju direktnog proizvoda. Imamo, naime

**Definicija 12.1** *Grupa* $\mathbf{G}$ *je poludirektni proizvod svojih podgrupa* $\mathbf{H}$ *i* $\mathbf{K}$, *u oznaci* $\mathbf{H} \rtimes \mathbf{K}$, *akko su ispunjeni sledeći uslovi:*

(1) $\mathbf{H} \lhd \mathbf{G}$;

(2) $HK = G$;

*i*

(3) $\mathbf{H} \cap \mathbf{K} = \mathbf{E}$.

Izgubili smo, dakle, uslov da i $\mathbf{K}$ mora biti normalna podgrupa.

Treba imati u vidu da je u $\mathbf{H} \rtimes \mathbf{K}$ podgrupa $\mathbf{H}$ normalni faktor, što, naravno, ne isključuje mogućnost da je i $\mathbf{K}$ normalna podgrupa. Koristi se i $\mathbf{K} \ltimes \mathbf{H}$ (jasno, opet sa $\mathbf{H}$ kao normalnim faktorom).

**Primer 12.2** (*a*) $\mathbf{S}_n = \mathbf{A}_n \rtimes \langle (0,1) \rangle$;

(*b*) $\mathbf{D}_n = \langle \rho \rangle \rtimes \langle \sigma \rangle$, *gde je* $\rho = \rho_{\frac{2\pi}{n}}$ *rotacija za ugao* $\frac{2\pi}{n}$ *i* $\sigma = \sigma_y$ *simetrija s obzirom na y-osu;*

(*c*) $\mathbf{GL}_n(\mathbf{Re}) = \langle \{B \mid det(B) > 0\}, \cdot \rangle \rtimes \langle \{E, A\}, \cdot \rangle$, *gde je*

$$A = \begin{bmatrix} -1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}.$$

Sve su ovo primeri opšteg stava

**Lema 12.3** *Ako grupa* $\mathbf{G}$ *ima podgrupu* $\mathbf{N}$ *indeksa* 2 *i element* $g$ *reda* 2 *koji nije u* $N$, *tada je* $\mathbf{G} = \mathbf{N} \rtimes \langle g \rangle$.

**Lema 12.4** *Neka je* $\varphi$ *idempotentan endomorfizam grupe* $\mathbf{G}$ ($\varphi^2 = \varphi$), *tzv. retrakcija grupe* $\mathbf{G}$. *Tada je* $\mathbf{G} = \mathbf{Ker}(\varphi) \rtimes (\mathbf{G})\varphi$.

**Dokaz**. Pretpostavimo da je $a$ u $Ker(\varphi) \cap (G)\varphi$. No ako je $a = (b)\varphi$, onda je $e = (a)\varphi = (b)\varphi^2 = (b)\varphi = a$, pa je $\mathbf{Ker}(\varphi) \cap (\mathbf{G})\varphi = \mathbf{E}$. Kako je, za svako $g \in G$, $g \cdot (g^{-1})\varphi \in Ker(\varphi)$ ($(g \cdot (g^{-1})\varphi)\varphi = (g)\varphi \cdot (g^{-1})\varphi = e$), imamo i $\mathbf{G} = \mathbf{Ker}(\varphi)(\mathbf{G})\varphi$.

Primetimo još da je $\mathbf{Ker}(\varphi) = \langle \{g \cdot (g^{-1})\varphi \mid g \in G\} \rangle$ i da se podgrupa $(\mathbf{G})\varphi$ zove *retrakt grupe* $\mathbf{G}$.□

**Korolar 12.5** *Postoji (svega) pet grupa reda* 8.

**Dokaz**. Sa pet neizomorfnih grupa reda 8 smo se već upoznali, i to sa tri Abelove: $\mathbf{C}_8$, $\mathbf{C}_4 \times \mathbf{C}_2$ i $\mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_2 \cong \mathbf{K} \times \mathbf{C}_2$ ($\mathbf{K}$ – Kleinova grupa), i sa dve neabelove: grupom kvaterniona $\mathbf{Q}$ i dijedarskom grupom stepena 4 – $\mathbf{D}_4$. Preostaje nam, znači, da pokažemo da drugih nema.

Neka je $\mathbf{G}$ Abelova grupa reda 8. Ako ima element reda 8, onda je ciklična. Ako su svi elementi reda 2, tada je $\mathbf{G}$ direktni proizvod cikličnih grupa reda 2 (10.33). Pretpostavimo, konačno, da $\mathbf{G}$ nije ciklična i da ima element $a$ reda 4. Neka je $\mathbf{A} = \langle a \rangle$ i $G = A \cup bA$. Ako je $b$ element reda 2, dobijamo: $\mathbf{G} = \mathbf{A} \times \langle b \rangle$. Ako je $b$ element reda 4, s obzirom da je $b^2 \in A$ ($b^2 \in bA$ bi impliciralo $b \in A$), mora biti $b^2 = a^2$. No tada je $c = ab$ element reda 2, $c \notin A$, i opet je $\mathbf{G} = \mathbf{A} \times \langle c \rangle$.



Neka je sada $\mathbf{G}$ neabelova grupa reda 8, $a$ jedan njen element reda 4 (takav mora postojati, u suprotnom bi $\mathbf{G}$ bila Abelova grupa), $\mathbf{A}$ ciklična podgrupa generisana sa $a$ i neka je $G = A \cup bA$. $\mathbf{A}$ je, kao podgrupa indeksa 2, normalna. Ako je $b$ element reda 2, $\langle b \rangle$ ne može biti normalna podgrupa (jer je $\mathbf{G}$ nekomutativna grupa) i $\mathbf{G}$ je poludirektni proizvod podgrupa $\mathbf{A}$ i $\langle b \rangle$. Kako je $b^{-1}ab$ element iz $A$ reda 4, a isključeno je $b^{-1}ab = a$, sledi $b^{-1}ab = a^3$, tj. $ab = ba^3$, i $\mathbf{G}$ je dijedarska grupa stepena 4. Ako je pak $b$ element reda 4, ponovo je $b^2 \in A$ i $b^2 = a^2$. Ostaje i $ab = ba^3$, te je $\mathbf{G}$ grupa kvaterniona.□

**Teorema 12.6** *(Gaschütz). Neka je* $\mathbf{A}$ *Abelova normalna podgrupa eksponenta* $k$ *grupe* $\mathbf{G}$. *Ako je* $\mathbf{B}$ *podgrupa grupe* $\mathbf{G}$ *konačnog indeksa* $m$ *i ako je* $\mathbf{B} = \mathbf{A} \rtimes \mathbf{C}$ *(za neku podgrupu* $\mathbf{C}$*)* *i* $(k, m) = 1$, *onda je i* $\mathbf{G}$ *poludirektni proizvod sa normalnim faktorom* $\mathbf{A}$.

**Dokaz**. Ako je $S$ desna transverzala podgrupe $\mathbf{B}$ u $\mathbf{G}$ (po uslovu teoreme je $|S| = m$) i $C$ desna transverzala podgrupe $\mathbf{A}$ u $\mathbf{B}$, onda je $CS = T$ desna transverzala podgrupe $\mathbf{A}$ u $\mathbf{G}$ (3.14). Jasno, $CT = C(CS) = (CC)S = CS = T$ i $G = AT = TA$ ($T$ je, s obzirom na normalnost podgrupe $\mathbf{A}$, i leva transverzala). Neka je, za $g \in G$, $g = (g)\tau \cdot (g)\alpha$, gde je $(g)\tau \in T$, $(g)\alpha \in A$ (podsećamo: $\tau$ je reprezentativno preslikavanje domena $G$ na $T$, $\alpha$ projekcija domena $G$ na $A$ – 3.16). Za $c \in C$, $s \in S$ i $t \in T$ važi: $(cst)\alpha = (st)\alpha$; jer, $cst = (cst)\tau \cdot (cst)\alpha = c \cdot (st)\tau \cdot (st)\alpha$ i $c \cdot (st)\tau \in CT = T$. Pošto su, za svako $s_1, s_2 \in S$ i svako $g \in G$, elementi $s_1 g$ i $s_2 g$ u istom desnom kosetu podgrupe $\mathbf{B}$ akko je $s_1 = s_2$, važi takođe za svako $x, y \in T$:

$$\prod_{s \in S}(sx)\alpha = \prod_{s \in S}((sy)\tau \cdot x)\alpha \qquad (1).$$

Koristili smo: $\mathbf{A}$ je Abelova grupa i ako je $(s_1 y)\tau = (s_2 y)\tau = cs' \in T$, tada je i $s_1 = s_2$. Naime, onda je, za neke elemente $a_1, a_2 \in A$, $s_1 y = a_1 cs'$, $s_2 y = a_2 cs'$ ($s_i y = (s_i y)\tau \cdot (s_i y)\alpha \in (s_i y)\tau A = A(s_i y)\tau$, $i = 1, 2$), te je $Bs_1 y = Bs_2 y = Bs'$. Prema tome, ako je $(sy)\tau = c \cdot s' \in CS = T$, važi: kada $s$ "prođe" skupom $S$, to učini i $s'$. Preostaje još da se iskoristi jednakost $(cs'x)\alpha = (s'x)\alpha$.

Za svako $a \in A$ i svako $g \in G$ je $(ga)\alpha = (g)\alpha \cdot a$ (zbog $(g)\tau \cdot (g)\alpha \cdot a = ga = (ga)\tau \cdot (ga)\alpha$ i $Ag = gA = (ga)A = A(ga)$). Stoga, za sve elemente $x, y, z \in T$, iz $(xy)z = (xy)\tau \cdot (xy)\alpha \cdot z = (xy)\tau \cdot z \cdot ((xy)\alpha)u_z$ sledi:

$$((xy)z)\alpha = ((xy)\tau \cdot z \cdot ((xy)\alpha)u_z)\alpha = ((xy)\tau \cdot z)\alpha \cdot ((xy)\alpha)u_z.$$

Slično, $x(yz) = x \cdot (yz)\tau \cdot (yz)\alpha$ i $(x(yz))\alpha = (x \cdot (yz)\tau)\alpha \cdot (yz)\alpha$. Iz dobijenih relacija proizilazi:

$$(x \cdot (yz)\tau)\alpha = ((xy)\tau \cdot z)\alpha \cdot ((xy)\alpha)u_z \cdot ((yz)\alpha)^{-1} \qquad (2).$$

Neka su, dalje, $u$ i $v$ celi brojevi takvi da je $uk + vm = -1$ (dakle, $vm \equiv -1\ (mod\ k)$) i neka je $T^* = \{t \cdot \prod_{s\in S}((st)\alpha)^v \mid t \in T\}$ nova desna, kao i leva, transverzala podgrupe $\mathbf{A}$ u $\mathbf{G}$. Pokazaćemo da je $T^*$ domen polugrupe, a onda i podgrupe, $\mathbf{T^*}$ (3.15($b$)), te će biti: $\mathbf{G} = \mathbf{A} \rtimes \mathbf{T^*}$. Za $t_1, t_2 \in T$ imamo:

$$(t_1 \cdot \prod_{s\in S}((st_1)\alpha)^v) \cdot (t_2 \cdot \prod_{s\in S}((st_2)\alpha)^v) =$$

$$t_1t_2 \cdot (\prod_{s\in S}((st_1)\alpha)^v)u_{t_2} \cdot \prod_{s\in S}((st_2)\alpha)^v =$$

$$(t_1t_2)\tau \cdot (t_1t_2)\alpha \cdot (\prod_{s\in S}((st_1)\alpha)^v)u_{t_2} \cdot \prod_{s\in S}((st_2)\alpha)^v.$$

Prema (2) je pak:

$$(t_1t_2)\tau \cdot \prod_{s\in S}((s \cdot (t_1t_2)\tau)\alpha)^v =$$

$$(t_1t_2)\tau \cdot \prod_{s\in S}(((st_1)\tau \cdot t_2)\alpha)^v \cdot \prod_{s\in S}(((st_1)\alpha)u_{t_2})^v \cdot \prod_{s\in S}(((t_1t_2)\alpha)^{-1})^v.$$

No, $\prod_{s\in S}(((t_1t_2)\alpha)^{-1})^v = (((t_1t_2)\alpha)^{-1})^{vm} = (((t_1t_2)\alpha)^{uk+1} = (t_1t_2)\alpha$ ($\mathbf{A}$ je eksponenta $k$), prema (1) je $\prod_{s\in S}((st_2)\alpha)^v = \prod_{s\in S}(((st_1)\tau \cdot t_2)\alpha)^v$ i, jasno, $\prod_{s\in S}(((st_1)\alpha)u_{t_2})^v = (\prod_{s\in S}((st_1)\alpha))^v)u_{t_2}$. Desne strane poslednjih jednačina su, dakle, jednake pa je:

$$(t_1 \cdot \prod_{s\in S}((st_1)\alpha)^v) \cdot (t_2 \cdot \prod_{s\in S}((st_2)\alpha)^v) = (t_1t_2)\tau \cdot \prod_{s\in S}((s \cdot (t_1t_2)\tau)\alpha)^v \in T^*.\blacksquare$$

**Teorema 12.7** *(Teorema Schura). Neka je* $\mathbf{A}$ *Abelova normalna podgrupa grupe* $\mathbf{G}$ *takva da je* $a^m = e$ *za svako* $a \in A$. *Ako je grupa* $\mathbf{G/A}$ *reda* $n$ *i ako su* $m$ *i* $n$ *uzajamno prosti brojevi, onda je* $\mathbf{G}$ *poludirektni proizvod sa normalnim faktorom* $\mathbf{A}$.

**Dokaz**. Neposredna posledica prethodne teoreme. Dajemo i direktni dokaz prema [92].

Označimo elemente faktor grupe $\mathbf{G/A}$ malim grčkim slovima $\alpha, \beta, \ldots$ i neka je $\{g_\alpha \mid \alpha \in G/A\}$ (jedna) transverzala podgrupe $\mathbf{A}$ (podrazumevamo, naravno, da je $g_\alpha \in \alpha$; dakle, $\alpha = g_\alpha A$). Prema tome je:

$$g_\alpha \cdot g_\beta = g_{\alpha\beta}a_{\alpha,\beta}$$

za neki (jedinstveno određen) element $a_{\alpha,\beta} \in A$ (jer je $\alpha \cdot \beta = g_\alpha A \cdot g_\beta A = g_\alpha g_\beta A = g_{\alpha\beta}A$). Imajući u vidu asocijativnost (u grupi $\mathbf{G}$) izvodimo:

$$g_\alpha(g_\beta g_\gamma) = g_\alpha(g_{\beta\gamma}a_{\beta,\gamma}) = g_{\alpha\beta\gamma}a_{\alpha,\beta\gamma}a_{\beta,\gamma}$$

i

$$(g_\alpha g_\beta)g_\gamma = (g_{\alpha\beta}a_{\alpha,\beta})g_\gamma = g_{\alpha\beta}g_\gamma(a_{\alpha,\beta})u_{g_\gamma} = g_{\alpha\beta\gamma}a_{\alpha\beta,\gamma}(a_{\alpha,\beta})u_{g_\gamma},$$

pa je odatle

$$a_{\alpha,\beta\gamma}a_{\beta,\gamma} = a_{\alpha\beta,\gamma}(a_{\alpha,\beta})u_{g_\gamma}.$$



Fiksirajući $\beta$ i $\gamma$ i uzimajući proizvod po $\alpha$ ($\mathbf{G/A}$ je reda $n$) dobijamo

$$\prod_{\alpha\in G/A}(a_{\alpha,\beta\gamma} \cdot a_{\beta,\gamma}) = \prod_{\alpha\in G/A}(a_{\alpha\beta,\gamma}(a_{\alpha,\beta})u_{g_\gamma}),$$

tj. (zbog komutativnosti podgrupe $\mathbf{A}$)

$$\prod_{\alpha\in G/A} a_{\alpha,\beta\gamma} \cdot (a_{\beta,\gamma})^n = \prod_{\alpha\in G/A} a_{\alpha\beta,\gamma} \cdot (\prod_{\alpha\in G/A} a_{\alpha,\beta})u_{g_\gamma}.$$

U cilju pojednostavljenja notacije označićemo $\prod_{\alpha\in G/A} a_{\alpha,\beta}$ kraće sa $c_\beta$, pa prethodna jednakost dobija oblik:

$$c_{\beta\gamma} \cdot (a_{\beta,\gamma})^n = c_\gamma \cdot (c_\beta)u_{g_\gamma}$$

(koristili smo , jasno, činjenicu da kada $\alpha$ "prođe" skupom $G/A$, onda i $\alpha\beta$ "prođe" tim skupom).

Kako su $m$ i $n$ uzajamno prosti, postoje celi brojevi $k$ i $l$ takvi da je $nk + ml = 1$, te iz

$$(c_{\beta\gamma} \cdot (a_{\beta,\gamma})^n)^{-k} = (c_\gamma \cdot (c_\beta)u_{g_\gamma})^{-k}$$

sledi

$$c_{\beta\gamma}^{-k} \cdot a_{\beta,\gamma}^{-1} = c_\gamma^{-k}((c_\beta)u_{g_\gamma})^{-k} = c_\gamma^{-k} \cdot (c_\beta^{-k})u_{g_\gamma}.$$

Stavljamo konačno $c_\delta^{-k} = d_\delta$ (opet radi lakšeg zapisa); dakle

$$d_{\beta\gamma} \cdot a_{\beta,\gamma}^{-1} = d_\gamma \cdot (d_\beta)u_{g_\gamma},$$

tj.

$$d_{\beta\gamma} = a_{\beta,\gamma} \cdot d_\gamma \cdot (d_\beta)u_{g_\gamma}.$$

Neka je sada $B = \{g_\alpha d_\alpha \mid \alpha \in G/A\}$. To je domen grupoida jer je:

$$g_\alpha d_\alpha \cdot g_\beta d_\beta = g_\alpha g_\beta g_\beta^{-1} d_\alpha g_\beta d_\beta = g_{\alpha\beta}a_{\alpha,\beta}(d_\alpha)u_{g_\beta}d_\beta = g_{\alpha\beta}d_{\alpha\beta};$$

no u pitanju je, zapravo, grupa, s obzirom da je prema pokazanom preslikavanje $\varphi : G/A \longrightarrow B$ dato sa $(\alpha)\varphi = g_\alpha d_\alpha$ homomorfizam i to, očigledno, bijektivni. Evidentno je, takođe, da je $\mathbf{A} \cap \mathbf{B} = \mathbf{E}$ (jer $(m, n) = 1$), kao i da je $G = AB$ ($g \in \alpha$ implicira: za neko $a \in A$ je $g = g_\alpha a = g_\alpha d_\alpha(d_\alpha^{-1}a) \in BA = AB$).$\blacksquare$

**Lema 12.8** *Neka je* $\mathbf{A}$ *Abelova grupa,* $\overline{\mathbf{H}}$ *podgrupa konačnog reda* $n$ *grupe* $\mathbf{Aut(A)}$ *i neka svaki element iz* $\mathbf{A}$ *ima jedinstveni* $n$*-ti koren* $(\forall a\, \exists_1 b\ a = b^n)$. *Tada važi: ako je* $\mathbf{B}$ *direktni faktor grupe* $\mathbf{A}$ *takav da je* $(\mathbf{B})\varphi \leq \mathbf{B}$ *za svako* $\varphi \in \overline{H}$, *onda* $\mathbf{B}$ *ima komplement sa istim svojstvom.*

**Dokaz**. Neka je $\mathbf{A} = \mathbf{B} \times \mathbf{C}$, $\pi_B$ projekcija grupe grupe $\mathbf{A}$ na $\mathbf{B}$ ($(bc)\pi_B = b$) i $\psi : A \longrightarrow A$ preslikavanje koje svakom elementu dodeljuje njegov $n$-ti koren ($\psi$ je, s obzirom na uslov o jednoznačnosti $n$-tih korena, endomorfizam grupe $\mathbf{A}$). Onda je preslikavanje $\theta : A \longrightarrow A$ dato sa $(a)\theta = \prod_{\varphi\in\overline{H}}(a)(\varphi^{-1} \circ \pi_B \circ \varphi \circ \psi)$ endomorfizam grupe $\mathbf{A}$ koji je preslikava na $\mathbf{B}$ i $\theta|_B = \imath_B$; ako je, za $b_1 \in B$ i $c_1 \in C$, $b_1c_1$ $n$-ti koren elementa $b \in B$, tada iz $b = b_1^n c_1^n$, tj. $b_1^{-n}b = c_1^n \in B \cap C = \{e\}$, sledi: $c_1^n = e$, odnosno $c_1 = e$, pa je $(b)\theta = \prod_{\varphi\in\overline{H}}(b)(\varphi^{-1} \circ \pi_B \circ \varphi \circ \psi) = \prod_{\varphi\in\overline{H}}(b)\psi = b_1^n = b$. Naravno, $\mathbf{B} \cap \mathbf{Ker}(\theta) = \mathbf{E}$, a imamo i $A = Ker(\theta) \cdot B$ (dakle, $\mathbf{A} = \mathbf{B} \times \mathbf{Ker}(\theta)$). Jer, za svako $a \in A$ je $(a)\theta^2 = (a)\theta$, te je $(a \cdot (a^{-1})\theta)\theta = (a)\theta \cdot ((a)\theta^2)^{-1} = (a)\theta \cdot ((a)\theta)^{-1} = e$ i $a \cdot (a^{-1})\theta \in Ker(\theta)$; znači, $a \in Ker(\theta)\,(a)\theta \subseteq Ker(\theta) \cdot B$. Konačno je, za $\phi \in \overline{H}$ i $d \in Ker(\theta)$: $((d)\phi)\theta = (\prod_{\varphi\in\overline{H}}((d)\phi)(\varphi^{-1} \circ \pi_B \circ \varphi))\psi = (\prod_{\phi\varphi^{-1}\in\overline{H}}(d)(\phi\varphi^{-1} \circ \pi_B \circ \varphi\phi^{-1}))(\phi \circ \psi) = ((d)\theta)(\phi \circ \psi) = (e)(\phi \circ \psi) = e$ i prema tome $(\mathbf{Ker}(\theta))\phi \leq \mathbf{Ker}(\theta)$.□

**Korolar 12.9** *Neka je* $\mathbf{A}$ *Abelova normalna podgrupa grupe* $\mathbf{G}$ *eksponenta* $m$ *i indeksa* $k$*, koji su uzajamno prosti brojevi, i neka je* $\mathbf{B}$ *direktni faktor grupe* $\mathbf{A}$ *koji je i normalna podgrupe grupe* $\mathbf{G}$*. Tada je* $\mathbf{G} = \mathbf{B} \rtimes \mathbf{D}$ *za neku podgrupu* $\mathbf{D}$ *koja je poludirektni proizvod sa normalnim faktorom* $\mathbf{D} \cap \mathbf{A}$.

**Dokaz**. Prema teoremi Schura je $\mathbf{G} = \mathbf{A} \rtimes \mathbf{H}$ (za neku podgrupu $\mathbf{H}$). Pokazaćemo, što je evidentno i dovoljno, da $\mathbf{B}$ ima komplement u $\mathbf{A}$ koji je normalan u $\mathbf{G}$. Neka je, za $h \in H$, $\varphi_h = u_h|_A$ ($\in Aut(\mathbf{A})$ – jer je $\mathbf{A} \lhd \mathbf{G}$) i neka je $\overline{\mathbf{H}} = \langle\{\varphi_h \mid h \in H\}, \circ\rangle$ ($\leq \mathbf{Aut}(\mathbf{A})$). $\overline{\mathbf{H}}$ je reda $l = [\mathbf{H} : \mathbf{C}(\mathbf{A}) \cap \mathbf{H}]$ (za $h_1, h_2 \in H$ je: $\varphi_{h_1} = \varphi_{h_2}$ akko $h_2^{-1}h_1 \in C(\mathbf{A}) \cap H$); dakle, $l$ je delilac broja $k$ ($= [\mathbf{G} : \mathbf{A}] = |H|$). Kako su $k$ i $m$ uzajamno prosti brojevi, to je i $(l, m) = 1$ i svaki element iz $\mathbf{A}$ ima jedinstveni $l$-ti koren (ako je, za cele brojeve $u$ i $v$, $ul + vm = 1$, onda je, za $a \in A$, $a = a^{ul+vm} = (a^u)^l$; analogno se pokazuje i da su koreni jedinstveni: $a_1^l = a_2^l$ implicira $a_1^{ul} = a_2^{ul}$, tj. $a_1^{1-vm} = a_2^{1-vm}$, tj. $a_1 = a_2$). S obzirom da je i $\mathbf{B}$ normalna podgrupa važi $(\mathbf{B})\varphi_h \leq \mathbf{B}$ za svako $\varphi_h \in \overline{H}$, te prema prethodnoj lemi $\mathbf{B}$ ima komplement u $\mathbf{A} - \mathbf{C}$, koji je takođe invarijantan za automorfizme iz $\overline{\mathbf{H}}$, samim tim i normalna podgrupa grupe $\mathbf{G}$. Tako dobijamo: $\mathbf{G} = \mathbf{A} \rtimes \mathbf{H} = (\mathbf{B} \times \mathbf{C}) \rtimes \mathbf{H} = \mathbf{B} \rtimes (\mathbf{C}\,\mathbf{H})$ (normalnost podgrupe $\mathbf{C}$ garantuje da je $CH$ domen tražene podgrupe – $\mathbf{D} = \mathbf{C} \rtimes \mathbf{H}$ i, jasno, $\mathbf{D} \cap \mathbf{A} = \mathbf{C}$).□

**Teorema 12.10** *Svaka grupa* $\mathbf{G}$ *je normalni faktor poludirektnog proizvoda sa svojstvom da su svi automorfizmi grupe* $\mathbf{G}$ *inducirani unutrašnjim automorfizmima tog proizvoda.*

**Dokaz**. Neka je $\Phi$ utapanje grupe $\mathbf{G}$ u $\mathbf{S}_G$ dato sa $(a)\Phi = d_a$, gde je $(g)d_a \stackrel{\text{def}}{=} ga$ (videti 9.30), i neka je $\overline{\mathbf{G}}$ njena izomorfna slika. Normalizator grupe $\overline{\mathbf{G}}$ u $\mathbf{S}_G$, $\mathbf{N}(\overline{\mathbf{G}})$, zove se *holomorf* grupe $\mathbf{G}$. Pokazaćemo (a time i dati dokaz



teoreme – $\mathbf{G}$ identifikujemo sa $\overline{\mathbf{G}}$) da je $\mathbf{N}(\overline{\mathbf{G}}) = \overline{\mathbf{G}} \rtimes \mathbf{Aut}(\mathbf{G})$ kao i da su svi automorfizmi grupe $\overline{\mathbf{G}}$ inducirani unutrašnjim automorfizmima grupe $\mathbf{N}(\overline{\mathbf{G}})$.

$Aut(\mathbf{G}) \subseteq N(\overline{\mathbf{G}})$, jer ako je $\psi \in Aut(\mathbf{G})$ i $d_a \in \overline{G}$, tada je, za $g \in G$,

$$(g)(\psi^{-1}\, d_a\, \psi) = ((g)\psi^{-1} \cdot a)\psi = g \cdot (a)\psi = (g)d_{(a)\psi},$$

tj. $\psi^{-1}\, d_a\, \psi = d_{(a)\psi}$. Jasno, $\overline{\mathbf{G}} \cap \mathbf{Aut}(\mathbf{G}) = \mathbf{E}$ (ako je, za $b, c \in G$, $(bc)d_a = (b)d_a\,(c)d_a$, odnosno $bca = baca$, onda je $a = e$ i $d_e = \imath_G$ – identično preslikavanje skupa $G$). Dalje je $Aut(\overline{\mathbf{G}}) = \{\Phi^{-1}\,\psi\Phi \mid \psi \in Aut(\mathbf{G})\}$ (videti 2.10($e$)). Kako je za $\psi \in Aut(\mathbf{G})$:

$$(d_a)(\Phi^{-1}\,\psi\,\Phi) = ((a)\psi)\Phi = d_{(a)\psi} = \psi^{-1}\, d_a\psi = (d_a)\, u_\psi,$$

gde je $u_\psi$ unutrašnji automorfizam grupe $\mathbf{S}_G$ koji odgovara elementu $\psi$, to je $\Phi^{-1}\,\psi\,\Phi = u_\psi|_{\overline{G}}$. Ali $\psi \in N(\overline{\mathbf{G}})$, pa je $u_\psi|_{N(\overline{\mathbf{G}})}$ unutrašnji automorfizam grupe $\mathbf{N}(\overline{\mathbf{G}})$ i $\Phi^{-1}\,\psi\,\Phi = (u_\psi|_{N(\overline{\mathbf{G}})})|_{\overline{G}}$.

Preostaje još da se pokaže da je $\mathbf{N}(\overline{\mathbf{G}}) = \overline{\mathbf{G}}\,\mathbf{Aut}(\mathbf{G})$. Dokazujemo prvo: $\overline{\mathbf{G}}\,\mathbf{Inn}(\mathbf{G}) = \overline{\mathbf{G}}\,\mathbf{C}(\overline{\mathbf{G}})$ ($\mathbf{C}(\overline{\mathbf{G}})$ je centralizator grupe $\overline{\mathbf{G}}$, prema tome i normalna podgrupa grupe $\mathbf{N}(\overline{\mathbf{G}})$).

Ako je $\varphi \in C(\overline{\mathbf{G}})$, onda je $\varphi\, d_a = d_a\, \varphi$ za svako $a \in G$. Odatle, posebno, $(e)(d_a\,\varphi) = (e)(\varphi\, d_a)$, i ako je $(e)\varphi = g$, tada je $(a)\varphi = ga$. S druge strane je i za svako $b \in G$ preslikavanje $l_b : G \longrightarrow G$ određeno sa $(a)l_b \stackrel{\text{def}}{=} ba$ (množenje sleva elemenata grupe $\mathbf{G}$ elementom $b$) u centralizatoru podgrupe $\overline{\mathbf{G}}$:

$$(c)(l_b\, d_a) = (bc)d_a = bca = b((c)d_a) = ((c)d_a)l_b = (c)(d_a\, l_b).$$

Proizilazi, uzgred rečeno, da je $\mathbf{C}(\overline{\mathbf{G}}) \cong \mathbf{G}$, jer je, prema navedenom, preslikavanje $\theta : G \longrightarrow C(\overline{G})$ dato sa $(g)\theta \stackrel{\text{def}}{=} l_{g^{-1}}$ surjektivno a trivijalno je injektivno i homomorfno.

Zbog $(a)u_g = g^{-1}ag = (ag)l_{g^{-1}} = (a)(d_g\, l_{g^{-1}})$, tj. $u_g = d_g\, l_{g^{-1}}$, važi

$$\mathbf{Inn}(\mathbf{G}) \leq \overline{\mathbf{G}} \cdot \mathbf{C}(\overline{\mathbf{G}}),$$

a ista relacija daje i

$$\mathbf{C}(\overline{\mathbf{G}}) \leq \overline{\mathbf{G}} \cdot \mathbf{Inn}(\mathbf{G}).$$

Stoga je

$$\overline{\mathbf{G}} \cdot \mathbf{C}(\overline{\mathbf{G}}) = \overline{\mathbf{G}} \cdot \mathbf{Inn}(\overline{\mathbf{G}}).$$

Neka je sada $\phi \in N(\overline{\mathbf{G}})$. $u_\phi|_{\overline{G}}$ je automorfizam grupe $\overline{\mathbf{G}}$ ($\lhd \mathbf{N}(\overline{\mathbf{G}})$), te je (već smo pokazali) $u_\phi|_{\overline{G}} = u_\psi|_{\overline{G}}$ za neko $\psi \in Aut(\mathbf{G})$. Znači, $\phi^{-1}\, d_a\, \phi = \psi^{-1}\, d_a\, \psi$ za svako $d_a \in \overline{G}$, odnosno $\phi\,\psi^{-1} \in C(\overline{\mathbf{G}}) \subseteq \overline{G}\, Inn(\mathbf{G})$. Proizilazi: $\phi \in \overline{G}\, Inn(\mathbf{G})\, Aut(\mathbf{G}) = \overline{G}\, Aut(\mathbf{G})$, pa je dokazana i relacija

$$\mathbf{N}(\overline{\mathbf{G}}) \leq \overline{\mathbf{G}}\,\mathbf{Aut}(\mathbf{G}).$$

U vezi sa ovom teoremom videti i 28.4.■

Naredna lema pokazuje da smo do holomorfa mogli doći i drugim putem. No prvo

**Definicija 12.11** *Bijektivno preslikavanje $\varphi$ domena grupe $\mathbf{G}$ na sebe je holomorfizam grupe $\mathbf{G}$ akko važi:* $\forall a,b,c\ (ab^{-1}c)\varphi = (a)\varphi((b)\varphi)^{-1}(c)\varphi$.

**Lema 12.12** *Skup holomorfizama $H$ grupe $\mathbf{G}$ je domen holomorfa grupe $\mathbf{G}$.*

**Dokaz.** Pokazaćemo prvo da je $\mathbf{H} = \langle H, \mathrm{o}\rangle$ podgrupa grupe $\mathbf{S}_G$. Jasno, $\imath \in H$, a ako $\varphi \in H$, onda i $\varphi^{-1} \in H$. Jer, ako je $(a_1)\varphi = a$, $(b_1)\varphi = b$ i $(c_1)\varphi = c$, tada je $(ab^{-1}c)\varphi^{-1} = ((a_1)\varphi((b_1)\varphi)^{-1}(a_1)\varphi)\varphi^{-1} = ((a_1b_1^{-1}c_1)\varphi)\varphi^{-1} = a_1b_1^{-1}c_1 = (a)\varphi^{-1}((b)\varphi^{-1})^{-1}(c)\varphi^{-1}$. Još lakše se proverava da je kompozicija dva holomorfizma holomorfizam.

Očigledno, $Aut(\mathbf{G}) \subseteq H$. Takođe i $\overline{G} = \{d_g \mid g \in G\} \subseteq H$ (koristimo notaciju iz prethodne teoreme):

$$(ab^{-1}c)d_g = ab^{-1}cg = agg^{-1}b^{-1}cg = (a)d_g((b)d_g)^{-1}(c)d_g.$$

Prema tome je $\mathbf{N}(\overline{\mathbf{G}}) = \overline{\mathbf{G}} \cdot \mathbf{Aut}(\mathbf{G}) \leq \mathbf{H}$. S druge strane, ako je $\varphi \in H$, imamo:

$$(a)(\varphi^{-1} \circ d_g \circ \varphi) = ((a)\varphi^{-1} \cdot g)\varphi = a((e)\varphi)^{-1}(g)\varphi = (a)d_{((e)\varphi)^{-1}(g)\varphi}.$$

Znači, $\varphi^{-1}\overline{G}\varphi \subseteq \overline{G}$, tj. $\varphi \in N(\overline{\mathbf{G}})$.□

**Lema 12.13** *(R. Baer). Grupa bez centra je savršena grupa (definicija 9.28) ako i samo ako je direktni faktor svake grupe čija je normalna podgrupa.*

**Dokaz.** ($\Longleftarrow$) Neka je savršena nejedinična grupa $\mathbf{A}$ normalna podgrupa grupe $\mathbf{G}$ i neka je $\mathbf{B}$ centralizator podgrupe $\mathbf{A}$ u $\mathbf{G}$. Pokazaćemo: $\mathbf{G} = \mathbf{A} \times \mathbf{B}$.

Kao prvo $G = BA$ $(= AB)$. Jer, ako je $g \in G$, tada je $u_g|_A \in Aut(\mathbf{A})$ (pošto je $\mathbf{A}$ normalna podgrupa), pa je $u_g|_A = u_a|_A$ za neko $a \in A$ (svi automorfizmi grupe $\mathbf{A}$ su unutrašnji). Prema tome je $g^{-1}hg = a^{-1}ha$ za svako $h \in A$, znači $ga^{-1} \in B$ i $g = (ga^{-1})a \in BA$. Dalje, $\mathbf{A} \cap \mathbf{B} = \mathbf{Z}(\mathbf{A}) = \mathbf{E}$. Konačno, i pogrupa $\mathbf{B}$ je normalna: zbog $g = ba$ (za neko $b \in B$ i neko $a \in A$) imamo: $g^{-1}\mathbf{B}g = (a^{-1}b^{-1})\mathbf{B}ba = a^{-1}\mathbf{B}a = \mathbf{B}$ ($a$ je permutabilno sa svim elementima grupe $\mathbf{B}$).

($\Longrightarrow$) Neka je sada $\mathbf{A}$ grupa bez centra i sa svojstvom da je direktni faktor svake grupe čija je normalna podgrupa i neka je $\psi$ jedan njen automorfizam. Posmatrajmo podgrupu $\overline{\mathbf{A}} \rtimes \langle\psi\rangle$ njenog holomorfa $(\overline{\mathbf{A}} \rtimes \mathbf{Aut}(\mathbf{A}))$. Prema već pokazanom je $\psi^{-1} \circ d_a \circ \psi = d_{(a)\psi}$ za svako $a \in A$. S druge strane, $\overline{\mathbf{A}} \rtimes \langle\psi\rangle$ je direktni proizvod $\overline{\mathbf{A}} \times \mathbf{B}$ (za neku podgrupu $\mathbf{B}$), pa je, za neko $b \in A$ i neko $\beta \in B$, $\psi = d_b \circ \beta$. Odatle, $d_{(a)\psi} = \psi^{-1} \circ d_a \circ \psi = \beta^{-1} \circ (d_{b^{-1}} \circ d_a \circ d_b) \circ \beta = \beta^{-1} \circ d_{b^{-1}ab} \circ \beta = d_{(a)u_b}$, odnosno $(a)\psi = (a)u_b$.□



**Korolar 12.14** *Grupa $\mathbf{G}$ je savršena akko ima karakterističnu podgrupu $\mathbf{K}$ takvu da su ispunjeni sledeći uslovi:*

*(1) Svaki automorfizam grupe $\mathbf{K}$ je restrikcija nekog unutrašnjeg automorfizma grupe $\mathbf{G}$;*

*(2) Centralizator podgrupe $\mathbf{K}$ je jedinična podgrupa.*

**Dokaz.** ($\Longrightarrow$) Trivijalno; uzeti $\mathbf{K} = \mathbf{G}$;

($\Longleftarrow$) Neka je $\mathbf{K}$ karakteristična podgrupa grupe $\mathbf{G}$ za koju su ispunjeni uslovi (1) i (2) i neka je $\mathbf{G}$ normalna podgrupa grupe $\mathbf{H}$. Pokazaćemo, što je prema prethodnoj lemi i dovoljno, da je $\mathbf{G}$ direktni faktor grupe $\mathbf{H}$. S obzirom da je $\mathbf{K}$ normalna podgrupa grupe $\mathbf{H}$, za (ma koji) element $h \in H$ je $u_h|_K$ automorfizam grupe $\mathbf{K}$, te je, prema uslovu (1), za neki element $g \in G$ (koji je u funkciji od $h$): $u_g|_K = u_h|_K$. Stoga je $hg^{-1} \in C(\mathbf{K})$. Prema 4.4($g$), $\mathbf{C}(\mathbf{K})$ je takođe normalna podgrupa, po uslovu (2) je $\mathbf{G} \cap \mathbf{C}(\mathbf{K}) = \mathbf{C}_{\mathbf{G}}(\mathbf{K}) = \mathbf{E}$ i, jasno, $\mathbf{H} = \mathbf{C}(\mathbf{K})\,\mathbf{G}$ $(= \mathbf{G}\,\mathbf{C}(\mathbf{K}))$, pa je $\mathbf{H} = \mathbf{G} \times \mathbf{C}(\mathbf{K})$.□

**Korolar 12.15** *Ako je $\mathbf{G}$ direktni proizvod neabelovih prostih grupa, onda je $\mathbf{Aut}(\mathbf{G})$ savršena grupa.*

**Dokaz.** Pokazaćemo da je $\mathbf{Inn}(\mathbf{G})$ ($\cong \mathbf{G}$, jer je $\mathbf{Z}(\mathbf{G}) = \mathbf{E}$) karakteristična podgrupa grupe $\mathbf{Aut}(\mathbf{G})$ koja ispunjava uslove (1) i (2) prethodnog korolara. Neka je $\overline{\psi} \in Aut(\mathbf{Aut}(\mathbf{G}))$ i $\overline{\mathbf{H}} = \mathbf{Inn}(\mathbf{G}) \cap (\mathbf{Inn}(\mathbf{G}))\overline{\psi}$. Kako je $\mathbf{Inn}(\mathbf{G})$ normalna podgrupa grupe $\mathbf{Aut}(\mathbf{G})$ (4.4($d$)), to je i $(\mathbf{Inn}(\mathbf{G}))\overline{\psi}$ normalna podgrupa, te je $\overline{\mathbf{H}}$ normalna podgrupa grupa $\mathbf{Inn}(\mathbf{G})$ i $(\mathbf{Inn}(\mathbf{G}))\overline{\psi}$. Prema 10.32 je $\mathbf{Inn}(\mathbf{G}) = \overline{\mathbf{H}} \times \mathbf{C}_{\mathbf{Inn}(\mathbf{G})}(\overline{\mathbf{H}}) = \overline{\mathbf{H}} \times (\mathbf{Inn}(\mathbf{G}) \cap \mathbf{C}_{\mathbf{Aut}(\mathbf{G})}(\overline{\mathbf{H}}))$ i $(\mathbf{Inn}(\mathbf{G}))\overline{\psi} = \overline{\mathbf{H}} \times ((\mathbf{Inn}(\mathbf{G}))\overline{\psi} \cap \mathbf{C}_{\mathbf{Aut}(\mathbf{G})}(\overline{\mathbf{H}}))$ (u nastavku ćemo, kako je već običaj, pisati jednostavno $\mathbf{C}(\overline{\mathbf{H}})$ umesto $\mathbf{C}_{\mathbf{Aut}(\mathbf{G})}(\overline{\mathbf{H}})$). Na osnovu 6.10($a$) je pak

$$[\mathbf{Inn}(\mathbf{G}) \cap \mathbf{C}(\overline{\mathbf{H}}), (\mathbf{Inn}(\mathbf{G})\overline{\psi} \cap \mathbf{C}(\overline{\mathbf{H}})] \leq \mathbf{Inn}(\mathbf{G}) \cap (\mathbf{Inn}(\mathbf{G}))\overline{\psi} \cap \mathbf{C}(\overline{\mathbf{H}}) =$$

$$\overline{\mathbf{H}} \cap \mathbf{C}(\overline{\mathbf{H}}) = \overline{\mathbf{E}}.$$

Prema tome, elementi podgrupe $(\mathbf{Inn}(\mathbf{G}))\overline{\psi} \cap \mathbf{C}(\overline{\mathbf{H}})$ su permutabilni sa elementima podgrupa $\mathbf{Inn}(\mathbf{G}) \cap \mathbf{C}(\overline{\mathbf{H}})$ i $\overline{\mathbf{H}}$, a onda i sa elementima podgrupe $\mathbf{Inn}(\mathbf{G})$; dakle, $(\mathbf{Inn}(\mathbf{G}))\overline{\psi} \cap \mathbf{C}(\overline{\mathbf{H}}) \leq \mathbf{C}(\mathbf{Inn}(\mathbf{G})) = \overline{\mathbf{E}}$ (8.23), što nam uzgred daje i uslov (2). Proizilazi: $(\mathbf{Inn}(\mathbf{G}))\overline{\psi} = \overline{\mathbf{H}}$, tj. $(\mathbf{Inn}(\mathbf{G}))\overline{\psi} \leq \mathbf{Inn}(\mathbf{G})$.

Uslov (1) je evidentan. Ako je $\overline{\varphi} \in Aut(\mathbf{Inn}(\mathbf{G}))$, onda je preslikavanje $\varphi : G \longrightarrow G$ dato sa: $(a)\varphi = b$ akko $(u_a)\overline{\varphi} = u_b$ (znači, $(u_a)\overline{\varphi} = u_{(a)\varphi}$) automorfizam grupe $\mathbf{G}$ (ponavljamo: $\mathbf{G} \cong \mathbf{Inn}(\mathbf{G})$) i za $u_\varphi \in Inn(\mathbf{Aut}(\mathbf{G}))$ i $u_a \in Inn(\mathbf{G})$ imamo: $(u_a)u_\varphi = \varphi^{-1} \circ u_a \circ \varphi = u_{(a)\varphi} = (u_a)\overline{\varphi}$, odnosno $\overline{\varphi} = u_\varphi|_{Inn(\mathbf{G})}$.□

**Korolar 12.16** *Grupa automorfizma neabelove proste grupe je savršena grupa.*

**Lema 12.17** *Za svaku prebrojivu grupu* **A** *postoji dvoelementno generisana grupa koja sadrži izomorfnu sliku izvodne podgrupe grupe* **A**.

**Dokaz**. Neka je $A = \{a_n \mid n \in N\}$, $\mathbf{B} = \prod_{k\in Z}^{c} \mathbf{A}_k$, gde je $\mathbf{A}_k = \mathbf{A}$ za svako $k \in Z$, i $\overline{\mathbf{B}} \rtimes \mathbf{Aut}(\mathbf{B})\ (\leq \mathbf{S}_B)$ holomorf grupe **B**. Jedan automorfizam grupe **B**, $\tau$, dat je sa: $(f)\tau = f_1$ i $(m)f_1 = (m+1)f$. $\tau$ je očigledno bijektivno preslikavanje skupa $B = \prod_{k\in Z} A_k$, a imamo i

$$(m)((f\cdot g)\tau) = (m)(f\cdot g)_1 = (m+1)(f\cdot g) = (m+1)f\cdot(m+1)g =$$

$$(m)f_1\cdot(m)g_1 = (m)((f)\tau)\cdot(m)((g)\tau) = (m)((f)\tau\cdot(g)\tau).$$

Generalno je $(f)\tau^r = f_r$ i $(m)f_r = (m+r)f$. Neka je, dalje, za $h \in B$, $(m)h = \begin{cases} a_r & m = 2^r,\ r > 0 \\ e & \text{inače} \end{cases}$. Pokazaćemo da podgrupa $\langle d_h, \tau\rangle$ holomorfa grupe **B** sadrži izomorfnu kopiju grupe $\mathbf{A}'$. Grupa **A** je izomorfna podgrupi $\overline{\mathbf{A}}_2$ grupe **B** čiji su elementi $\overline{a}_r^2$: $(m)\overline{a}_r^2 = \begin{cases} a_r & m = 2 \\ e & \text{inače} \end{cases}$. No, za $a_r, a_s \in A$ je $[\overline{a}_r^2, \overline{a}_s^2] = \overline{a}^2_{[a_r,a_s]}$ i, što se takođe lako proverava, $\overline{a}_r^s = (h)\tau^{2^r-2}$ (odnosno, u skladu sa uvedenom notacijom, $(h)\tau^{2^r-2} = h_{2^r-2}$), pa je:

$$[d_{\overline{a}_r^2}, d_{\overline{a}_s^2}] = d_{[\overline{a}_r^2,\overline{a}_s^2]} = [(d_{(h)\tau^{2^r-2}}, d_{(h)\tau^{2^s-2}}] =$$

$$[(\tau^{2^r-2})^{-1}\circ d_h\circ\tau^{2^r-2}, (\tau^{2^s-2})^{-1}\circ d_h\circ\tau^{2^s-2}] \in \langle d_h,\tau\rangle'.$$

U vezi sa ovim tvrđenjem videti i 14.6.□

# 13 Ekstenzije grupa

**Definicija 13.1** *Grupa* **G** *je ekstenzija grupe* **A** *grupom* **B** *akko je* **A** *normalna podgrupa grupe* **G** *a faktor grupa* $\mathbf{G}/\mathbf{A}$ *izomorfna sa* **B**.

Naravno, u razmatranju ekstenzija dozvoljavaćemo mogućnost da **G** ne sadrži baš **A** kao (normalnu) podgrupu već neku njoj izomorfnu grupu.

Za bilo koje dve grupe **A** i **B** postoji ekstenzije od **A** sa $\mathbf{B}$ – $\mathbf{A}\times\mathbf{B}$. S druge strane, ekstenzija nije u opštem jednoznačno određena. Na primer, i ciklična grupa reda 4 i Kleinova grupa su ekstenzije ciklične grupe reda 2 istom takvom grupom; ciklična grupa reda 6 i simetrična grupa $\mathbf{S}_3$ su ekstenzije ciklične grupe reda 3 cikličnom grupom reda 2. Dakle, ekstenzija Abelove grupe Abelovom grupom ne mora biti Abelova. U navedenim primerima ekstenzija **G** je sadržavala i podgrupu izomorfnu grupi $\mathbf{B}(\cong \mathbf{G}/\mathbf{A})$. No to nije pravilo. Grupa kvaterniona **Q** je ekstenzija svog centra $\mathbf{Z}(\mathbf{Q}) = \langle\{I, A^2\},\cdot\rangle$ (prema oznakama iz 5.7($a$)), Kleinovom grupom $\langle\{Z(\mathbf{Q}), A\,Z(\mathbf{Q}), B\,Z(\mathbf{Q}), AB\,Z(\mathbf{Q})\},\cdot\rangle$, dok sama grupa **Q** ne sadrži Kleinovu grupu kao podgrupu.



**Lema 13.2** *Ako je* **G** *poludirektni proizvod podgrupa* **A** *i* **B** $(\mathbf{A} \lhd \mathbf{G})$, *onda je* **G** *ekstenzija grupe* **A** *grupom* **B**.

**Dokaz**. Prema drugoj teoremi o izomorfizmu je:

$$\mathbf{G}/\mathbf{A} = \mathbf{AB}/\mathbf{A} \cong \mathbf{B}/(\mathbf{A}\cap\mathbf{B}) \cong \mathbf{B}.$$

Grupa kvaterniona potvrđuje da obrat ovog tvrđenja ne važi.□

**Lema 13.3** *Neka je grupa* **G** *ekstenzija grupe* **A** *grupom* **B**. *Tada važi:*

($a$) $|G| = |A|\cdot|B|$;

($b$) *Ako su* **A** *i* **B** *lokalno konačne grupe, onda je i* **G** *lokalno konačna; posebno, ako su* **A** *i* **B** *periodične grupe, onda je i* **G** *periodična grupa;*

($c$) *Ako su* **A** *i* **B** *grupe bez centra, onda je i grupa* **G** *bez centra.*

($d$) *Ako grupe* **A** *i* **B** *ispunjavaju uslov rastućih (opadajućih) lanaca (tj. uslov maksimalnosti (minimalnosti) podgrupa), onda i* **G** *ispunjava uslov rastućih (opadajućih) lanaca.*

($e$) *Ako grupe* **A** *i* **B** *ispunjavaju uslov maksimalnosti (minimalnosti) normalnih podgrupa, onda i grupa* **G** *ispunjava uslov maksimalnosti (minimalnosti) normalnih podgrupa.*

**Dokaz**. ($a$) $|G| = |A|\cdot[\mathbf{G}:\mathbf{A}] = |A|\cdot|B|$;

($b$) Uočimo prvo da iz periodičnosti grupa **A** i **B** sledi periodičnost grupe **G**. Jer, za $g \in G$, $gA$ je element konačnog reda grupe $\mathbf{G}/\mathbf{A}$ $(\cong \mathbf{B})$, recimo $m$, pa je $g^m \in A$, a onda je, za neko $n$, $(g^m)^n = g^{mn} = e$. Neka je, dalje, $C = \{g_0,\ldots,g_k\}$ konačan podskup domena grupe **G**. S obzirom da je **B** lokalno konačna grupa, $\mathbf{H}/\mathbf{A} = \langle g_0A,\ldots,g_kA\rangle$ je konačna podgrupa grupe $\mathbf{G}/\mathbf{A}$. Neka je $\{g_0,\ldots,g_k\}\cup\{g_{k+1},\ldots,g_r\} = C\cup D$ skup predstavnika svih koseta podgrupe **A** u **H** (moguće je da neki elementi određuju iste kosete; dozvoljavamo takođe mogućnost da je skup $D$ prazan). Svaki element podgrupe $\langle C\cup D\rangle$ je proizvod elemenata iz $C\cup D$ jer je **G** periodična grupa, a za svaka dva elementa $g_i$, $g_j$ iz $C\cup D$ proizvod $g_ig_j$ je oblika $g_ma_{ij}$, gde je $g_m \in C\cup D$ i $a_{ij} \in A$; u slučaju da je $g_ig_j \in g_mA = g_nA$, opredelićemo se za "manji indeks i time jednoznačno odrediti predstavnika koseta i podgrupe **A**. Proizilazi da je svaki element iz $\langle C\cup D\rangle$ proizvod jednog elementa iz $C\cup D$ i jednog elementa (konačne) podgrupe grupe **A** generisane skupom $\{a_{ij} \mid 1\leq i,j\leq r\}$, pa je i podgrupa $\langle C\rangle$ grupe **G** konačna.

($c$) Pretpostavimo da su grupe **A** i **B** bez centra, ali da je $\mathbf{Z}(\mathbf{G}) \neq \mathbf{E}$. U tom slučaju dobijamo, međutim, $\mathbf{A}\cap\mathbf{Z}(\mathbf{G}) = \mathbf{E}$, te prema drugoj teoremi o izomorfizmu sledi:

$$\mathbf{Z}(\mathbf{G}) \cong \mathbf{A}\,\mathbf{Z}(\mathbf{G})/\mathbf{A} \leq \mathbf{Z}(\mathbf{G}/\mathbf{A}) \cong \mathbf{Z}(\mathbf{B}),$$

kontradikcija.

Obrat ovog tvrđenja ne važi; već smo videli (jedan) kontraprimer – grupa $\mathbf{S}_3$.

Tačke $(d)$ i $(e)$ su već dokazane u 8.15.□

**Korolar 13.4** *Direktan proizvod* $\mathbf{G}_1 \times \cdots \times \mathbf{G}_n$ *ispunjava uslov maksimalnosti (minimalnosti) podgrupa (normalnih podgrupa) akko svaki od njegovih faktora* $\mathbf{G}_i$, $i = 1, \ldots, n$, *ispunjava uslov maksimalnosti (minimalnosti) podgrupa (normalnih podgrupa).*

**Napomena.** Prethodni korolar se ne može uopštiti, tj. ne važi i za direktni proizvod beskonačno mnogo grupa. Npr. u grupi $\prod_{k\geq 2} \mathbf{C}_k$ imamo beskonačan opadajući niz podgrupa:

$$\prod_{k\geq 2} \mathbf{C}_k > \prod_{k\geq 3} \mathbf{C}_k > \cdots > \prod_{k\geq n} \mathbf{C}_k > \cdots,$$

kao i beskonačan rastući niz:

$$\mathbf{C}_2 < \mathbf{C}_2 \times \mathbf{C}_3 < \cdots < \mathbf{C}_2 \times \cdots \times \mathbf{C}_n < \cdots;$$

jasno, ovde je, recimo, $\prod_{k\geq 5}^{d} C_k = \{f \in \prod_{j\geq 2}^{d} C_j \mid (i)f = e_i \in C_i \text{ za } i = 2,3,4\}$; $C_2 \times C_3 = \{f \in \prod_{k\geq 2}^{d} C_k \mid (i)f = e_i \in C_i \text{ za svako } i > 3\}$.

**Definicija 13.5** *Neka su* $\mathbf{G}$ *i* $\mathbf{H}$ *ekstenzije grupe* $\mathbf{A}$ *grupom* $\mathbf{B}$ *i neka su* $\varphi$ *i* $\psi$ *izomorfna preslikavanja, respektivno, faktor grupa* $\mathbf{G}/\mathbf{A}$ *i* $\mathbf{H}/\mathbf{A}$ *na grupu* $\mathbf{B}$. $\mathbf{G}$ *i* $\mathbf{H}$ *su ekvivalentne ekstenzije akko postoji izomorfno preslikavanje* $\theta$ *grupe* $\mathbf{G}$ *na grupu* $\mathbf{H}$ *koje ispunjava sledeće uslove:*

$$\theta|_A = \imath_A \quad i \quad \forall g \in G \ \ (gA)\theta = (gA)(\varphi \circ \psi^{-1})$$

*(jasno,* $(gA)\theta$ *je ovde slika koseta* $gA$*, kao podskupa skupa* $G$*); rečima, restrikcija od* $\theta$ *nad* $A$ *je identično preslikavanje, a u korespondenciji su koseti podgrupe* $\mathbf{A}$ *u* $\mathbf{G}$ *i* $\mathbf{H}$ *koji odgovaraju istom elementu iz* $B$.

U razmatranju koje sledi elemente grupe $\mathbf{A}$ (i $\mathbf{G}$) obeležavaćemo malim latiničnim slovima, a elemente grupe $\mathbf{B}$ grčkim slovima $\alpha, \beta, \gamma, \ldots$.

Neka je $\mathbf{G}$ ekstenzija grupe $\mathbf{A}$ grupom $\mathbf{B}$ i neka je $\varphi$ izomorfno preslikavanje faktor grupe $\mathbf{G}/\mathbf{A}$ na $\mathbf{B}$. Ako je $\{g_\alpha \mid \alpha \in B\}$ transverzala podgrupe $\mathbf{A}$, gde je $(g_\alpha A)\varphi = \alpha$, biće, s obzirom da je $\varphi$ izomorfizam: $g_\alpha A \cdot g_\beta A = g_{\alpha\beta} A$, te je $g_\alpha g_\beta \in g_{\alpha\beta} A$. Neka je $a_{\alpha,\beta}$ (jedinstveno određen) element iz $A$ takav da je $g_\alpha g_\beta = g_{\alpha\beta} a_{\alpha,\beta}$. Podskup $\{a_{\alpha,\beta} \mid \alpha, \beta \in B\}$ domena $A$ zovemo *faktor sistemom transverzale* $\{g_\alpha \mid \alpha \in B\}$. Kako je $\mathbf{A}$ normalna podgrupa, za svaki unutrašnji automorfizam $u_g$ grupe $\mathbf{G}$ je $u_g|_A \in Aut(\mathbf{A})$. U nastavku ćemo $u_{g_\alpha}|_A$ kraće označavati sa $u_\alpha$. Za svako $a \in A$ imamo:

$$(a)(u_\alpha \circ u_\beta) = (g_\alpha g_\beta)^{-1} a (g_\alpha g_\beta) = (g_{\alpha\beta} a_{\alpha,\beta})^{-1} a (g_{\alpha\beta} a_{\alpha,\beta}) = (a)(u_{\alpha\beta} \circ u_{a_{\alpha,\beta}}),$$



pa je

$$u_\alpha \circ u_\beta = u_{\alpha\beta} \circ u_{a_{\alpha,\beta}} \tag{1};$$

primetimo da, za $a \in A$, $u_a$ tretiramo kao (unutrašnji) automorfizam grupe $\mathbf{A}$, a ne kao restrikciju odgovarajućeg unutrašnjeg automorfizma grupe $\mathbf{G}$ nad $A$, premda, sem u notaciji, to ne čini nikakvu razliku.

Zbog asocijativnosti operacija u $\mathbf{G}$ i $\mathbf{B}$ dobijamo:

$$(g_\alpha g_\beta) g_\gamma = (g_{\alpha\beta} a_{\alpha,\beta}) g_\gamma = g_{\alpha\beta} g_\gamma g_\gamma^{-1} a_{\alpha,\beta} g_\gamma = g_{\alpha\beta\gamma} a_{\alpha\beta,\gamma} (a_{\alpha,\beta}) u_\gamma =$$

$$g_\alpha (g_\beta g_\gamma) = g_\alpha g_{\beta\gamma} a_{\beta,\gamma} = g_{\alpha\beta\gamma} a_{\alpha,\beta\gamma} a_{\beta,\gamma},$$

i nakon skraćivanja:

$$a_{\alpha,\beta\gamma} \cdot a_{\beta,\gamma} = a_{\alpha\beta,\gamma} \cdot (a_{\alpha,\beta}) u_\gamma \tag{2}.$$

Konačno je, za proizvoljne elemente $g_\alpha a$, $g_\beta b$, $a, b \in A$, $\alpha, \beta \in B$ (grupe $\mathbf{G}$):

$$g_\alpha a \cdot g_\beta b = g_\alpha g_\beta g_\beta^{-1} a g_\beta b = g_{\alpha\beta} \cdot a_{\alpha,\beta} \cdot (a) u_\beta \cdot b \tag{3}.$$

Pokazaćemo sada da izvedene relacije definišu (na neki način) ekstenziju grupe $\mathbf{A}$ grupom $\mathbf{B}$ do na ekvivalentnost.

**Teorema 13.6** *Svaki sistem elemenata* $\{a_{\alpha,\beta} \mid \alpha, \beta \in B\}$ *i automorfizama* $\{\phi_\alpha \mid \alpha \in B\}$ *grupe* $\mathbf{A}$ *koji ispunjavaju uslove*

$$\phi_\alpha \circ \phi_\beta = \phi_{\alpha\beta} \circ u_{a_{\alpha,\beta}} \tag{I}$$

*i*

$$a_{\alpha,\beta\gamma} \cdot a_{\beta,\gamma} = a_{\alpha\beta,\gamma} \cdot (a_{\alpha,\beta}) \phi_\gamma \tag{II}$$

*određuju do na ekvivalentnost ekstenziju grupe* $\mathbf{A}$ *grupom* $\mathbf{B}$*, takvu da je, za svako* $\alpha \in B$*,* $\phi_\alpha$ *restrikcija nad* $A$ *unutrašnjeg automorfizma ekstenzije koji korespondira nekom elementu odgovarajuće transverzale podgrupe* $\mathbf{A}$*, dok je* $\{a_{\alpha,\beta} \mid \alpha, \beta \in B\}$ *faktor sistem te transverzale.*

**Dokaz.** Na skupu simbola $\overline{G} = \{g_\alpha a \mid a \in A, \alpha \in B\}$ definišimo (inspirisani sa (3)) operaciju $*$ sa:

$$g_\alpha a * g_\beta b = g_{\alpha\beta} (a_{\alpha,\beta}(a) \phi_\beta b) \tag{III}$$

(zagrade za proizvod elemenata iz $\mathbf{A}$ izostavljaćemo nadalje). Grupoid $\overline{\mathbf{G}} = \langle \overline{G}, * \rangle$ je, tvrdimo, tražena ekstenzija.

Proveravamo prvo asocijativnost operacije $*$ (koristeći asocijativnost operacija grupa $\mathbf{A}$ i $\mathbf{B}$):

$$(g_\alpha a * g_\beta b) * g_\gamma c = g_{\alpha\beta} a_{\alpha,\beta}(a) \phi_\beta b * g_\gamma c = g_{\alpha\beta\gamma} a_{\alpha\beta,\gamma} (a_{\alpha,\beta}(a) \phi_\beta b) \phi_\gamma c =$$

$$g_{\alpha\beta\gamma}a_{\alpha\beta,\gamma}(a_{\alpha,\beta})\phi_\gamma(a)(\phi_\beta\circ\phi_\gamma)(b)\phi_\gamma c = g_{\alpha\beta\gamma}a_{\alpha\beta,\gamma}(a_{\alpha,\beta})\phi_\gamma(a)(\phi_{\beta\gamma}\circ u_{a_{\beta,\gamma}})(b)\phi_\gamma c$$

$$= g_{\alpha\beta\gamma}a_{\alpha,\beta\gamma}a_{\beta,\gamma}a_{\beta,\gamma}^{-1}(a)\phi_{\beta\gamma}a_{\beta,\gamma}(b)\phi_\gamma c = g_{\alpha\beta\gamma}a_{\alpha,\beta\gamma}(a)\phi_{\beta\gamma}a_{\beta,\gamma}(b)\phi_\gamma c,$$

no i:

$$g_\alpha a * (g_\beta b * g_\gamma c) = g_\alpha a * g_{\beta\gamma}a_{\beta,\gamma}(b)\phi_\gamma c = g_{\alpha\beta\gamma}a_{\alpha,\beta\gamma}(a)\phi_{\beta\gamma}a_{\beta,\gamma}(b)\phi_\gamma c.$$

Ako je $\varepsilon$ jedinični element grupe $\mathbf{B}$, onda je prema $(I)$:

$$\phi_\varepsilon\circ\phi_\varepsilon = \phi_\varepsilon\circ u_{a_{\varepsilon,\varepsilon}},$$

i odatle (u grupi smo $\mathbf{Aut(A)}$ pa možemo koristiti kancelaciju):

$$\phi_\varepsilon = u_{a_{\varepsilon,\varepsilon}} \qquad (IV).$$

$(II)$ nam pak daje za $\beta=\gamma=\varepsilon$:

$$a_{\alpha,\varepsilon}\cdot a_{\varepsilon,\varepsilon} = a_{\alpha,\varepsilon}(a_{\alpha,\varepsilon})\phi_\varepsilon,$$

odnosno, zbog $(IV)$:

$$a_{\varepsilon,\varepsilon} = (a_{\alpha,\varepsilon})\phi_\varepsilon = a_{\varepsilon,\varepsilon}^{-1}a_{\alpha,\varepsilon}a_{\varepsilon,\varepsilon}.$$

Prema tome je za svako $\alpha\in B$:

$$a_{\alpha,\varepsilon} = a_{\varepsilon,\varepsilon} \qquad (V).$$

Ako se u $(II)$ stavi $\alpha=\beta=\varepsilon$, onda se dobija:

$$a_{\varepsilon,\gamma}\cdot a_{\varepsilon,\gamma} = a_{\varepsilon,\gamma}(a_{\varepsilon,\varepsilon})\phi_\gamma,$$

tj.

$$a_{\varepsilon,\gamma} = (a_{\varepsilon,\varepsilon})\phi_\gamma \qquad (VI).$$

Izvedene relacije nam dokazuju da je $g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}$ desni jedinični element polugrupe $\overline{\mathbf{G}}$:

$$g_\alpha a * g_\varepsilon a_{\varepsilon,\varepsilon}^{-1} = g_{\alpha\varepsilon}a_{\alpha,\varepsilon}(a)\phi_\varepsilon a_{\varepsilon,\varepsilon}^{-1} = g_\alpha a_{\varepsilon,\varepsilon}a_{\varepsilon,\varepsilon}^{-1}aa_{\varepsilon,\varepsilon}a_{\varepsilon,\varepsilon}^{-1} = g_\alpha a.$$

Za dati desni jedinični element svaki element ima desni inverzni. Desni inverzni element elementa $g_\alpha a$ je $g_{\alpha^{-1}}((a)\phi_{\alpha^{-1}})^{-1}a_{\alpha,\alpha^{-1}}^{-1}a_{\varepsilon,\varepsilon}^{-1}$. Zaista,

$$g_\alpha a * g_{\alpha^{-1}}((a)\phi_{\alpha^{-1}})^{-1}a_{\alpha,\alpha^{-1}}^{-1}a_{\varepsilon,\varepsilon}^{-1} =$$

$$g_{\alpha\alpha^{-1}}a_{\alpha,\alpha^{-1}}(a)\phi_{\alpha^{-1}}((a)\phi_{\alpha^{-1}})^{-1}a_{\alpha,\alpha^{-1}}^{-1}a_{\varepsilon,\varepsilon}^{-1} = g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}.$$

$\overline{\mathbf{G}}$ je, dakle, grupa.



Preslikavanje $\psi: A\longrightarrow\overline{G}$ dato sa $(a)\psi = g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}a$ utapanje je grupe $\mathbf{A}$ u grupu $\overline{\mathbf{G}}$. Očigledno, $\psi$ je dobro definisano i injektivno, a važi i

$$(a)\psi * (b)\psi = g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}a * g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}b = g_{\varepsilon\varepsilon}a_{\varepsilon,\varepsilon}(a_{\varepsilon,\varepsilon}^{-1}a)\phi_\varepsilon a_{\varepsilon,\varepsilon}^{-1}b =$$

$$g_\varepsilon a_{\varepsilon,\varepsilon}a_{\varepsilon,\varepsilon}^{-1}a_{\varepsilon,\varepsilon}^{-1}aa_{\varepsilon,\varepsilon}a_{\varepsilon,\varepsilon}^{-1}b = g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}ab = (ab)\psi.$$

$(\mathbf{A})\psi = \overline{\mathbf{A}}$ je i normalna podgrupa grupe $\overline{\mathbf{G}}$ – trivijalno se pokazuje, imajući u vidu proveru asocijativnosti, da je konjugat svakog elementa iz $\overline{\mathbf{A}}$ takođe u $\overline{\mathbf{A}}$.

Lako se proverava da je $\{g_\alpha e \mid \alpha\in B,\ e$ jedinični element grupe $\mathbf{A}\}$ jedna transverzala podgrupe $\overline{\mathbf{A}}$:

$$g_\alpha a * g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}a^{-1} = g_\alpha a_{\alpha,\varepsilon}a_{\varepsilon,\varepsilon}^{-1}aa_{\varepsilon,\varepsilon}a_{\varepsilon,\varepsilon}^{-1}a^{-1} = g_\alpha e,$$

a za različite elemente $\alpha,\beta$ iz $B$ je $g_\alpha e\overline{A}\cap g_\beta e\overline{A} = \emptyset$. Ponovimo: $g_\alpha e\overline{A} = \{g_\alpha a \mid a\in A\}$.

Preslikavanje $\theta: \overline{G}/\overline{A}\longrightarrow B$ dato sa $(g_\alpha e\overline{A})\theta = \alpha$ izomorfno je preslikavanje grupe $\overline{\mathbf{G}}/\overline{\mathbf{A}}$ na grupu $\mathbf{B}$; bijektivnost preslikavanja je očigledna, a tu je i homomorfnost:

$$(g_\alpha e\overline{A}\cdot g_\beta e\overline{A})\theta = ((g_\alpha e * g_\beta e)\overline{A})\theta = ((g_{\alpha\beta}a_{\alpha,\beta}(e)\phi_\beta e)\overline{A})\theta =$$

$$(g_{\alpha\beta}a_{\alpha,\beta}\overline{A})\theta = (g_{\alpha\beta}e\overline{A})\theta = \alpha\beta = (g_\alpha e\overline{A})\theta\cdot(g_\beta e\overline{A})\theta;$$

napomenimo za svaki slučaj, premda verovatno nepotrebno, da za operacije u svim grupama, s izuzetkom grupe $\overline{\mathbf{G}}$, koristimo, ukoliko ga uopšte koristimo, znak $\cdot$.

Automorfizmu $\phi_\alpha$ grupe $\mathbf{A}$ odgovara automorfizam $\overline{\phi}_\alpha$ grupe $\overline{\mathbf{A}}$, gde je

$$(g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}a)\overline{\phi}_\alpha \overset{\text{def}}{=} g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}(a)\phi_\alpha,$$

koji je pak restrikcija nad $\overline{A}$ unutrašnjeg automorfizma $u_{g_{\alpha e}}$ grupe $\overline{\mathbf{G}}$:

$$(g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}a)u_{g_{\alpha e}} = (g_\alpha e)^{-1} * g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}a * g_\alpha e =$$

$$g_{\alpha^{-1}}((e)\phi_{\alpha^{-1}})^{-1}a_{\alpha,\alpha^{-1}}^{-1}a_{\varepsilon,\varepsilon}^{-1} * g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}a * g_\alpha e =$$

$$g_{\alpha^{-1}\varepsilon\alpha}a_{\alpha^{-1},\varepsilon\alpha}(a_{\alpha,\alpha^{-1}}^{-1}a_{\varepsilon,\varepsilon}^{-1})\phi_\alpha a_{\varepsilon,\alpha}(a_{\varepsilon,\varepsilon}^{-1}a)\phi_\alpha e =$$

$$g_\varepsilon a_{\alpha^{-1},\alpha}((a_{\alpha,\alpha^{-1}})\phi_\alpha)^{-1}a_{\varepsilon,\alpha}^{-1}a_{\varepsilon,\alpha}a_{\varepsilon,\alpha}^{-1}(a)\phi_\alpha = g_\varepsilon a_{\alpha^{-1},\alpha}(a_{\varepsilon,\alpha}(a_{\alpha,\alpha^{-1}})\phi_\alpha)^{-1}(a)\phi_\alpha =$$

$$g_\varepsilon a_{\alpha^{-1},\alpha}(a_{\alpha,\varepsilon}a_{\alpha^{-1},\alpha})^{-1}(a)\phi_\alpha = g_\varepsilon a_{\alpha^{-1},\alpha}a_{\alpha^{-1},\alpha}^{-1}a_{\alpha,\varepsilon}^{-1}(a)\phi_\alpha =$$

$$g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}(a)\phi_\alpha = (g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}a)\overline{\phi}_\alpha.$$

Relacija $a_{\varepsilon,\alpha}(a_{\alpha,\alpha^{-1}})\phi_\alpha = a_{\alpha,\varepsilon}a_{\alpha^{-1},\alpha}$ je direktna posledica uslova $(II)$ (staviti $\beta=\alpha^{-1}$, $\gamma=\alpha$).

$\{g_\varepsilon a_{\varepsilon,\varepsilon}^{-1} a_{\alpha,\beta} \mid \alpha,\beta \in B\}$ je faktor sistem transverzale $\{g_\alpha e \mid \alpha \in B\}$, jer je:

$$g_\alpha e * g_\beta e = g_{\alpha\beta} a_{\alpha,\beta}(e)\phi_{\beta e} = g_{\alpha\beta} a_{\alpha,\beta},$$

a i

$$g_{\alpha\beta} e * g_\varepsilon a_{\varepsilon,\varepsilon}^{-1} a_{\alpha,\beta} = g_{\alpha\beta\varepsilon} a_{\alpha\beta,\varepsilon}(e)\phi_\varepsilon a_{\varepsilon,\varepsilon}^{-1} a_{\alpha,\beta} = g_{\alpha\beta} a_{\alpha,\beta}.$$

Za automorfizme $\overline{\phi}_\alpha$, $\alpha \in B$, i elemente $g_\varepsilon a_{\varepsilon,\varepsilon}^{-1} a_{\alpha,\beta}$, $\alpha,\beta \in B$, grupe $\overline{\mathbf{A}}$ evidentno važi $(I)$ i $(II)$. Tako je npr.

$$(g_\varepsilon a_{\varepsilon,\varepsilon}^{-1} a)(\overline{\phi}_\alpha \circ \overline{\phi}_\beta) = g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}(a)(\phi_\alpha \circ \phi_\beta) = g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}(a)(\phi_{\alpha\beta} \circ u_{a_{\alpha,\beta}}) =$$

$$g_\varepsilon a_{\varepsilon,\varepsilon}^{-1} a_{\alpha,\beta}^{-1}(a)\phi_{\alpha\beta} a_{\alpha,\beta} = g_\varepsilon a_{\varepsilon,\varepsilon}^{-1} a_{\alpha,\beta}^{-1} * g_\varepsilon a_{\varepsilon,\varepsilon}^{-1}(a)\phi_{\alpha\beta} * g_\varepsilon a_{\varepsilon,\varepsilon}^{-1} a_{\alpha,\beta} =$$

$$(g_\varepsilon a_{\varepsilon,\varepsilon}^{-1} a)(\overline{\phi}_{\alpha\beta} \circ u_{g_\varepsilon a_{\varepsilon,\varepsilon}^{-1} a_{\alpha,\beta}}).$$

Ovim je kompletiran dokaz o egzistenciji ekstenzije koja ispunjava uslove teoreme. Ostaje još da se proveri i njena jednoznačnost do na ekvivalentnost.

Neka je i $\mathbf{H}$ ekstenzija grupe $\mathbf{A}$ grupom $\mathbf{B}$ sa transverzalom podgrupe $\mathbf{A}$ $\{h_\alpha \mid \alpha \in B\}$ čiji je faktor sistem $\{a_{\alpha,\beta} \mid \alpha,\beta \in B\}$ i neka elementi tog sistema i skupa automorfizama grupe $\mathbf{A}$ – $\{\varphi_\alpha \mid \alpha \in B\}$, gde je $\varphi_\alpha \overset{\text{def}}{=} u_{h_\alpha}|_A$, zadovoljavaju relacije $(I)$ i $(II)$. Naravno, onda je $h_\alpha a\, h_\beta b = h_{\alpha\beta} a_{\alpha,\beta}(a) u_{h_\beta} b$, a preslikavanje $\Phi : \overline{G} \longrightarrow H$ definisano sa $(g_\alpha a)\Phi = h_\alpha a$ izomorfizam je grupa $\overline{\mathbf{G}}$ i $\mathbf{H}$, koji ujedno pokazuje da su ove grupe ekvivalentne ekstenzije. Provera je rutinska i u mnogome ponavljanje već viđenog.■

Neka su u ekstenziji $\mathbf{G}$ grupe $\mathbf{A}$ grupom $\mathbf{B}$, za fiksni izomorfizam $\varphi$ grupa $\mathbf{G/A}$ i $\mathbf{B}$, $\{g_\alpha \mid \alpha \in B\}$ i $\{\overline{g}_\alpha \mid \alpha \in B\}$ dve transverzale grupe $\mathbf{A}$, pri čemu je $(g_\alpha A)\varphi = (\overline{g}_\alpha A)\varphi = \alpha$ (dakle, $g_\alpha A = \overline{g}_\alpha A$), $\{a_{\alpha,\beta} \mid \alpha,\beta \in B\}$ i $\{\overline{a}_{\alpha,\beta} \mid \alpha,\beta \in B\}$, respektivno, faktor sistemi, a $\{u_\alpha \mid \alpha \in B\}$ i $\{\overline{u}_\alpha \mid \alpha \in B\}$ odgovarajući automorfizmi grupe $\mathbf{A}$ ($u_\alpha = u_{g_\alpha}|_A$, $\overline{u}_\alpha = u_{\overline{g}_\alpha}|_A$). Ako je $\overline{g}_\alpha = g_\alpha a_\alpha$, onda iz

$$\overline{g}_\alpha \overline{g}_\beta = \overline{g}_{\alpha\beta}\overline{a}_{\alpha,\beta} = g_{\alpha\beta} a_{\alpha\beta}\overline{a}_{\alpha,\beta} = g_\alpha a_\alpha g_\beta a_\beta = g_{\alpha\beta} a_{\alpha,\beta}(a_\alpha) u_\beta a_\beta$$

dobijamo

$$\overline{a}_{\alpha,\beta} = a_{\alpha\beta}^{-1} a_{\alpha,\beta}(a_\alpha) u_\beta a_\beta \qquad (4).$$

Za $a \in A$ i $\overline{u}_\alpha$, $\alpha \in B$, imamo

$$(a)\overline{u}_\alpha = \overline{g}_\alpha^{-1} a \overline{g}_\alpha = (g_\alpha a_\alpha)^{-1} a (g_\alpha a_\alpha) = (a)(u_\alpha \circ u_{a_\alpha}),$$

pa je

$$\overline{u}_\alpha = u_\alpha \circ u_{a_\alpha} \qquad (5).$$



**Lema 13.7** *Neka su* $\mathbf{G}$ *i* $\overline{\mathbf{G}}$ *ekstenzije grupe* $\mathbf{A}$ *grupom* $\mathbf{B}$, *zadane, kao u prethodnoj teoremi, sistemima elemenata* $\{a_{\alpha,\beta} \mid \alpha,\beta \in B\}$ *i* $\{\overline{a}_{\alpha,\beta} \mid \alpha,\beta \in B\}$ *i automorfizama* $\{u_\alpha \mid \alpha \in B\}$, $\{\overline{u}_\alpha \mid \alpha \in B\}$ *grupe* $\mathbf{A}$ *koji zadovoljavaju relacije* $(I)$ *i* $(II)$. *Tada su* $\mathbf{G}$ *i* $\overline{\mathbf{G}}$ *ekvivalentne ekstenzije akko za svako* $\alpha,\beta$ *iz* $B$ *postoje elementi* $a_\alpha, a_\beta$ *iz* $A$ *takvi da važe relacije* (4) *i* (5).

**Dokaz.** ($\Longrightarrow$) Neka su $\{g_\alpha \mid \alpha \in B\}$ i $\{\overline{g}_\alpha \mid \alpha \in B\}$ odgovarajuće transverzale grupe $\mathbf{A}$ u, respektivno, $\mathbf{G}$ i $\overline{\mathbf{G}}$ i neka je $\psi : G \longrightarrow \overline{G}$ izomorfizam grupa $\mathbf{G}$ i $\overline{\mathbf{G}}$ takav da je $\psi|_A = \imath_A$ i, za svako $\alpha \in B$, $(g_\alpha A)\psi = \overline{g}_\alpha A$. No, $(g_\alpha A)\psi = (g_\alpha)\psi A$, pa je, za neko $a_\alpha \in A$, $\overline{g}_\alpha = (g_\alpha)\psi a_\alpha = (g_\alpha a_\alpha)\psi$ i

$$\overline{g}_\alpha \overline{g}_\beta = \overline{g}_{\alpha\beta}\overline{a}_{\alpha,\beta} = (g_{\alpha\beta})\psi a_{\alpha\beta}\overline{a}_{\alpha,\beta} = (g_\alpha)\psi a_\alpha (g_\beta)\psi a_\beta =$$

$$(g_\alpha a_\alpha)\psi(g_\beta a_\beta)\psi = (g_\alpha a_\alpha g_\beta a_\beta)\psi = (g_{\alpha\beta} a_{\alpha,\beta}(a_\alpha) u_\beta a_\beta)\psi =$$

$$(g_{\alpha\beta})\psi a_{\alpha,\beta}(a_\alpha) u_\beta a_\beta.$$

Sledi

$$\overline{a}_{\alpha,\beta} = a_{\alpha\beta}^{-1} a_{\alpha,\beta}(a_\alpha) u_\beta a_\beta.$$

Dalje je, za svako $a \in A$ i svako $\alpha \in B$:

$$(a)\overline{u}_\alpha = \overline{g}_\alpha^{-1} a \overline{g}_\alpha = ((g_\alpha a_\alpha)\psi)^{-1} a (g_\alpha a_\alpha)\psi =$$

$$((g_\alpha a_\alpha)^{-1} a g_\alpha a_\alpha)\psi = ((a)(u_\alpha \circ u_{a_\alpha}))\psi = (a)(u_\alpha \circ u_{a_\alpha});$$

prema tome je

$$\overline{u}_\alpha = u_\alpha \circ u_{a_\alpha}.$$

($\Longleftarrow$) Neka su $a_\alpha$, $\alpha \in B$, elementi skupa $A$ koji ispunjavaju uslove leme i neka je $\theta : \overline{G} \longrightarrow G$ preslikavanje definisano sa $(\overline{g}_\alpha a)\theta = g_\alpha a_\alpha a$. Pokazujemo prvo da je $\theta$ homomorfno preslikavanje (bijektivnost je očigledna):

$$(\overline{g}_\alpha a\, \overline{g}_\beta b)\theta = (\overline{g}_{\alpha\beta}\overline{a}_{\alpha,\beta}(a)\overline{u}_\beta b)\theta = g_{\alpha\beta} a_{\alpha\beta}\overline{a}_{\alpha,\beta}(a)\overline{u}_\beta b =$$

$$g_{\alpha\beta} a_{\alpha\beta} a_{\alpha\beta}^{-1} a_{\alpha,\beta}(a_\alpha) u_\beta a_\beta(a)(u_\beta \circ u_{a_\beta}) b = g_{\alpha\beta} a_{\alpha,\beta} g_\beta^{-1} a_\alpha g_\beta a_\beta a_\beta^{-1} g_\beta^{-1} a g_\beta a_\beta b =$$

$$g_{\alpha\beta} a_{\alpha,\beta}(a_\alpha a) u_\beta a_\beta b = g_\alpha a_\alpha a\, g_\beta a_\beta b = (\overline{g}_\alpha a)\theta\,(\overline{g}_\beta b)\theta.$$

Znamo da je $\overline{u}_\alpha^{-1} = (u_{\overline{g}_\alpha}|_A)^{-1} = u_{\overline{g}_\alpha^{-1}}|_A$, a iz

$$((a)\overline{u}_\alpha^{-1})\theta = (\overline{g}_\alpha a \overline{g}_\alpha^{-1})\theta = (\overline{g}_\alpha a)\theta\,(\overline{g}_\alpha^{-1})\theta = g_\alpha a_\alpha a\,(g_\alpha a_\alpha)^{-1} =$$

$$(a)(u_{a_\alpha}^{-1} \circ u_\alpha^{-1}) = (a)(u_\alpha \circ u_{a_\alpha})^{-1} = (a)\overline{u}_\alpha^{-1}$$

sledi $\theta|_A = \imath_A$ (jer $\overline{u}_\alpha^{-1}$ je automorfizam grupe $\mathbf{A}$, pa kada $a$ prođe skupom $A$, i $(a)\overline{u}_\alpha^{-1}$ prođe skupom $A$).□

Vratimo se na komentar koji je prethodio teoremi 13.6. Prema (1) je preslikavanje $\theta_1 : B \longrightarrow Aut(\mathbf{A})/Inn(\mathbf{A})$ dato sa $(\alpha)\theta_1 = u_{g_\alpha}|_A Inn(\mathbf{A}) =$

$u_\alpha Inn(\mathbf{A})$ homomorfno preslikavanje grupe $\mathbf{B}$ u faktor grupu $\mathbf{Aut(A)/Inn(A)}$. Ako je $\mathbf{A}$ Abelova normalna podgrupa grupe $\mathbf{G}$, preslikavanje $\theta : B \longrightarrow Aut\mathbf{A})$, gde je $(\alpha)\theta = u_\alpha$, homomorfno je preslikavanje grupe $\mathbf{B}$ u grupu $\mathbf{Aut(A)}$ (sada je $\mathbf{Inn(A)}$ jedinična grupa). Situacija se u tom slučaju generalno pojednostavljuje. Sledeća lema je uveliko ponavljanje već rečenog. Dokaz dajemo više vežbe radi.

**Lema 13.8** *Neka je $\theta$ homomorfno preslikavanje grupe $\mathbf{B}$ u grupu automorfizama grupe $\mathbf{A}$. Tada je $\overline{\mathbf{G}} = \langle\{(\alpha, a) \mid a \in A, \alpha \in B\}, \star\rangle$, gde je $(\alpha, a) \star (\beta, b) \stackrel{\text{def}}{=} (\alpha\beta, (a)\phi_\beta b)$ i $\phi_\beta = (\beta)\theta$ $(\in Aut(\mathbf{A}))$, ekstenzija (izomorfne slike) grupe $\mathbf{A}$ grupom $\mathbf{B}$.*

**Dokaz.** $\langle\overline{G}, \star\rangle$ je polugrupa jer je:

$$(\alpha, a) \star ((\beta, b) \star (\gamma, c)) = (\alpha\beta\gamma, (a)\phi_{\beta\gamma}(b)\phi_\gamma c) = ((\alpha, a) \star (\beta, b)) \star (\gamma, c).$$

Desni neutralni element ove polugrupe je $(\epsilon, e)$ (opet je $\epsilon$ neutralni element grupe $\mathbf{B}$, a $e$ grupe $\mathbf{A}$; prema tome je i $\phi_\epsilon = \imath_A$). Desni neutralni element elementa $(\alpha, a)$ je $(\alpha^{-1}, ((a)\phi_{\alpha^{-1}})^{-1})$. Dakle, $\langle\overline{G}, \star\rangle$ je grupa, a $\overline{\mathbf{A}} = \langle\{(\epsilon, a) \mid a \in A\}, \star\rangle$ je izomorfna slika grupe $\mathbf{A}$, koja je ujedno i normalna podgrupa grupe $\overline{\mathbf{G}}$; jer, $(\epsilon, a) \star (\epsilon, b) = (\epsilon, ab)$ i

$$(\alpha^{-1}, ((a)\phi_{\alpha^{-1}}))^{-1} \star (\epsilon, b) \star (\alpha, a) = (\epsilon, (((a)\phi_{\alpha^{-1}})^{-1})\phi_\alpha(b)\phi_\alpha a) =$$

$$(\epsilon, a^{-1}(b)\phi_\alpha a) \in \overline{A}$$

(imali smo u vidu: $\phi_{\alpha^{-1}} \circ \phi_\alpha = \phi_{\alpha^{-1}\alpha} = \phi_\epsilon = \imath_A$). Konačno, korespondencija $\varphi : \overline{G}/\overline{A} \longrightarrow B$ data sa $((\alpha, a)\overline{A})\varphi = \alpha$ izomorfno je preslikavanje grupe $\overline{\mathbf{G}}/\overline{\mathbf{A}}$ na grupu $\mathbf{B}$. Ako je $(\alpha, a)\overline{A} = (\beta, b)\overline{A}$, tj. $(\beta^{-1}, ((b)\phi_{\beta^{-1}})^{-1}) \star (\alpha, a) \in \overline{A}$, onda mora biti $\beta\alpha^{-1} = \epsilon$, odnosno $\alpha = \beta$. Stoga je $\varphi$ i dobro definisano i injektivno, a surjektivnost je očigledna. Važi i svojstvo homomorfnosti:

$$((\alpha, a)\overline{A} \cdot (\beta, b)\overline{A})\varphi = (((\alpha, a) \star (\beta, b))\overline{A})\varphi = ((\alpha\beta, (a)\phi_\beta b)\overline{A})\varphi =$$

$$\alpha\beta = ((\alpha, a)\overline{A})\varphi \cdot ((\beta, b)\overline{A})\varphi.$$

Automorfizmu $\phi_\alpha$ grupe $\mathbf{A}$ odgovara automorfizam $\overline{\phi}_\alpha$ grupe $\overline{\mathbf{A}}$, gde je $((\epsilon, a))\overline{\phi}_\alpha \stackrel{\text{def}}{=} (\epsilon, (a)\phi_\alpha)$. Ponavljamo samo:

$$((\epsilon, a))(\overline{\phi}_\alpha \circ \overline{\phi}_\beta) = (((\epsilon, a))\overline{\phi}_\alpha)\overline{\phi}_\beta = (\epsilon, ((a)\phi_\alpha)\phi_\beta) =$$

$$(\epsilon, (a)(\phi_\alpha \circ \phi_\beta)) = (\epsilon, (a)\phi_{\alpha\beta}) = ((\epsilon, a))\overline{\phi}_{\alpha\beta}.$$

Za grupu $\overline{\mathbf{G}}$, koju obeležavamo sa $\mathbf{A} \times_\theta \mathbf{B}$, kazaćemo da realizuje $\theta$ u smislu da je za svako $\alpha \in B$ (i svako $a \in A$):

$$\overline{(\alpha)\theta} = \overline{\phi}_\alpha = u_{(\alpha,e)}|_{\overline{A}}$$



Zaista, prema gore navedenom je:

$$((\epsilon, a))\overline{\phi}_\alpha = (\epsilon, (a)\phi_\alpha) = (\alpha, e)^{-1} \star (\epsilon, a) \star (\alpha, e).$$

U slučaju da je $\mathbf{A}$ Abelova grupa, imamo generalno (za svako $a \in A$):

$$\overline{(\alpha)\theta} = u_{(\alpha,a)}|_{\overline{A}}.\square$$

**Korolar 13.9** *Grupa $\mathbf{G}$ je poludirektni proizvod normalne podgrupe $\mathbf{A}$ i podgrupe $\mathbf{B}$ akko je izomorfna grupi $\mathbf{A} \times_\theta \mathbf{B}$ za neko homomorfno preslikavanje $\theta$ grupe $\mathbf{B}$ u grupu $\mathbf{Aut(A)}$.*

**Dokaz.** ($\Longleftarrow$) Sa notacijom iz prethodne leme, $\overline{\mathbf{B}} = \langle\{(\alpha, e) \mid \alpha \in B\}, \star\rangle$ je podgrupa grupe $\overline{\mathbf{G}} = \mathbf{A} \times_\theta \mathbf{B}$, izomorfna grupi $\mathbf{B}$ (imamo npr. $(\alpha, e) \star (\beta, e) = (\alpha\beta, e)$, a očigledna je bijektivnost preslikavanja $\psi : \overline{B} \longrightarrow B$ datog sa $(\alpha)\psi = (\alpha, e)$). Već smo videli da je $\overline{\mathbf{A}} \lhd \overline{\mathbf{G}}$, a jasno: $\overline{A} \cap \overline{B} = \{(\epsilon, e)\}$ i $\overline{G} = \overline{B}\,\overline{A} = \overline{A}\,\overline{B}$ (jer je $(\alpha, a) = (\alpha, e) \star (\epsilon, a) = (\epsilon, (a)\phi_{\alpha^{-1}}) \star (\alpha, e)$); znači, $\overline{\mathbf{G}} = \overline{\mathbf{A}} \rtimes \overline{\mathbf{B}}$.

($\Longrightarrow$) Neka je $\mathbf{G} = \mathbf{A} \rtimes \mathbf{B}$. Preslikavanje $\theta : B \longrightarrow Aut(\mathbf{A})$ dato sa $(\alpha)\theta = u_\alpha|_A$ homomorfno je preslikavanje grupe $\mathbf{B}$ u grupu $\mathbf{Aut(A)}$, a $\psi : A \times_\theta B \longrightarrow G$, gde je $((\alpha, a))\psi \stackrel{\text{def}}{=} \alpha a$, izomorfno je preslikavanje grupe $\mathbf{A} \times_\theta \mathbf{B}$ na grupu $\mathbf{G}$. Dovoljno je samo proveriti svojstvo homomorfnosti preslikavanja $\psi$ (bijektivnost je očigledna):

$$((\alpha, a) \star (\beta, b))\psi = ((\alpha\beta, (a)u_\beta|_A b))\psi = \alpha\beta\beta^{-1}a\beta b =$$

$$\alpha a \cdot \beta b = ((\alpha, a))\psi \cdot ((\beta, b))\psi.\square$$

**Lema 13.10** *(a) Ako su $\theta_1$ i $\theta_2$ dva izomorfna preslikavanja grupe $\mathbf{B}$ na istu podgrupu grupe automorfizama grupe $\mathbf{A}$, onda je $\mathbf{A} \times_{\theta_1} \mathbf{B} \cong \mathbf{A} \times_{\theta_2} \mathbf{B}$.*

*(b) Ako je $\mathbf{B} = \langle\beta\rangle$ ciklična grupa i ako su $\theta_1$ i $\theta_2$ dva izomorfna preslikavanja grupe $\mathbf{B}$ u $\mathbf{Aut(A)}$ takva da su podgrupe $(\mathbf{B})\theta_1$ i $(\mathbf{B})\theta_2$ konjugovane, onda je $\mathbf{A} \times_{\theta_1} \mathbf{B} \cong \mathbf{A} \times_{\theta_2} \mathbf{B}$.*

**Dokaz.** *(a)* Operaciju u grupi $\mathbf{A} \times_{\theta_i} \mathbf{B}$, $i = 1, 2$, obeležićemo sa $\star_i$ (onda nema potrebe da koristimo različite oznake za elemente tih grupa). Definišimo preslikavanje $\Phi : A \times_{\theta_1} B \longrightarrow A \times_{\theta_2} B$ sa $((\alpha, a))\Phi = ((\alpha)(\theta_1 \circ \theta_2^{-1}), a)$. $\Phi$ je, evidentno, bijektivno preslikavanje, a važi i:

$$((\alpha, a) \star_1 (\beta, b))\Phi = ((\alpha\beta, (a)((\beta)\theta_1)b))\Phi = ((\alpha\beta)(\theta_1 \circ \theta_2^{-1}), (a)((\beta)\theta_1)b) =$$

$$((\alpha)(\theta_1 \circ \theta_2^{-1}) \cdot (\beta)(\theta_1 \circ \theta_2^{-1}), (a)(((\beta)(\theta_1 \circ \theta_2^{-1}))\theta_2)b) =$$

$$((\alpha)(\theta_1 \circ \theta_2^{-1}), a) \star_2 ((\beta)(\theta_1 \circ \theta_2^{-1}), b) = ((\alpha, a))\Phi \star_2 ((\beta, b))\Phi.$$

*(b)* Zadržavamo notaciju iz tačke *(a)*. Neka je, za $\varphi \in Aut(\mathbf{A})$, $\varphi^{-1}(\mathbf{B})\theta_1\varphi = (\mathbf{B})\theta_2$ i neka je $\varphi^{-1}(\beta)\theta_1\varphi = ((\beta)\theta_2)^n$. Onda je preslikavanje $\Phi : (\beta^k, a) \longrightarrow$

$(\beta^{kn},(a)\varphi)$ izomorfno preslikavanje grupe $\mathbf{A}\times_{\theta_1}\mathbf{B}$ na grupu $\mathbf{A}\times_{\theta_2}\mathbf{B}$. Očigledno je bijektivno, a ima i svojstvo homomorfnosti jer je:

$$((\beta^k,a)\star_1(\beta^l,b))\Phi=((\beta^{k+l},(a)((\beta^l)\theta_1)\cdot b))\Phi=(\beta^{(k+l)n},((a)((\beta^l)\theta_1)\cdot b)\varphi)=$$

$$(\beta^{kn+ln},((a)\varphi)(\varphi^{-1}\circ(\beta^l)\theta_1\circ\varphi)\cdot(b)\varphi)=(\beta^{kn+ln},((a)\varphi)(\varphi^{-1}\circ(\beta)\theta_1\circ\varphi)^l\cdot(b)\varphi)=$$

$$(\beta^{kn+ln},((a)\varphi)((\beta)\theta_2)^{ln}\cdot(b)\varphi)=(\beta^{kn+ln},((a)\varphi)(\beta^{ln})\theta_2\cdot(b)\varphi)=$$

$$(\beta^{kn},(a)\varphi)\star_2(\beta^{ln},(b)\varphi)=((\beta^k,a))\Phi\star_2((\beta^l,b))\Phi.\square$$

**Lema 13.11** *Neka je Abelova grupa* $\mathbf{A}$ *direktni proizvod karakterističnih podgrupa* $\mathbf{A}_1$ *i* $\mathbf{A}_2$ *i neka je, dalje,* $\theta: B\longrightarrow Aut(\mathbf{A})$, *gde je* $(\alpha)\theta=\phi_\alpha$, *homomorfno preslikavanje grupe* $\mathbf{B}$ *u* $\mathbf{Aut}(\mathbf{A})$. $\theta$ *na prirodan način određuje homomorfno preslikavanje* $\Phi$ *grupe* $\mathbf{B}$ *u* $\mathbf{Aut}(\mathbf{A}_1)\times\mathbf{Aut}(\mathbf{A}_2)$ - $(\alpha)\Phi=(\phi_\alpha|_{A_1},\phi_\alpha|_{A_2})$ *(videti 10.27). Ako je* $\phi_\alpha|_{A_1}=\imath_{A_1}$ *za svako* $\alpha$, *onda je* $\mathbf{A}\times_\theta\mathbf{B}\cong\mathbf{A}_1\times(\mathbf{A}_2\times_\psi\mathbf{B})$, *gde je* $\psi\in Hom(\mathbf{B},\mathbf{Aut}(\mathbf{A}_2))$ *dato sa* $(\alpha)\psi=\phi_\alpha|_{A_2}$.

**Dokaz.** Preslikavanje $\Psi: A\times_\theta B\longrightarrow A_1\times(A_2\times_\psi B)$ dato sa $(\alpha,a_1a_2)\longrightarrow(a_1,(\alpha,a_2))$ dokazuje tvrđenje. Njegova bijektivnost je očigledna, a

$$((\alpha,a_1a_2)\star(\beta,b_1b_2))\Psi=((\alpha\beta,(a_1a_2)\phi_\beta b_1b_2))\Psi=((\alpha\beta,a_1(a_2)\phi_\beta b_1b_2))\Psi=$$

$$((\alpha\beta,a_1b_1(a_2)\phi_\beta b_2))\Psi=(a_1b_1,(\alpha\beta,(a_2)\phi_\beta b_2))=(a_1,(\alpha,a_2))\cdot(b_1,(\beta,b_2))=$$

$$((\alpha,a_1a_2))\Psi\cdot((\beta,b_1b_2))\Psi.\square$$

**Primer 13.12** (*a*) *Holomorf grupe* $\mathbf{A}$ *izomorfan je grupi* $\mathbf{A}\times_\imath\mathbf{Aut}(\mathbf{A})$, *gde je* $\imath$ *identično preslikavanje grupe* $\mathbf{Aut}(\mathbf{A})$ *na sebe.*

**Dokaz.** Preslikavanje $\Psi$ grupe $\mathbf{A}\times_\imath\mathbf{Aut}(\mathbf{A})$ u holomorf Abelove grupe $\mathbf{A}-\mathbf{N}(\overline{\mathbf{G}})=\overline{\mathbf{A}}\rtimes\mathbf{Aut}(\mathbf{A})$ (12.10), dato sa $(\varphi,a)\Psi=\varphi\circ d_a$, izomorfno je preslikavanje. Bijektivnost je očigledna, a

$$((\varphi,a)\star(\phi,b))\Psi=((\varphi\circ\phi,(a)\phi b))\Psi=(\varphi\circ\phi)\circ d_{(a)\phi b}=\varphi\circ\phi\circ d_{(a)\phi}\circ d_b=$$

$$\varphi\circ(\phi\circ d_{(a)\phi}\circ\phi^{-1})\circ\phi\circ d_b=\varphi\circ d_{((a)\phi)\phi^{-1}}\circ\phi\circ d_b=((\varphi,a))\Psi\circ((\phi,b))\Psi.$$

(*b*) *Neka su* $p$ *i* $q$ *prosti brojevi i neka je* $p>q$. *Tada postoje najviše dva poludirektna proizvoda cikličnih grupa* $\mathbf{C}_p$ *i* $\mathbf{C}_q$.

**Dokaz.** Ako cikličnu grupu $\mathbf{C}_p$ uzmemo kao normalni faktor, svaki takav proizvod je izomorfan grupi $\mathbf{C}_p\times_\theta\mathbf{C}_q$ za neko homomorfno preslikavanje grupe $\mathbf{C}_q$ u grupu $\mathbf{Aut}(\mathbf{C}_p)$ ($\cong\mathbf{C}_{p-1}$). Jasno, opet će $\mathbf{C}_p$ i $\mathbf{C}_q$ biti baš $\mathbf{Z}_p$, odnosno $\mathbf{Z}_q$. Prema 8.24 radi se o homomorfnom preslikavanju grupe $\mathbf{Z}_q$ u grupu $\mathbf{Aut}(\mathbf{Z}_p)=\langle\{\varphi_k\mid 1\le k\le p-1\},\circ\rangle$, gde je $\varphi_k\circ\varphi_l=\varphi_{k\cdot_p l}$ (8.24). Pitanje je, prvo, da li pored trivijalnog homomorfizma (koji sve elemente preslikava u jedinični) postoji još neki. Takav bi, prema 8.2, bio injektivan, pa bi ciklična



grupa $\mathbf{Aut}(\mathbf{Z}_p)$, reda $p-1$, imala podgrupu reda $q$, dakle, $q$ bi delilo $p-1$. S druge strane, ako $q|p-1$, ciklična grupa $\mathbf{Aut}(\mathbf{Z}_p)$ ima jedinstvenu podgrupu reda $q$, koja je, naravno, izomorfna grupi $\mathbf{Z}_q$. Prema tome, netrivijalno homomorfno preslikavanje grupe $\mathbf{Z}_q$ u grupu $\mathbf{Aut}(\mathbf{Z}_p)$ postoji akko $q|p-1$. S obzirom da netrivijalni homomorfizmi (u slučaju da postoje) preslikavaju grupu $\mathbf{Z}_q$ na istu podgrupu grupe $\mathbf{Aut}(\mathbf{Z}_p)$, koja je pak generisana bilo kojim elementom reda $q$, nebitno je, prema poslednjoj lemi, koje od mogućih utapanja posmatramo. Rezimiramo: ako $q$ ne deli $p-1$, imamo samo trivijalni homomorfizam $\theta_0$ ($(k)\theta_0=\imath$ - identično preslikavanje skupa $Z_p$, za svako $k$) i tom slučaju odgovarajući poluproizvod je baš direktni proizvod: $\mathbf{Z}_p\times_{\theta_0}\mathbf{Z}_q\cong\mathbf{Z}_p\times\mathbf{Z}_q(\cong\mathbf{Z}_{pq})$. Jer je, u usvojenoj notaciji, za $a,b\in Z_p$, $k,l\in Z_q$:

$$(k,a)\star(l,b)=(k+_q l,(a)((l)\theta_0)+_p b)=(k+_q l,a+_p b),$$

te se lako proverava da je preslikavanje $(k,a)\longrightarrow(a,k)$ izomorfno preslikavanje grupe $\mathbf{Z}_p\times_{\theta_0}\mathbf{Z}_q$ na grupu $\mathbf{Z}_p\times\mathbf{Z}_q$.

Ako je $\varphi_m$ generatorni element grupe $\mathbf{Aut}(\mathbf{Z}_p)$ i ako $q|p-1$, recimo $p-1=qr$, onda je preslikavanje $\theta_1: Z_q\longrightarrow Aut(\mathbf{Z}_p)$ dato sa $(1)\theta_1=(\varphi_m)^r=\varphi_{m^r-[\frac{m^r}{p}]p}$ utapanje grupe $\mathbf{Z}_q$ u grupu $\mathbf{Aut}(\mathbf{Z}_p)$. U opštem je

$$(k)\theta_1=(\underbrace{1+\cdots+1}_{k-puta})\theta_1=\underbrace{\varphi_{m^r-[\frac{m^r}{p}]p}\circ\cdots\circ\varphi_{m^r-[\frac{m^r}{p}]p}}_{k-puta}=$$

$$\underbrace{\varphi_{(m^r-[\frac{m^r}{p}]p)\cdot_p\cdots\cdot_p(m^r-[\frac{m^r}{p}]p)}}_{k-puta}=\varphi_{(m^r-[\frac{m^r}{p}]p)^k-[\frac{(m^r-[\frac{m^r}{p}]p)^k}{p}]p}.$$

Posmatrajmo proizvod $(1,0)^{-1}\star(0,1)\star(1,0)\in\overline{Z}_p$ ($\overline{\mathbf{Z}}_p$ je izomorfna slika grupe $\mathbf{Z}_p$ u poludirektnom proizvodu $\mathbf{Z}_p\times_{\theta_1}\mathbf{Z}_q$ - njen generatorni element je $(0,1)$, a $(1,0)$ je generatorni element slike $\overline{\mathbf{Z}}_q$ grupe $\mathbf{Z}_q$). Već smo videli da je $(1,0)^{-1}=(q-1,0)$, a

$$(q-1,0)\star(0,1)\star(1,0)=((q-1)+_q 0+_q 1,(0)[(0)\theta_1\circ(1)\theta_1]+_p(1)[(1)\theta_1]+_p 0)=$$

$$(0,(1)\varphi_{m^r-[\frac{m^r}{p}]p})=(0,m^r-[\frac{m^r}{p}]p)=\underbrace{(0,1)\star\cdots\star(0,1)}_{m^r-puta}=(0,1)^{m^r}.$$

Jasno, $m^r-[\frac{m^r}{p}]p\neq 1$, u suprotnom bi element $\varphi_m$ bio reda manjeg od ili jednak $r$, a ne reda $p-1$. Indukcijom se lako pokazuje da ako je u nekoj grupi $b^{-1}ab=a^t$, onda je $b^{-k}ab^k=a^{t^k}$ (uostalom to ćemo i demonstrirati na jednom drugom primeru). Stoga je

$$(0,1)=(1,0)^{-q}\star(0,1)\star(1,0)^q=(0,1)^{(m^r)^q},$$

te je, što smo i inače znali, $(m^r)^q \equiv 1\,(mod\ p)$.

Primetimo još da za $q = 2$ uvek imamo netrivijalno homomorfno preslikavanje grupe $\mathbf{Z}_2$ u grupu $\mathbf{Aut}(\mathbf{Z}_p)$, pa, dakle, i dva poludirektna proizvoda cikličnih grupa redova $p$ i 2. Kada je reč o netrivijalnom homomorfizmu $\theta_1$, tada je $(1)\theta_1 = \varphi_{p-1}$ jer je $p-1$ jedini element reda 2 u grupi $\langle\{k \mid 1 \leq k \leq p-1\}, \cdot_p\rangle$. Tako će sada biti:

$$(1,0)^{-1} \star (0,1) \star (1,0) = (1,0) \star (0,1) \star (1,0) = (0,(1)((1)\theta_1)) =$$

$$(0,(1)\varphi_{p-1}) = (0,p-1) = (0,1)^{p-1}.$$

U pitanju je dijedarska grupa stepena $p$, gde $(0,1)$ odgovara rotaciji za ugao $\frac{2\pi}{p}$, a $(1,0)$ simetriji u odnosu na $y$-osu.

Recimo na kraju da se uzimanjem ciklične grupe $\mathbf{Z}_q$ kao normalnog faktora ne dobija ništa novo. Postoji samo trivijalno preslikavanje grupe $\mathbf{Z}_p$ u grupu $\mathbf{Aut}(\mathbf{Z}_q)$ (reda $q-1$), a ono nam daje, kao što smo videli, direktni proizvod datih cikličnih grupa.□

## 14 Spleteni proizvodi

Neka su date grupa $\mathbf{A}$, grupa permutacija nepraznog skupa $X$, $\mathbf{B}\ (\leq \mathbf{S}_X)$, i neka je $\mathbf{C} = \prod^c_{x\in X} \mathbf{A}_x$ $(\mathbf{C} = \prod_{x\in X} \mathbf{A}_x)$, gde je, za svako $x \in X$, $\mathbf{A}_x = \mathbf{A}$. Elementi grupe $\mathbf{A}$ će biti $a, b, c, \ldots$ i jedinični element $e$, grupe $\mathbf{B}$ $\alpha, \beta, \gamma, \ldots$ i jedinični $\epsilon$, grupe $\mathbf{C}$ $f, g, h, \ldots, \overline{a}, \overline{b}, \overline{c}, \ldots$ i jedinični $\overline{e}$ i skupa $X$ $x, y, z, \ldots$. Definišimo preslikavanje $\Phi : B \longrightarrow Aut(\mathbf{C})$ sa: $(\alpha)\Phi = \phi_\alpha$, gde je $(f)\phi_\alpha = f^\alpha$ i, za svako $x \in X$, $(x)f^\alpha = (x\alpha^{-1})f$ ($x\alpha^{-1}$ je, jasno, slika elementa $x$ za permutaciju $\alpha^{-1}$). $\phi_\alpha$ je odista automorfizam grupe $\mathbf{C}$. Tako je $(x)((f \cdot g)\phi^\alpha) = (x\alpha^{-1})(f \cdot g) = (x\alpha^{-1})f \cdot (x\alpha^{-1})g = (x)f^\alpha \cdot (x)g^\alpha = (x)(f^\alpha \cdot g^\alpha)$, tj. $(f \cdot g)\phi_\alpha = (f)\phi_\alpha \cdot (g)\phi_\alpha$ (po ustaljenom pravilu operacije u grupama obeležavamo istim znakom $-\cdot$). Ako je $(x)f \neq (x)g$ za neko $x \in X$, tada je i $(x\alpha)f^\alpha \neq (x\alpha)g^\alpha$; drugim rečima $(f)\phi_\alpha \neq (g)\phi_\alpha$. I surjektivnost je očigledna: tako je $f = (f^{\alpha^{-1}})\phi_\alpha$ $((x)(f^{\alpha^{-1}})^\alpha = (x\alpha^{-1})f^{\alpha^{-1}} = ((x\alpha^{-1})\alpha)f = (x)f)$. Preslikavanje $\Phi$ je injektivni homomorfizam. Iz $(x)f^{\alpha\beta} = ((x\beta^{-1})\alpha^{-1})f = (x\beta^{-1})f^\alpha = (x)(f^\alpha)^\beta$ sledi $(f)\phi_{\alpha\beta} = f^{\alpha\beta} = (f^\alpha)^\beta = (f)(\phi_\alpha \circ \phi_\beta)$; dakle, $(\alpha\beta)\Phi = \phi_{\alpha\beta} = \phi_\alpha \circ \phi_\beta = (\alpha)\Phi \circ (\beta)\Phi$. Ako je pak $\alpha \neq \beta$ (znači i $\alpha^{-1} \neq \beta^{-1}$), tada je i $\phi_\alpha \neq \phi_\beta$. Jer, neka je $a$ (bilo koji) nejedinični element grupe $\mathbf{A}$ i $(x)\alpha^{-1} \neq (x)\beta^{-1}$. Onda je, za $f \in C$, dato sa $(y)f = \begin{cases} a & y = (x)\alpha^{-1} \\ e & \text{inače} \end{cases}$, $f^\alpha \neq f^\beta$ $((x)f^\alpha = a \neq e = (x)f^\beta)$.

Sa uvedenim grupama i preslikavanjima na red je došla i

**Definicija 14.1** *Neograničeni (kartezijanski, potpun) spleteni (venačni) proizvod (eng. unrestricted wreath product) grupe* $\mathbf{A}$ *sa grupom permutacija skupa* $X$, $\mathbf{B}$, *u oznaci* $\mathbf{A}\ Wr\ \mathbf{B}$, *poludirektni je proizvod* $\prod^c_{x\in X} \mathbf{A}_x \times_\Phi \mathbf{B}$.



*Ograničeni (direktan) spleteni (venačni) proizvod (eng. restricted wreath product) grupe* $\mathbf{A}$ *sa* $\mathbf{B}$, *u oznaci* $\mathbf{A}\ wr\ \mathbf{B}$, *poludirektni je proizvod* $\prod_{x\in X} \mathbf{A}_x \times_\Phi \mathbf{B}$.

**Napomena.** Za prevod engleskog termina *wreath product*, koji doslovno znači venačni proizvod, našli smo kompromisno rešenje. Fusnota u [67] na strani 96 kaže da je oko njegovog prevoda na ruski takođe bilo nedoumica. Prevladao je izraz *сплетение – декартово сплетение*, odnosno *прямое сплетение групп* $\mathbf{A}$ *и* $\mathbf{B}$ ([78], [92], [156] itd.). Tako bismo i mi mogli govoriti o *spletu grupa* $\mathbf{A}$ *i* $\mathbf{B}$. S druge strane, mi smo zadržali i koristimo i doslovan prevod engleskog *unrestricted, restricted.*

Kao i dosad, za domen neograničenog (ograničenog) spletenog proizvoda uzimamo $B \times \prod_{x\in X} A_x$ $(B \times \prod^d_{x\in X} A_x)$, a "množenje" je, znamo, dato sa:

$$(\alpha, f) \star (\beta, g) = (\alpha\beta, (f)\phi_\beta \cdot g) = (\alpha\beta, f^\beta \cdot g).$$

Shodno praksi grupu $\mathbf{B}$ ćemo izjednačavati sa (njenom izomorfnom slikom) $\overline{\mathbf{B}} = \langle\{(\alpha, \overline{e}) \mid \alpha \in B\}, \star\rangle$ u grupi $\mathbf{A}\ Wr\ \mathbf{B}$ ($\mathbf{A}\ wr\ \mathbf{B}$), grupu $\mathbf{C}$ sa podgrupom $\overline{\mathbf{C}} = \langle\{(\epsilon, f) \mid f \in C\}, \star\rangle$.

**Definicija 14.2** *Skup konstantnih funkcija (elemenata) iz* $C$ *(*$f$ *je konstantna funkcija akko je* $(x)f = (y)f$ *za svako* $x, y \in X$*) zove se dijagonala neograničenog spletenog proizvoda* $\mathbf{A}\ Wr\ \mathbf{B}$.

Jasno, dijagonala je domen podgrupe $(\overline{\mathbf{A}})$ grupe $\mathbf{C}$ izomorfne sa grupom $\mathbf{A}$. Kad govorimo o odgovarajućoj podgrupi grupe $\mathbf{A}\ Wr\ \mathbf{B}$, koju ćemo, prirodno, zvati *dijagonala*, mislimo, naravno, na podgrupu sa domenom $\{(\epsilon, \overline{a}) \mid a \in A\}$, gde je $(x)\overline{a} = a$ za svako $x \in X$ (u skladu sa oznakom za jedinični element – $\overline{e}$, konstantne funkcije obeležavaćemo sa $\overline{a}, \overline{b}, \ldots$).

U slučaju da je $X$ beskonačan skup i $\mathbf{A}$ nejedinična grupa, $\overline{e}$ je jedina konstantna funkcija u direktnom proizvodu $\prod_{x\in X} \mathbf{A}_x$; stoga dijagonalu i ne dovodimo u vezu sa ograničenim spletenim proizvodima.

Ako je $\mathbf{A} = \mathbf{E}$ – jedinična grupa, onda je $\mathbf{E}\ Wr\ \mathbf{B} = \mathbf{E}\ wr\ \mathbf{B} \cong \mathbf{B}$. Opet, ako je $\mathbf{B} = \mathbf{E}$, tada je $\mathbf{A}\ Wr\ \mathbf{E} \cong \prod^c_{x\in X} \mathbf{A}_x$, $\mathbf{A}\ wr\ \mathbf{E} \cong \prod_{x\in X} \mathbf{A}_x$. Prema tome, ovi slučajevi nisu od interesa.

Ako je baš $X = B$ i $(\alpha)f^\beta \stackrel{\text{def}}{=} (\alpha\beta^{-1})f$, gde je sada $\alpha\beta^{-1}$ proizvod elemenata $\alpha$ i $\beta^{-1}$ u grupi $\mathbf{B}$, onda je $\mathbf{A}\ Wr\ \mathbf{B}$ tzv. *standardni neograničeni unakrsni proizvod*, $\mathbf{A}\ wr\ \mathbf{B}$ *standardni ograničeni spleteni proizvod.* Ubuduće ćemo podrazumevati da se, ako ne spominjemo indeksni skup, radi o standardnim ograničenim ili neograničenim spletenim proizvodima. To nas ujedno oslobađa monotonog ponavljanja "standardni ...".

**Lema 14.3** *(a)* $\mathbf{A}\ Wr\ \mathbf{B} = \mathbf{A}\ wr\ \mathbf{B}$ *akko je ili* $\mathbf{A}$ *jedinična grupa ili* $\mathbf{B}$ *konačna grupa;*

(*b*) *Dijagonala grupe* $\mathbf{A}\ Wr\ \mathbf{B}$ *sadržana je u centralizatoru podgrupe* $\overline{\mathbf{B}}$;

(*c*) *Ako su* $\mathbf{A}$ *i* $\mathbf{B}$ *nejedinične grupe, centar grupe* $\mathbf{A}\ Wr\ \mathbf{B}$ *jednak je centru dijagonale;*

*Ako je* $\mathbf{B}$ *beskonačna grupa, grupa* $\mathbf{A}\ wr\ \mathbf{B}$ *je bez centra;*

(*d*) *Ako su grupe* $\mathbf{A}$ *i* $\mathbf{B}$ *eksponenata, respektivno,* $m$ *i* $n$*, onda eksponent grupe* $\mathbf{A}\ Wr\ \mathbf{B}$ *deli* $mn$;

(*e*) *Ako su* $\mathbf{A}$ *i* $\mathbf{B}$ *p-grupe, onda je* $\mathbf{A}\ wr\ \mathbf{B}$ *takođe p-grupa, dok je* $\mathbf{A}\ Wr\ \mathbf{B}$ *p-grupa akko je* $\mathbf{A}$ *konačnog eksponenta.*

**Dokaz.** (*b*) Očigledno, ako je $f \equiv \overline{a}$, onda je, za svako $\alpha \in B$, $(\overline{a})\phi_\alpha = \overline{a}^\alpha = \overline{a}$ i stoga: $(\epsilon, \overline{a}) \star (\alpha, \overline{e}) = (\alpha, \overline{e}) \star (\epsilon, \overline{a}) = (\alpha, \overline{a})$.

(*c*) Ako je $(\epsilon, \overline{a})$ u centru dijagonale (dakle, $a \in Z(\mathbf{A})$), imamo, za svako $g \in C$, $\overline{a} \cdot g = g \cdot \overline{a}$ $((\alpha)(\overline{a} \cdot g) = (\alpha)\overline{a} \cdot (\alpha)g = a \cdot (\alpha)g = (\alpha)g \cdot a = (\alpha)(g \cdot \overline{a}))$, pa je $(\alpha, g) \star (\epsilon, \overline{a}) = (\alpha, g \cdot \overline{a}) = (\alpha, \overline{a} \cdot g) = (\epsilon, \overline{a}) \star (\alpha, g)$ (upravo smo konstatovali: $\overline{a}^\alpha = \overline{a}$). Ali isto tako iz $f^\alpha = f$ za svako $\alpha \in B$, sledi da je $f$ konstanta. Pretpostavka: $(\alpha)f \neq (\beta)f$, za neke elemente $\alpha, \beta$, vodi u kontradikciju – $(\epsilon)f = (\epsilon)f^{\alpha^{-1}} = (\alpha)f \neq (\beta)f = (\epsilon)f^{\beta^{-1}} = (\epsilon)f$. Prema tome, ako je $(\alpha, f) \in Z(\mathbf{A}\ Wr\ \mathbf{B})$, iz $(\alpha, f) \star (\beta, \overline{e}) = (\beta, \overline{e}) \star (\alpha, f)$, tj. $(\alpha\beta, f^\beta) = (\beta\alpha, f)$, proizilazi da je $f$ konstanta i to, jasno, iz centra dijagonale ($f \equiv \overline{a}$ i $(\alpha, \overline{a}) \star (\epsilon, \overline{b}) = (\epsilon, \overline{b}) \star (\alpha, \overline{a})$ daju $\overline{a} \cdot \overline{b} = \overline{b}^\alpha \cdot \overline{a} = \overline{b} \cdot \overline{a}$). Konačno, $\alpha$ mora biti baš jedinični element; u suprotnom bi, za neko $g \in C$, bilo $g^\alpha \neq g$ ($\phi_\alpha \neq \imath_C$), te bi, ako je $b = (\beta)g \neq (\beta)g^\alpha = c$, iz $(\alpha, \overline{a}) \star (\epsilon, g) = (\epsilon, g) \star (\alpha, \overline{a})$ dobili $\overline{a} \cdot g = g^\alpha \cdot \overline{a}$ i odatle: $a \cdot b = (\beta)(\overline{a} \cdot g) = (\beta)(g^\alpha \cdot \overline{a}) = c \cdot a = a \cdot c$, kontradikcija.

U slučaju ograničenih spletenih proizvoda, ako je $\mathbf{B}$ beskonačna grupa i $\mathbf{A}$ nejedinična grupa, dijagonala sadrži, već smo rekli, samo jedinični element.

(*d*) Indukcijom se dokazuje da je za prirodan broj $k$:

$$(\alpha, f)^k = (\alpha^k, f^{\alpha^{k-1}} f^{\alpha^{k-2}} \cdots f^\alpha f),$$

i kako je, za $0 \leq r \leq m-1$:

$$f^{\alpha^{n(m-r)-1}} f^{\alpha^{n(m-r)-2}} \cdots f^{\alpha^{n(m-r)-(n-1)}} f^{\alpha^{n(m-r)-n}} = f^{\alpha^{-1}} f^{\alpha^{-2}} \cdots f^{\alpha^{-(n-1)}} f,$$

biće

$$(\alpha, f)^{mn} = ((\alpha^n)^m, (f^{\alpha^{-1}} f^{\alpha^{-2}} \cdots f^{\alpha^{-(n-1)}} f)^m) = (\epsilon, \overline{e});$$

ako je $\mathbf{A}$ eksponenta $m$, tada je $g^m = \overline{e}$ za svako $g$ ($\in C$), jer je $(\alpha)g^m = ((\alpha)g)^m = e$ za svako $\alpha \in B$.

(*e*) Neka je dat element $(\alpha, f) \in A\ wrB$, gde je $\alpha$ reda $p^m$ i neka je $g = f^{\alpha^{-1}} f^{\alpha^{-2}} \cdots f^{\alpha^{-(p^m-1)}} f$ i $S(f) = \{\beta \in B \mid (\beta)f \neq e\}$. Onda je $S(g) \subseteq S(f) \cup S(f)\alpha^{-1} \cup S(f)\alpha^{-2} \cup \ldots \cup S(f)\alpha^{-(p^m-1)}$ (koristimo: $S(f^\gamma) = S(f)\gamma$ (=



$\{\beta\gamma \mid \beta \in S(f)\})$), pa ako je $p^n = max\{red((\gamma)g) \mid \gamma \in S(g)\}$, tada je $(\alpha, f)^{p^{m+n}} = ((\alpha^{p^m})^{p^n}, g^{p^n}) = (\epsilon, \overline{e})$.

Kada je u pitanju drugi deo tvrđenja, pravac ($\Longleftarrow$) je već dokazan. Što se tiče drugog pravca, neka je $\mathbf{B}$ beskonačna grupa, a $\mathbf{A}$ bez (konačnog) eksponenta. Za beskonačan niz elemenata iz $B$, $\langle \alpha_n \mid n \in \omega \rangle$ neka je element $f \in \prod_{\beta \in B} A_\beta$ dat sa $(\alpha)f = \begin{cases} a_k & \alpha = \alpha_k \\ e & \text{inače} \end{cases}$, pri čemu je ispunjeno: $red(a_k) = p^{n_k}$ i $n_0 < n_1 < \cdots < n_k < \cdots$. Element $(\epsilon, f)$ je, evidentno, beskonačnog reda (za svako $k \in \omega$ i svako $l > k$ je $(\alpha_l)f^{p^k} \neq e$).□

**Primer 14.4** (*a*) *Grupa* $\mathbf{C}_p\ wr\ \mathbf{p}^\infty$ *je beskonačna p-grupa bez centra.*

**Dokaz.** Direktno, na osnovu tačaka (*c*) i (*e*) prethodne leme.

(*b*) $\mathbf{C}_2\ Wr\ \mathbf{C}_2 \cong \mathbf{D}_4$.

**Dokaz.** Neka su date ciklične grupe $\mathbf{A} = \langle \{e, a\}, \cdot \rangle$ i $\mathbf{B} = \langle \{\epsilon, \beta\}, \cdot \rangle$ i neka su elementi grupe $\mathbf{C} = \mathbf{A}_\epsilon \times \mathbf{A}_\beta$ ($\mathbf{A} = \mathbf{A}_\epsilon = \mathbf{A}_\beta$): $\overline{e} = (e, e)$, $f = (e, a)$, $g = (a, e)$ i $h = (a, a)$. Za $(\beta)\Phi = \phi_\beta$ imamo: $(\overline{e})\phi_\beta = \overline{e}$, $(f)\phi_\beta = f^\beta = g$, $(g)\phi_\beta = g^\beta = f$ i $(h)\phi_\beta = h^\beta = h$. Element $(\beta, f)$ grupe $\mathbf{A}\ Wr\ \mathbf{B}$ je reda 4: $(\beta, f)^2 = (\beta^2, f^\beta f) = (\epsilon, g \cdot f) = (\epsilon, h)$, a $(\epsilon, h)^2 = (\epsilon^2, h^2) = (\epsilon, e)$ (uzgred, $(\beta, f)^3 = (\beta, g)$). Pored toga je, za element $(\epsilon, g)$ reda 2: $(\epsilon, g) \star (\beta, f) = (\beta, f)^3 \star (\epsilon, g)$ $(= (\beta, e))$.

(*c*) $\mathbf{C}_3\ Wr\ \mathbf{C}_2 \cong \mathbf{C}_3 \times \mathbf{S}_3$.

**Dokaz.** Neka su date ciklične grupe $\mathbf{A} = \langle \{e, a, a^2\}, \cdot \rangle$ i $\mathbf{B} = \langle \{\epsilon, \beta\}, \cdot \rangle$. Generatorni elementi grupe $\mathbf{C} = \mathbf{A}_\epsilon \times \mathbf{A}_\beta$ su $f = (e, a)$ i $g = (a, e)$, a grupe $\mathbf{A}\ Wr\ \mathbf{B}$ $(\epsilon, f)$, $(\epsilon, g)$ i $(\beta, \overline{e})$. Opet je, kao u prethodnom slučaju, $(x, y)\phi_\beta = (y, x)$ $(x, y \in A)$, posebno $(f)\phi_\beta = f^\beta = g$ i $(g)\phi_\beta = g^\beta = f$. Element $(\epsilon, f \cdot g)$ je reda 3 i ciklična grupa njime generisana je normalna podgrupa grupe $\mathbf{A}\ Wr\ \mathbf{B}$; permutabilnost elementa $(\epsilon, f \cdot g)$ sa $(\epsilon, f)$ i $(\epsilon, g)$ je evidentna, a i $(\beta, \overline{e}) \star (\epsilon, f \cdot g) = (\epsilon, f \cdot g) \star (\beta, \overline{e})$ $(= (\beta, f \cdot g))$. Dalje, očigledno je element $(\epsilon, f^2 \cdot g)$ reda 3, $(\beta, \overline{e})$ reda 2 i osim toga je $(\beta, \overline{e}) \star (\epsilon, f^2 \cdot g) = (\epsilon, f^2 \cdot g)^2 \star (\beta, \overline{e}) = (\beta, f^2 \cdot g)$, pa je podgrupa generisana tim elementima dijedarska grupa stepena 3, tj. simetrična grupa $\mathbf{S}_3$. To je i normalna podgrupa grupe $\mathbf{A}\ Wr\ \mathbf{B}$, jer je $(\epsilon, f^2) \star (\beta, \overline{e}) \star (\epsilon, f) = (\beta, f \cdot g^2)$ (i isto tako: $(\epsilon, g^2) \star (\beta, \overline{e}) \star (\epsilon, g) = (\beta, f^2 \cdot g)$). Kako je presek podgrupa $\langle (\epsilon, f \cdot g) \rangle$ i $\langle (\epsilon, f^2 \cdot g), (\beta, \overline{e}) \rangle$ jedinična grupa, zaključujemo: $\mathbf{A}\ Wr\ \mathbf{B} = \langle (\epsilon, f \cdot g) \rangle \times \langle (\epsilon, f^2 \cdot g), (\beta, \overline{e}) \rangle$.□

**Teorema 14.5** *(B. H. Neuman, H. Neuman). Ako je* $\mathbf{B}$ *beskonačna ciklična grupa ili konačna ciklična grupa čiji je red deljiv eksponentom grupe* $\mathbf{A}$*, onda izvodna podgrupa grupe* $\mathbf{A}\ Wr\ \mathbf{B}$ *sadrži podgrupu izomorfnu sa* $\mathbf{A}$.

**Dokaz.** Dijagonala grupe $\mathbf{A}\ Wr\ \mathbf{B}$ – $\overline{\mathbf{A}}$, izomorfna je grupi $\mathbf{A}$, a pokazaćemo i da je svaki njen element komutator. Neka je $\beta$ generatorni element (ciklične)

grupe $\mathbf{B}$ i za $a \in A$ neka je $f_a \in C = \prod A_{\beta^k}$ dato sa: $(\beta^k)f_a = a^{-k}$ za svaki ceo broj $k$. Tada je: $[(\epsilon, f_a), (\beta, \overline{e})] = (\epsilon, f_a^{-1} \cdot f_a^{\beta})$, dok je, pod navedenim uslovima, $f_a^{-1} \cdot f_a^{\beta} = \overline{a}$. Ako je $\mathbf{B}$ beskonačna ciklična grupa, imamo za svaki ceo broj $k$: $(\beta^k)(f_a^{-1} \cdot f_a^{\beta}) = ((\beta^k)f_a)^{-1} \cdot (\beta^k)f_a^{\beta} = (a^{-k})^{-1} \cdot (\beta^{k-1})f_a = a^k \cdot a^{1-k} = a$; ako je pak grupa $\mathbf{A}$ konačnog eksponenta $m$ i $|B| = n = km$, imamo: $(\epsilon)(f_a^{-1} \cdot f_a^{\beta}) = ((\epsilon)f_a)^{-1} \cdot (\epsilon)f_a^{\beta} = e \cdot (\beta^{-1})f_a = (\beta^{n-1})f_a = a^{1-n} = a$ i uopšte, za $0 < r \leq n-1$, $(\beta^r)(f_a^{-1} \cdot f_a^{\beta}) = ((\beta^r)f_a)^{-1} \cdot (\beta^{r-1})f_a = a^r \cdot a^{1-r} = a$.

Vidimo da u slučaju kada je $\mathbf{B}$ konačna ciklična grupa reda $n$, uslov $f_a^{-1} \cdot f_a^{\beta} = \overline{a}$ implicira da je $\mathbf{A}$ konačnog eksponenta koji deli $n$; iz $(\epsilon)(f_a^{-1} \cdot f_a^{\beta}) = e \cdot (\beta^{-1})f_a = a = (\beta^{n-1})f_a = a^{1-n}$ sledi $a^n = e$.■

**Korolar 14.6** *Svaka prebrojiva grupa* $\mathbf{A}$ *se može utopiti u dvoelementno generisanu grupu.*

**Dokaz.** Prema prethodnoj teoremi, za pogodno izabranu cikličnu grupu $\mathbf{B}$, dijagonala $\overline{\mathbf{A}}$ grupe $\mathbf{A}\ Wr\ \mathbf{B}$, izomorfna grupi $\mathbf{A}$, sadržana je u izvodnoj podgrupi. Ako je, s notacijom iz prethodne teoreme, $\overline{\mathbf{H}} = \langle \{(\epsilon, f_a) \mid a \in A\} \cup \{(\beta, e) \mid \beta \in B\} \rangle$, onda je $\overline{\mathbf{A}} \leq \overline{\mathbf{H}}'$, $\overline{\mathbf{H}}$ je prebrojiva grupa i, prema 12.17, $\overline{\mathbf{H}}'$ se može utopiti u neku dvoelementno generisanu grupu.□

**Definicija 14.7** *Element* $g$ *grupe* $\mathbf{G} = \langle G, \cdot \rangle$ *je deljiv sa pozitivnim prirodnim brojem* $n$ *akko jednačina* $g = x^n$ *ima rešenje u* $\mathbf{G}$, *tj. akko je* $g$ $n$*-ti stepen nekog elementa iz* $\mathbf{G}$.

*Grupa* $\mathbf{G}$ *je deljiva akko je svaki njen element deljiv svim pozitivnim prirodnim brojevima.*

**Lema 14.8** *U grupi* $\mathbf{A}\ Wr\ \mathbf{C}_n$ *svaki element podgrupe* $\overline{\mathbf{A}}$ *je deljiv sa* $n$.

**Dokaz.** Neka je $\mathbf{C}_n = \mathbf{B} = \langle \beta \rangle$, a za $a \in A$ neka je $g_a \in A_\epsilon \times A_\beta \times \cdots \times A_{\beta^{n-1}}$ definisano sa: $(\beta^k)g_a = \begin{cases} a & k = 0 \\ e & 0 < k \leq n-1 \end{cases}$. Odatle je, za $0 < k, r \leq n-1$, $(\beta^k)g_a^{\beta^r} = (\beta^{k+_n(n-r)})g_a = \begin{cases} a & k = r \\ e & \text{inače} \end{cases}$, pa su elementi $g_a = g_a^{\beta^0}$, $g_a^{\beta}$, $\ldots$, $g_a^{\beta^{n-1}}$ uzajamno permutabilni, a važi i $\prod_{i=0}^{n-1} g_a^{\beta^i} = \overline{a}$. Konačno, već smo videli u dokazu tačke $(d)$ leme 14.3 da je $(\beta, g_a)^n = (\beta^n, \prod_{i=0}^{n-1} g_a^{\beta^i})$, odnosno, u ovom slučaju, $(\beta, g_a)^n = (\epsilon, \overline{a})$.□

**Teorema 14.9** *Svaka grupa* $\mathbf{A}$ *se može utopiti u deljivu grupu.*

**Dokaz.** Definišimo rekurzivno: $\mathbf{A}_1 = \mathbf{A}$, $\mathbf{A}_2 = \mathbf{A}_1\ Wr\ \mathbf{C}_2$, $\mathbf{A}_3 = \mathbf{A}_2\ Wr\ \mathbf{C}_3$, $\ldots$, $\mathbf{A}_{n+1} = \mathbf{A}_n\ Wr\ \mathbf{C}_{n+1}, \ldots$. Neka je, dalje, $\varphi_{k,k+1}$ "standardno" utapanje grupe $\mathbf{A}_k$ u grupu $\mathbf{A}_{k+1}$ $((a)\varphi_{k,k+1} \stackrel{\text{def}}{=} (\epsilon, \overline{a}))$ i generalno, za $i < j$, $\varphi_{ij} = \varphi_{i,i+1} \circ \varphi_{i+1,i+2} \circ \cdots \circ \varphi_{j-1,j}$, a za svako $k$, $\varphi_{kk}$ identično preslikavanje – jedinični



automorfizam grupe $\mathbf{A}_k$. Tada je $\langle \langle N, \leq \rangle, \{\mathbf{A}_k \mid k \in N\}, \{\varphi_{ij} \mid i \leq j\} \rangle$ usmerena familija grupa, dok je usmereni limit koju ona generiše deljiva grupa. Jer, ako je $[a] \in A_\infty$, $n$ ma koji prirodan broj veći od 1, $a \in A_k$ i $m$ ma koji prirodan broj (možemo uzeti baš najmanji) za koji je $m \cdot n > k$, onda je, prema 14.8, element $(a)\varphi_{k,mn} = ((a)\varphi_{k,mn-1})\varphi_{mn-1,mn}$ $(\in A_{mn-1}\ Wr\ \mathbf{C}_{mn} = A_{mn})$ deljiv sa $mn$ u grupi $\mathbf{A}_{mn}$, pa sledi, za neko $b \in A_{mn}$: $[a] = [(a)\varphi_{k,mn}] = [b^{mn}] = [b^m]^n$.■

**Teorema 14.10** *Ako je* $\mathbf{A}$ *normalna podgrupa grupe* $\mathbf{B}$, *onda je* $\mathbf{B}$ *izomorfna podgrupi grupe* $\mathbf{A}\ Wr\ (\mathbf{B}/\mathbf{A})$.

**Dokaz.** Neka je $B/A = \{b_\alpha A \mid \alpha < \lambda\ (= |B/A|)\}$ – fiksirali smo jednu transverzalu podgrupe $\mathbf{A}$. Koset $b_\alpha A$ označavaćemo kraće sa $\overline{b}_\alpha$, i uopšte biće: $bA = \overline{b}$. Neka je dalje $\varphi : B \longrightarrow B/A$ kanoničko homomorfno preslikavanje grupe $\mathbf{B}$ na faktor grupu $\mathbf{B}/\mathbf{A}$, a preslikavanje $\psi : B/A \longrightarrow B$ neka je definisano sa $(\overline{b}_\alpha)\psi = b_\alpha$ ($\psi$ nije homomorfizam). Za $b \in B$ je, jasno, $(b)(\varphi \circ \psi) = (bA)\psi = b_\alpha$, gde je $bA = b_\alpha A$; posebno, $(b\overline{b}^{-1})\psi \in A$. Konačno, za $b \in B$, neka je $f_b \in \prod_{\overline{b}_\alpha \in B/A} A_{\overline{b}_\alpha}$ dato sa: $(\overline{b}_\alpha)f_b = (\overline{b}_\alpha \cdot \overline{b}^{-1})\psi \cdot b \cdot b_\alpha^{-1}$ $(\in A)$ (ako je $\overline{b}_\alpha \cdot \overline{b}^{-1} = \overline{b}_\beta$, tj. ako je, za neko $a \in A$, $b_\beta = ab_\alpha b^{-1}$, onda je $(\overline{b}_\alpha)f_b = b_\beta b b_\alpha^{-1} = ab_\alpha b^{-1} b b_\alpha^{-1} = a$). Sada je preslikavanje: $\theta : B \longrightarrow A\ Wr\ (B/A)$ dato sa $(b)\theta = (\overline{b}, f_b)$ izomorfno preslikavanje grupe $\mathbf{B}$ u grupu $\mathbf{A}\ Wr\ (\mathbf{B}/\mathbf{A})$. Prvo, injektivno je; jer ako je, za $b, c \in B$, $(\overline{b}, f_b) = (\overline{c}, f_c)$, tada je $\overline{b} = \overline{c}$, što sa $f_b = f_c$ implicira $b = c$ – iz $(\overline{b}_\alpha \overline{b}^{-1})\psi \cdot b \cdot b_\alpha^{-1} = (\overline{b}_\alpha)f_b = (\overline{b}_\alpha)f_c = (\overline{b}_\alpha \overline{c}^{-1})\psi \cdot c \cdot b_\alpha^{-1}$ se, nakon kancelacije, dobija $b = c$. Homomorfnost preslikavanja $\theta$ proizilazi pak iz relacije $f_{bc} = f_b^{\overline{c}} \cdot f_c$; zaista:

$$(\overline{b}_\alpha)f_{bc} = (\overline{b}_\alpha \overline{bc}^{-1})\psi \cdot bc \cdot b_\alpha^{-1} = ((\overline{b_\alpha c^{-1} \overline{b}^{-1}})\psi \cdot b \cdot ((\overline{b_\alpha c^{-1}})\psi)^{-1}) \cdot (\overline{b_\alpha c^{-1}})\psi \cdot c \cdot b_\alpha^{-1} =$$

$$(\overline{b}_\alpha \overline{c}^{-1})f_b \cdot (\overline{b}_\alpha)f_c = (\overline{b}_\alpha)f_b^{\overline{c}} \cdot (\overline{b}_\alpha)f_c = (\overline{b}_\alpha)(f_b^{\overline{c}} \cdot f_c).\blacksquare$$

# 15 Transfer

Neka je $\mathbf{H}$ podgrupa konačnog indeksa $n$ grupe $\mathbf{G}$ i neka je $\{g_0, \ldots, g_{n-1}\}$ jedna leva transverzala podgrupe $\mathbf{H}$. Tada, jasno, za svako $a \in G$ i svako $i \in n\ (= \{0, \ldots, n-1\})$, postoje jedinstven element $h_i \in H$ i jedinstven indeks $(i)\varphi \in n$, takvi da je

$$ag_i = g_{(i)\varphi}h_i \qquad (*).$$

Za fiksno $a \in G$, funkcija $\varphi$ je permutacija skupa $n$. Dovoljno je, naravno, pokazati da je $\varphi$ injektivna funkcija. Neka je $(i)\varphi = (j)\varphi$. Tada iz $ag_i = g_{(i)\varphi}h_i$ i $ag_j = g_{(j)\varphi}h_j$ sledi: $g_i^{-1}g_j = (ag_i)^{-1}ag_j = h_i^{-1}g_{(i)\varphi}^{-1}g_{(j)\varphi}h_j = h_i^{-1}h_j \in H$, tj. $g_iH = g_jH$, pa je $i = j$.

Ako je i $\{g'_0, \dots, g'_{n-1}\}$ leva transverzala podgrupe $\mathbf{H}$ i $ag'_i = g'_{(i)\psi}h'_i$, onda važi: $(h_0 \dots h_{n-1})H' = (h'_0 \dots h'_{n-1})H'$. Jer, ako je za $i = 0, \dots, n-1$, $g'_i = g_{(i)\theta}h''_i$ (i odatle: $g'_{(i)(\theta\varphi\theta^{-1})} = g_{(i)(\theta\varphi)}h''_{(i)(\theta\varphi\theta^{-1})}$), onda je

$$g'_{(i)\psi}h'_i = ag'_i = ag_{(i)\theta}h''_i = g_{((i)\theta)\varphi}h_{(i)\theta}h''_i = g'_{(i)(\theta\varphi\theta^{-1})}(h''_{(i)(\theta\varphi\theta^{-1})})^{-1}h_{(i)\theta}h''_i,$$

te je $\theta\varphi\theta^{-1} = \psi$, $h'_i = (h''_{(i)\psi})^{-1}h_{(i)\theta}h''_i$ i stoga (pošto je $\mathbf{H}/\mathbf{H}'$ Abelova grupa i $\psi, \theta \in S_n$):

$$(h'_0 \dots h'_{n-1})H' = (\prod_{i=0}^{n-1} h'_i)H' = (\prod_{i=0}^{n-1}(h''_{(i)\psi})^{-1}h_{(i)\theta}h''_i)H' =$$

$$(\prod_{i=0}^{n-1}(h''_i)^{-1})H' \cdot (\prod_{i=0}^{n-1} h''_i)H' \cdot (\prod_{i=0}^{n-1} h_i)H' = (\prod_{i=0}^{n-1} h_i)H'.$$

Proizilazi da je $\Phi_t : G \longrightarrow H/H'$ dato sa $(a)\Phi_t = (h_0 \dots h_{n-1})H'$ dobro definisano preslikavanje (funkcija), tzv. *transfer* grupe $\mathbf{G}$ u $\mathbf{H}$. Štaviše, sa usvojenim pretpostavkama i notacijom, važi

**Lema 15.1** *$\Phi_t$ je homomorfno preslikavanje grupe $\mathbf{G}$ u faktor grupu $\mathbf{H}/\mathbf{H}'$.*

**Dokaz.** U pitanju je samo homomorfnost preslikavanja $\Phi_t$. Neka je, za $b \in G$, $bg_i = g_{(i)\psi}h'_i$; za $a$ $(\in G)$ ostaje na snazi $(*)$. Onda je $(ab)g_i = a(bg_i) = (ag_{(i)\psi})h'_i = g_{(i)(\psi\varphi)}h_{(i)\psi}h'_i$, pa je

$$(ab)\Phi_t = (\prod_{i=0}^{n-1} h_{(i)\psi}h'_i)H' = (\prod_{i=0}^{n-1} h_{(i)\psi})H' \cdot (\prod_{i=0}^{n-1} h'_i)H' = (a)\Phi_t \cdot (b)\Phi_t$$

(ponovo smo koristili komutativnost grupe $\mathbf{H}/\mathbf{H}'$).□

**Napomena.** Ako je $\mathbf{H}$ Abelova grupa (odnosno $\mathbf{H}' = \mathbf{E}$), $\Phi_t$ možemo smatrati homomorfnim preslikavanjem grupe $\mathbf{G}$ u $\mathbf{H}$. Jasno, $\mathbf{Ker}(\Phi_t) \geq \mathbf{G}'$ $(\mathbf{G}/\mathbf{Ker}(\Phi_t) \cong (\mathbf{G})\Phi_t \leq \mathbf{H}/\mathbf{H}'$, dakle $\mathbf{G}/\mathbf{Ker}(\Phi_t)$ je Abelova grupa). Odatle je preslikavanje $\Phi_t^* : G/G' \longrightarrow H/H'$ dato sa $(gG')\Phi_t^* = (g)\Phi_t$ homomorfno preslikavanje (kompozicija homomorfnih preslikavanja $G/G' \longrightarrow G/Ker(\Phi_t) \longrightarrow (G)\Phi_t$).

**Lema 15.2** *Neka su $\mathbf{H}$ i $\mathbf{K}$ podgrupe konačnog indeksa grupe $\mathbf{G}$, neka je $\mathbf{K}$ podgrupa grupe $\mathbf{H}$ i neka je $\Phi_t$ transfer grupe $\mathbf{G}$ u $\mathbf{H}$, $\Psi_t$ transfer grupe $\mathbf{G}$ u $\mathbf{K}$ i $\Theta_t$ transfer grupe $\mathbf{H}$ u $\mathbf{K}$. Tada je $\Psi_t^* = \Phi_t^* \circ \Theta_t^*$.*

**Dokaz.** Promenićemo malo oznake. Neka je $[\mathbf{G} : \mathbf{H}] = m$, $[\mathbf{H} : \mathbf{K}] = n$ i neka je $\{b_0, \dots, b_{m-1}\}$ leva transverzala podgrupe $\mathbf{H}$, $\{c_0, \dots, c_{n-1}\}$ leva transverzala podgrupe $\mathbf{K}$ u $\mathbf{H}$. Onda je $\{b_ic_j \mid 0 \leq i \leq m-1, 0 \leq j \leq n-1\}$ leva transverzala podgrupe $\mathbf{K}$ (u $\mathbf{G}$). Neka je dalje, za $a \in G$, $ab_i = b_{(i)\varphi}h_i$ i za svako $i$, $i = 0, \dots, m-1$, $h_ic_j = c_{(j)\psi_i}k_{i,j}$. Tada je $a(b_ic_j) = (ab_i)c_j = b_{(i)\varphi}(h_ic_j) = b_{(i)\varphi}c_{(j)\psi_i}k_{i,j}$, $(aG')\Psi_t^* = (a)\Psi_t = (\prod_{i,j} k_{i,j})K'$, a i $(a)(\Phi_t^* \circ \Theta_t^*) = ((a)\Phi_t^*)\Theta_t^* = ((\prod_{i=0}^{m-1} h_i)H')\Theta_t^* = \prod_{i=0}^{m-1}(h_iH')\Theta_t^* = \prod_{i=0}^{m-1}(\prod_{j=0}^{n-1} k_{i,j}K') = (\prod_{i,j} k_{i,j})K'$.□



**Teorema 15.3** *Neka je $\{g_0, \dots, g_{n-1}\}$ leva transverzala podgrupe $\mathbf{H}$ konačnog indeksa $n$ grupe $\mathbf{G}$, $a \in G$ i neka je $\Phi_t$ transfer grupe $\mathbf{G}$ u $\mathbf{H}$. Tada postoje podskup $\{i_0, \dots, i_{r-1}\}$ skupa $n$ i skup pozitivnih prirodnih brojeva $n_t$, $t = 0, \dots, r-1$, takvi da važi: $(a)\Phi_t = (\prod_{t=0}^{r-1} g_{i_t}^{-1}a^{n_t}g_{i_t})H'$, $\sum_{t=0}^{r-1} n_t = n$ $(= [\mathbf{G} : \mathbf{H}])$ i $n_t$ je najmanji među pozitivnim prirodnim brojevima $(u)$ za koje je $g_{i_t}^{-1}a^u g_{i_t} \in H$.*

**Dokaz.** Neka je, kao i dosad, $ag_i = g_{(i)\varphi}h_i$ i neka je $(j_0 \dots j_{k-1})$ jedan ciklus koji se javlja u razlaganju permutacije $\varphi$ (skupa $n$) u proizvod disjunktnih ciklusa. Onda je, za $l = 0, \dots, k-1$, $ag_{j_l} = g_{j_l+_k1}h_{j_l}$ i odatle:

$$h_{j_{k-1}}h_{j_{k-2}} \dots h_{j_1}h_{j_0} = g_{j_0}^{-1}ag_{j_{k-1}} \cdot g_{j_{k-1}}^{-1}ag_{j_{k-2}} \cdot \dots \cdot g_{j_2}^{-1}ag_{j_1} \cdot g_{j_1}^{-1}ag_{j_0} =$$

$$g_{j_0}^{-1}a^k g_{j_0} \in H.$$

Za $0 < s < k-1$ je pak:

$$h_{j_s}h_{j_{s-1}} \dots h_{j_1}h_{j_0} = g_{j_{s+1}}^{-1}ag_{j_s} \cdot g_{j_s}^{-1}ag_{j_{s-1}} \cdot \dots \cdot g_{j_2}^{-1}ag_{j_1} \cdot g_{j_1}^{-1}ag_{j_0} = g_{j_{s+1}}^{-1}a^{s+1}g_{j_0} =$$

$$g_{j_{s+1}}^{-1}g_{j_0} \cdot g_{j_0}^{-1}a^{s+1}g_{j_0}$$

pa $g_{j_0}^{-1}a^{s+1}g_{j_0} = g_{j_0}^{-1}g_{j_{s+1}}(h_{j_s} \dots h_{j_0}) \notin H$; znači, $k$ je najmanji među pozitivnim prirodnim brojevima $m$ za koje je $g_{j_0}^{-1}a^m g_{j_0} \in H$. Zaključujemo: $r$ je broj disjunktnih ciklusa permutacije $\varphi$, a $n_t$ i $i_t$, $t = 0, \dots, r-1$, dužina (moguće 1), odnosno indeks prvog člana odgovarajućeg ciklusa; zbog komutativnosti grupe $\mathbf{H}/\mathbf{H}'$ važi $(a)\Phi_t = (\prod_{t=0}^{r-1}(g_{i_t}^{-1}a^{n_t}g_{i_t}))H'$.■

**Lema 15.4** *Neka su $\mathbf{H}$ i $\mathbf{K}$ podgrupe grupe $\mathbf{G}$, $[\mathbf{G} : \mathbf{H}] = n$ i $\Phi_t$ transfer grupe $\mathbf{G}$ u $\mathbf{H}$. Onda važi:*

*(a) Ako je $G = HK$ $(= KH)$ i $\mathbf{H} \cap \mathbf{K} = \mathbf{E}$, tada je $\mathbf{K} \leq \mathbf{Ker}(\Phi_t)$;*

*(b) Ako je $G = HK$, $\mathbf{H} \leq \mathbf{C}(\mathbf{K})$ i $a \in G$, tada je $(a)\Phi_t = a^nH'$;*

*(c) Ako je $\mathbf{H} \leq \mathbf{Z}(\mathbf{G})$, tada je $(a)\Phi_t = a^n$ za svako $a \in G$;*

*(d) Ako je $\mathbf{H}$ Hallova podgrupa sadržana u centru grupe $\mathbf{G}$, tada je $\mathbf{G} = \mathbf{H} \times \mathbf{Ker}(\Phi_t)$.*

**Dokaz.** *(a)* Neka je $\{k_0, \dots, k_{n-1}\}$ leva transverzala podgrupe $\mathbf{H}$, gde je $k_i \in K$ za svako $i = 0, \dots, n-1$ (takav izbor je moguć zbog uslova $G = HK$). Ako je, za $k \in K$ i $i = 0, \dots, n-1$, $kk_i = k_{(i)\varphi}h_i$, onda je $h_i \in H \cap K = \{e\}$, pa je $(k)\Phi_t = H'$ i $\mathbf{K} \leq \mathbf{Ker}(\Phi_t)$.

*(b)* Neka je i dalje $\{k_0, \dots, k_{n-1}\}$ leva transverzala podgrupe $\mathbf{H}$ i neka je, za $a \in G$, $ak_i = k_{(i)\varphi}h_i$. Kao i u prethodnoj teoremi, neka je $(j_0 \dots j_{t-1})$ jedan ciklus permutacije $\varphi$. Zbog $\mathbf{H} \leq \mathbf{C}(\mathbf{K})$, iz $ak_{j_s} = k_{j_s+_t1}h_{j_s}$, $0 \leq s \leq t-1$, sledi $a = k_{j_s+_t1}k_{j_s}^{-1}h_{j_s}$ i odatle:

$$a^t = k_{j_0}k_{j_{t-1}}^{-1}h_{j_{t-1}} \cdot k_{j_{t-1}}k_{j_{t-2}}^{-1}h_{j_{t-2}} \cdot \dots \cdot k_{j_2}k_{j_1}^{-1}h_{j_1} \cdot k_{j_1}k_{j_0}^{-1}h_{j_0} =$$

$(k_{j_0}k_{j_{t-1}}^{-1}\cdot k_{j_{t-1}}k_{j_{t-2}}^{-1}\cdot\ldots\cdot k_{j_2}k_{j_1}^{-1}\cdot k_{j_1}k_{j_0}^{-1})h_{j_{t-1}}h_{j_{t-2}}\ldots h_{j_1}h_{j_0} = h_{j_{t-1}}h_{j_{t-2}}\ldots h_{j_1}h_{j_0}$.
Permutabilnost grupe $\mathbf{H}/\mathbf{H}'$ daje konačno:

$$(a)\Phi_t = (\prod_{i=0}^{n} h_i)H' = a^n H'.$$

(*c*) Direktna posledica prethodne tačke ($\mathbf{H} \leq \mathbf{Z(G)} \leq \mathbf{C(K)}$). Sada je i $\mathbf{H}' = \mathbf{E}$, te $\Phi_t$ tretiramo, shodno dogovoru, kao homomorfno preslikavanje grupe $\mathbf{G}$ u podgrupu $\mathbf{H}$.

(*d*) Neka je $|H| = m$ (dakle, $(m,n) = 1$). Prema prethodnoj tački je $(a)\Phi_t = a^n$ za svako $a \in G$. Ako je $a \in Ker(\Phi_t)$, tj. $a^n = e$ i $a \neq e$, onda $a \notin H$; u suprotnom, ako je za cele brojeve $u$ i $v$ $um + vn = 1$, imali bismo: $a = a^{um+vn} = (a^m)^u(a^n)^v = e$, kontradikcija. Takođe je, za svako $b \in G$, $b^m \in Ker(\Phi_t)$ jer je $(b^m)\Phi_t = b^{mn} = e$, i stoga je $b = (b^n)^v(b^m)^u \in H\,Ker(\Phi_t)$. Prema tome: $\mathbf{G} = \mathbf{H} \times \mathbf{Ker}(\Phi_t)$ ($\mathbf{H} \lhd \mathbf{G}$ jer $\mathbf{H} \leq \mathbf{Z(G)}$).□

Naredno tvrđenje smo već ranije dokazali (6.5).

**Korolar 15.5** *(Schur). Ako je centar grupe konačnog indeksa $n$, onda je $\mathbf{G}'$ konačna grupa i $(\mathbf{G}')^n = \mathbf{E}$.*

**Dokaz**. Prema prethodnoj lemi, preslikavanje $g \longrightarrow g^n$ je transfer, $\Phi_t$, grupe $\mathbf{G}$ u $\mathbf{Z(G)}$, pa je $\mathbf{G}' \leq \mathbf{Ker}(\Phi_t)$ i stoga $(\mathbf{G}')^n$ $(= \{\{g^n \mid g \in G'\}\}) = \mathbf{E}$. Dalje, neka je $\{g_0, \ldots, g_{n-1}\}$ leva transverzala centra grupe $\mathbf{Z(G)}$. Ako su $g_i a$ i $g_j b$, $a, b \in Z(\mathbf{G})$, dva elementa grupe onda je prema 6.2(*d*),(*e*):

$$[g_i a, g_j b] = a^{-1}[g_i, g_j b]a[a, g_j b] = [g_i, g_j b] = [g_i, b]b^{-1}[g_i, g_j]b = [g_i, g_j],$$

što će reći da je izvodna grupa $\mathbf{G}'$ generisana konačnim skupom (kardinalnosti $\binom{n}{2}$) $\{[g_i, g_j] \mid 0 \leq i < j \leq n-1\}$. Kako je $\mathbf{G}'/(\mathbf{G}' \cap \mathbf{Z(G)})$ $(\cong (\mathbf{G}'\mathbf{Z(G)})/\mathbf{Z(G)} \leq \mathbf{G}/\mathbf{Z(G)})$ konačna grupa, proizilazi da je i $\mathbf{G}' \cap \mathbf{Z(G)}$ konačno generisana grupa (9.39), a kao Abelova je i konačna (32.2). Odatle je i $\mathbf{G}'$ konačna grupa.□

**Korolar 15.6** *(B. H. Neumann). Ako je $\mathbf{G}$ $FC$-grupa, tada je skup svih njenih elemenata konačnog reda domen potpuno invarijantne podgrupe koja sadrži izvodnu podgrupu $\mathbf{G}'$.*

**Dokaz**. $\mathbf{G}/\mathbf{Z(G)}$ je, prema 5.18 i 5.20, lokalno konačna (i normalna) grupa. Neka je $\mathbf{H}$ konačno generisana podgrupa grupe $\mathbf{G}$. Tada je $\mathbf{H}/(\mathbf{H} \cap \mathbf{Z(G)})$ $(\cong (\mathbf{HZ(G)})/\mathbf{Z(G)})$ konačna grupa, te je i $\mathbf{H}/\mathbf{Z(H)}$ konačna grupa (jasno, $\mathbf{H} \cap \mathbf{Z(G)} \leq \mathbf{Z(H)}$). Prema prethodnom korolaru je $\mathbf{H}'$ konačna grupa, pa je $\mathbf{G}'$ periodična grupa. Neka su, dalje, $a$ i $b$ elementi konačnih redova, respektivno, $m$ i $n$. Kako je $\mathbf{G}/\mathbf{G}'$ Abelova grupa, to je $(ab^{-1})^{mn}G' = G'$, tj. $(ab^{-1})^{mn} \in G'$. Stoga je $(ab^{-1})^{mn}$, a onda i $ab^{-1}$, element konačnog reda, što će reći da je skup elemenata konačnog reda domen podgrupe i to, očigledno, potpuno invarijantne.□



**Korolar 15.7** *Grupa je $FC$-grupa akko je podgrupa direktnog proizvoda torziono slobodne Abelove i lokalno konačne i normalne grupe.*

**Dokaz**. Neka je $\mathbf{G}$ $FC$-grupa i $t\mathbf{G}$ njena podgrupa čiji je domen skup svih elemenata konačnog reda (tzv. periodični deo grupe $\mathbf{G}$ – o ovom terminu će biti reči i u uvodnom delu poglavlja o Abelovim grupama). Pošto je $\mathbf{G}' \leq t\mathbf{G}$, $\mathbf{G}/t\mathbf{G}$ je torziono slobodna Abelova grupa. Neka je $\mathbf{H}$ maksimalna torziono slobodna podgrupa centra grupe (čiju egzistenciju, ukoliko već centar nije torziono slobodna grupa, garantuje Zornova lema). Kako su i $\mathbf{Z(G)}/\mathbf{H}$ i $\mathbf{G}/\mathbf{Z(G)}$ periodične grupe (u slučaju prve faktor grupe to je posledica maksimalnosti podgrupe $\mathbf{H}$, u slučaju druge pozivamo se na 5.20), proizilazi da je i $\mathbf{G}/\mathbf{H}$ periodična grupa (imamo u vidu treću teoremu o izomorfizmu: $\mathbf{G}/\mathbf{Z(G)} \cong (\mathbf{G}/\mathbf{H})/(\mathbf{Z(G)}/\mathbf{H})$). Kao homomorfna slika $FC$-grupe, $\mathbf{G}/\mathbf{H}$ je takođe $FC$-grupa, dakle, prema 5.18, i lokalno konačna i normalna grupa. Konačno, s obzirom da je $t\mathbf{G} \cap \mathbf{H} = \mathbf{E}$, grupa $\mathbf{G}$ se utapa u direktni proizvod $\mathbf{G}/t\mathbf{G} \times \mathbf{G}/\mathbf{H}$ (10.15).

Obrat je direktna posledica korolara 5.18 i (vrlo) očiglednih činjenica da je direktni proizvod $FC$-grupa $FC$-grupa kao i da je podgrupa $FC$-grupe $FC$-grupa.□

**Definicija 15.8** *Grupa je $BFC$-grupa akko postoji pozitivan prirodan broj $m$ takav da je broj konjugata bilo kog (njenog) elementa manji od ili jednak $m$.*

**Korolar 15.9** *(B. H. Neumann). Grupa $\mathbf{G}$ je $BFC$-grupa akko je $\mathbf{G}'$ konačna grupa.*

**Dokaz**. Neka je $|G'| = m$ i $a \in G$. Onda je $|\{[a,g] \mid g \in G\}| \leq m$, pa je i broj konjugata elementa $a$ manji od ili jednak $m$.

Pretpostavimo sada da je $\mathbf{G}$ $BFC$-grupa i neka je $m = max\{[\mathbf{G} : \mathbf{C}(g)] \mid g \in G\}$. Recimo da je za element $a$ baš $[\mathbf{G} : \mathbf{C}(a)] = m$. Ako je $\{b_1, \ldots, b_m\}$ desna transverzala centralizatora elementa $a$, onda su $b_1^{-1}ab_1, \ldots, b_m^{-1}ab_m$ svi konjugati elementa $a$. Prema 3.18, podgrupa $\mathbf{H} = \mathbf{C}(b_1) \cap \ldots \cap \mathbf{C}(b_m)$ je konačnog indeksa. Neka je $\{c_1, \ldots, c_k\}$ njena desna transverzala, a $\mathbf{N}$ normalno zatvorenje skupa $\{a, c_1, \ldots, c_k\}$. Kako je $\mathbf{N}$ konačno generisana $FC$-grupa, njen centar je konačnog indeksa (prema 5.18 i 5.20 – $\mathbf{N}/\mathbf{Z(N)}$ je periodična, konačno generisana $FC$-grupa, dakle, konačno generisana lokalno konačna i normalna grupa, dakle konačna grupa). Ponovo izvodimo, kao u dokazu korolara 15.6, da je skup elemenata konačnog reda grupe $\mathbf{N}$ domen (potpuno invarijantne) podgrupe – $t\mathbf{N}$. Pokazaćemo, a to će biti i dovoljno s obzirom da je $\mathbf{G}'$ periodična grupa (15.6), da $\mathbf{G}' \leq \mathbf{N}$. Polazimo od toga da je $\mathbf{G} = \mathbf{NH}$, pa dokazujemo da je $\mathbf{H}' \leq \mathbf{N}$; jer tada $\mathbf{G}' = (\mathbf{NH})' \leq \mathbf{NH}' = \mathbf{N}$ (koristimo: ako $c, d \in N$ i $x, y \in H$, onda, prema 6.2(*d*),(*e*), $[ax, by] = x^{-1}([a,y] \cdot y^{-1}[a,b]y)x \cdot [x,y] \cdot y^{-1}[x,b]y \in NH'$). Za $x \in H$ i $i = 1, \ldots, m$ je

$b_i^{-1}(xa)b_i = x \cdot b_i^{-1}ab_i$ (zbog $x \in C(b_i)$), te su $b_i^{-1}(xa)b_i$, $i = 1, \ldots, m$, svi konjugati elementa $xa$ u grupi $\mathbf{G}$. Stoga, za (dato) $y \in H$, postoji $j \in \{1, \ldots, m\}$ takvo da je $y^{-1}(xa)y = b_j^{-1}(xa)b_j$. Odatle, $y^{-1}xy = x \cdot b_j^{-1}ab_j \cdot y^{-1}a^{-1}y$, odnosno, $[x, y] = b_j^{-1}ab_j \cdot y^{-1}a^{-1}y \in N$ i prema tome $\mathbf{H}' \leq \mathbf{N}$.□

## 16 Sylowe podgrupe, teoreme Sylowa

Teoreme Sylowa i rezultati vezani za njih moćno su sredstvo u ispitivanju grupa, posebno konačnih. To će se stalno, kroz ceo tekst, potvrđivati.

**Definicija 16.1** *Neka je* $\Pi$ *neprazan (konačan ili beskonačan) podskup skupa prostih brojeva. Prirodan broj je* $\Pi$*-broj akko se svi njegovi prosti faktori nalaze u* $\Pi$.

*Periodična grupa je* $\Pi$*-grupa akko je red svakog njenog nejediničnog elementa* $\Pi$*-broj.*

$\Pi$*-podgrupa* $\mathbf{H}$ *grupe* $\mathbf{G}$ *je Sylowa* $\Pi$*-podgrupa, kaže se i* $\Pi$*-Sylowa podgrupa, akko nije strogo sadržana u nekoj drugoj* $\Pi$*-podgrupi grupe* $\mathbf{G}$.

Jasno, ako je $\Pi$ skup svih prostih brojeva, onda je klasa $\Pi$-grupa klasa svih periodičnih grupa, a ako je pak $\Pi$ jednoelementni skup $\{p\}$, imamo poznati slučaj klase $p$-grupa (ostajemo pri uvedenoj i standardnoj notaciji – nećemo pisati $\{p\}$-grupa). Jedinična grupa je trivijalno $\Pi$-grupa za svako $\Pi$.

**Lema 16.2** *Svaka grupa sadrži Sylowu* $\Pi$*-podgrupu.*

**Dokaz.** Neka je data grupa $\mathbf{G}$ i neka je $\langle \mathcal{P}, \leq \rangle$ familija svih $\Pi$-podgrupa grupe $\mathbf{G}$ uređena relacijom inkluzije (ne zaboravimo, uvek je $\mathbf{E} \in \mathcal{P}$). Kako je unija lanca $\Pi$-podgrupa opet $\Pi$-podgrupa, prema lemi Zorna u $\mathcal{P}$ postoji maksimalni element.□

**Korolar 16.3** *Svaka* $\Pi$*-podgrupa* $\mathbf{H}$ *(date) grupe* $\mathbf{G}$ *sadržana je u Sylowoj* $\Pi$*-podgrupi.*

**Dokaz.** Razlika u dokazu (u odnosu na prethodni) je utoliko što umesto familije svih $\Pi$-podgrupa grupe $\mathbf{G}$ sada posmatramo familiju $\{\mathbf{K} \mid \mathbf{K}$ je $\Pi$-podgrupa i $\mathbf{H} \leq \mathbf{K}\}$.□

**Lema 16.4** *Ako je* $\mathbf{H}$ *Sylowa* $\Pi$*-podgrupa grupe* $\mathbf{G}$ *i* $\varphi \in Aut(\mathbf{G})$*, tada je i* $(\mathbf{H})\varphi$ *Sylowa* $\Pi$*-podgrupa grupe* $\mathbf{G}$.

**Dokaz.** $(\mathbf{H})\varphi$ je, takođe, $\Pi$-grupa (elementi $g$ i $(g)\varphi$ su istog reda). Ako bi podgrupa $(\mathbf{H})\varphi$ bila strogo sadržana u $\Pi$-podgrupi $\mathbf{K}$, imali bismo $H = ((H)\varphi)\varphi^{-1} \subset (K)\varphi^{-1}$, protivrečno pretpostavci da je $\mathbf{H}$ Sylowa $\Pi$-podgrupa.□



**Lema 16.5** *Ako su* $\mathbf{A}$ *i* $\mathbf{B}$ $\Pi$*-podgrupe grupe* $\mathbf{G}$*, pri čemu je još* $\mathbf{A}$ *normalna podgrupa, onda je i* $\mathbf{AB}$ $\Pi$*-podgrupa.*

**Dokaz.** Neka je $ab$ element grupe $\mathbf{AB}$, $a \in A$, $b \in B$. Ako je $b$ element reda $m$, onda je $(ab)^m = \overline{a}b^m = \overline{a}$ za neki element $\overline{a} \in A$ (koristimo: $ba = (bab^{-1})b = a_1 b$, $bab^{-1} = a_1 \in A$). Ako je, dalje, $\overline{a}$ element reda $n$ proizilazi: $(ab)^{mn} = e$, te su i prosti faktori reda elementa $ab$ sadržani u $\Pi$.□

**Korolar 16.6** (*a*) *Normalna* $\Pi$*-podgrupa sadržana je u svakoj Sylowoj* $\Pi$*-podgrupi;*

(*b*) *Sylowa* $\Pi$*-podgrupa je jedinstvena Sylowa* $\Pi$*-podgrupa akko je normalna;*

(*c*) *Sylowa* $\Pi$*-podgrupa je jedinstvena Sylowa* $\Pi$*-podgrupa svog normalizatora.*

Uočimo da iz tačke (*c*) korolara sledi: Ako je $\mathbf{H}$ $\Pi$-podgrupa i ako su prosti faktori elementa $g$ (konačnog reda) iz normalizatora podgrupe $\mathbf{H}$ sadržani u $\Pi$, onda je $g$ i u $H$. Posebno, ako je $\mathbf{H}$ normalna Sylowa $\Pi$-podgrupa grupe $\mathbf{G}$ i ako je element $g$ iz $G \setminus H$ konačnog reda, onda bar jedan prost faktor njegovog reda nije u $\Pi$.

**Korolar 16.7** *Neka je* $\mathbf{G} = \mathbf{A} \rtimes \mathbf{H}$ *i neka je* $\mathbf{A} = \mathbf{B} \times \mathbf{C}$ *za neke normalne podgrupe* $\mathbf{B}$ *i* $\mathbf{C}$ *grupe* $\mathbf{G}$*. Ako je* $\mathbf{B}$ *i Sylowa* $\Pi$*-podgrupa grupe* $\mathbf{A}$*, a* $\mathbf{D}$ *ma koja Sylowa* $\Pi$*-podgrupa grupe* $\mathbf{G}$*, onda je* $\mathbf{D} \cap \mathbf{A} = \mathbf{B}$ *i* $\mathbf{D} = \mathbf{B} \rtimes (\mathbf{D} \cap \mathbf{CH})$.

**Dokaz.** Prema prvoj tački prethodnog korolara je $\mathbf{B} \leq \mathbf{D}$, pa je $\mathbf{B} \leq \mathbf{D} \cap \mathbf{A}$, a prema drugoj je i $\mathbf{D} \cap \mathbf{A} \leq \mathbf{B}$. Drugi deo tvrđenja je još očigledniji.□

**Korolar 16.8** *Ako je* $\mathbf{A}$ *Sylowa* $\Pi$*-podgrupa i* $\mathbf{B}$ $\Pi$*-podgrupa grupe* $\mathbf{G}$*, onda je* $\mathbf{N_B(A)} = \mathbf{A} \cap \mathbf{B}$.

**Dokaz.** U grupi $\mathbf{N(A)}$ je $\mathbf{A}$ normalna Sylowa $\Pi$-podgrupa, a kako je i $\mathbf{N_B(A)A}$ njena $\Pi$-podgrupa, to je $\mathbf{N_B(A)\,A} = \mathbf{A}$. Dakle, $\mathbf{N_B(A)} \leq \mathbf{A}$, prema tome i $\mathbf{N_B(A)} \leq \mathbf{A} \cap \mathbf{B}$, a trivijalno $\mathbf{A} \cap \mathbf{B} \leq \mathbf{N_B(A)}$.□

**Lema 16.9** (*a*) *Ako je* $\mathbf{H}$ *podgrupa grupe* $\mathbf{G}$ *i ako su* $\mathbf{A}$ *i* $\mathbf{B}$ *različite Sylowe* $\Pi$*-podgrupe grupe* $\mathbf{H}$*, onda one ne mogu biti podgrupe iste Sylowe* $\Pi$*-podgrupe grupe* $\mathbf{G}$*;*

(*b*) *Neka je* $\{\mathbf{G}_\alpha \mid \alpha < \lambda\}$ *lanac grupa (za svako* $\alpha < \beta < \lambda$*,* $\mathbf{G}_\alpha \leq \mathbf{G}_\beta$*). Ako je* $\mathbf{H}_\alpha$ *Sylowa* $\Pi$*-podgrupa grupe* $\mathbf{G}_\alpha$ *za svako* $\alpha$ *i ako je, za* $\alpha < \beta$*,* $\mathbf{H}_\alpha \leq \mathbf{H}_\beta$*, onda je* $\mathbf{H} = \bigcup_{\alpha \in \lambda} \mathbf{H}_\alpha$ *Sylowa* $\Pi$*-podgrupa grupe* $\mathbf{G} = \bigcup_{\alpha \in \lambda} \mathbf{G}_\alpha$*;*

(*c*) *Ako je* $\mathbf{H}$ *Sylowa* $\Pi$*-podgrupa grupe* $\mathbf{G}$*, onda je* $\mathbf{N(N(H))} = \mathbf{N(H)}$.

**Dokaz.** ($a$) Pretpostavka da su $\mathbf{A}$ i $\mathbf{B}$ podgrupe iste Sylowe $\Pi$-podgrupe grupe $\mathbf{C}$ vodi u kontradikciju: grupa $\mathbf{A}$ je strogo sadržana u $\mathbf{C} \cap \mathbf{H}$ (jer je i $\mathbf{B} \leq \mathbf{C} \cap \mathbf{H}$), dok je, naravno, i $\mathbf{C} \cap \mathbf{H}$ $\Pi$-grupa.

($b$) Neka je $\mathbf{H}$ prava podgrupa $\Pi$-podgrupe $\mathbf{K}$ grupe $\mathbf{G}$. Ako je $g \in K \setminus H$ i $g \in G_\alpha$, sledi: $\mathbf{H}_\alpha = \mathbf{G}_\alpha \cap \mathbf{H}$ je prava podgrupa grupe $\mathbf{G}_\alpha \cap \mathbf{K}$, kontradikcija.

($c$) Pretpostavimo: $g \in N(\mathbf{N}(\mathbf{H})) \setminus N(\mathbf{H})$. No onda je $\mathbf{H} \neq g^{-1}\mathbf{H}g \leq g^{-1}\mathbf{N}(\mathbf{H})g = \mathbf{N}(\mathbf{H})$, pa $\mathbf{N}(\mathbf{H})$ pored $\mathbf{H}$ sadrži još jednu Sylowu $\Pi$-podgrupu, što je, videli smo, nemoguće.□

**Korolar 16.10** *Broj Sylowih $\Pi$-podgrupa podgrupe $\mathbf{H}$ grupe $\mathbf{G}$ manji je ili jednak od broja Sylowih $\Pi$-podgrupa grupe $\mathbf{G}$.*

**Dokaz.** Direktna posledica korolara 16.3 i tačke ($a$) prethodne leme.□

**Lema 16.11** *Neka su sve Sylowe $\Pi$-podgrupe grupe $\mathbf{G}$ međusobno konjugovane. Ako je $\mathbf{N}$ normalna i $\mathbf{A}$ Sylowa $\Pi$-podgrupa grupe $\mathbf{G}$, onda je $\mathbf{N} \cap \mathbf{A}$ Sylowa $\Pi$-podgrupa grupe $\mathbf{N}$.*

**Dokaz.** Neka je $\mathbf{N} \cap \mathbf{A}$ strogo sadržana u Sylowoj $\Pi$-podgrupi $\mathbf{B}$ grupe $\mathbf{N}$, koja je, opet, sadržana u Sylowoj $\Pi$-podgrupi $\mathbf{C}$ grupe $\mathbf{G}$. Kako je po uslovu leme $g^{-1}\mathbf{C}g = \mathbf{A}$ za neko $g \in G$, sledi: $g^{-1}\mathbf{B}g \leq g^{-1}\mathbf{C}g \cap g^{-1}\mathbf{N}g = \mathbf{A} \cap \mathbf{N}$, tj. $(\mathbf{B})u_g \leq \mathbf{A} \cap \mathbf{N}$. No $u_g|_N \in Aut(\mathbf{N})$, te je $(\mathbf{B})u_g$ Sylowa $\Pi$-podgrupa grupe $\mathbf{N}$ strogo sadržana u Sylowoj $\Pi$-podgrupi $\mathbf{B}$, kontradikcija.□

**Lema 16.12** *Neka je $\mathbf{A}$ normalna podgrupa grupe $\mathbf{G}$ sa svojstvom:*

*ako su $\mathbf{C}$ i $\mathbf{D}$ dve njene izomorfne Sylowe $\Pi$-podgrupe (dakle, za neko $\varphi \in Aut(\mathbf{A})$, $(\mathbf{C})\varphi = \mathbf{D}$), onda su $\mathbf{C}$ i $\mathbf{D}$ i konjugovane u $\mathbf{A}$.*

*Tada je $\mathbf{G} = \mathbf{A}\mathbf{N}(\mathbf{B})$ za svaku Sylowu $\Pi$-podgrupu $\mathbf{B}$ grupe $\mathbf{A}$.*

**Dokaz.** Neka je $\mathbf{B}$ (ma koja) Sylowa $\Pi$-podgrupa grupe $\mathbf{A}$ i neka je $g$ element grupe $\mathbf{G}$. Kako je $\mathbf{A}$ normalna podgrupa grupe $\mathbf{G}$, to je i $\mathbf{C} = (\mathbf{B})u_g = g^{-1}\mathbf{B}g$ ($\leq (\mathbf{A})u_g = \mathbf{A}$) Sylowa $\Pi$-podgrupa grupe $\mathbf{A}$ (ponavljamo: $u_g|_A \in Aut(\mathbf{A})$). Prema uslovu leme je onda $\mathbf{C} = a^{-1}\mathbf{B}a$ za neko $a \in A$, pa je $ga^{-1} \in N(\mathbf{B})$, tj. $g \in N(\mathbf{B})A = AN(\mathbf{B})$.□

**Korolar 16.13** *Neka je $\mathbf{A}$ podgrupa grupe $\mathbf{G}$ koja sadrži normalizator Sylowe $\Pi$-podgrupe $\mathbf{B}$ i ima svojstvo definisano u prethodnoj lemi. Tada je $\mathbf{N}(\mathbf{A}) = \mathbf{A}$.*

**Dokaz.** Kako je $\mathbf{A}$ normalna podgrupa svog normalizatora $\mathbf{N}(\mathbf{A})$, ispunjeni su uslovi prethodne leme s obzirom na grupu $\mathbf{N}(\mathbf{A})$. Stoga je $\mathbf{N}(\mathbf{A}) = \mathbf{A}\mathbf{N}_{\mathbf{N}(\mathbf{A})}(\mathbf{B}) = \mathbf{A}\mathbf{N}(\mathbf{B}) = \mathbf{A}$ (jasno: $\mathbf{N}_{\mathbf{N}(\mathbf{A})}(\mathbf{B}) = \mathbf{N}(\mathbf{A}) \cap \mathbf{N}(\mathbf{B})$, a po uslovu korolara je $\mathbf{N}(\mathbf{B}) \leq \mathbf{A} \leq \mathbf{N}(\mathbf{A})$).□



**Korolar 16.14** *Neka je $\mathbf{B}$ Sylowa $\Pi$-podgrupa grupe $\mathbf{G}$ i neka je $\mathbf{N}(\mathbf{B})$ podgrupa grupe $\mathbf{A}$ čije su sve Sylowe $\Pi$-podgrupe međusobno konjugovane. Tada je $\mathbf{N}(\mathbf{A}) = \mathbf{A}$. Posebno, $\mathbf{N}(\mathbf{N}(\mathbf{B})) = \mathbf{N}(\mathbf{B})$.*

U nastavku ćemo se skoncentrisati na Sylowe $p$-podgrupe i to uglavnom konačnih grupa ($p$ će u pravilu biti prost broj i kada to zaboravimo da naglasimo). Teoreme Sylowa su, ponovimo, jedno od osnovnih sredstava u ispitivanju struktura grupa, posebno konačnih.

Za početak treba nam sledeća

**Lema 16.15** *Ako prost broj $p$ deli red konačne Abelove grupe, onda ona ima element reda $p$.*

**Dokaz.** Služimo se indukcijom po redu grupe. Pretpostavimo da je tvrđenje tačno za sve Abelove grupe reda $< n(> 1)$ i neka je $\mathbf{G}$ Abelova grupa reda $n$ i neka $p$ deli $n$. Trivijalan je (i već obrađen) slučaj kada je $\mathbf{G}$ ciklična grupa. Pretpostavimo stoga da $\mathbf{G}$ nije ciklična grupa i neka je $a$ nejedinični element grupe $\mathbf{G}$ reda $m$. Ako $p$ deli $m$, ciklična grupa $\mathbf{A} = \langle a \rangle$, pa dakle, i grupa $\mathbf{G}$, ima element reda $p$. Ako $m$ nije deljivo sa $p$, onda $p$ deli red faktor grupe $\mathbf{G}/\mathbf{A}$ – $\frac{n}{m} < n$, te u $\mathbf{G}/\mathbf{A}$ postoji element $gA$ reda $p$. Proizilazi da je $g^p \in A$, a tada je i $(g^m)^p = e$. $g^m$, napomenimo još, nije jedinični element – u suprotnom bismo imali: $(gA)^m = g^m A = A$, odatle i $p|m$.□

Iskoristimo usput ovu lemu i za dokaz sledećeg stava

**Korolar 16.16** *Za prost broj $p$ i pozitivan prirodan broj $n$ grupa reda $p^n$ ima normalnu podgrupu reda $p^{n-1}$.*

*Sve podgrupe reda $p^{n-1}$ grupe reda $p^n$ su normalne.*

**Dokaz.** Oba tvrđenja dokazujemo simultano, indukcijom po $n$. Pretpostavimo da su tačna za svako $k < n(> 1)$ (slučaj $n = 1$ je trivijalan) i neka je $\mathbf{G}$ grupa reda $p^n$, $a$ jedan element njenog centra reda $p$ (videti 4.12) i $\mathbf{A}$ ciklična grupa generisana sa $a$. Faktor grupa $\overline{\mathbf{G}} = \mathbf{G}/\mathbf{A}$ ima, po induktivnoj pretpostavci, normalnu podgrupu $\overline{\mathbf{H}}$ reda $p^{n-2}$, a onda je (prema 8.7) njena inverzna slika (za kanonički homomorfizam $\varphi : \mathbf{G} \longrightarrow \overline{\mathbf{G}}$) normalna podgrupa grupe $\mathbf{G}$ reda $p^{n-1}$.

Neka je i $\mathbf{K}$ podgrupa grupe $\mathbf{G}$ reda $p^{n-1}$. Ako bismo pretpostavili da nije normalna, imali bismo $\mathbf{Z}(\mathbf{G}) \leq \mathbf{N}(\mathbf{K}) = \mathbf{K}$. Ali tada je $\mathbf{K}/\mathbf{Z}(\mathbf{G})$ podgrupa indeksa $p$ grupe $\mathbf{G}/\mathbf{Z}(\mathbf{G})$, dakle, opet po induktivnoj pretpostavci, i normalna. Sledi da je $\mathbf{K}$ normalna podgrupa grupe $\mathbf{G}$, kontradikcija.

Dodajmo na kraju: drugi deo tvrđenja je samo poseban slučaj korolara 9.37 – tu posebnost smo iskoristili i da ponudimo još jedan dokaz.□

**Teorema 16.17** *(Prva teorema Sylowa). Grupa reda $p^k m$, gde je $p$ prost broj i $(p, m) = 1$, ima (bar jednu) podgrupu reda $p^k$.*

**Dokaz**. Indukcijom po redu grupe. Pretpostavimo da je tvrđenje tačno za sve grupe reda $< n$ i neka je $\mathbf{G}$ grupa reda $n = p^k m$ $(k \geq 1)$. Ako $p$ deli red centra grupe, tada prema prethodnoj lemi postoji normalna podgrupa $\mathbf{A}$ $(\leq \mathbf{Z}(\mathbf{G}))$ grupe $\mathbf{G}$ reda $p$. Po induktivnoj hipotezi, faktor grupa $\overline{\mathbf{G}} = \mathbf{G}/\mathbf{A}$ ima $p$-podgrupu $\overline{\mathbf{P}}$ reda $p^{k-1}$, a onda je njena inverzna slika $\mathbf{P}$ (za kanoničko homomorfno preslikavanje grupe $\mathbf{G}$ u $\overline{\mathbf{G}}$) podgrupa grupe $\mathbf{G}$ reda $p^k$ $(\mathbf{A} \leq \mathbf{P}$ i $\overline{\mathbf{P}} = \mathbf{P}/\mathbf{A})$.

Ako $p$ ne deli red centra grupe, onda, prema 4.12, za bar jedan element $g$ van centra grupe, $p$ ne deli indeks njegovog centralizatora $[\mathbf{G} : \mathbf{C}(g)]$. Stoga $p^k$ deli $|C(g)|$ $(< |G|)$, pa s obzirom na induktivnu pretpostavku, $\mathbf{C}(g)$ ima podgrupu reda $p^k$.■

**Korolar 16.18** *Red konačne p-grupe je stepen od p.*

**Dokaz**. Pretpostavimo da prost broj $q$ (različit od $p$) deli red konačne grupe $\mathbf{G}$. No onda $\mathbf{G}$ ima $q$-podgrupu (čiji je red najveći stepen od $q$ koji deli $|G|$), a redovi elemenata te podgrupe su stepeni od $q$.□

Setimo se da smo obrat ovog tvrđenja već dokazali – 5.6$(c)$. Sada možemo i ovo zaključiti: centar (ma koje) konačne $p$-grupe je nejedinična podgrupa (4.13), dok beskonačne $p$-grupe mogu biti bez centra – videti primer 14.4$(a)$.

Korolar nam ujedno kazuje da su $p$-podgrupe čiju nam egzistenciju garantuje prva teorema Sylowa baš Sylowe $p$-podgrupe.

**Korolar 16.19** *Skup prostih faktora redova elemenata konačne grupe jednak je skupu prostih faktora reda te grupe.*

Sledeći korolar je uopštenje tvrđenja 4.13.

**Korolar 16.20** *Ako p-grupa* $\mathbf{G}$ *ima jednu konačnu klasu konjugovanih elemenata različitih od jediničnog, onda je* $\mathbf{Z}(\mathbf{G}) \neq \mathbf{E}$.

**Dokaz**. Neka je $A = \{g^{-1}ag \mid g \in G\}$ jedna konačna klasa konjugovanih nejediničnih elemenata grupe $\mathbf{G}$. Prema 5.17 podgrupa $\mathbf{H} = \langle A \rangle$ je konačna normalna podgrupa grupe $\mathbf{G}$. Ranije smo konstatovali da je relacija konjugovanosti elemenata relacija ekvivalencije. Kao takva ona vrši particiju skupa $H$. Neka je

$$H = [e] \cup [b_1] \cup \ldots \cup [b_m], \quad m \geq 1,$$

gde je $[b_i]$ klasa elemenata konjugovanih sa $b_i$, ta particija. Kako je red podgrupe $\mathbf{H}$ neki stepen broja $p$, recimo $p^n$ imamo:

$$|H| = p^n = |[e]| + |[b_1]| + \cdots + |[b_m]| = 1 + |[b_1]| + \cdots + |[b_m]|.$$

Pošto je $|[b_j]| = [\mathbf{H} : \mathbf{C}_{\mathbf{H}}(b_j)]$ = neki stepen (eventualno nulti) broja $p$ (4.11), proizilazi da za bar jedan indeks $i$, $1 \leq i \leq m$, i mora biti nulti stepen u pitanju. Ali $|[b_i]| = 1$ ekvivalentno je sa $b_i \in Z(\mathbf{G})$ (imamo u vidu normalnost podgrupe $\mathbf{H}$ – svi konjugati elementa $b_i$ su u $H$).□



**Korolar 16.21** *Ako je* $\mathbf{A}$ *podgrupa konačnog indeksa* $\Pi$*-grupe* $\mathbf{G}$, *onda je taj indeks* $\Pi$*-broj.*

**Dokaz**. Neka je $\mathbf{N}$ normalna podgrupa grupe $\mathbf{G}$ koja je sadržana u $\mathbf{A}$ i konačnog je indeksa. Tada je $\mathbf{G}/\mathbf{N}$ konačna $\Pi$-grupa, red joj je, dakle, $\Pi$-broj, pa kako indeks podgrupe $\mathbf{A}$ deli njen red, to je i on $\Pi$-broj.□

**Korolar 16.22** *Ako je* $\mathbf{H}$ *konačna nejedinična normalna podgrupa p-grupe* $\mathbf{G}$, *onda je* $\mathbf{H} \cap \mathbf{Z}(\mathbf{G}) \neq \mathbf{E}$.

*Posebno je, za* $|H| = p$, $\mathbf{H} \leq \mathbf{Z}(\mathbf{G})$.

**Dokaz**. Relacija konjugovanosti vrši particiju domena $H$, a s obzirom na normalnost podgrupe $\mathbf{H}$, $H$ sadrži samo kompletne klase konjugovanih elemenata. Kao u 4.12 izvodimo:

$$|H| = |H \cap Z(\mathbf{G})| + \sum_{h \in \mathcal{R}} [\mathbf{G} : \mathbf{C}(h)],$$

gde je $\mathcal{R}$ skup reprezenata klasa ekvivalencija sa više elemenata. Prema prethodnom korolaru je, za $h \in \mathcal{R}$, $[\mathbf{G} : \mathbf{C}(h)]$ konačan broj deljiv sa $p$, pa $p$ deli i $|H \cap Z(\mathbf{G})|$.

U vezi ovog korolara videti i 48.9, 48.16.□

**Korolar 16.23** $(a)$ *Ako je* $\mathbf{A}$ *Sylowa p-podgrupa reda* $p^k$, *a* $\mathbf{B}$ *p-podgrupa konačne grupe* $\mathbf{G}$ *reda* $p^k m$, $(p, m) = 1$, *onda je* $\mathbf{B}$ *podgrupa nekog konjugata grupe* $\mathbf{A}$;

$(b)$ *(Druga teorema Sylowa). Sve Sylowe p-podgrupe konačne grupe su međusobno konjugovane (dakle i istog reda).*

**Dokaz**. $(a)$ Prema 4.11 i 4.14, uzimajući za $\mathcal{A}$ skup $\{g^{-1}\mathbf{A}g \mid g \in G\}$, važi:

$$|\mathcal{A}| = \sum_{\mathbf{C} \in \mathcal{R}} [\mathbf{B} : \mathbf{N}_{\mathbf{B}}(\mathbf{C})] = [\mathbf{G} : \mathbf{N}(\mathbf{A})],$$

gde je $\mathcal{R}$ skup predstavnika klasa relacije ekvivalencije $\sim_{\mathbf{B}}$. Prema 16.8 je $\mathbf{N}_{\mathbf{B}}(\mathbf{C}) = \mathbf{B} \cap \mathbf{C}$, jer je podgrupa $\mathbf{C}$ kao konjugat Sylowe $p$-podgrupe i sama Sylowa $p$-podgrupa. Pretpostavka da je $\mathbf{B} \neq \mathbf{B} \cap \mathbf{C}$ za svako $\mathbf{C} \in \mathcal{R}$ implicirala bi da je $[\mathbf{G} : \mathbf{N}(\mathbf{A})]$ deljivo sa $p$, što je nemoguće (red grupe $\mathbf{A}$ deli red normalizatora $\mathbf{N}(\mathbf{A})$, pa je red faktor grupe $\mathbf{G}/\mathbf{N}(\mathbf{A})$ uzajamno prost sa $p$).□

**Napomena**. Primetimo da druga teorema Sylowa ne važi za beskonačne grupe (videti npr. 16.53$(k)$ i 26.11) kao ni za podskupove skupa prostih brojeva kardinalnosti veće od 1 (čak i ako su konačne grupe u pitanju). Nudimo kontraprimer iz [97].

Neka je $\Pi = \{2, 5\}$. Svaka Sylowa 2-podgrupa grupe $\mathbf{A}_5$ (koja je, uzgred rečeno, Kleinova) ujedno je i Sylowa $\Pi$-podgrupa. Doista, ako bi Sylowa 2-podgrupa $\mathbf{A}$ bila strogo sadržana u nekoj $\Pi$-podgrupi $\mathbf{B}$, ova bi bila reda

20, dakle indeksa 3, i u tom bi slučaju $\mathbf{A}_5$, kao prosta grupa, bila utopiva u $\mathbf{S}_3$ (videti 9.36), kontradikcija. No i podgrupa generisana elementima $\alpha = (01234)$ i $\beta = (14)(23)$, inače reda 10, takođe je Sylowa $\Pi$-podgrupa (svi elementi te podgrupe su oblika $\alpha^k\beta^j$, $0 \leq k < 5$, $0 \leq j < 2$, jer je $\beta^{-1}\alpha\beta = ((0)\beta\,(1)\beta\,(2)\beta\,(3)\beta\,(4)\beta) = (04321) = \alpha^4$, a $\alpha^k\beta^j = \alpha^{k_1}\beta^{j_1}$ je ekvivalentno sa $k = k_1$, $j = j_1$).

U neku ruku može se reći da ne važi ni prva teorema Sylowa, jer je broj 20 najveći $\Pi$-broj manji od 60, a grupa $\mathbf{A}_5$ nema, kao što smo videli, Sylowih $\Pi$-podgrupa reda 20.

U narednom paragrafu ćemo pokazati da konjugovanost Sylowih $p$-podgrupa važi i u jednoj mnogo široj klasi od klasa konačnih grupa – u klasi lokalno konačnih i normalnih grupa (17.5).

**Teorema 16.24** *(Treća teorema Sylowa). U konačnoj grupi* $\mathbf{G}$ *broj Sylowih p-podgrupa (za dati prost broj p) deli red grupe i kongruentan je sa* 1 *po modulu p.*

**Dokaz.** Neka je $s_p$ broj Sylowih $p$-podgrupa i neka je $\mathbf{A}$ jedna od njih. Tada je $\mathcal{A} = \{g^{-1}\mathbf{A}g \mid g \in G\}$ skup svih Sylowih $p$-podgrupa, pa imamo:

$$s_p = |\mathcal{A}| = [\mathbf{G} : \mathbf{N}(\mathbf{A})] = \sum_{\mathbf{R}\in\mathcal{R}} [\mathbf{A} : \mathbf{N}_{\mathbf{A}}(\mathbf{R})],$$

gde je $\mathcal{R}$ skup reprezenata klasa relacije ekvivalencije $\sim_{\mathbf{A}}$. Odatle direktno dobijamo: $s_p$ deli red grupe $\mathbf{G}$ i $s_p \equiv 1 \ (mod\ p)$. Opet koristimo $\mathbf{N}_{\mathbf{A}}(\mathbf{R}) = \mathbf{A} \cap \mathbf{R}$ i činjenicu da se samo jedna klasa ekvivalencije sastoji od samo jednog elementa, dok je broj elemenata u ostalim deljiv sa $p$.■

**Napomena.** Broj Sylowih $p$-podgrupa date grupe $\mathbf{G}$ označava se, osim sa $s_p$, i sa $n_p$, odnosno sa $s_p(\mathbf{G})$, $n_p(\mathbf{G})$, kada se želi naglasiti o kojoj je grupi reč.

**Definicija 16.25** *Grupa (konačna ili beskonačna) je S-grupa akko za svaki prost broj p ima jedinstvenu Sylowu p-podgrupu.*

**Lema 16.26** *Podgrupa S-grupe je S-grupa.*

**Dokaz.** Već dat – 16.10.□

**Lema 16.27** *Skup elemenata konačnog reda S-grupe* $\mathbf{G}$ *je domen normalne podgrupe, tzv. periodičnog dela grupe* $\mathbf{G}$*, koja je direktni proizvod Sylowih podgrupa.*

**Dokaz.** Neka je $a$ element grupe $\mathbf{G}$ reda $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Tada je, za neke cele brojeve $u_1, \ldots, u_k$, $u_1 \cdot \frac{n}{p_1^{\alpha_1}} + \cdots + u_k \cdot \frac{n}{p_k^{\alpha_k}} = 1$ (jasno, $(\frac{n}{p_1^{\alpha_1}}, \ldots, \frac{n}{p_k^{\alpha_k}}) = 1$), pa ako je, za $1 \leq i \leq k$, $a_i = a^{\frac{n}{p_i^{\alpha_i}}}$, tada je $a = a_1^{u_1} \cdot \ldots \cdot a_k^{u_k}$, a elementi



$a_1, \ldots, a_k$ su uzajamno permutabilni, jer pripadaju različitim i jedinstvenim (stoga i normalnim) Sylowim podgrupama ($a_i$ je reda $p_i^{\alpha_i}$). Odatle sledi da je proizvod dva elementa konačnih redova opet element konačnog reda, a ostalo je još očiglednije.□

Druga i treća teorema Sylowa su specijalni slučaj sledećeg stava.

**Teorema 16.28** *Ako grupa* $\mathbf{G}$ *ima Sylowu p-podgrupu* $\mathbf{A}$ *sa konačno mnogo konjugata, onda je familija* $\mathcal{A}$ *svih konjugata podgrupe* $\mathbf{A}$ *ujedno i familija svih Sylowih p-podgrupa grupe* $\mathbf{G}$ *i kardinalnost te familije je broj oblika* $1 + kp$ *(za neki prirodan broj k).*

**Dokaz.** Neka je $\mathbf{B}$ proizvoljna $p$-podgrupa grupe $\mathbf{G}$ i $\mathcal{P}(\mathbf{B}) = \{\mathbf{C} \mid \mathbf{C} \in \mathcal{A} \text{ i } \mathbf{B} \not\leq \mathbf{N}(\mathbf{C})\}$. Primetimo da je za $\mathbf{A} = \mathbf{E}$ $\mathcal{P}(\mathbf{B}) = \emptyset$, no slučaj $\mathbf{A} = \mathbf{E}$ je odista trivijalan; ali $\mathcal{P}(\mathbf{B})$ i inače može biti prazan skup. Uočimo dalje da ako je $\mathbf{C} \in \mathcal{P}(\mathbf{B})$, onda je i $b^{-1}\mathbf{C}b \in \mathcal{P}(\mathbf{B})$ za svako $b \in B$. Jer, $\mathbf{B} \leq \mathbf{N}(b^{-1}\mathbf{C}b)$ bi impliciralo $\mathbf{B} \leq \mathbf{N}(\mathbf{C})$ (imali bismo: za svako $c \in B$, $c^{-1}b^{-1}\mathbf{C}bc = b^{-1}\mathbf{C}b$, tj. $bc^{-1}b^{-1} \in N(\mathbf{C})$, dakle, $\mathbf{B} \leq \mathbf{N}(\mathbf{C})$). Znamo da je, za $\mathbf{C} \in \mathcal{P}(\mathbf{B})$, $|\{b^{-1}\mathbf{C}b \mid b \in B\}| = [\mathbf{B} : \mathbf{N}_{\mathbf{B}}(\mathbf{C})] = [\mathbf{B} : \mathbf{B} \cap \mathbf{N}(\mathbf{C})]$ i to mora biti stepen broja $p$ veći od 1 (zbog $\mathbf{B} \not\leq \mathbf{N}(\mathbf{C})$). Prema 4.14, $p$ deli $|\mathcal{P}(\mathbf{B})|$.

Posebno, $\mathcal{P}(\mathbf{A})$ sadrži sve konjugate grupe $\mathbf{A}$, osim same te grupe (ukoliko takvih ima), jer je $\mathbf{A}$ jedina Sylowa $p$-podgrupa svog normalizatora – 16.6($c$), i kako je $|\mathcal{P}(\mathbf{A})| = kp$ za neko $k \geq 0$, to $\mathbf{A}$ ima $kp + 1$ konjugata.

Ako je i $\mathbf{C}$ Sylowa $p$-podgrupa, onda u $\mathcal{P}(\mathbf{C})$ ne mogu biti svi konjugati grupe $\mathbf{A}$ (jer takvih je $1 + kp$, dok je $|\mathcal{P}(\mathbf{C})|$ deljivo sa $p$); stoga je, za neko $g \in G$, $g^{-1}\mathbf{A}g \leq \mathbf{N}(\mathbf{C})$, pa, kako je $\mathbf{C}$ jedina Sylowa $p$-podgrupa svog normalizatora, mora biti $\mathbf{C} = g^{-1}\mathbf{A}g$. Zaključujemo: sve Sylowe $p$-podgrupe su konjugovane sa $\mathbf{A}$.■

**Korolar 16.29** *Ako grupa* $\mathbf{G}$ *ima konačno mnogo (netrivijalnih) Sylowih p-podgrupa, tada* $\mathbf{G}$ *ima normalnu p-podgrupu koja je sadržana u svakoj Sylowoj p-podgrupa i u svakoj od njih ima isti konačni indeks.*

*Posebno, konačna grupa sa* $1 + p$ *Sylowih p-podgrupa ili nije prosta ili njen red nije deljiv sa* $p^2$.

**Dokaz.** Upravo smo pokazali, pošto ih je konačno mnogo, da su sve Sylowe $p$-podgrupe konjugovane, kao i da je $s_p$ broj oblika $1 + kp$. Neka su $\mathbf{A}_1, \ldots, \mathbf{A}_{kp+1}$ sve Sylowe $p$-podgrupe i neka je $\mathbf{B} = \bigcap_{i=1}^{kp+1} \mathbf{A}_i$. $\mathbf{B}$ je normalna podgrupa grupe $\mathbf{G}$ (kao presek jedne klase konjugovanih podgrupa), i ako je $\mathbf{A}_i = g_i^{-1}\mathbf{A}_1 g_i$, $i = 2, \ldots, kp + 1$, onda je

$$[\mathbf{A}_1 : \mathbf{B}] = [(\mathbf{A}_1)u_{g_i} : (\mathbf{B})u_{g_i}] = [\mathbf{A}_i : \mathbf{B}].$$

Dakle, $\mathbf{B}$ ima isti indeks u svakoj od podgrupa $\mathbf{A}_i$ i taj indeks je konačan. Jer je, prema 3.18, $[\mathbf{A}_1 : \mathbf{B}] \leq \prod_{i=2}^{kp+1} [\mathbf{A}_1 : \mathbf{A}_1 \cap \mathbf{A}_i]$, a $\mathbf{A}_1 \cap \mathbf{A}_i = \mathbf{N}_{\mathbf{A}_1}(\mathbf{A}_i)$

i (videti 4.14) $s_p = 1 + kp = \sum_i [\mathbf{A}_1 : \mathbf{N}_{\mathbf{A}_1}(\mathbf{A}_i)]$ (nismo specifikovali skup indeksa – znamo da se radi o predstavnicima klasa relacije ekvivalencije $\sim_{\mathbf{A}_1}$).

Ako je $s_p = 1 + p$, zaključujemo iz poslednje relacije da postoje samo dve klase ekvivalencije, jedna sa samo jednim elementom ($\mathbf{A}_1$) i ona druga kojoj pripadaju sve ostale Sylowe $p$-podgrupe. Kada je grupa i konačna, $\mathbf{N}_{\mathbf{A}_1}(\mathbf{A}_i) = \mathbf{A}_1 \cap \mathbf{A}_i$ je, za (bilo koje) $i > 1$, podgrupa indeksa $p$ $p$-podgrupe $\mathbf{A}_1$, dakle normalna. Prema tome, ako je, za $k > 1$, $i \neq k$ i $a_k \in A_1$, $\mathbf{A}_k = a_k^{-1}\mathbf{A}_i a_k$, imaćemo:

$$\mathbf{A}_1 \cap \mathbf{A}_i = (\mathbf{A}_1 \cap \mathbf{A}_i)u_{a_k} = \mathbf{A}_1 \cap \mathbf{A}_k.$$

Stoga je $\mathbf{B} = \bigcap_{j=1}^{1+p} \mathbf{A}_j = \mathbf{A}_1 \cap \mathbf{A}_j$ za svako $j > 1$ i $\mathbf{B}$ je normalna podgrupa indeksa $p$ svake Sylowe $p$-podgrupe. Odatle direktno sledi da konačna grupa čiji je red deljiv sa $p^k$, gde je $k \geq 2$, i ima $1 + p$ Sylowih $p$-podgrupa ne može biti prosta.□

**Korolar 16.30** *(Argument Frattinija). Ako je* $\mathbf{A}$ *normalna podgrupa grupe* $\mathbf{G}$ *sa konačno mnogo Sylowih p-podgrupa i* $\mathbf{B}$ *jedna Sylowa p-podgrupa grupe* $\mathbf{A}$*, tada je* $\mathbf{G} = \mathbf{A} \cdot \mathbf{N}(\mathbf{B})$.

**Dokaz.** Prema 16.12 i drugoj teoremi Sylowa.□

**Korolar 16.31** *(Opšta lema Frattinija). Neka je* $\mathbf{A}$ *normalna podgrupa grupe* $\mathbf{G}$ *i* $\mathbf{B}$ *podgrupa grupe* $\mathbf{A}$ *takva da je svaka podgrupa grupe* $\mathbf{A}$ *koja je konjugovana sa* $\mathbf{B}$ *u* $\mathbf{G}$ *konjugovana sa* $\mathbf{B}$ *i u* $\mathbf{A}$ *(zapisano formulom:* $\forall g \in G\, \exists a \in A\ g^{-1}\mathbf{B}g = a^{-1}\mathbf{B}a$*). Tada je* $\mathbf{G} = \mathbf{A} \cdot \mathbf{N}(\mathbf{B})$.

**Korolar 16.32** *Neka je* $\mathbf{G}$ *grupa sa konačno mnogo Sylowih p-podgrupa,* $\mathbf{B}$ *jedna njena Sylowa p-podgrupa i* $\mathbf{A}$ *podgrupa grupe* $\mathbf{G}$ *koja sadrži normalizator podgrupe* $\mathbf{B}$*. Tada je* $[\mathbf{A}] = \mathbf{G}$.

**Dokaz.** Prema uslovima korolara imamo:

$$\mathbf{B} \leq \mathbf{N}(\mathbf{B}) \leq [\mathbf{A}] \lhd \mathbf{G},$$

pa je $\mathbf{G} = [\mathbf{A}]\,\mathbf{N}(\mathbf{B}) = [\mathbf{A}]$.□

**Korolar 16.33** *Ako konačna podgrupa* $\mathbf{A}$ *grupe* $\mathbf{G}$ *sadrži normalizator (neke) Sylowe p-podgrupe grupe* $\mathbf{G}$*, tada je ona jednaka svom normalizatoru.*

**Lema 16.34** *Neka je* $\mathbf{G}$ *grupa sa konačno mnogo Sylowih p-podgrupa i neka je* $\mathbf{A}$ *jedna od njih. Tada važi:*

*(a) Ako su normalne podgrupe* $\mathbf{B}$ *i* $\mathbf{C}$ *(pod)grupe* $\mathbf{A}$ *konjugovane u* $\mathbf{G}$*, konjugovane su i u* $\mathbf{N}(\mathbf{A})$*;*

*(b) Ako su elementi b i c podgrupe* $\mathbf{C}(\mathbf{A})$ *konjugovani u* $\mathbf{G}$*, konjugovani su i u* $\mathbf{N}(\mathbf{A})$*. Posebno, ako su elementi centra podgrupe* $\mathbf{A}$ *konjugovani u* $\mathbf{G}$*, konjugovani su i u* $\mathbf{N}(\mathbf{A})$.



**Dokaz.** *(a)* Neka je, za $g \in G$, $\mathbf{C} = g^{-1}\mathbf{B}g$. Kako je $\mathbf{B} \lhd \mathbf{A}$, to je i $\mathbf{C} = g^{-1}\mathbf{B}g \lhd g^{-1}\mathbf{A}g$. Prema tome, $\mathbf{A}$ i $g^{-1}\mathbf{A}g$ su Sylowe $p$-podgrupe grupe $\mathbf{N}(\mathbf{C})$, pa je, za neko $h \in N(\mathbf{C})$, $\mathbf{A} = h^{-1}(g^{-1}\mathbf{A}g)h = (gh)^{-1}\mathbf{A}gh$. Dakle, $gh \in N(\mathbf{A})$ i $(gh)^{-1}\mathbf{B}(gh) = h^{-1}(g^{-1}\mathbf{B}g)h = h^{-1}\mathbf{C}h = \mathbf{C}$.

*(b)* Imamo potpunu analogiju sa prethodnim slučajem. Neka je, za $g \in G$, $c = g^{-1}bg$. Onda je $c \in C(g^{-1}\mathbf{A}g)$, znači $\mathbf{A}$ i $g^{-1}\mathbf{A}g$ su Sylowe $p$-podgrupe grupe $\mathbf{C}(c)$. Stoga je, za neko $h \in C(g)$, $\mathbf{A} = (gh)^{-1}\mathbf{A}(gh)$, $gh \in N(\mathbf{A})$ i $(gh)^{-1}b(gh) = h^{-1}(g^{-1}bg)h = h^{-1}ch = c$.□

**Lema 16.35** *Neka za neki prost broj p broj Sylowih p-podgrupa konačne grupe* $\mathbf{G}$ $(s_p)$ *nije kongruentan sa 1 po modulu* $p^2$*. Tada* $\mathbf{G}$ *ima dve Sylowe p-podgrupe* $\mathbf{P}$ *i* $\mathbf{Q}$ *takve da je njihov presek indeksa p u svakoj od njih (prema tome i normalna podgrupa svake od njih).*

**Dokaz.** Neka je $\mathbf{P}$ jedna Sylowa $p$-podgrupa grupe $\mathbf{G}$. Prema 4.14 i 16.8 imamo, za familiju svih Sylowih $p$-podgrupa $\mathcal{A} = \{g^{-1}\mathbf{P}g \mid g \in G\}$,

$$|\mathcal{A}| = s_p = \sum\nolimits_{R \in \mathcal{R}} [\mathbf{P} : \mathbf{N}_{\mathbf{P}}(\mathbf{R})] = [\mathbf{P} : \mathbf{P} \cap \mathbf{R}].$$

Klasa ekvivalencije (s obzirom na konjugovanost koju određuje podgrupa $\mathbf{P}$) kojoj pripada $\mathbf{P}$ sadrži samo tu podgrupu. Kako, po pretpostavci, $s_p \not\equiv 1\ (mod\ p^2)$, to je, za bar jedno $\mathbf{Q} \in \mathcal{R}$, $[\mathbf{P} : \mathbf{P} \cap \mathbf{Q}] = p$, a tada, naravno, i $[\mathbf{Q} : \mathbf{P} \cap \mathbf{Q}] = p$. Prema 16.16 je $\mathbf{P} \cap \mathbf{Q}$ normalna podgrupa grupa $\mathbf{P}$ i $\mathbf{Q}$.

Primetimo na kraju da smo, zapravo, dokazali (s obzirom da u izboru Sylowe $p$-podgrupe $\mathbf{P}$ nije bilo nikakvih ograničenja) da za svaku Sylowu $p$-podgrupu $\mathbf{P}$ postoji Sylowa $p$-podgrupa $\mathbf{Q}$ takva da je

$$[\mathbf{P} : \mathbf{P} \cap \mathbf{Q}] = [\mathbf{Q} : \mathbf{P} \cap \mathbf{Q}] = p.$$□

**Korolar 16.36** *Ako je* $\mathbf{G}$ *konačna grupa i* $s_p \not\equiv 1\ (mod\ p^k)$ *za neko* $k > 1$*, onda postoje Sylowe p-podgrupe* $\mathbf{A}$ *i* $\mathbf{B}$ *takve da je* $|A \cap B| < p^k$.

**Lema 16.37** *Neka je* $\mathbf{G}$ *grupa sa konačno mnogo Sylowih p-podgrupa i neka je* $\mathbf{A}$ *jedna od njih, dok je* $\mathbf{H}$ *normalna podgrupa grupe* $\mathbf{G}$*. Tada je* $\mathbf{H} \cap \mathbf{A}$ *Sylowa p-podgrupa grupe* $\mathbf{H}$.

**Dokaz.** Direktna posledica leme 16.11 i teoreme 16.28.

U slučaju konačnih grupa u pitanju je direktna posledica korolara 8.13*(c)*.□

**Lema 16.38** *Neka je* $\Pi$ *skup prostih faktora reda konačne grupe* $\mathbf{G}$*. Ako za svako* $p \in \Pi$ $\mathbf{G}$ *ima normalnu Sylowu p-podgrupu* $\mathbf{H}_p$*, tada je* $\mathbf{G} = \prod_{p \in \Pi} \mathbf{H}_p$.

**Dokaz.** Prema 16.5 je, za $Q \subseteq \Pi$, $\langle \bigcup_{q \in Q} H_q \rangle$ $Q$-grupa, pa je, za $p \notin Q$, $\mathbf{H}_p \cap \langle \bigcup_{q \in Q} H_q \rangle = \mathbf{E}$. Prema tome je, imajući u vidu i 3.21*(c)*, $|G| = \prod_{p \in \Pi} |H_p|$ (dakle i $\mathbf{G} = \langle \bigcup_{p \in \Pi} H_p \rangle$), a onda i $\mathbf{G} = \prod_{p \in \Pi} \mathbf{H}_p$.□

**Korolar 16.39** *Konačna abelova grupa je ciklična akko je svaka njena Sylowa podgrupa ciklična.*

**Dokaz.** Prema prethodnom korolaru i 10.45($a$).□

**Korolar 16.40** *Ako su* $\mathbf{A}$ *i* $\mathbf{B}$ *konačne Abelove grupe uzajamno prostih redova, onda postoji samo jedna Abelova ekstenzija grupe* $\mathbf{A}$ *grupom* $\mathbf{B}$.

**Dokaz.** Neka je $\mathbf{G}$ Abelova ekstenzija grupe $\mathbf{A}$ pomoću $\mathbf{B}$. Ako je $|B| = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, onda je za svako $i$ $(1 \leq i \leq k)$, $p_i^{\alpha_i}$ najveći stepen (prostog) broja $p_i$ koji deli red grupe $\mathbf{G}$ ($|G| = |A| \cdot |B|$). Ako su, dalje, $\mathbf{H}_{p_i}$, $1 \leq i \leq k$, odgovarajuće Sylowe podgrupe (jedinstvene zbog normalnosti), onda je $\mathbf{G} = \mathbf{A} \times \mathbf{H}$, gde je $\mathbf{H} = \mathbf{H}_{p_1} \times \cdots \times \mathbf{H}_{p_k}$. Podgrupa $\mathbf{H}$ je, znamo, izomorfna sa $\mathbf{G}/\mathbf{A}$ ($\cong \mathbf{B}$), pa je $\mathbf{G} \cong \mathbf{A} \times \mathbf{B}$.□

**Korolar 16.41** *Ako je red (konačne) Abelove grupe* $\mathbf{G}$ *deljiv sa* $n$, *onda* $\mathbf{G}$ *ima podgrupu i faktor grupu reda* $n$.

**Dokaz.** Direktno prema dokazu prethodne leme i 16.16.□

**Lema 16.42** *Ako su sve maksimalne podgrupe konačne grupe* $\mathbf{G}$ *normalne, onda je i svaka njena Sylowa* $p$*-podgrupa normalna.*

**Dokaz.** Neka je $\mathbf{A}$ Sylowa $p$-podgrupa grupe $\mathbf{G}$. Pretpostavimo da je $\mathbf{N}(\mathbf{A}) \neq \mathbf{G}$ (tj. da $\mathbf{A}$ nije normalna podgrupa). No tada je grupa $\mathbf{N}(\mathbf{A})$ sadržana u nekoj maksimalnoj podgrupi $\mathbf{B}$ grupe $\mathbf{G}$, pa je $\mathbf{B} = \mathbf{N}(\mathbf{B}) = \mathbf{G}$ (videti 16.13), kontradikcija.

Primetimo još: ovo tvrđenje je deo jednog opštijeg stava o nilpotentnim grupama – videti 48.28.□

**Lema 16.43** *Ako je* $\mathbf{G}$ *konačna grupa i* $\mathbf{N}$ *jedna njena normalna podgrupa, tada važi:*

($a$) $\overline{\mathbf{A}}$ *je Sylowa* $p$*-podgrupa grupe* $\overline{\mathbf{G}} = \mathbf{G}/\mathbf{N}$ *akko je* $\overline{\mathbf{A}} = (\mathbf{BN})/\mathbf{N}$ *za neku Sylowu* $p$*-podgrupu* $\mathbf{B}$ *grupe* $\mathbf{G}$;

($b$) *Broj Sylowih* $p$*-podgrupa grupe* $\overline{\mathbf{G}}$ *manji je ili jednak od broja Sylowih* $p$*-podgrupa grupe* $\mathbf{G}$ ($s_p(\overline{\mathbf{G}}) \leq s_p(\mathbf{G})$).

**Dokaz.** ($a$) ($\Longleftarrow$) Neka je $\mathbf{B}$ Sylowa $p$-podgrupa grupe $\mathbf{G}$. Onda je $(\mathbf{BN})/\mathbf{N}$ ($\cong \mathbf{B}/(\mathbf{B} \cap \mathbf{N})$) $p$-podgrupa grupe $\overline{\mathbf{G}}$, a prema 8.7 $[\overline{\mathbf{G}} : (\mathbf{BN})/\mathbf{N}] = [\mathbf{G} : \mathbf{BN}]$. Odatle, $p$ ne deli $[\overline{\mathbf{G}} : (\mathbf{BN})/\mathbf{N}]$, pa je $(\mathbf{BN})/\mathbf{N}$ Sylowa $p$-podgrupa grupe $\mathbf{G}$.

($\Longrightarrow$) Neka je $\overline{\mathbf{A}}$ Sylowa $p$-podgrupa grupe $\overline{\mathbf{G}}$ i $\varphi$ kanoničko homomorfno preslikavanje grupe $\mathbf{G}$ na $\overline{\mathbf{G}}$. Ako je $\mathbf{A} = (\overline{\mathbf{A}})\varphi^{-1}$, tada je, ponovo prema 8.7, $[\overline{\mathbf{G}} : \overline{\mathbf{A}}] = [\mathbf{G} : \mathbf{A}]$, te je, pošto $p$ ne deli $[\mathbf{G} : \mathbf{A}]$, svaka Sylowa $p$-podgrupa



podgrupe $\mathbf{A}$ ujedno i Sylowa $p$-podgrupa grupe $\mathbf{G}$. Neka je $\mathbf{B}$ jedna takva. Prema prvom delu tvrđenja, $(\mathbf{BN})/\mathbf{N} = (\mathbf{B})\varphi$ ($\leq (\mathbf{A})\varphi = \overline{\mathbf{A}}$) je Sylowa $p$-podgrupa grupe $\overline{\mathbf{G}}$ i stoga baš važi jednakost: $(\mathbf{BN})/\mathbf{N} = \overline{\mathbf{A}}$.

($b$) Primetimo: generalno ne mora da važi jednakost; recimo, grupa $\mathbf{S}_3$ ima tri Sylowe 2-podgrupe, dok je grupa $\mathbf{S}_3/\mathbf{A}_3$ reda 2.□

**Korolar 16.44** *Homomorfna slika konačne* $S$*-grupe je* $S$*-grupa.*

**Napomena.** Prethodna dva tvrđenja se ne mogu uopštiti, tj. ne važe za beskonačne grupe, čak i ako zadržimo uslov da ove imaju konačno mnogo Sylowih podgrupa. Tako npr. znamo da je, za prost broj $p$, $\mathbf{Z}_p \cong \mathbf{Z}/p\mathbf{Z}$ ($p\mathbf{Z} \stackrel{\text{def}}{=} \langle \{pz \mid z \in Z\}, + \rangle$), a Sylowa $p$-podgrupa grupe $\mathbf{Z}$ je jedinična (nula) podgrupa. Ili, recimo, slobodne grupe su, kao torziono slobodne, trivijalno $S$-grupe (videti 21.8 i 23.3), dok je svaka grupa homomorfna slika neke slobodne grupe (21.9($c$)).

**Definicija 16.45** *Familija podgrupa* $\{\mathbf{P}_1, \ldots, \mathbf{P}_n\}$ *grupe* $\mathbf{G}$ *je Sylow toranj akko je, za svako* $i$, $i = 1, \ldots, n$, $\mathbf{P}_i$ *Sylowa* $p_i$*-podgrupa grupe* $\mathbf{G}$, $p_1 > \cdots > p_n$ $i$, *za* $k = 1, \ldots, n$, $P_1 \ldots P_k$ *je domen normalne podgrupe grupe* $\mathbf{G}$, *a* $\mathbf{P}_1 \ldots \mathbf{P}_n = \mathbf{G}$.

**Lema 16.46** *Neka je* $\mathbf{G}$ *grupa konačnog eksponenta takva da ima konačno mnogo Sylowih* $p$*-podgrupa za svaki prost faktor* $p$ *eksponenta. Tada važi: ako je svaka maksimalna podgrupa grupe* $\mathbf{G}$ *prostog indeksa, onda* $\mathbf{G}$ *ima Sylow toranj.*

**Dokaz.** Indukcijom po eksponentu. Trivijalan je slučaj ako je on prost broj ili stepen prostog broja. Pretpostavimo da je tvrđenje tačno za sve grupe eksponenta manjeg od $k$ i neka je $\mathbf{G}$ grupa eksponenta $k$ čiji su prosti faktori $\Pi = \{p_1, \ldots, p_n\}$, gde je $p_1 > \cdots > p_n$ i $n \geq 2$. $\mathbf{G}$ je, dakle $\Pi$-grupa. Neka je $\mathbf{P}_1$ (jedna) Sylowa $p_1$-podgrupa. $\mathbf{P}_1$ je i normalna podgrupa. Zaista, krenimo od toga da je $\mathbf{N}(\mathbf{P}_1)$ prava podgrupa grupe $\mathbf{G}$ sadržana u maksimalnoj podgrupi $\mathbf{H}$ indeksa $q$. Prema 16.28, $[\mathbf{G} : \mathbf{N}(\mathbf{P}_1)]$ i $[\mathbf{H} : \mathbf{N}(\mathbf{P}_1)]$ su kongruentni sa 1 po modulu $p_1$, a onda je i $[\mathbf{G} : \mathbf{H}]$ $(= \frac{[\mathbf{G}:\mathbf{N}(\mathbf{P}_1)]}{[\mathbf{H}:\mathbf{N}(\mathbf{P}_1)]})$ kongruentno sa 1 po modulu $p_1$. Ali, prema 16.21, $[\mathbf{G} : \mathbf{H}]$ je $\Pi$-broj, uz to, po uslovu leme, i prost broj, znači jedan od brojeva $p_1, \ldots, p_n$, i eto kontradikcije. Faktor grupa $\overline{\mathbf{G}} = \mathbf{G}/\mathbf{P}_1$ je eksponenta manjeg od $k$, čiji su prosti faktori $\{p_2, \ldots, p_n\}$ $(= \Pi \setminus \{p_1\})$ ($\mathbf{P}_1$ sadrži sve elemente čiji je red stepen prostog broja $p_1$ – 16.5). Po induktivnoj hipotezi, $\overline{\mathbf{G}}$ sadrži Sylow toranj $\{\overline{\mathbf{P}}_2, \ldots, \overline{\mathbf{P}}_n\}$, gde je, za $i = 2, \ldots, n$, $\overline{\mathbf{P}}_i = (\mathbf{P}_1 \cdot \mathbf{P}_i)/\mathbf{P}_1$, za neku Sylowu $p_i$-podgrupu $\mathbf{P}_i$ (16.43). Kako su, za $k = 2, \ldots, n$, $\overline{\mathbf{P}}_2 \ldots \overline{\mathbf{P}}_k$ normalne podgrupe grupe $\overline{\mathbf{G}}$ i kako je $\overline{\mathbf{P}}_2 \ldots \overline{\mathbf{P}}_n = \overline{\mathbf{G}}$, to su i $\mathbf{P}_1\mathbf{P}_2 \ldots \mathbf{P}_k$ normalne podgrupe grupe $\mathbf{G}$, a $\mathbf{P}_1\mathbf{P}_2 \ldots \mathbf{P}_n = \mathbf{G}$.□

**Teorema 16.47** *(Gaschütz). Neka je* $\mathbf{A}$ *normalna Abelova podgrupa grupe* $\mathbf{G}$ *konačnog eksponenta,* $k$*, i konačnog indeksa. Tada je* $\mathbf{G}$ *poludirektni proizvod sa normalnim faktorom* $\mathbf{A}$ *akko je, za svaki prost broj* $p$ *koji deli* $k$*, svaka Sylowa* $p$*-podgrupa,* $\mathbf{K}$*, grupe* $\mathbf{G}$*, poludirektni proizvod sa normalnim faktorom* $\mathbf{K} \cap \mathbf{A}$.

**Dokaz.** ($\Longrightarrow$) Ovaj pravac je direktna posledica korolara 16.7 – Abelova grupa $\mathbf{A}$ ima, za svaki prost $p$, jedinstvenu Sylowu $p$-podgrupu, koja je, kao karakteristična u $\mathbf{A}$, normalna u $\mathbf{G}$, a pošto je $\mathbf{A}$ i periodična, Sylowe podgrupe su i njeni direktni sumandi (30.5).

($\Longleftarrow$) Indukcijom po $k$ ($> 1$) (slučaj $k = 1$ je trivijalan – $\mathbf{A}$ je jedinična grupa). Ako je $k$ prost broj, u pitanju je posledica teoreme 12.6. Naime, ako je $\mathbf{K}$ Sylowa $k$-podgrupa grupe $\mathbf{G}$, onda je $\mathbf{A} \leq \mathbf{K}$ i, prema uslovu teoreme, $\mathbf{K}$ je poludirektni proizvod, recimo; $\mathbf{K} = \mathbf{A} \rtimes \mathbf{K}_1$. S druge strane, $\mathbf{K}/\mathbf{A}$ je Sylowa $k$-podgrupa konačne grupe $\mathbf{G}/\mathbf{A}$, pa je indeks $[\mathbf{G}/\mathbf{A} : \mathbf{K}/\mathbf{A}] = [\mathbf{G} : \mathbf{K}]$ uzajamno prost sa $k$. Ako je baš $\mathbf{K} = \mathbf{A}$, radi se o teoremi Schura (12.7).

Pretpostavimo u nastavku da je tvrđenje tačno za sve slučajeve kada je eksponent normalne Abelove podgrupe manji od $k$ ($> 1$) i neka je $k$ složen broj, $p$ jedan njegov prost faktor, a $\mathbf{K}$ jedna Sylowa $p$-podgrupa grupe $\mathbf{G}$ (ostajemo pri notaciji iz formulacije teoreme). Po uslovu teoreme je $\mathbf{K} = (\mathbf{K} \cap \mathbf{A}) \rtimes \mathbf{K}_1$ (za neku podgrupu $\mathbf{K}_1$). $\mathbf{K} \cap \mathbf{A}$ je pak jedinstvena Sylowa $p$-podgrupa grupe $\mathbf{A}$ (ako bi $\mathbf{K} \cap \mathbf{A}$ bila prava podgrupa Sylowe $p$-podgrupe grupe $\mathbf{A}$, neka je to $\mathbf{B}$, onda bi $\mathbf{B}$, ponavljamo se, kao karakteristična podgrupa grupe $\mathbf{A}$, bila normalna u $\mathbf{G}$ i $\mathbf{BK}$ bi bila $p$-podgrupa grupe $\mathbf{G}$ koja strogo sadrži $\mathbf{K}$ – 16.5). Stoga je $\mathbf{A} = (\mathbf{K} \cap \mathbf{A}) \times \mathbf{A}_1$, gde je $\mathbf{A}_1$ Sylowa $\Pi$-podgrupa grupe $\mathbf{A}$, za $\Pi = \{q \mid q$ je prost faktor broja $k$ različit od $p\}$ (ponovo se pozivamo na gotovo očiglednu činjenicu da je periodična Abelova grupa direktna suma Sylowih podgrupa – dokaz je, već smo rekli, dat u 30.5). U faktor grupi $\mathbf{G}/\mathbf{A}_1$ imamo: $(\mathbf{KA}_1)/\mathbf{A}_1 = ((\mathbf{K} \cap \mathbf{A}) \rtimes \mathbf{K}_1)\mathbf{A}_1)/\mathbf{A}_1 = ((\mathbf{K} \cap \mathbf{A})\mathbf{A}_1)/\mathbf{A}_1 \rtimes (\mathbf{K}_1\mathbf{A}_1)/\mathbf{A}_1 = \mathbf{A}/\mathbf{A}_1 \rtimes (\mathbf{K}_1\mathbf{A}_1)/\mathbf{A}_1$ i, prema 12.6, $\mathbf{G}/\mathbf{A}_1 = \mathbf{A}/\mathbf{A}_1 \rtimes \mathbf{H}/\mathbf{A}_1$ (za neku podgrupu $\mathbf{H}$, $\mathbf{A}_1 \leq \mathbf{H} \leq \mathbf{G}$). Odatle, $\mathbf{A} \cap \mathbf{H} = \mathbf{A}_1$ i $\mathbf{G} = \mathbf{AH} = (\mathbf{A} \cap \mathbf{K}) \rtimes \mathbf{H}$. Za $q \in \Pi$, Sylowe $q$-podgrupe grupe $\mathbf{H}$ su ujedno i Sylowe $q$-podgrupe grupe $\mathbf{G}$; ako je npr. $\mathbf{L}$ Sylowa $q$-podgrupa grupe $\mathbf{H}$, onda je $\mathbf{L} \cong ((\mathbf{A} \cap \mathbf{K})\mathbf{L})/(\mathbf{A} \cap \mathbf{K})$ Sylowa $q$-podgrupa grupe $((\mathbf{A} \cap \mathbf{K})\mathbf{H})/(\mathbf{A} \cap \mathbf{K}) = \mathbf{G}/(\mathbf{A} \cap \mathbf{K}) \cong \mathbf{H}$, te je $\mathbf{L}$ Sylowa $q$-podgrupa i grupe $\mathbf{G}$. Po uslovu teoreme za svaku Sylowu $q$-podgrupu $\mathbf{L}$ grupe $\mathbf{H}$ (dakle i grupe $\mathbf{G}$) važi: $\mathbf{L} = (\mathbf{L} \cap \mathbf{A}_1) \rtimes \mathbf{L}_1$ ($\leq \mathbf{H}$) (za neku podgrupu $\mathbf{L}_1$), pa je, po induktivnoj hipotezi, za neku podgrupu $\mathbf{M}$: $\mathbf{H} = \mathbf{A}_1 \rtimes \mathbf{M}$; $\mathbf{A}_1$ je Abelova normalna podgrupa grupe $\mathbf{H}$, eksponenta $k'$ ($< k$) i konačnog indeksa: $\mathbf{G}/\mathbf{A} = (\mathbf{AH})/\mathbf{A} \cong \mathbf{H}/(\mathbf{A} \cap \mathbf{H}) = \mathbf{H}/\mathbf{A}_1$. No onda je i $\mathbf{G} = \mathbf{AH} = \mathbf{A}(\mathbf{A}_1\mathbf{M}) = (\mathbf{AA}_1)\mathbf{M} = \mathbf{AM}$, i pošto je $\mathbf{A} \cap \mathbf{M} \leq \mathbf{A} \cap \mathbf{H} = \mathbf{A}_1$, to je $\mathbf{A} \cap \mathbf{M} \leq \mathbf{A}_1 \cap \mathbf{M} = \mathbf{E}$ i $\mathbf{G} = \mathbf{A} \rtimes \mathbf{M}$.■

**Lema 16.48** *Neka je* $\mathbf{G}$ *grupa sa konačno mnogo Sylowih* $p$*-podgrupa, neka su Sylowe* $p$*-podgrupe grupe* $\mathbf{G}$ *Abelove i neka je presek familije svih Sylowih*



*p-podgrupa grupe* $\mathbf{G}$ *jedinična podgrupa. Onda je i presek neke dve Sylowe* $p$*-podgrupe jedinična podgrupa.*

**Dokaz.** Pretpostavimo da tvrđenje ne važi i neka je $\mathbf{G}$ grupa sa najmanjim brojem, $s_p$, Sylowih $p$-podgrupa koja je kontraprimer tvrđenju. Onda postoji neka podfamilija $\{\mathbf{A}_0, \ldots, \mathbf{A}_{k-1}\}$, $3 \leq k \leq s_p$, familije svih Sylowih $p$-podgrupa grupe $\mathbf{G}$, takva da je $\bigcap_{j=0}^{k-1} \mathbf{A}_j = \mathbf{E}$, ali $\bigcap_{j=1}^{k-1} \mathbf{A}_j = \mathbf{B} \neq \mathbf{E}$ (dakle, $\mathbf{A}_0 \cap \mathbf{B} = \mathbf{E}$). Podgrupa $\mathbf{A}_0$ nije sadržana u $\mathbf{C}(\mathbf{B})$; u suprotnom bi $\mathbf{A}_0\mathbf{B}$ bila $p$-podgrupa (elementi podgrupa $\mathbf{A}_0$ i $\mathbf{B}$ bi bili uzajamno permutabilni) koja strogo sadrži $\mathbf{A}_0$. S druge strane je, zbog komutativnosti Sylowih $p$-podgrupa, $\mathbf{A}_j \leq \mathbf{C}(\mathbf{B})$ za svako $j > 0$. Prema 16.10 broj Sylowih $p$-podgrupa grupe $\mathbf{C}(\mathbf{B})$ je konačan, zapravo je strogo manji od $s_p$, jer Sylowe $p$-podgrupe (pod)grupe $\mathbf{C}(\mathbf{B})$ su i Sylowe $p$-podgrupe grupe $\mathbf{G}$ (zbog $\mathbf{A}_j \leq \mathbf{C}(\mathbf{B})$, $j = 1, \ldots, k-1$) i $\mathbf{A}_0 \not\leq \mathbf{C}(\mathbf{B})$. Sylowe $p$-podgrupe grupe $\mathbf{C}(\mathbf{B})/\mathbf{B}$ su pak, prema 16.43($a$), oblika $(\mathbf{AB})/\mathbf{B}$, gde je $\mathbf{A}$ Sylowa $p$-podgrupa grupe $\mathbf{C}(\mathbf{B})$ i broj tih podgrupa je, prema već konstatovanom, manji od $s_p$. Presek familije tih podgrupa je jedinična podgrupa (jer je, zbog $\bigcap_{j=1}^{k-1} \mathbf{A}_j = \mathbf{B}$, i $\bigcap_{j=1}^{k-1}(A_jB)/B = \overline{E} = \{B\}$), te je, s obzirom na pretpostavku o $s_p$, za neke Sylowe $p$-podgrupe $\mathbf{C}$ i $\mathbf{D}$ grupe $\mathbf{C}(\mathbf{B})$, $(CB)/B \cap (DB)/B = \{B\}$, tj. $\mathbf{C} \cap \mathbf{D} = \mathbf{B}$. Grupa $\mathbf{A}_0 \cap \mathbf{C}(\mathbf{B})$ je opet sadržana u nekoj Sylowoj $p$-podgrupi $\mathbf{F}$ grupe $\mathbf{C}(\mathbf{B})$, a prema 16.28 su sve Sylowe $p$-podgrupe grupe $\mathbf{C}(\mathbf{B})$ konjugovane u $\mathbf{C}(\mathbf{B})$ (kao što su i Sylowe $p$-podgrupe grupe $\mathbf{G}$ konjugovane). Stoga je, za neko $g \in C(\mathbf{B})$, $g^{-1}\mathbf{C}g = \mathbf{F}$, a odatle $\mathbf{B} = g^{-1}\mathbf{B}g = g^{-1}(\mathbf{C} \cap \mathbf{D})g = g^{-1}\mathbf{C}g \cap g^{-1}\mathbf{D}g = \mathbf{F} \cap g^{-1}\mathbf{D}g$ i, konačno, $\mathbf{E} \neq \mathbf{A}_0 \cap g^{-1}\mathbf{D}g \leq (\mathbf{A}_0 \cap g^{-1}\mathbf{D}g) \cap (\mathbf{A}_0 \cap \mathbf{C}(\mathbf{B})) \leq \mathbf{A}_0 \cap (g^{-1}\mathbf{D}g \cap \mathbf{F}) = \mathbf{A}_0 \cap \mathbf{B} = \mathbf{E}$, kontradikcija.□

**Teorema 16.49** *(Teorema Schur - Zassenhausa). Ako je* $\mathbf{H}$ *Hallova normalna podgrupa grupe* $\mathbf{G}$*, onda* $\mathbf{G}$ *sadrži podgrupu reda* $|G/H|$ *i* $\mathbf{G}$ *je poludirektni proizvod tih grupa.*

**Dokaz.** Indukcijom po redu grupe $\mathbf{G}$. Naravno, više je nego trivijalan slučaj: $\mathbf{H} = \mathbf{E}$. Pretpostavimo da je tvrđenje tačno za sve grupe reda $< n$ i neka je $|G| = n$, $|H| = m$ ($> 1$) (prema tome, $(m, \frac{n}{m}) = 1$). Neka je $p$ prost faktor broja $m$. Kako najveći stepen od $p$ koji deli $n$ deli i $m$, to je Sylowa $p$-podgrupa grupe $\mathbf{H}$ ujedno i Sylowa $p$-podgrupa grupe $\mathbf{G}$, a kako su sve Sylowe $p$-podgrupe uzajamno konjugovane i $\mathbf{H}$ je normalna podgrupa, to su sve Sylowe $p$-podgrupe grupe $\mathbf{G}$ ujedno i Sylowe $p$-podgrupe grupe $\mathbf{H}$.

Neka je $\mathbf{A}$ jedna Sylowa $p$-podgrupa. Prema 16.12 je $\mathbf{G} = \mathbf{H}\,\mathbf{N}(\mathbf{A})$. Iz

$$s_p = [\mathbf{G} : \mathbf{N}(\mathbf{A})] = [\mathbf{H} : \mathbf{N}_{\mathbf{H}}(\mathbf{A})] = [\mathbf{H} : \mathbf{H} \cap \mathbf{N}(\mathbf{A})]$$

i

$$[\mathbf{G} : \mathbf{N}(\mathbf{A})] \cdot [\mathbf{N}(\mathbf{A}) : \mathbf{N}(\mathbf{A}) \cap \mathbf{H}] = [\mathbf{G} : \mathbf{H}] \cdot [\mathbf{H} : \mathbf{H} \cap \mathbf{N}(\mathbf{A})],$$

pak sledi

$$[\mathbf{N(A)} : \mathbf{N(A)} \cap \mathbf{H}] = [\mathbf{G} : \mathbf{H}] = |G/H|.$$

$\mathbf{N(A)} \cap \mathbf{H}$ je normalna podgrupa grupe $\mathbf{N(A)}$ i prema trećoj teoremi o izomorfizmu imamo:

$$\mathbf{N(A)}/(\mathbf{N(A)} \cap \mathbf{H}) \cong (\mathbf{N(A)}/\mathbf{A})/(\mathbf{N(A)} \cap \mathbf{H}/\mathbf{A}).$$

Sada je $(\mathbf{N(A)} \cap \mathbf{H})/\mathbf{A}$ Hallova normalna podgrupa grupe $\mathbf{N(A)}/\mathbf{A}$ reda manjeg od $n$ (jer je njena faktor grupa reda $\frac{n}{m}$, dok $|(\mathbf{N(A)} \cap \mathbf{H})/\mathbf{A}|$ deli $m$), pa prema induktivnoj pretpostavci $\mathbf{N(A)}/\mathbf{A}$ ima podgrupu $\mathbf{B}/\mathbf{A}$ reda $\frac{n}{m}$ ($\mathbf{A} \leq \mathbf{B} \leq \mathbf{N(A)}$). Centar grupe $\mathbf{A}$ je, prema 4.13, netrivijalna podgrupa, a prema 4.34, normalna podgrupa grupe $\mathbf{N(A)}$. Prema trećoj teoremi o izomorfizmu je

$$\mathbf{B}/\mathbf{A} \cong (\mathbf{B}/\mathbf{Z(A)})/(\mathbf{A}/\mathbf{Z(A)}),$$

dakle, $\mathbf{A}/\mathbf{Z(A)}$ je Hallova normalna podgrupa grupe $\mathbf{B}/\mathbf{Z(A)}$ (njen red je stepen od $p$, znači, uzajamno prost sa redom njene faktor grupe $\frac{n}{m}$). Opet po induktivnoj pretpostavci, $\mathbf{B}/\mathbf{Z(A)}$ ima podgrupu $\mathbf{C}/\mathbf{Z(A)}$ reda $\frac{n}{m}$. Konačno, prema 12.7 ($\mathbf{Z(A)}$ je $p$-normalna Abelova podgrupa grupe $\mathbf{C}$ i $(p, \frac{n}{m}) = 1$), $\mathbf{C}$ ima podgrupu $\mathbf{D}$ reda $\frac{n}{m}$.■

**Napomena**. Naravno, teoremu Schur-Zassenhausa smo mogli i ovako definisati:

*Svaka normalna Hallova podgrupa ima komplement.*

Dopunu ove teoreme daćemo u 49.46.

**Teorema 16.50** *(Teorema Burnsidea). Neka je $\mathbf{G}$ konačna grupa, $\mathbf{A}$ jedna njena Sylowa $p$-podgrupa i neka je $\mathbf{N(A)} = \mathbf{C(A)}$. Tada važi:*

*(a) $\mathbf{A}$ ima normalni komplement u $\mathbf{G}$;*

*(b) Red izvodne podgrupe grupe $\mathbf{G}$ nije deljiv sa $p$.*

**Dokaz**. (a) $\mathbf{A}$ je, zbog uslova $\mathbf{N(A)} = \mathbf{C(A)}$, Abelova grupa. Neka je $\Phi_t$ transfer grupe $\mathbf{G}$ u $\mathbf{A}$ i $a$ nejedinični element iz $A$. Prema 15.3, postoji skup elemenata $\{g_0, \ldots, g_{k-1}\}$ (podskup jedne leve transverzale podgrupe $\mathbf{A}$) i skup pozitivnih prirodnih brojeva $n_j$, $j = 0, \ldots, k-1$, takvi da je $(a)\Phi_t = \prod_{j=0}^{k-1}(g_j^{-1}a^{n_j}g_j)$, $\sum_{j=0}^{k-1} n_j = [\mathbf{G} : \mathbf{A}]$ i, za svako $j$, $n_j$ je najmanji među pozitivnim prirodnim brojevima, $m$ za koje je $g_j^{-1}a^m g_j \in A$. Kako su $a^{n_j}$ i $g_j^{-1}a^{n_j}g_j$ konjugovani elementi (u $\mathbf{G}$), konjugovani su i u $\mathbf{N(A)}$ (16.34(b)), te je, za neko $b \in N(\mathbf{A})$ $(= C(\mathbf{A}))$, $a^{n_j} = b^{-1}a^{n_j}b = g_j^{-1}a^{n_j}g_j$. Sledi: $(a)\Phi_t = \prod_{j=0}^{k-1} a^{n_j} = a^{\sum_{j=0}^{k-1} n_j} = a^{[\mathbf{G}:\mathbf{A}]} \neq e$ (jer, $(p, [\mathbf{G} : \mathbf{A}]) = 1$ i $a \neq e$). Prema tome, $\mathbf{Ker}(\Phi_t) \cap \mathbf{A} = \mathbf{E}$ i $\Phi_t|_A$ je injektivno preslikavanje; dakle, $(\mathbf{A})\Phi_t = \mathbf{A}$ i $\mathbf{A} = (\mathbf{G})\Phi_t \cong \mathbf{G}/\mathbf{Ker}(\Phi_t)$. Odatle, $|G| = |A| \cdot |Ker(\Phi_t)| = |A\, Ker(\Phi_t)|$ (zbog $\mathbf{A} \cap \mathbf{Ker}(\Phi_t) = \mathbf{E}$ – 3.21), tj. $\mathbf{G} = \mathbf{A}\,\mathbf{Ker}(\Phi_t)$; $\mathbf{Ker}(\Phi_t)$ je, znači, normalni komplement podgrupe $\mathbf{A}$.



(b) Pošto je, prema dokazu prethodne tačke, $\mathbf{G}/\mathbf{Ker}(\Phi_t)$ $(\cong \mathbf{A})$ Abelova grupa, to je $\mathbf{G}' \leq \mathbf{Ker}(\Phi_t)$, a red podgrupe $\mathbf{Ker}(\Phi_t)$, $|Ker(\Phi_t)| = \frac{|G|}{|A|}$, nije deljiv sa $p$.■

**Korolar 16.51** *Ako je $p$ najmanji prost broj koji deli red konačne grupe $\mathbf{G}$ i ako je Sylowa $p$-podgrupa $\mathbf{A}$ (grupe $\mathbf{G}$), reda $p^n$, ciklična, onda ona ima normalni komplement.*

**Dokaz**. Prema 8.26 i 8.27 ($N/C$-teorema) grupa $\mathbf{N(A)}/\mathbf{C(A)}$ je izomorfna podgrupi grupe $\mathbf{Aut(A)}$ $(\cong \mathbf{Z}_{p^{n-1}(p-1)})$. Red grupe $\mathbf{N(A)}/\mathbf{C(A)}$ nije deljiv sa $p$ (zbog $\mathbf{A} \leq \mathbf{C(A)}$), pa $|\frac{N(\mathbf{A})}{C(\mathbf{A})}|$ deli $p-1$. No $|\frac{N(\mathbf{A})}{C(\mathbf{A})}|$ deli i red grupe $\mathbf{G}$ i kako je (po uslovu) $p$ najmanji prost faktor reda grupe, to je $|\frac{N(\mathbf{A})}{C(\mathbf{A})}| = 1$, odnosno, $\mathbf{N(A)} = \mathbf{C(A)}$, te prema prethodnoj teoremi $\mathbf{A}$ ima normalni komplement.□

**Korolar 16.52** *Ako je $\mathbf{G}$ prosta grupa reda $pm$, gde je $m > 1$, $p$ – prost broj i $(p, m) = 1$, i ako je $\mathbf{A}$ jedna njena Sylowa $p$-podgrupa, tada je $\mathbf{C(A)}$ prava podgrupa grupe $\mathbf{N(A)}$ i $[\mathbf{N(A)} : \mathbf{C(A)}]$ deli $p-1$.*

**Dokaz**. Pošto je $\mathbf{G}$ prosta grupa, $\mathbf{N(A)}$ je njena prava podgrupa, a $\mathbf{C(A)}$ je prava podgrupa grupe $\mathbf{N(A)}$ (u suprotnom bi, prema prethodnoj teoremi, podgrupa $\mathbf{A}$ imala normalni komplement). $\mathbf{N(A)}/\mathbf{C(A)}$ je pak izomorfna podgrupi grupe $\mathbf{Aut(A)}$ $(\cong \mathbf{Z}_{p-1})$, pa $[\mathbf{N(A)} : \mathbf{C(A)}]$ deli $p-1$.□

**Primer 16.53** *(a) Neka su $p$ i $q$ prosti brojevi i neka je $p > q$. Tada postoji najviše dve grupe reda $pq$ (i nijedna od njih nije prosta).*

*Za svaki neparan prost broj $p$ postoje dve grupe reda $2p$ – ciklična grupa $\mathbf{C}_{2p}$ i dijedarska grupa stepena $p$ – $\mathbf{D}_p$.*

**Dokaz**. Jasno, s obzirom na uslove, u svakoj grupi reda $pq$ Sylowa $p$-podgrupa je jedinstvena (znači i normalna). Prema tome, uvek je u pitanju poludirektni proizvod (normalne) ciklične podgrupe reda $p$ i ciklične grupe reda $q$ (jedne Sylowe $q$-podgrupe). Ako $q$ ne deli $p-1$, onda je i Sylowa $q$-podgrupa jedinstvena, pa imamo samo direktni proizvod cikličnih grupa redova, respektivno, $p$ i $q$, odnosno, cikličnu grupu reda $pq$. Ako $q$ deli $p-1$, pored ciklične grupe reda $pq$ postoji i poludirektni proizvod u kome je, za generatorne elemente $a$ i $b$ Sylowe $p$-podgrupe i jedne od $(p)$ Sylowih $q$-podgrupa, $ab = ba^{m^r}$, gde je $m$ generatorni element grupe $\langle\{k \mid 1 \leq k \leq p-1\}, \cdot_p\rangle$ $(\cong \mathbf{Aut}(\mathbf{C}_p))$. Dokazi navedenih činjenica dati su u 13.12(b).

**Napomena**. U narednom razmatranju, kao i u većini kasnijih, nećemo se upuštati u ispitivanje i da li su svi tretirani slučajevi stvarno mogući; bitno će nam biti da pokažemo da nas svi slučajevi koje ne možemo apriori odbaciti vode do grupe sa normalnom podgrupom.

*(b) Ne postoji prosta grupa reda $p^2q$, gde su $p$ i $q$ prosti brojevi.*

**Dokaz.** Slučaj $p = q$ je poznat – 16.16.

Neka je $\mathbf{G}$ grupa reda $p^2q$, $p \neq q$, i neka je $s_p = q$ ($s_p = 1$ znači da je jedinstvena Sylowa $p$-podgrupa normalna, što odmah završava dokaz). Neka su $\mathbf{A}$ i $\mathbf{B}$ dve različite Sylowe $p$-podgrupe. Ako je $|A \cap B| = p$, onda je $\mathbf{A} \cap \mathbf{B} \lhd \mathbf{A}$ i $\mathbf{A} \cap \mathbf{B} \lhd \mathbf{B}$. Prema tome je $AB \subseteq N(\mathbf{A} \cap \mathbf{B})$, i kako je $|AB| = \frac{|A| \cdot |B|}{|A \cap B|} = p^3$ (3.21) i $p^2 \mid |N(\mathbf{A} \cap \mathbf{B})|$, mora biti $N(\mathbf{A} \cap \mathbf{B}) = G$, tj. $\mathbf{A} \cap \mathbf{B} \lhd \mathbf{G}$ (pažljivi čitalac će primetiti da smo, faktički, ponovili dokaz leme 16.35). Ako je, s druge strane, presek svake dve Sylowe $p$-podgrupe jedinična grupa, tada unija svih Sylowih $p$-podgrupa sadrži $q(p^2 - 1) + 1$ elemenata, pa van te unije ima svega $q - 1$ elemenata, što implicira da postoji samo jedna Sylowa $q$-podgrupa.

(*c*) *Ako su $p$ i $q$ različiti prosti brojevi, grupe reda $p^2q^2$ i $p^2q^3$ imaju normalnu Sylowu podgrupu.*

**Dokaz.** Neka je $p < q$ i $\mathbf{G}$ grupa reda $p^2q^2$. Ako je $s_q = 1$, onda je jedinstvena Sylowa $q$-podgrupa i normalna. Ako je $s_q = p^2$ i $\mathbf{A}$ jedna (od) Sylowih $q$-podgrupa, tada je $|N(\mathbf{A})| = \frac{|G|}{p^2} = q^2$, pa je $\mathbf{A} = \mathbf{C}(\mathbf{A}) = \mathbf{N}(\mathbf{A})$ i prema teoremi Burnsidea, $\mathbf{A}$ ima normalni komplement. No taj je reda $p^2$.

Neka je i dalje $p < q$, a $\mathbf{G}$ grupa reda $p^2q^3$ bez normalne Sylowe $q$-podgrupe. Onda, opet, $s_q = p^2$ i, odatle, $q$ deli $p^2 - 1$, te je $q = p + 1$; znači $p = 2$, $q = 3$, $s_3 = 4$. Neka je $\mathbf{A}$ jedna od Sylowih 3-podgrupa. Ako je $\mathbf{A}$ Abelova grupa, prema teoremi Burnsidea ima normalni komplement i to je Sylowa 2-podgrupa ($|N(\mathbf{A})| = \frac{2^2 3^3}{2^2} = 3^3$ i $\mathbf{A} = \mathbf{C}(\mathbf{A}) = \mathbf{N}(\mathbf{A})$). Pretpostavimo da $\mathbf{A}$ nije Abelova grupa. Tada je, prema 4.13 i 8.19, $|Z(\mathbf{A})| = 3$. Prema 16.35 (videti dokaz leme), za neku Sylowu 3-podgrupu $\mathbf{B}$ je: $|A \cap B| = 9$ i $\mathbf{A} \cap \mathbf{B} \lhd \mathbf{A}$, $\mathbf{A} \cap \mathbf{B} \lhd \mathbf{B}$. Prema tome, $|AB| = 3^4 \leq |N(\mathbf{A} \cap \mathbf{B})|$ i stoga $\mathbf{N}(\mathbf{A} \cap \mathbf{B}) = \mathbf{G}$, tj. $\mathbf{A} \cap \mathbf{B} \lhd \mathbf{G}$. Jasno, $\mathbf{Z}(\mathbf{A}) < \mathbf{A} \cap \mathbf{B}$; u suprotnom bi važilo: $\mathbf{A} = (\mathbf{A} \cap \mathbf{B}) \times \mathbf{Z}(\mathbf{A})$ i $\mathbf{A}$ bi bila Abelova grupa (uostalom, tu je i opšti stav 16.22). Prema $N/C$-teoremi (8.27), grupa $\mathbf{N}(\mathbf{Z}(\mathbf{A}))/\mathbf{C}(\mathbf{Z}(\mathbf{A}))$ je izomorfna podgrupi grupe $\mathbf{Aut}(\mathbf{Z}(\mathbf{A}))$ ($\cong \mathbf{Z}_2$). Ako je $\mathbf{N}(\mathbf{Z}(\mathbf{A})) = \mathbf{G}$ (odnosno $\mathbf{Z}(\mathbf{A}) \lhd \mathbf{G}$), onda je i $\mathbf{C}(\mathbf{Z}(\mathbf{A})) = \mathbf{G}$ ili, drugim rečima, $\mathbf{Z}(\mathbf{A}) \leq \mathbf{Z}(\mathbf{G})$. Jer grupa $\mathbf{G}$ nema podgrupa indeksa 2. Naime, ako bi $\mathbf{K}$ bila jedna takva ($|K| = 54$) i $\mathbf{C}$ njena jedinstvena Sylowa 3-podgrupa, dakle i karakteristična, sledilo bi $\mathbf{C} \lhd \mathbf{G}$, kontradikcija. Prema prvom delu tvrđenja i našoj pretpostavci, faktor grupa $\mathbf{G}/\mathbf{Z}(\mathbf{A})$, reda $2^2 3^2$, ima normalnu podgrupu reda $2^2$, $\overline{\mathbf{M}}$ (ako bi grupa $\mathbf{G}/\mathbf{Z}(\mathbf{A})$ imala normalnu podgrupu reda $3^2$, grupa $\mathbf{G}$ bi imala, prema 8.7, normalnu Sylowu 3-podgrupu). Ako je, za $\mathbf{Z}(\mathbf{A}) < \mathbf{M} < \mathbf{G}$, $\overline{\mathbf{M}} = \mathbf{M}/\mathbf{A}$, tada je $\mathbf{M}$ normalna podgrupa reda 12. Zbog $\mathbf{G} = \mathbf{C}(\mathbf{Z}(\mathbf{A}))$, grupa $\mathbf{M}$ ima jedinstvenu, a onda i karakterističnu, Sylowu 2-podgrupu $\mathbf{D}$ (zapravo je $\mathbf{M} = \mathbf{Z}(\mathbf{A}) \times \mathbf{D}$ i $\mathbf{D} \lhd \mathbf{G}$). Ovim je dokaz i završen, jer pretpostavka da $\mathbf{Z}(\mathbf{A})$ nije normalna podgrupa vodi u protivurečnost. Zaista, pošto $\mathbf{G}$ nema podgrupa reda 54, bilo bi $\mathbf{A} = \mathbf{N}(\mathbf{Z}(\mathbf{A}))$ i centar podgrupe



$\mathbf{A}$ bi imao četiri konjugata ($[\mathbf{G} : \mathbf{A}] = 4$), svi sadržani u $\mathbf{A} \cap \mathbf{B}$ ($\lhd \mathbf{G}$). Ako bi to bili $\mathbf{H}_0 = \mathbf{Z}(\mathbf{A})$, $\mathbf{H}_1 = g_1^{-1}\mathbf{H}_0 g$, $\mathbf{H}_2 = g_2^{-1}\mathbf{H}_0 g_2$ i $\mathbf{H}_3 = g_3^{-1}\mathbf{H}_0 g_3$ (za neke elemente $g_1, g_2, g_3$), tada bi, za element $g$ reda 2 i npr. $g^{-1}\mathbf{H}_0 g = \mathbf{H}_1$, bilo: $g^{-1}\mathbf{H}_1 g = \mathbf{H}_0$, $g^{-1}\mathbf{H}_2 g = \mathbf{H}_3$ i $g^{-1}\mathbf{H}_3 g = \mathbf{H}_2$ (recimo, $g\mathbf{H}_2 g = \mathbf{H}_2$ bi dalo: $g_2 g g_2^{-1} \in N(\mathbf{H}_0) = A$, dok je element $g_2 g g_2^{-1}$ reda 2). Ali, $a \in H_0$ i $gag = b$ ($\in H_1$) impliciralo bi: $gbg = a$ i $g(ab)g = gag \cdot gbg = ba = ab$, kontradikcija (ako je, recimo, $ab \in H_3$, njegova slika bi morala biti u $H_4$).

(*d*) *Ne postoji prosta grupa reda $p^k m$, gde je $p$ prost broj, $k \geq 1$ i $m < p$.*

(*e*) *Ne postoji prosta grupa složenog reda manjeg od* 60.

**Dokaz.** Sadržan u već izvedenim stavovima. U nekim slučajevima se možemo istovremeno pozvati na više njih. Tako npr. da grupe reda 6, 10, 14 nisu proste pokazuje tačka (*a*) ali i činjenica da ne postoji prosta grupa reda $4n + 2$ za $n \geq 1$ (9.32).

Grupe reda 12, 24, 48 nisu proste prema 16.29 (ali i prema 16.35) – u svim slučajevima $s_2$ je ili 1 ili $3 = 1 + 2$, a red grupe je deljiv sa $2^2$.

Grupe reda 9, 25, 49 nisu proste prema 10.26.

Grupa reda 36 nije prosta prema tački (*c*).

Grupa reda 54 ima jedinstvenu Sylowu 3-podgrupu (to smo već konstatovali u dokazu tačke (*c*)).

Grupa reda $56 = 2^3 \cdot 7$ nije prosta, jer ako je $s_7 = 8$ (ponavljamo: ne ulazimo u to da li je taj slučaj i stvarno moguć, odnosno da li postoji grupa reda 56 sa osam Sylowih 7-podgrupa), onda unija svih Sylowih 7-podgrupa ima $8 \cdot 6 + 1 = 49$ elemenata (u cikličnoj grupi prostog reda svaki nejedinični element je generatoran), te postoji samo jedna Sylowa 2-podgrupa.

(*f*) *Postoji samo jedna prosta grupa reda* 60.

**Dokaz.** Za jednu već znamo: $\mathbf{A}_5$ – alternativna grupa stepena 5.

Neka je $\mathbf{G}$ prosta grupa reda $60 = 2^2 \cdot 3 \cdot 5$. Konstatujmo odmah da je onda $s_5 = 6$ (znači, grupa $\mathbf{G}$ je izomorfna nekoj podgrupi grupe $\mathbf{A}_6$). Za $s_2$ imamo sledeći izbor: 5, 15; 16.29 isključuje $s_2 = 3$; ali i 9.36: grupa $\mathbf{G}$ bi se mogla utopiti (izomorfno preslikati) u grupu $\mathbf{A}_3$ – normalizator bilo koje Sylowe 2-podgrupe bio bi indeksa 3. No 9.36 takođe implicira i da se za $s_2 = 5$ $\mathbf{G}$ izomorfno preslikava u $\mathbf{A}_5$, odnosno da su grupe $\mathbf{G}$ i $\mathbf{A}_5$ izomorfne. Pretpostavimo, stoga (jer smo u potrazi za još nekom prostom grupom reda 60), da je $s_2 = 15$. $s_3$ pak mora biti 10; $s_3 = 4$ ne ide, ponovo zbog i 16.29 i 9.36. Unija svih Sylowih 3- i 5-podgrupa ima $10 \cdot 2 + 6 \cdot 4 + 1 = 45$ elemenata. Kako grupa $\mathbf{G}$ ima ukupno 60 elemenata, postoji nejedinični element $a$ koji se javlja u barem dve Sylowe 2-podgrupe, recimo $\mathbf{A}$ i $\mathbf{B}$ (koje su, kao grupe reda 4, Abelove). Ali tada $AB \subseteq C(a)$ (= centalizator elementa $a$). S obzirom da je $|AB| = \frac{4 \cdot 4}{2} = 8$ i red od $C(a)$ faktor broja 60 deljiv sa 4, sledi $|C(a)| \geq 12$. Dakle, $[\mathbf{G} : \mathbf{C}(a)] \leq 5$ i opet bi se grupa $\mathbf{G}$ izomorfno preslikala u $\mathbf{A}_5$, kontradikcija.

Sylowe 2-podgrupe alternativne grupe $\mathbf{A}_5$ su Kleinove grupe, ima ih, rekli smo, pet i oblika su $\langle\{\imath,(i\,j)(k\,l),(i\,k)(j\,l),(i\,l)(j\,k)\},\circ\rangle$ ($i,j,k,l$ su različiti elementi skupa $5=\{0,1,2,3,4\}$). Sylowe 3-podgrupe su ciklične, generisane tercetima $(i\,j\,k)$, i ima ih $10=\frac{1}{2}\cdot\frac{V_3^5}{3}$ – postoji 20 različitih terceta, a po dva, uzajamno inverzna, ulaze u istu (cikličnu) Sylowu 3-podgrupu. Šest Sylowih 5-podgrupa su takođe ciklične grupe i generisane su ciklusima dužine 5 – takvih, različitih, ima $\frac{V_5^5}{5}=24$, a po četiri su u istoj Sylowoj 5-podgrupi.

($g$) *Za prost broj $p$ grupa $\mathbf{S}_p$ ima $(p-2)!$ Sylowih $p$-podgrupa.*

**Dokaz.** Neka je $A$ skup svih elemenata reda $p$ grupe $\mathbf{S}_p$. Već znamo (radi se o $p$-ciklusima): $|A|=\frac{V_p^p}{p}=(p-1)!$. Ako $\alpha,\beta\in A$, onda i $\langle\alpha\rangle\setminus\{\imath\}\subseteq A$, a ili je $\langle\alpha\rangle=\langle\beta\rangle$ ili $\langle\alpha\rangle\cap\langle\beta\rangle=\{\imath\}$. Prema tome, Sylowih $p$-podgrupa, a one su reda $p$ (jer, jasno, $p^2$ ne deli $p!$), ima $\frac{(p-1)!}{p-1}=(p-2)!$

Prema navedenom $p|((p-2)!-1)$. Neposredna posledica tog rezultata je *Wilsonova teorema* (J. Wilson, 1741-1793) iz teorije brojeva: $p|((p-1)!+1)$. Jer, $(p-1)!+1=p(p-2)!-[(p-2)!-1]$.

($h$) *Ne postoji prosta grupa reda $2^3\cdot 3\cdot 7\cdot 23$.*

**Dokaz.** Pretpostavimo da je $\mathbf{G}$ prosta grupa datog reda. Onda je $s_{23}=24$, pa ako je $\mathbf{A}$ Sylowa 23-podgrupa, onda je $|N(\mathbf{A})|=7\cdot 23$ $(=\frac{|G|}{24})$, a prema 16.52, $\mathbf{C}(\mathbf{A})$ je prava podgrupa grupe $\mathbf{N}(\mathbf{A})$, dakle reda 23 ($\mathbf{A}$ je ciklična grupa, što će reći: $\mathbf{A}\leq\mathbf{C}(\mathbf{A})$) i $[\mathbf{N}(\mathbf{A}):\mathbf{C}(\mathbf{A})]=7$ deli 22, kontradikcija.

($i$) *Ako je $\mathbf{H}$ normalna Sylowa $p$-podgrupa grupe $\mathbf{G}$, onda je i potpuno invarijantna.*

**Dokaz.** Direktno, prema 16.3 i 16.28.

($j$) *U grupi $\mathbf{G}=\mathbf{S}_3\times\mathbf{S}_3$ postoje tri različite Sylowe 2-podgrupe, $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, takve da je $\mathbf{A}\cap\mathbf{B}=\mathbf{E}$ i $\mathbf{A}\cap\mathbf{C}\neq\mathbf{E}$.*

**Dokaz.** Neka su elementi grupe $\mathbf{G}$ uređeni parovi $(\alpha,\beta)$, $\alpha,\beta\in S_3$. Data grupa ima ukupno 9 Sylowih 2-podgrupa i to su Kleinove grupe. Generalno, za svake dve transpozicije $\alpha,\beta\in S_3$ postoji Sylowa 2-podgrupa $\mathbf{H}_{\alpha,\beta}$ sa domenom $\{(\imath,\imath),(\alpha,\imath),(\imath,\beta),(\alpha,\beta)\}$ ($\imath$ – jedinični element grupe $\mathbf{S}_3$). Ako uzmemo da je npr. $\mathbf{A}=\mathbf{H}_{(0\,1),(0\,1)}$, $\mathbf{B}=\mathbf{H}_{(0\,2),(0\,2)}$ i $\mathbf{C}=\mathbf{H}_{(0\,1),(0\,2)}$, tada je $\mathbf{A}\cap\mathbf{B}=\mathbf{E}$ i $\mathbf{A}\cap\mathbf{C}=\langle((0\ 1),\imath)\rangle$.

($k$) *Sylowe 2-podgrupe grupe $\mathbf{G}=\prod_{n<\omega}\mathbf{S}_3^n$, gde je, za svaki prirodan broj $n$, $\mathbf{S}_3^n$ "kopija" simetrične grupe $\mathbf{S}_3$, ne čine klasu konjugovanih podgrupa.*

**Dokaz.** Ako je, za $n<\omega$, $\mathbf{H}^n$ (jedna) podgrupa reda 2 grupe $\mathbf{S}_3^n$, tada je $\mathbf{H}=\prod_{n<\omega}\mathbf{H}^n$ Sylowa 2-podgrupa grupe $\mathbf{G}$ (jasno, svaka podgrupa grupe $\mathbf{G}$ koja strogo sadrži $\mathbf{H}$ ima element reda 3). Kako grupa $\mathbf{S}_3$ ima tri podgrupe reda 2, grupa $\mathbf{G}$ ima $2^{\aleph_0}=c$ mnogo Sylowih 2-podgrupa (koliko ima i beskonačnih nizova čiji su članovi iz skupa $\{1,2,3\}$), i pošto je prebrojiva ne mogu sve njene Sylowe 2-podgrupe biti uzajamno konjugovane.□



Paragraf završavamo sa tri rezultata vezanih za lokalno konačne grupe.

**Lema 16.54** *Ako lokalno konačna grupa ima konačnu Sylowu $p$-podgrupu, onda su sve njene Sylowe $p$-podgrupe konjugovane.*

**Dokaz.** Neka je $\mathbf{G}$ lokalno konačna grupa sa konačnom Sylowom $p$-podgrupom $\mathbf{P}$. Ako je $\mathbf{P}_1$ konačna $p$-podgrupa grupe $\mathbf{G}$, onda je, s obzirom na lokalnu konačnost grupe $\mathbf{G}$, podgrupa $\langle P\cup P_1\rangle$ konačna i, evidentno, $\mathbf{P}$ je njena Sylowa $p$-podgrupa. Prema 18.5($a$), podgrupa $\mathbf{P}_1$ je sadržana u nekom konjugatu podgrupe $\mathbf{P}$. Odatle sledi $|P_1|\leq|P|$ i dalje, da su sve Sylowe $p$-podgrupe konačne. Ponavljajući argument zaključujemo i da su sve Sylowe $p$-podgrupe grupe $\mathbf{G}$ konjugovane.□

**Teorema 16.55** *(Asar). Ako svaka prebrojiva podgrupa lokalno konačne grupe $\mathbf{G}$ ima samo prebrojivo mnogo Sylowih $p$-podgrupa, onda su sve Sylowe $p$-podgrupe grupe $\mathbf{G}$ konjugovane.*

**Dokaz.** Jasno, polazimo od toga da nema konačnih Sylowih podgrupa pa pokazujemo da pretpostavka da grupa $\mathbf{G}$ ima dve Sylowe $p$-podgrupe koje nisu uzajamno konjugovane vodi u kontradikciju. Dokazujemo to u tri koraka.

Prvo pokazujemo:

**Stav 1.** *Postoji Sylowa $p$-podgrupa sa svojstvom da je svaka njena konačna podgrupa sadržana u bar dve Sylowe $p$-podgrupe.*

**Dokaz.** Neka su $\mathbf{P}$ i $\mathbf{Q}$ Sylowe $p$-podgrupe koje nisu konjugovane i neka gornje tvrđenje nije tačno za podgrupu $\mathbf{Q}$; neka je $\mathbf{K}$ njena konačna podgrupa koja nije sadržana ni u jednoj drugoj Sylowoj $p$-podgrupi grupe $\mathbf{G}$. Ako je $\mathbf{H}$ bilo koja konačna podgrupa grupe $\mathbf{P}$, tada je podgrupa $\mathbf{M}=\langle H\cup K\rangle$ konačna, a $\mathbf{M}\cap\mathbf{Q}$ je njena Sylowa $p$-podgrupa. Zaista, $\mathbf{M}\cap\mathbf{Q}$ je sadržano u nekoj Sylowoj $p$-podgrupi $\mathbf{Q}_1$ grupe $\mathbf{M}$, koja je pak sadržana u nekoj Sylowoj $p$-podgrupi $\mathbf{Q}_2$ grupe $\mathbf{G}$. No kako je $\mathbf{K}\leq\mathbf{M}\cap\mathbf{Q}\leq\mathbf{Q}_2$, mora biti $\mathbf{Q}=\mathbf{Q}_2$, a tada i $\mathbf{M}\cap\mathbf{Q}=\mathbf{Q}_1$. Stoga je, za neko $g\in M$, $\mathbf{H}\leq g^{-1}(\mathbf{M}\cap\mathbf{Q})g\leq g^{-1}\mathbf{Q}g\neq\mathbf{P}$, pa je navedeno tvrđenje tačno za podgrupu $\mathbf{P}$.□

Za podgrupu $\mathbf{P}$ važi i:

**Stav 2.** *Za svaku konačnu podgrupu $\mathbf{H}$ grupe $\mathbf{P}$ postoje konačna podgrupa $\mathbf{H}_0$ grupe $\mathbf{P}$ i njen konjugat $\mathbf{H}_1$ takve da je: $\mathbf{H}<\mathbf{H}_0$, $\mathbf{H}<\mathbf{H}_1$ i $\langle H_0\cup H_1\rangle$ nije $p$-grupa.*

**Dokaz.** Podgrupa $\mathbf{H}$ je, prema izboru podgrupe $\mathbf{P}$, sadržana u još nekoj Sylowoj $p$-podgrupi, recimo $\mathbf{Q}$. Jasno, za $a\in Q\setminus P$, $\mathbf{K}=\langle\{a\}\cup H\rangle$ je konačna $p$-podgrupa grupe $\mathbf{Q}$. $\mathbf{M}=\mathbf{P}\cap\mathbf{K}$ je prava podgrupa grupe $\mathbf{K}$ i, prema 4.29, $\mathbf{M}<\mathbf{N}_{\mathbf{K}}(\mathbf{M})$. Kako je $\mathbf{N}_{\mathbf{K}}(\mathbf{M})$ $p$-grupa i $\mathbf{P}$ jedina Sylowa $p$-podgrupa grupe $\mathbf{N}_{\mathbf{G}}(\mathbf{P})$, ne može biti $\mathbf{N}_{\mathbf{K}}(\mathbf{M})\leq\mathbf{N}_{\mathbf{G}}(\mathbf{P})$ (u suprotnom bismo odmah imali: $\mathbf{N}_{\mathbf{K}}(\mathbf{M})\leq\mathbf{P}$, kontradikcija). Neka je $b\in N_{\mathbf{K}}(\mathbf{M})\setminus N_{\mathbf{G}}(\mathbf{P})$. Onda, jasno, (pod)grupa $\langle P\cup b^{-1}Pb\rangle$ nije $p$-grupa (inače, $b^{-1}Pb=P$ i $b\in$

$N_{\mathbf{G}}(\mathbf{P})$), pa postoji konačna podgrupa $\mathbf{H}_0$ grupe $\mathbf{P}$, koja sadrži $\mathbf{M}$ i takva je da $\langle H_0 \cup b^{-1}H_0b\rangle$ nije $p$-grupa. Stavimo: $\mathbf{H}_1 = b^{-1}\mathbf{H}_0b$. Sada: $\mathbf{H} \leq \mathbf{M} = b^{-1}\mathbf{M}b \leq b^{-1}\mathbf{H}_0b = \mathbf{H}_1$ i $\mathbf{H} < \mathbf{H}_0$, pošto je $\langle H \cup b^{-1}Hb\rangle$ podgrupa $p$-grupe $\mathbf{M}$ (naravno, $\mathbf{H}$ je i prava podgrupa grupe $\mathbf{H}_1$).□

Konačno, imajući u vidu dokaz Stava 2, kao i činjenicu da Stavovi 1 i 2 važe za bilo koji konjugat grupe $\mathbf{P}$, zaključujemo prema Stavu 2 da startujući od bilo koje konačne podgrupe $\mathbf{H}$ grupe $\mathbf{P}$ i bilo kog beskonačnog niza $\alpha = (k_0, k_1, \ldots)$, čiji su elementi 0 i 1, možemo formirati strogo rastući niz konačnih $p$-podgrupa

$$\mathbf{H} < \mathbf{H}_{k_0} < \mathbf{H}_{k_0k_1} < \cdots \qquad (*_\alpha)$$

sa svojstvom da, za svaki prirodan broj $r$, $\langle H_{k_0\ldots k_r0} \cup H_{k_0\ldots k_r1}\rangle$ nije $p$-grupa. Ako je $\mathbf{H}_\alpha$ unija podgrupa lanca $(*_\alpha)$, onda, očigledno, za različite nizove $\alpha$ i $\beta$ podgrupe $\mathbf{H}_\alpha$ i $\mathbf{H}_\beta$ ne pripadaju istoj $p$-podgrupi grupe $\mathbf{G}$. No sada je podgrupa $\mathbf{K}$ grupe $\mathbf{G}$ generisana unijom domena svih podgrupa $\mathbf{H}_\alpha$, tj. unijom domena svih (konačnih) podgrupa $\mathbf{H}_{k_0\ldots k_r}$ (gde je $r \in \omega$ i $(k_0, \ldots, k_r)$ konačan niz sa elementima 0 i 1), prebrojiva, dok s druge strane sadrži kontinuum mnogo Sylowih $p$-podgrupa (onoliko koliko ima i beskonačnih nizova sa elementima 0 i 1).■

**Korolar 16.56** *Neka je $\mathbf{G}$ prebrojiva lokalno konačna grupa. Tada su sve Sylowe $p$-podgrupe grupe $\mathbf{G}$ konjugovane akko ih ima prebrojivo mnogo.*

**Dokaz**. Pravac ($\Longrightarrow$) je jasan. Što se tiče suprotnog "smera", prema prethodnoj teoremi dovoljno je da pokažemo da svaka podgrupa grupe $\mathbf{G}$ sadrži takođe prebrojivo mnogo Sylowih $p$-podgrupa. Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$ i $\mathbf{P}$ Sylowa $p$-podgrupa grupe $\mathbf{H}$. Ako je $\mathbf{Q}$ Sylowa $p$-podgrupa grupe $\mathbf{G}$ koja sadrži $\mathbf{P}$, onda je, jasno, $\mathbf{P} = \mathbf{H} \cap \mathbf{Q}$. Prema tome, Sylowe $p$-podgrupe grupe $\mathbf{H}$ se dobijaju u preseku podgrupe $\mathbf{H}$ sa Sylowim $p$-podgrupama grupe $\mathbf{G}$, pa ih je prebrojivo mnogo.□

**Napomena**. Poslednja tačka poslednjeg primera nam kaže da bez uslova o prebrojivosti Sylowih $p$-podgrupa prebrojive lokalno konačne grupe nemamo nužno ni konjugovanost tih podgrupa.

## 17 Lokalna svojstva

Neka je $\mathcal{R}$ neko svojstvo koje se odnosi na podgrupe. Obično se kaže da je $\mathcal{R}$ lokalno svojstvo grupe $\mathbf{G}$ akko ga ima svaka konačno generisana podgrupa grupe $\mathbf{G}$. Tako smo već imali primere lokalno konačnih, lokalno konačnih i normalnih i lokalno cikličnih grupa (tj. grupa gde su sve konačno generisane podgrupe konačne, odnosno konačnih normalnih zatvorenja, odnosno ciklične). U opštem, iz činjenice da je $\mathcal{R}$ lokalno svojstvo grupe $\mathbf{G}$ ne sledi da i sama grupa $\mathbf{G}$ ima to svojstvo; lokalno konačne grupe ne moraju biti konačne



(recimo, direktni proizvod beskonačno mnogo konačnih nejediničnih grupa), lokalno ciklične grupe ne moraju biti ciklične (videli smo da su **Ra** i Prüferove $p$-grupe lokalno ciklične). A. G. Kuroš i S. N. Černikov su pojam lokalnog svojstva uopštili uvodeći pojam lokalnog sistema podgrupa. Formalno

**Definicija 17.1** *Familija podgrupa $\mathcal{S} = \{\mathbf{H}_i \mid i \in I\}$ grupe $\mathbf{G}$ je lokalni sistem podgrupa akko važi:* (1) $G = \bigcup_{i\in I} H_i\ (= \bigcup \mathcal{S})$ *i* (2) *svake dve podgrupe iz $\mathcal{S}$ sadržane su u (nekoj) podgrupi iz $\mathcal{S}$.*

*Grupe $\mathbf{G}$ ima svojstvo $\mathcal{R}$ lokalno akko postoji lokalni sistem podgrupa $\mathcal{S}$ grupe $\mathbf{G}$ takav da svaka podgrupa iz $\mathcal{S}$ ima svojstvo $\mathcal{R}$.*

*Lokalna teorema za svojstvo $\mathcal{R}$ važi akko ma koja grupa $\mathbf{G}$ ima to svojstvo kad god ga ima lokalno.*

Familija konačno generisanih, normalnih, svih podgrupa primeri su lokalnih sistema. Konačno, $\{\mathbf{G}\}$ je takođe lokalni sistem podgrupa.

**Napomena**. Ako je svojstvo $\mathcal{R}$ *heriditarno* (*nasledno*), tj. prenosivo na podgrupe, onda grupa $\mathbf{G}$ ima svojstvo $\mathcal{R}$ lokalno (u smislu prethodne definicije) akko svaka njena konačno generisana podgrupa ima svojstvo $\mathcal{R}$; drugim rečima, u slučaju heriditarnih svojstava uobičajena definicija (s početka paragrafa) i njena uopštena verzija (prethodna definicija) se podudaraju. Jer, upravo smo konstatovali, familija konačno generisanih podgrupa je lokalni sistem; s druge strane, ako je dat lokalni sistem $\mathcal{S}$ grupe $\mathbf{G}$ čije sve podgrupe imaju svojstvo $\mathcal{R}$, onda je svaka konačno generisana podgrupa $\mathbf{A}$ grupe $\mathbf{G}$ podgrupa i neke podgrupe sistema $\mathcal{S}$ (prema tačkama (1) i (2) definicije lokalnog sistema), pa s obzirom na heriditarnost svojstva $\mathcal{R}$ i podgrupa $\mathbf{A}$ ima svojstvo $\mathcal{R}$.

Ovu napomenu ćemo često kasnije, kada je reč o heriditarnim svojstvima grupa, prećutno imati u vidu.

Teorema koja sledi koristi se kao (jedna) generalna metoda u dokazu da lokalno teorema važi. Opšteg je karaktera i od interesa je i u rešavanju problema drugih vrsta (i iz drugih grana matematike). Polazimo od parcijalnog uređenja familije $\mathcal{S}$ konačnih skupova $\langle\{A_i \mid i \in I\}\ (= \mathcal{S}), \leq\rangle$ koje ispunjava sledeće uslove:

(1) $\mathcal{S}$ je usmereni parcijalno uređeni skup (3.22 – podsećamo, to znači: za svaka dva elementa $A_i, A_j$ iz $\mathcal{S}$ postoji $A_k$ u $\mathcal{S}$ takvo da je $A_i \leq A_k$, $A_j \leq A_k$);

(2) za svako $A_i, A_j$ iz $\mathcal{S}$, ako je $A_i \leq A_j$, postoji surjektivno preslikavanje, tzv. *projekcija*, $\pi_{ji}$ skupa $A_j$ na skup $A_i$, i za sve projekcije važi:

(2)($a$) ako $A_i \leq A_j$ i $A_j \leq A_k$, onda je $\pi_{ki} = \pi_{kj} \circ \pi_{ji}$;

(2)($b$) $\pi_{ii}$ je identično preslikavanje na skupu $A_i$.

Neprazan skup $\mathcal{P} \subseteq \bigcup_{i\in I} A_i$ je *projekcioni skup* akko za svako $a, b \in \mathcal{P}$ postoji $c \in \mathcal{P}$ čije su slike, za neke projekcije, $a$ i $b$ – kažemo kraće i neformalno

da $a$ i $b$ imaju zajedničku inverznu sliku.

Iz definicije projekcionog skupa odmah sledi: za svako $i \in I$, $|A_i \cap \mathcal{P}| \leq 1$ ($a, b \in A_i \cap \mathcal{P}$, $a \neq b$ i $c \in \mathcal{P}$ ($\cap A_j$) dalo bi $(c)\pi_{ji} = a = b$, kontradikcija). Isto tako, ako je $a \in \mathcal{P} \cap A_i$, $b \in \mathcal{P} \cap A_j$ i $A_i \leq A_j$, tada je $a = (b)\pi_{ji}$.

Ako je za projekcioni skup $\mathcal{P}$ još ispunjeno: $|A_i \cap \mathcal{P}| = 1$ za svako $i \in I$, onda je $\mathcal{P}$ *kompletan (potpun) projekcioni skup.*

**Teorema 17.2** *Svaki projekcioni skup $\mathcal{P}$ parcijalno uređenog skupa $\mathcal{S}$ ($= \{A_i \mid i \in I\}$) koji ispunjava uslove* (1) *i* (2)($a$),($b$), *može se kompletirati, tj. deo je nekog kompletnog projekcionog skupa.*

**Dokaz.** Uvedimo jedno dobro uređenje na skupu $\mathcal{S}$, nezavisno od parcijalnog uređenja $\leq$ i za koje važi: svako $A_i$ koje ima neprazan presek sa $\mathcal{P}$ ispred svakog je $A_j$ koje je disjunktno sa $\mathcal{P}$ (jednostavno, ako je $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$, gde je $\mathcal{S}_1 = \{A_i \in \mathcal{S} \mid |A_i \cap \mathcal{P}| = 1\}$ i $\mathcal{S}_2 = \mathcal{S} \setminus \mathcal{S}_1$, možemo koristeći se dobrim uređenjima skupova $\mathcal{S}_1$, $\mathcal{S}_2$, na šta imamo pravo prema aksiomi izbora, dobro urediti skup $\mathcal{S}$ tako da su elementi iz $\mathcal{S}_1$ ispred elemenata iz $\mathcal{S}_2$). Neka je, s obzirom na uvedeno dobro uređenje, za neki ordinal $\mu$, $\mathcal{S} = \{A^\alpha \mid \alpha < \mu\}$; podrazumevamo, za $\alpha < \beta$ ($< \mu$), $A^\alpha$ je "ispred" $A^\beta$. Transfinitnom rekurzijom ćemo obeležiti (markirati) u svakom skupu $A^\alpha$ po jedan element ($a^\alpha$) tako da svaki konačan skup obeleženih elemenata ima zajedničku inverznu sliku, kao i da je svaki element projekcionog skupa $\mathcal{P}$ među obeleženim elementima. Recimo da je to već urađeno za sve ordinale manje od $\gamma$; ako je $\mathcal{S}_1 = \{A^\alpha \mid \alpha < \nu\}$, možemo odmah pretpostaviti, a tako ćemo i učiniti, da je $\gamma \geq \nu$. Naime, izbor dobrog uređenja (gde je svaki element iz $\mathcal{S}_1$ ispred svakog elementa iz $\mathcal{S}_2$) upravo nam omogućuje da sve elemente iz $\mathcal{P}$ direktno uključimo u skup obeleženih elemenata. U tom smislu mogli smo poći od nekog dobrog uređenja skupa $\mathcal{S}_2$ (ako je $\mathcal{S}_2 = \emptyset$ nemamo šta raditi) i "obeležavati" elemente (u elementima skupa $\mathcal{S}_2$) tako da unija skupa $\mathcal{P}$ i skupa obeleženih elemenata ispunjava postavljene uslove. Neka je $A^\gamma = A_k = \{b_1, \ldots, b_n\}$. Pretpostavka da za svaki element $b_i$ postoji konačan skup $B_{b_i}$ već obeleženih elemenata takav da elementi skupa $B_{b_i} \cup \{b_i\}$ nemaju zajedničku inverznu sliku vodi u kontradikciju. Jer, elementi skupa $B = \bigcup_{i=1}^{n} B_{b_i}$ imaju zajedničku inverznu sliku, recimo $c$ u $A_i$, pa ako je $d$ (ma koja) inverzna slika elementa $c$ u $A_j$, gde je $A_i \leq A_j$, $A^\gamma = A_k \leq A_j$, i ako je $(d)\pi_{jk} = b_m$ ($1 \leq m \leq n$), proizilazi da elementi skupa $B \cup \{b_m\}$ imaju zajedničku inverznu sliku, suprotno hipotezi. Među elementima iz $A^\gamma$ koji imaju zajedničku inverznu sliku sa elementima svakog konačnog (pod)skupa već obeleženih elemenata biramo jedan, neka je to $a^\gamma$; možemo i svaki od skupova $A^\alpha$ smatrati dobro uređenim, te u slučaju da nam je na raspolaganju više kandidata za izbor obeleženog elementa, uzimati prvi po "spisku". Skup svih obeleženih elemenata – $\overline{\mathcal{P}} = \{a^\alpha \mid \alpha < \mu\}$ – je, tvrdimo, kompletan projekcioni skup. Zaista, elementi $a^\alpha$ ($\in A^\alpha = A_i$) i $a^\beta$ ($\in A^\beta = A_j$) imaju zajedničku inverznu sliku, neka je to $c$ iz $A^\gamma = A_k$, ali i



$a^\alpha, a^\beta, a^\gamma$ imaju zajedničku inverznu sliku, recimo $d$ iz $A^\delta = A_l$, te je i $a^\gamma$ zajednička inverzna slika elemenata $a^\alpha, a^\beta$ ($a^\alpha = (d)\pi_{li} = ((d)\pi_{lk})\pi_{ki} = (a^\gamma)\pi_{ki}$, $a^\beta = (d)\pi_{lj} = ((d)\pi_{lk})\pi_{kj} = (a^\gamma)\pi_{kj}$).■

**Napomena.** Egzistencija kompletnog projekcionog skupa (samo sada ne nužno ekstenzija bilo kog projekcionog skupa) zagarantovana je i ako se izgubi uslov da su projekcije $\pi_{ji}$ surjektivna preslikavanja. U tom slučaju formiramo familiju $\mathcal{S}' = \{A'_i \mid i \in I\}$, gde je, za svako $i \in I$, $\emptyset \neq A'_i \subseteq A_i$, i gde su, za $A'_i \leq A'_j$ (dakle, $A_i \leq A_j$), projekcije $\pi'_{ji} = \pi_{ji}|_{A'_j} : A'_j \longrightarrow A'_i$ surjektivna preslikavanja. Stvarno, u svakom skupu $A_i = \{a_1, \ldots, a_m\}$ postoji bar jedan element koji ima inverznu sliku u svakom od skupova $A_j$, $A_i \leq A_j$. Jer, pretpostavimo suprotno i neka za $r = 1, \ldots, m$, $a_r$ nema inverznu sliku u $A_{j_r}$, $A_i \leq A_{j_r}$. Ali tada, za svako $k \in I$ za koje je $A_{j_r} \leq A_k$ za svako $r = 1, \ldots, m$, uopšte ne bi postojala projekcija $(\pi_{ki})$ skupa $A_k$ u skup $A_i$, kontradikcija (ako $b \in A_k$, onda $(b)\pi_{ki} = ((b)\pi_{kj_r})\pi_{j_r i} \neq a_r$ za svako $r = 1, \ldots, m$). Neka je $A'_i = \{b_1, \ldots, b_s\}$ skup svih elemenata skupa $A_i$ koji imaju inverznu sliku u svim skupovima $A_j$ za koje je $A_i \leq A_j$. No tada je $\pi'_{ij} = \pi_{ij}|_{A'_j} : A'_j \longrightarrow A'_i$ surjektivno preslikavanje; ako npr. $b_1$ ne bi bio slika nijednog od elemenata $c_1, \ldots, c_t$ skupa $A'_j$ i ako je $\{b_1\}\pi_{ji}^{-1} = \{d_1, \ldots, d_u\}$ ($\subseteq A_j$), $d_1, \ldots, d_u \notin A'_j$, a $d_m$, $m = 1, \ldots, u$, nema inverznu sliku u $A_{k_m}$ ($A_j \leq A_{k_m}$), tada nijedan od elemenata $d_m$ ne bi imao inverznu sliku u $A_k$, $A_k \geq A_{k_m}$, $m = 1, \ldots, u$, pa ni elemet $b_1$ ne bi imao inverznu sliku u $A_k$, kontradikcija.

Primenićemo prethodnu teoremu u dokazu sledeće, no prvo

**Lema 17.3** *Neka je* $\mathbf{P}$ *Sylowa $p$-podgrupa i* $\mathbf{H}$ *konačna normalna podgrupa lokalno konačne i normalne grupe* $\mathbf{G}$. *Tada je* $\mathbf{P} \cap \mathbf{H}$ *Sylowa $p$-podgrupa grupe* $\mathbf{H}$.

**Dokaz.** Neka je, za svaku konačnu normalnu podgrupu $\mathbf{H}$ grupe $\mathbf{G}$, $\mathcal{A}_\mathbf{H} = \{\mathbf{P}_1^H, \ldots, \mathbf{P}_{i_H}^H\}$ skup svih Sylowih $p$-podgrupa grupe $\mathbf{H}$ koje sadrže $\mathbf{P} \cap \mathbf{H}$. Uređenje $\leq$ na skupu $\mathcal{S} = \{\mathcal{A}_\mathbf{H} \mid \mathbf{H}$ je konačna normalna podgrupa grupe $\mathbf{G}\}$ dato sa: $\mathcal{A}_\mathbf{H} \leq \mathcal{A}_\mathbf{K}$ ako je $\mathbf{H}$ podgrupa grupe $\mathbf{K}$ očigledno je parcijalno uređenje. No radi se zapravo o usmerenom parcijalnom uređenju. Pokazaćemo da su ispunjeni i uslovi (2)($a$),($b$) za podesno izabrane projekcije, koje sada neće nužno biti surjektivna preslikavanja; napomena uz prethodnu teoremu nas oslobađa tog dosta jakog uslova. Ako je $\mathbf{H} \leq \mathbf{K}$ i $\mathbf{P}^K \in \mathcal{A}_\mathbf{K}$ (dakle, $\mathbf{P} \cap \mathbf{K} \leq \mathbf{P}^K$; nećemo notaciju nepotrebno komplikovati donjim indeksima), onda je, prema 16.11 i 16.23($b$), $\mathbf{P}^K \cap \mathbf{H} = \mathbf{P}^H$ Sylowa $p$-podgrupa grupe $\mathbf{H}$ (u konačnoj grupi $\mathbf{K}$ su sve Sylowe podgrupe konjugovane), pa $\mathbf{P}^H \in \mathcal{A}_\mathbf{H}$. Stavljamo: $(\mathbf{P}^K)\pi_{KH} = \mathbf{P}^H$ ($= \mathbf{P}^K \cap \mathbf{H}$). Ako je $\mathbf{H} \leq \mathbf{K} \leq \mathbf{L}$ ($\mathbf{H}$, $\mathbf{K}$ i $\mathbf{L}$ su konačne normalne podgrupe grupe $\mathbf{G}$), tada je $(\mathbf{P}^L)\pi_{LH} = \mathbf{P}^L \cap \mathbf{H} = (\mathbf{P}^K \cap \mathbf{K}) \cap \mathbf{H} = (\mathbf{P}^K \cap \mathbf{K})\pi_{KH} = (\mathbf{P}^K)(\pi_{LK} \circ \pi_{KH})$ (upravo smo dokazali: $\mathbf{P}^L \cap \mathbf{K} \in \mathcal{A}_\mathbf{K}$). I naravno, $\pi_{HH}$ je identično preslikavanje.

Neka je, dalje, $\mathcal{P}$ kompletan projekcioni skup sistema $\mathcal{S}$. Prema tome, u svakoj konačnoj normalnoj podgrupi $\mathbf{H}$ grupe $\mathbf{G}$ imamo Sylowu $p$-podgrupu, neka je to opet $\mathbf{P}^H$, takvu da je ispunjeno: za bilo koje konačne normalne podgrupe $\mathbf{H}, \mathbf{K}$ postoji konačna normalna podgrupa $\mathbf{L}$ takva da je $\mathbf{H}, \mathbf{K} \leq \mathbf{L}$ i $\mathbf{P}^H, \mathbf{P}^K \leq \mathbf{P}^L$. Ali tada je $\bigcup\{\mathbf{P}^H \mid \mathbf{H}$ je konačna normalna podgrupa grupe $\mathbf{G}\}$ domen $p$-podgrupe grupe $\mathbf{G}$ koja sadrži $\mathbf{P}$ (ako je $a \in P$ i $\mathbf{N} = [\langle a \rangle]$ - normalno zatvorenje ciklične grupe $\langle a \rangle$, dakle, po uslovu leme, konačna grupa, onda $a \in P^N$ $(\supseteq P \cap N)$), te je baš $P = \bigcup\{P^H \mid \mathbf{H}$ je konačna normalna podgrupa grupe $\mathbf{G}\}$. Stoga, $\mathbf{P}^H = \mathbf{P} \cap \mathbf{H}$, što će reći da su skupovi $\mathcal{A}_\mathbf{H}$ jednoelementni.□

**Definicija 17.4** *Automorfizam $\varphi$ grupe $\mathbf{G}$ je lokalno konjugovan akko za svaki konačan podskup $A = \{a_1, \ldots, a_n\}$ skupa $G$ postoji element $b_A \in G$ ($b_A$ je u funkciji skupa $A$) takav da je, za svako $i = 1, \ldots, n$: $(a_i)\varphi = b_A^{-1} a_i b_A$.*

**Teorema 17.5** *Sylowe $p$-podgrupe lokalno konačne i normalne grupe $\mathbf{G}$ su lokalno konjugovane.*

**Dokaz.** Neka su $\mathbf{P}_1$ i $\mathbf{P}_2$ Sylowe $p$-podgrupe grupe $\mathbf{G}$ i neka je $\mathbf{H}$ konačna normalna podgrupa grupe $\mathbf{G}$. Prema prethodnoj lemi $\mathbf{P}_1 \cap \mathbf{H}$ i $\mathbf{P}_2 \cap \mathbf{H}$ su Sylowe $p$-podgrupe (konačne) grupe $\mathbf{H}$, znači i konjugovane (16.23($b$)). Neka je $\mathcal{A}_\mathbf{H} = \{\varphi \in Aut(\mathbf{H}) \mid \exists g \in G\ \varphi = u_g|_H$ i $(\mathbf{P}_1 \cap \mathbf{H})\varphi = \mathbf{P}_2 \cap \mathbf{H}\}$. Jasno, $\mathcal{A}_\mathbf{H}$ je neprazan konačan skup (ako je, za $h \in H$, $\mathbf{P}_2 \cap \mathbf{H} = h^{-1}(\mathbf{P}_1 \cap \mathbf{H})h$, onda je $u_h|_H \in \mathcal{A}_\mathbf{H}$). Na skupu $\{\mathcal{A}_\mathbf{H} \mid \mathbf{H}$ je konačna normalna podgrupa$\}$ definišimo relaciju $\leq$ sa: $\mathcal{A}_\mathbf{H} \leq \mathcal{A}_\mathbf{K}$ akko $\mathbf{H} \leq \mathbf{K}$ (u pitanju je očigledno parcijalno uređenje), a projekcije $\pi_{KH} : \mathcal{A}_\mathbf{K} \longrightarrow \mathcal{A}_\mathbf{H}$ sa (za $\varphi \in \mathcal{A}_\mathbf{K}$): $(\varphi)\pi_{KH} = \varphi|_H$; imamo u vidu: za neko $g \in G$ je $\varphi = u_g|_K$ i $(\mathbf{P}_1 \cap \mathbf{K})\varphi = g^{-1}(\mathbf{P}_1 \cap \mathbf{K})g = \mathbf{P}_2 \cap \mathbf{K}$, pa je, s obzirom na normalnost podgrupe $\mathbf{H}$, i $\varphi|_H = (u_g|_K)|_H = u_g|_H \in Aut(\mathbf{H})$ i $(\mathbf{P}_1 \cap \mathbf{H})u_g|_H = g^{-1}(\mathbf{P}_1 \cap \mathbf{H})g = g^{-1}((\mathbf{P}_1 \cap \mathbf{K}) \cap \mathbf{H})g = g^{-1}(\mathbf{P}_1 \cap \mathbf{K})g \cap g^{-1}\mathbf{H}g = (\mathbf{P}_2 \cap \mathbf{K}) \cap \mathbf{H} = \mathbf{P}_2 \cap \mathbf{H}$. Uslovi (1) i (2)($a$),($b$) su evidentno ispunjeni. Neka je, dalje, $\mathcal{P} = \{\varphi^H \mid \mathbf{H} \lhd \mathbf{G},\ |H| < \infty\}$ jedan kompletan projekcioni skup; dakle, svaka dva automorfizma $\varphi^H$, $\varphi^K$ indukovana su nekim trećim $\varphi^L$ ($\mathbf{H}, \mathbf{K} \leq \mathbf{L}$ i $\varphi^H = \varphi^L|_H$, $\varphi^K = \varphi^L|_K$). Zato je preslikavanje $\psi : G \longrightarrow G$ dato sa $(g)\psi = (g)\varphi^{[\langle g \rangle]}$ ($= (g)\varphi^H$, gde je $\mathbf{H}$ ma koja konačna normalna podgrupa grupe $\mathbf{G}$ čiji je element $g$), automorfizam grupe $\mathbf{G}$. Na primer, ako je $(a)\psi = (b)\psi$, onda je $(a)\varphi^{[\langle a,b \rangle]} = (b)\varphi^{[\langle a,b \rangle]}$ i $a = b$; surjektivnost i homomorfnost su još očiglednija svojstva. $\psi$ je, opet zbog lokalne normalnosti grupe $\mathbf{G}$, i lokalno konjugovani automorfizam. Konačno, $(\mathbf{P}_1)\psi = \mathbf{P}_2$; jer, ako je $a \in P_1$, tada je $\mathbf{P} \cap [\langle a \rangle]$ Sylowa $p$-podgrupa grupe $[\langle a \rangle]$, te je $(a)\psi = (a)\varphi^{[\langle a \rangle]} \in P_2 \cap [\langle a \rangle]$ i, prema tome, $(P_1)\psi \subseteq P_2$. Jasno, važi baš jednakost (u suprotnom bi $\mathbf{P}_1$ bila prava podgrupa $p$-grupe $(\mathbf{P}_2)\psi^{-1}$, kontradikcija).■



# 18 Grupe malog reda

U ovom paragrafu (uz malu pomoć prethodnih) upoznaćemo se sa svim grupama reda manjeg od ili jednakog 20 (što ne znači da nam nisu poznate i sve grupe reda 21 ili 22), kao i sa grupama reda 30 odnosno reda $p^3$, gde je $p$ bilo koji prost broj.

**Lema 18.1** *Postoji (svega) pet grupa reda* 12.

**Dokaz.** Grupe reda $12 = 2^2 \cdot 3$, videli smo, nisu proste. $s_2$ je ili 1 ili 3, $s_3$ je ili 1 ili 4.

Kombinacija $s_2 = 3$ i $s_3 = 4$ nije, međutim, moguća. Jer, unija četiri Sylowe 3-podgrupe bi već imala $4 \cdot 2 + 1 = 9$ elemenata i jednostavno "ne bi bilo mesta" za tri Sylowe 2-podgrupe.

Ako u grupi $\mathbf{G}$ reda 12 važi kombinacija $s_2 = 1$ i $s_3 = 1$, sledi da su (jedinstvene) Sylowe 2- i 3-podgrupe normalne i kako je njihov presek jedinična grupa, $\mathbf{G}$ je njihov direktni proizvod. Tu imamo svega dve mogućnosti, u zavisnosti od toga da li je Sylowa 2-podgrupa ciklična ili Kleinova: $\mathbf{C}_4 \times \mathbf{C}_3 \cong \mathbf{C}_{12}$ i $\mathbf{K} \times \mathbf{C}_3 \cong \mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_3$. Ovo su, znači, i jedine Abelove grupe reda 12.

Neka je, opet, grupa $\mathbf{G}$ reda 12 i neka je $s_2 = 1$, $s_3 = 4$. Pretpostavimo prvo da je jedina Sylowa 2-podgrupa ($\mathbf{A}$) ciklična: $\mathbf{A} = \langle a \rangle$. Ako je $\mathbf{D} = \langle d \rangle$ jedna od Sylowih 3-podgrupa, imali bismo: $\mathbf{G} = \mathbf{A} \rtimes \mathbf{D}$ i $d^{-1}ad = a^3$, tj. $ad = da^3$ ($d^{-1}ad$ je element reda 4, a mora biti $d^{-1}ad \neq a$). No, proizilazi da je $(da)^2 = d \cdot ad \cdot a = dda^3a = d^2$ i $(da)^3 = (da)^2da = d^2da = a$, kontradikcija (u cikličnoj grupi $\langle da \rangle$ reda 6 imali bismo element reda 4). Probajmo, dalje, sa Kleinovom grupom ($\mathbf{K}$) kao jedinom Sylowom 2-podgrupom; neka je njen domen $\{e, a, b, c\}$. Za bar jedan element $d$ reda 3 mora biti $d^{-1}ad \neq a$ (u suprotnom bi grupa $\mathbf{G}$ bila Abelova). Neka je $d^{-1}ad = b$, tj. $ad = db$. Sada je isključeno $d^{-1}bd = a$ (jer tada: $d^{-1}bd = dbd^{-1}$, odnosno $b = d^2bd^{-2}$, i pošto je $d^2 = d^{-1}$, $b = d^{-1}bd = a$). Ne može biti ni $d^{-1}bd = b$ ($d^{-1}bd = b \Longrightarrow d^{-1}bd = d^{-1}ad \Longrightarrow a = b$). Zaključujemo $d^{-1}bd = ab = c$ (kao jedini preostali nejedinični element Kleinove grupe), a onda je direktno implicirano $d^{-1}(ab)d = a$. Navedene relacije, ponovimo ih:

$$a^2 = b^2 = d^3 = e,\ \ ad = bd,\ \ bd = d(ab),\ \ (ab)d = da$$

određuju jedinstvenu grupu (sa generatornim skupom $\{a, b, d\}$) reda 12. Domen joj je skup $\{e, a, b, ab, d, d^2, ad, bd, (ab)d, ad^2, bd^2, (ab)d^2\}$ (primetimo, ilustracije radi: $d^2b = d^2bd^{-2}d^2 = d^{-1}bdd^2 = (ab)d^2$) - ostavljamo za vežbu da se pokaže da su navedeni elementi različiti. (Jedina) Sylowa 2-podgrupa je data Kleinova grupa, a četiri Sylowe 3-podgrupe su:

$$\langle \{e, d, d^2\}, \cdot \rangle,$$

$$\langle\{e, ad, (ad)^2 (= bd^2)\}, \cdot\rangle,$$
$$\langle\{e, bd, (bd)^2 (= (ab)d^2)\}, \cdot\rangle$$

i

$$\langle\{e, (ab)d, ((ab)d)^2 (= ad^2)\}, \cdot\rangle.$$

Ova grupa je, zapravo, izomorfna slika alternativne grupe $\mathbf{A}_4$. Jedan izomorfizam ($\varphi$) je dat sa:

$$(a)\varphi = (0\ 1)(2\ 3) = \alpha,\ \ (b)\varphi = (0\ 2)(1\ 3) = \beta,\ \ (d)\varphi = (1\ 2\ 3) = \gamma.$$

Znamo odranije da su $\alpha$ i $\beta$ permutabilne permutacije, jasno, $\alpha^2 = \beta^2 = \gamma^3 = \imath$, a lako se proveravaju i relacije $\gamma^{-1}\alpha\gamma = \beta$, $\gamma^{-1}\beta\gamma = \alpha\beta$, $\gamma^{-1}(\alpha\beta)\gamma = \alpha$.

Pređimo sada na slučaj $s_2 = 3, s_3 = 1$ sa cikličnim Sylowim 2-podgrupama. Neka je $\mathbf{A} = \langle a\rangle$ jedna od njih, a $\mathbf{D} = \langle d\rangle$ neka je jedina Sylowa 3-podgrupa. Element $a^{-1}da\,(\in D)$ mora biti različit od $d$ (inače bi, zbog $G = AD$, grupa $\mathbf{G}$ bila Abelova, dakle i $s_2 = 1$). Prema tome je $a^{-1}da = d^2$, tj. $da = ad^2$. Sada je determinisano: $a^{-1}d^2a = (a^{-1}da)^2 = (d^2)^2 = d$, odnosno $ad = d^2a$; korisno je imati u vidu i $a^2d = ad^2a = daa = da^2$. Generatorni skup $\{a, d\}$ i relacije:

$$a^4 = d^3 = e,\ ad^2 = da,\ ad = d^2a$$

u potpunosti određuju (jedinstvenu do na izomorfizam) grupu reda 12. Domen joj je $\{e, a, a^2, a^3, d, d^2, ad, a^2d, a^3d, ad^2, a^2d^2, a^3d^2\}$, Sylowe 2-podgrupe su, pored $\mathbf{A}$, i

$$\langle ad\rangle = \langle\{e, ad, a^2, a^3d\}, \cdot\rangle,\ \ \langle ad^2\rangle = \langle\{e, ad^2, a^2, a^3d^2\}, \cdot\rangle.$$

Elementi $a^2d$ i $a^2d^2 = (a^2d)^5$ su reda 6:

$$\langle a^2d\rangle = \langle a^2d^2\rangle = \langle a^2\rangle \times \langle d\rangle.$$

Cayleyeva tablica ove grupe je

| | $e$ | $a$ | $a^2$ | $a^3$ | $d$ | $d^2$ | $ad$ | $ad^2$ | $a^2d$ | $a^2d^2$ | $a^3d$ | $a^3d^2$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $a^3$ | $d$ | $d^2$ | $ad$ | $ad^2$ | $a^2d$ | $a^2d^2$ | $a^3d$ | $a^3d^2$ |
| $a$ | $a$ | $a^2$ | $a^3$ | $e$ | $ad$ | $ad^2$ | $a^2d$ | $a^2d^2$ | $a^3d$ | $a^3d^2$ | $d$ | $d^2$ |
| $a^2$ | $a^2$ | $a^3$ | $e$ | $a$ | $a^2d$ | $a^2d^2$ | $a^3d$ | $a^3d^2$ | $d$ | $d^2$ | $ad$ | $ad^2$ |
| $a^3$ | $a^3$ | $e$ | $a$ | $a^2$ | $a^3d$ | $a^3d^2$ | $d$ | $d^2$ | $ad$ | $ad^2$ | $a^2d$ | $a^2d^2$ |
| $d$ | $d$ | $ad^2$ | $a^2d$ | $a^3d^2$ | $d^2$ | $e$ | $a$ | $ad$ | $a^2d^2$ | $a^2$ | $a^3d$ | $a^3$ |
| $d^2$ | $d^2$ | $ad$ | $a^2d^2$ | $a^3d$ | $e$ | $d$ | $ad^2$ | $a$ | $a^2$ | $a^2d$ | $a^3d^2$ | $a^3d$ |
| $ad$ | $ad$ | $a^2d^2$ | $a^3d$ | $d^2$ | $ad^2$ | $a$ | $a^2$ | $a^2d$ | $a^3d^2$ | $a^3$ | $e$ | $d$ |
| $ad^2$ | $ad^2$ | $a^2d$ | $a^3d^2$ | $d$ | $a$ | $ad$ | $a^2d^2$ | $a^2$ | $a^3$ | $a^3d$ | $d^2$ | $e$ |
| $a^2d$ | $a^2d$ | $a^3d^2$ | $d$ | $ad^2$ | $a^2d^2$ | $a^2$ | $a^3$ | $a^3d$ | $d^2$ | $e$ | $a$ | $ad$ |
| $a^2d^2$ | $a^2d^2$ | $a^3d$ | $d^2$ | $ad$ | $a^2$ | $a^2d$ | $a^3d^2$ | $a^3$ | $e$ | $d$ | $ad^2$ | $a$ |
| $a^3d$ | $a^3d$ | $d$ | $ad$ | $a^2d^2$ | $a^3d^2$ | $a^3$ | $e$ | $d$ | $ad^2$ | $a$ | $a^2$ | $a^2d$ |
| $a^3d^2$ | $a^3d^2$ | $d$ | $ad^2$ | $a^2d$ | $a^3$ | $a^3d$ | $d^2$ | $e$ | $a$ | $ad$ | $a^2d^2$ | $a^2$. |



Pretpostavimo na kraju da je $s_2 = 3$, $s_3 = 1$ i da su Sylowe 2-podgrupe Kleinove. Neka je $\mathbf{D} = \langle d\rangle$ Sylowa 3-podgrupa i $\mathbf{K} = \langle\{e, a, b, c\}, \cdot\rangle$ jedna (od tri) Sylowe 2-podgrupa. Bar jedan nejedinični element podgrupe $\mathbf{K}$ nije permutabilan sa $d$ (inače bi grupa bila Abelova). Neka je npr. $a^{-1}da = d^2$, tj. $da = ad^2$; onda je $d^2a = aa^{-1}d^2a = a(a^{-1}da)^2 = a(d^2)^2 = ad$ i $\mathbf{H} = \langle a, d\rangle = \langle\{e, a, d, d^2, ad, ad^2\}, \cdot\rangle$ je dijedarska grupa stepena 3, normalna podgrupa grupe $\mathbf{G}$. Ako je, dalje, $bd = db$, grupa $\mathbf{B} = \langle b\rangle$ je normalna podgrupa i $\mathbf{G} = \mathbf{H} \times \mathbf{B}$. Ukoliko je $b^{-1}db = d^2$, tada je $(ab)d = d(ab)$ (tj. $cd = dc$) i $\mathbf{G} = \mathbf{H} \times \langle c\rangle$. U svakom slučaju dobijamo: $\mathbf{G} \cong \mathbf{D}_3 \times \mathbf{C}_2 \cong \mathbf{D}_6$ (10.24($i$)).

Ovim su ujedno iscrpljeni svi mogući slučajevi. Rezimiramo na kraju: Abelove grupe reda 12 su $\mathbf{C}_{12}$ i $\mathbf{K} \times \mathbf{C}_3$, neabelove: $\mathbf{A}_4$, grupa sa datom Cayleyevom tablicom i $\mathbf{D}_6$.□

**Teorema 18.2** *Postoji četrnaest grupa reda* 16.

**Dokaz**. 1. Uvek imamo cikličnu grupu reda 16.

Neka je $\mathbf{G}$ neciklična grupa reda 16 sa elementom $a$ reda 8 i neka je $b\,(\notin \langle a\rangle = A)$ takođe element reda 8. Onda je presek cikličnih grupa $\mathbf{A}$ i $\mathbf{B}$ $(= \langle b\rangle)$ reda 4. Možemo pretpostaviti da je $a^2 = b^2$ (znamo da mora biti $a^4 = b^4$, a ako bi bilo $b^2 = a^6$, uzeli bismo $a^3$ za generatorni element podgrupe $\mathbf{A}$). Elementi grupe će, prema tome, biti $a^kb^m$, $k \in 8$, $m \in 2$, a kako je $b^{-1}ab$ generatorni element podgrupe $\mathbf{A}$, to je $b^{-1}ab = a^k$, gde je $k$ neki od elemenata skupa $\{1, 3, 5, 7\}$.

2. Ako je $b^{-1}ab = a$, tj. $ab = ba$, grupa je Abelova, element $c = a^3b\,(\notin A)$ je reda 2 pa je $\mathbf{G} = \mathbf{A} \times \mathbf{C}$ $(\mathbf{C} = \langle c\rangle)$.

3. Ako je $b^{-1}ab = a^5$, tj. $ab = ba^5$ (odnosno $ba = a^5b$), onda je (za $k, r \in 8$, $m, s \in 2$):

$$a^kb^m \cdot a^rb^s = a^{k+_8 5^r 5^{m+_2 1} +_8 2ms} b^{m+_2 s}.$$

Ova grupa ima tri elementa reda 2 – $a^4$, $ab$, $a^5b$ i četiri elementa reda 4: $a^2$, $a^6$, $a^3b$, $a^7b$. $\mathbf{G}$ je, dakle, poludirektni proizvod (normalne) podgrupe $\mathbf{A}$ i podgrupe $\langle ab\rangle$ koji odgovara preslikavanju elementa $ab$ na automorfizam podgrupe $\mathbf{A}$ koji pak preslikava $a$ u $a^5$.

Slučajevi $k = 3$, $k = 7$ nisu, s obzirom na date pretpostavke, mogući. Tako bi npr. iz $b^{-1}ab = a^3$ sledilo $(b^{-1}ab)^2 = b^{-1}a^2b = a^2 = a^6$, suprotno pretpostavci da je $a$ element reda 8.

Ako je $b\,(\notin A)$ reda 4, onda je $b^2 = a^4$, a $b^{-1}ab$ je ili $a$ ili $a^3$ ili $a^5$ ili $a^7$.

4. Ako je $b^{-1}ab = a$, grupa je Abelova, element $a^2b$ je reda 2 i $\mathbf{G}$ je grupa koju smo već dobili – direktan proizvod cikličnih grupa redova, respektivno, 2 i 8.

5. Ako je $b^{-1}ab = a^3$, tj. $ab = ba^3$ (odatle i $ba = a^3b$), element $ab = c$ je reda 2 i $\mathbf{G}$ je poludirektni proizvod normalne podgrupe $\mathbf{A}$ i ciklične podgrupe

$\mathbf{C}$ (generisane elementom $c$). Ona odgovara preslikavanju elementa $c$ na automorfizam grupe $\mathbf{A}$ koji preslikava $a$ u $a^3$. Elementi su $a^k b^m$, $k \in 8$, $m \in 2$, "množenje" je dato sa (za $k, r \in 8$, $m, s \in 2$):

$$a^k b^m \cdot a^r b^s = a^{k+_8 3r 3^{m+_2 1}+_8 4ms} b^{m+_2 s}.$$

Ovaj poludirektni proizvod nije izomorfan sa ranije datim - jedan od dokaza za to je da ima pet elemenata reda 2 - $a^4$, $ab$, $a^3b$, $a^5$, $a^7b$.

6. Ako je $b^{-1}ab = a^5$, tj. $ab = ba^5$ (odatle i $ba = a^5b$), element $a^2b$ je reda 2 i $\mathbf{G}$ je poludirektni proizvod normalne ciklične grupe reda 8 i ciklične grupe reda 2. Ova grupa izomorfna je sa grupom iz 3. tačke; jedan izomorfizam je dat sa $\varphi : G_3 \longrightarrow G_6$ (smisao indeksa je jasan, a ista notacija, nadamo se, ne unosi zabunu), gde je $(a)\varphi = a$, $(b)\varphi = ab$.

7. Ako je $b^{-1}ab = a^7$, tj. $ab = ba^7$ (onda i $ba = a^7b$), svi elementi van podgrupe $\mathbf{A}$ su reda 4 (prema tome postoji samo jedan element reda 2):

$$a^k b^m \cdot a^r b^s = a^{k+_8 7r 7^{m+_2 1}+_8 4ms} b^{m+_2 s},$$

a odatle:

$$a^k b \cdot a^k b = a^{k+_8 7k+_8 4} = a^4.$$

Ova grupa izomorfna je podgrupi $\mathbf{GL}_2(Z_{41})$ generisanoj matricama $C = \begin{bmatrix} 3 & 0 \\ 0 & 14 \end{bmatrix}$ i $D = \begin{bmatrix} 0 & 1 \\ 40 & 0 \end{bmatrix}$, a izomorfizam je dat sa $a \longrightarrow C$, $b \longrightarrow D$.

Ako je $b$ ($\notin A$) element reda 2, grupa je poludirektni proizvod normalne ciklične grupe $\mathbf{A}$ i ciklične grupe $\mathbf{B}$ ($= \langle b \rangle$).

8. $b^{-1}ab = a$ daje direktan proizvod.

9. Ako je $b^{-1}ab = a^3$, dobijamo grupu izomorfnu grupi iz 5. tačke.

10. Ako je $b^{-1}ab = a^5$, grupa je izomorfna grupi iz 3., dakle i 6. tačke.

11. Ako je $b^{-1}ab = a^7$, tj. $ab = ba^7$, u pitanju je dijedarska grupa stepena 8 sa devet elemenata reda 2.

U daljem sledimo [16]. Pretpostavka je sada, jasno, da grupa nema elemenata reda 8.

12. Ako su svi elementi reda 2 grupa je direktan proizvod cikličnih grupa reda 2 (2.7($f$), 10.33).

Neka sada grupa ima bar jedan element reda 4. Tada važi:

**Stav 1** *Postoji element $a$ reda 2 iz centra grupe takav da je faktor grupa $\mathbf{G}/\langle a \rangle$ Abelova.*

**Dokaz**. Ako je $\mathbf{G}$ Abelova grupa tvrđenje očigledno važi.

Ako $\mathbf{G}$ nije Abelova grupa, centar je nejedinična podgrupa (4.13) koja, jasno, sadrži element reda 2 - neka je to $b$. Ako je $\mathbf{G}/\mathbf{B}$ ($\mathbf{B} = \langle b \rangle$) Abelova grupa, dokaz je završen ($b = a$). U suprotnom, $\mathbf{G}/\mathbf{B}$ je ili grupa kvaterniona



ili dijedarska grupa stepena 4, u svakom slučaju postoje elementi $cB$, $dB$ reda 4 takvi da je $(dB)^{-1}cBdB = (cB)^3$. Proizilazi da je i $c$ element reda 4 (većeg ne može biti po pretpostavci, a njegova homomorfna slika je reda 4). Iz date relacije sledi $d^{-1}cd \in \{c^3, c^3b\}$. Bez obzira na izbor, važi $(d^{-1}cd)^2 = c^2$. $c^2$ je, znači, komutativno sa $d$ (naravno i sa $b$), pa je $c^2 \in Z(\mathbf{G})$. Ako je, npr. $d^{-1}cd = c^3b$, uzimamo $c^2b$ za traženi element $a$, (slično bismo, za $d^{-1}cd = c^3$, imali $a = c^2$). Grupa $\mathbf{G}/\mathbf{A}$ ($\mathbf{A} = \langle a \rangle$) je Abelova jer su njeni generatorni elementi $cA$ i $dA$ uzajamno permutabilni:

$$(dA)^{-1}cAdA = (d^{-1}cd)A = (c^3b)A = (c \cdot a)A = cA.\square$$

U nastavku razmatramo moguće slučajeve za faktor grupu $\mathbf{G}/\mathbf{A}$ (sigurno, s obzirom na pretpostavke, isključena je mogućnost da je to ciklična grupa reda 8).

I $\mathbf{G}/\mathbf{A} = \mathbf{C}_4 \times \mathbf{C}_2$.

Neka je, da ne uvodimo nove oznake, $\mathbf{G}/\mathbf{A} = \langle bA \rangle \times \langle cA \rangle$, gde je $bA$ reda 4 i $cA$ reda 2. Stoga je $c^2$ ili $e$ ili $a$, a $c^{-1}bc$ je ili $b$ ili $ab$ ($(cA)^{-1} \cdot bA \cdot cA = bA$, pa je $c^{-1}bc \in bA$). Dobijamo, prema tome, četiri slučaja. Grupa je generisana elementima $a$, $b$ i $c$ i pri tome je:

13. $a^2 = b^4 = c^2 = e$, $ab = ba$, $ac = ca$, $bc = cb$.

Ove relacije određuju grupu $\mathbf{C}_4 \times \mathbf{C}_2 \times \mathbf{C}_2 \cong \mathbf{C}_4 \times \mathbf{K}$ ($\mathbf{K}$ - Kleinova grupa);

14. $a^2 = b^4 = c^2 = e$, $ab = ba$, $ac = ca$, $bc = cab$.

Sada je u pitanju poludirektan proizvod $(\mathbf{C}_4 \times \mathbf{C}_2) \times_\theta \mathbf{C}_2$, gde je $\theta : C \longrightarrow Aut(\mathbf{A} \times \mathbf{B})$ dato sa $(a)((c)\theta) = a$, $(b)((c)\theta) = ab$. Elementi grupe su $c^i a^j b^k$, $i, j \in 2$, $k \in 4$, a "množenje" je dato sa:

$$c^i a^j b^k \cdot c^p a^q b^r = c^{i+_2 p} a^{j+_2 q+_2 kp} b^{k+_4 r}.$$

Grupa ima sedam elemenata reda 2 - $a$, $c$, $ca$, $b^2$, $ab^2$, $cb^2$, $cab^2$ i osam elemenata reda 4.

15. $a^2 = b^4 = c^4 = e$, $c^2 = a$, $ab = ba$, $ac = ca$, $bc = cb$.

Relacije određuju direktan proizvod cikličnih grupa reda 4 - $\langle b \rangle \times \langle c \rangle$.

16. $a^2 = b^4 = c^4 = e$, $c^2 = a$, $ab = ba$, $ac = ca$, $bc = cab$.

Ciklična grupa $\mathbf{A}$ sadržana je, kao i u prethodnom slučaju, u cikličnoj grupi $\mathbf{C}$, pa je dovoljno uzeti za generatorne elemente $b$ i $c$ i posmatrati relacije koje ih vezuju: $b^4 = c^4 = e$, $bc = c^3b$. Elementi grupe su $c^k b^m$, $k, m \in 4$, a "množenje" je definisano sa (za $k, m, r, s \in 4$):

$$c^k b^m \cdot c^r b^s = c^{k+_4 3^m r} b^{m+_4 s}.$$

Ova grupa izomorfna je podgrupi direktnog proizvoda $\mathbf{Q} \times \mathbf{C}_4$, gde je $\mathbf{Q}$ grupa kvaterniona. Zaista, neka je grupa $\mathbf{Q}$ generisana elementima $x, y$, pri

čemu je $x^4 = y^4 = e$, $x^2 = y^2$, $yx = x^3y$ (videti 3.4(e)), i neka je $\mathbf{C}_4$, kao i obično, grupa $\mathbf{Z}_4$. Tada je preslikavanje $\varphi$ "naše" grupe u $\mathbf{Q} \times \mathbf{Z}_4$ dato sa: $(c)\varphi = (x, 0)$, $(b)\varphi = (y, 1)$ i uopšte:

$$(c^k b^m)\varphi = (x^{k +_4 [\frac{m}{2}]2} y^{m-[\frac{m}{2}]2}, m)$$

injektivni homomorfizam. Očigledno, samo je svojstsvo homomorfnosti u pitanju. S jedne strane imamo:

$$(c^k b^m \cdot c^r b^s)\varphi = (c^{k +_4 3^m r +_4 [\frac{m +_4 s}{2}]2} y^{(m+s)-[\frac{m+s}{2}]2}, m +_4 s),$$

a s druge strane:

$$(c^k b^m)\varphi \cdot (c^r b^s)\varphi = (x^{k +_4 [\frac{m}{2}]2} y^{m-[\frac{m}{2}]2}, m) \cdot (x^{r +_4 [\frac{s}{2}]2} y^{s-[\frac{s}{2}]2}, s) =$$

$$(x^{k +_4 [\frac{m}{2}]2 +_4 3^{m-[\frac{m}{2}]2}(r +_4 [\frac{s}{2}]2) +_4 [\frac{m-[\frac{m}{2}]2+s-[\frac{s}{2}]2}{2}]2} y^{m+s-[\frac{m}{2}]2-[\frac{s}{2}]2-[\frac{m+s-[\frac{m}{2}]2-[\frac{s}{2}]2}{2}]2},$$

$$m +_4 s).$$

S nešto malo truda (i malo više volje) cela stvar se svodi na proveru jednakosti:

$$k +_4 3^m r = k +_4 3^{m-[\frac{m}{2}]2} r,$$

a to je već trivijalno.

Recimo još da ova grupa ima tri elementa reda 2 – $c^2$, $b^2$ i $c^2b^2$, ostali su (sem jediničnog) reda 4.

II $\mathbf{G/A} = \mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_2$.

U ovom slučaju važe sledeća tvrđenja:

**Stav 2.** *Za svaka dva elementa $b$, $c$ postoji element $d$ (eventualno jedinični) centra grupe takav da je $c^{-1}bc = bd$.*

**Dokaz**. Za kanonsko homomorfno preslikavanje $\varphi$ grupe $\mathbf{G}$ na grupu $\mathbf{G/A}$ važi (jer je $\mathbf{G/A}$ komutativna grupa):

$$(c^{-1}bc)\varphi = (c^{-1}bc)A = (cA)^{-1}bAcA = bA.$$

Prema tome je $c^{-1}bc \in bA$, pa je ili $c^{-1}bc = b$ ili $c^{-1}bc = ab$.□

**Stav 3.** *Za ma koji element $b$ grupe $\mathbf{G}$ je $[\mathbf{G} : \mathbf{C}(b)] \leq 2$.*

**Dokaz**. Naravno, odmah ćemo pretpostaviti da grupa $\mathbf{G}$ nije Abelova (onda i $|Z(\mathbf{G})| < 8$ – videti 8.19).

Ako je $|Z(\mathbf{G})| = 4$ i $b \notin Z(\mathbf{G})$, onda $\mathbf{C}(b)$ ima osam elemenata (jer, trivijalno, $b \in C(b)$ i $Z(\mathbf{G}) \subseteq C(b)$).

Neka je sada $|Z(\mathbf{G})| = 2$, tj. $\mathbf{Z(G)} = \mathbf{A}$, i pretpostavimo $b \notin Z(\mathbf{G})$, $|C(b)| < 8$ i $c \notin C(b)$. Prema prethodnom stavu je $c^{-1}bc = ab$. Ako $d \notin C(b) \cup C(b)c$, onda i $d^{-1}bd = ab$. Stoga je $d^{-1}bd = c^{-1}bc$, tj. $dc^{-1} \in C(b)$, odnosno $d \in C(b)c$, kontradikcija.□



**Stav 4.** *Ako su $b$ i $c$ uzajamno nepermutabilni elementi grupe $\mathbf{G}$, tada je $\mathbf{H} = \langle b, c\rangle$ podgrupa reda 8, $|Z(\mathbf{H})| = 2$, $|C(\mathbf{H})| = 4$, $\mathbf{G} = \mathbf{H} \cdot \mathbf{C(H)}$ i $\mathbf{C(H)} = \mathbf{Z(G)}$.*

**Dokaz**. $(bA)^2 = (cA)^2 = A$ (po pretpostavci su, ne zaboravimo, u faktor grupi $\mathbf{G/A}$ svi elementi reda 2), pa je $b^2, c^2 \in \{e, a\}$. Ako su i $b$ i $c$ elementi reda 4, imamo direktno $|H| = \frac{4 \cdot 4}{2} = 8$. U drugim slučajevima lako se izvodi $|H| \leq 8$, no s obzirom da je to neabelova grupa, mora biti baš $|H| = 8$. Opet, prema 8.19 i 8.20, $\mathbf{Z(H)}$ je reda 2. Prema prethodnom stavu je $[\mathbf{G} : \mathbf{C}(b)] = [\mathbf{G} : \mathbf{C}(c)] = 2$, a kako je $\mathbf{C(H)} = \mathbf{C}(b) \cap \mathbf{C}(c)$ imamo (3.17):

$$[\mathbf{G} : \mathbf{C(H)}] \leq [\mathbf{G} : \mathbf{C}(b)] \cdot [\mathbf{G} : \mathbf{C}(c)] = 4,$$

te je $|C(\mathbf{H})| \geq 4$. Međutim, $|C(\mathbf{H})| = 8$ je isključeno, jer bi odatle sledilo $|H \cap C(\mathbf{H})| = 4$ (obe grupe su reda 8, a cela grupa ima 16 elemenata), no $\mathbf{H} \cap \mathbf{C(H)} \leq \mathbf{Z(H)}$, a $\mathbf{Z(H)}$ ima samo dva elementa. Ostaje, dakle, $|C(\mathbf{H})| = 4$.

$\mathbf{G} = \mathbf{H} \cdot \mathbf{C(H)}$ je očigledno ($\mathbf{H}$ je indeksa 2, a isključeno je, iz upravo navedenog razloga, $C(\mathbf{H}) \subseteq H$). Odatle direktno sledi i da je $\mathbf{C(H)} \leq \mathbf{Z(G)}$ i pošto $\mathbf{Z(G)}$ ne može biti reda 8, važi jednakost.□

U nastavku ispitujemo moguće slučajeve za $\mathbf{C(H)}$ (primetimo da smo sve Abelove grupe, njih pet, već dobili).

III $\mathbf{C(H)} = \mathbf{C}_2 \times \mathbf{C}_2 = \langle d\rangle \times \langle g\rangle$.

Bar jedan od elemenata $d$, $g$ nije u $H$ (u suprotnom bismo imali $\mathbf{C(H)} \leq \mathbf{H}$; isto tako znamo da je $|H \cap C(\mathbf{H})| = 2$), neka je to npr. $d$. Pošto je $\mathbf{C(H)} \leq \mathbf{Z(G)}$, $\mathbf{D} = \langle d\rangle \lhd \mathbf{G}$ i $\mathbf{G}$ je ili

17. direktan proizvod dijedarske grupe i ciklične grupe reda 2

ili

18. direktan proizvod grupe kvaterniona i ciklične grupe reda 2

(dijedarska i grupa kvaterniona su jedine, videli smo to, neabelove grupe reda 8).

IV $\mathbf{C(H)} = \mathbf{C}_4 = \langle d\rangle$.

19. Pretpostavimo prvo da je $\mathbf{H}$ grupa kvaterniona sa generatornim elementima $b$, $c$ pri čemu je $b^4 = c^4 = e$, $b^2 = c^2$, $cb = b^3c$. No onda mora biti $b^2 = d^2$, jer je, kao što smo rekli, $|H \cap C(\mathbf{H})| = 2$ i $b^2$ je jedini element reda 2 u $\mathbf{H}$ (videti 5.7(a)). S obzirom da je $d$ element centra možemo konstatovati, uzimajući u obzir sve relacije, da su elementi grupe $b^k c^m d^n$, $k \in 4$, $m, n \in 2$, i da je "množenje" dato sa (za $k, p \in 4$, $m, q, n, r \in 2$):

$$b^k c^m d^n \cdot b^p c^q d^r = b^{k +_4 3^m p +_4 [\frac{m+q}{2}]2 +_4 [\frac{n+r}{2}]2} c^{m+_2 q} d^{n+_2 r}.$$

Ova grupa, kao i grupa u 14. tački, ima sedam elemenata reda 2 – $b^2$, $bd$, $b^3d$, $cd$, $bcd$, $b^2cd$, $b^3cd$, i osam elemenata reda 4, ali nije "razloživa" u poludirektan proizvod.

20. Neka je, konačno, $\mathbf{H}$ dijedarska grupa $\mathbf{D}_4$ sa generatornim elementima $b$, $c$, pri čemu je $b^4 = c^2 = e$, $cb = b^3c$. Ali ova grupa je izomorfna prethodnoj. Uloge elemenata $b$, $c$, $d$ iz prethodne grupe sada preuzimaju elementi $b_1 = bcd$, $c_1 = cd$, $d_1 = d$. Lako se proverava da za njih važe relacije:

$$b_1^4 = c_1^4 = d_1^4 = e,\ b_1^2 = c_1^2 = d_1^2,\ c_1b_1 = b_1^3c_1,\ b_1d_1 = d_1b_1,\ c_1d_1 = d_1c_1,$$

a preslikavanje elemenata prethodne grupe $b$, $c$, $d$ u, respektivno, $b_1$, $c_1$, $d_1$ ove grupe određuje i izomorfno preslikavanje.

Kako su ispitani svi mogući slučajevi preostaje nam da konstatujemo da neizomorfnih grupa reda 16 ima 14: pet Abelovih – njih je lako ponoviti: $\mathbf{C}_{16}$, $\mathbf{C}_8 \times \mathbf{C}_2$, $\mathbf{C}_4 \times \mathbf{C}_4$, $\mathbf{C}_4 \times \mathbf{C}_2 \times \mathbf{C}_2$ (direktan proizvod ciklične grupe reda 4 i Kleinove grupe) i $\mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_2$ (direktan proizvod Kleinovih grupa), i devet neabelovih – tačke 3(6,10), 5(9), 7, 11, 14, 16, 17, 18, 19(20).■

**Lema 18.3** *Postoji (svega) pet grupa reda* 18.

**Dokaz.** Neka je $\mathbf{G}$ grupa reda 18 ($= 2 \cdot 3^2$). Jasno, $s_3 = 1$ pa je jedinstvena Sylowa 3-podgrupa normalna. Kako je presek Sylowe 3-podgrupe i (ma koje) Sylowe 2-podgrupe jedinična podgrupa, to je $\mathbf{G}$ poludirektni proizvod tih podgrupa. Grupa reda $3^2$ imamo samo dve: $\mathbf{C}_9$ i $\mathbf{C}_3 \times \mathbf{C}_3$. Pretpostavimo prvo da je Sylowa 3-podgrupa ciklična grupa reda 9; zašto da to ne bude opet $\mathbf{Z}_9$? $\mathbf{Z}_2$ će biti (jedna od) Sylowih 2-podgrupa. Pored trivijalnog homomorfnog preslikavanja grupe $\mathbf{Z}_2$ u $\mathbf{Aut}(\mathbf{Z}_9) = \langle\{\imath, \varphi_2, \varphi_4, \varphi_5, \varphi_7, \varphi_8\}, \circ\rangle$ (gde je, jasno, $\varphi_k \circ \varphi_l = \varphi_{k\cdot_9 l}$ i $(m)\varphi_k = m \cdot_9 k$) koji daje direktan proizvod $\mathbf{Z}_9 \times \mathbf{Z}_2 \cong \mathbf{Z}_{18}$, postoji još samo jedan homomorfizam – $\theta$ koji preslikava 1 u $\varphi_8$ ($\varphi_8$ je jedini element reda 2). U odgovarajućem poludirektnom proizvodu $\mathbf{Z}_9 \times_\theta \mathbf{Z}_2$ imaćemo:

$$(1,0)^{-1} \star (0,1) \star (1,0) = (0,(1)\varphi_8) = (0,8) = (0,1)^8,$$

tj.

$$(0,1) \star (1,0) = (1,0) \star (0,1)^8,$$

i $\mathbf{G}$ je dijedarska grupa stepena 9.

Neka je sada Sylowa 3-podgrupa $\mathbf{Z}_3 \times \mathbf{Z}_3$. Prema 10.45($f$), $\mathbf{Aut}(\mathbf{Z}_3 \times \mathbf{Z}_3) \cong \mathbf{GL}_2(Z_3)$, a, prema 10.46, $|GL_2(Z_3)| = (3^2 - 1) \cdot (3^2 - 3) = 48$. Nađimo elemente reda 2 u grupi $\mathbf{GL}_2(Z_3)$ (skrećemo još jednom pažnju da je sabiranje i množenje elemenata po modulu 3, radimo, dakle, u polju $\langle 3, +_3, \cdot_3\rangle$, ali ćemo, iz praktičnih razloga, koristiti notaciju $+, \cdot$). $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ daje sistem jednačina

$$a^2 + bc = 1$$



$$(a + d)b = 0$$

$$(a + d)c = 0$$

$$d^2 + bc = 1.$$

Ako je $a + d \neq 0$, onda je $b = c = 0$, $a = d$ ($\neq 0$) i $a^2 = 1$, tj. $a = 1$ ili $a = 2$. Imamo stoga svega dva rešenja u ovom slučaju: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ i $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$. Ako je $a + d = 0$, onda je $a = -d$ ($= 2d$). Za $a = d = 0$ je $bc = 1$ i rešenja su $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ i $\begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}$. Ako je npr. $a = 1$, $d = 2$, onda iz prve jednačine (ili četvrte, svejedno) sledi $bc = 0$, pa je ili $b$ ili $c$ nula. Rešenja su, znači, u ovom slučaju: $\begin{bmatrix} 1 & 0 \\ c & 2 \end{bmatrix}$, $\begin{bmatrix} 1 & b \\ 0 & 2 \end{bmatrix}$, $\begin{bmatrix} 2 & 0 \\ c & 1 \end{bmatrix}$, $\begin{bmatrix} 2 & b \\ 0 & 1 \end{bmatrix}$ (ukupno je trinaest elemenata-matrica reda 2). Jedinična matrica (tj. trivijalni homomorfizam) daje direktan proizvod $\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_2 \cong \mathbf{Z}_3 \times \mathbf{Z}_6$. Matrici $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$ odgovara automorfizam $\Phi_1$ grupe $\mathbf{Z}_3 \times \mathbf{Z}_3$ koji preslikava $(1,0)$ u $(2,0)$ i $(0,1)$ u $(0,2)$ (videti i 10.45($d$)), pa je, za utapanje $\Psi_1$ grupe $\mathbf{Z}_2$ u $\mathbf{Aut}(\mathbf{Z}_3 \times \mathbf{Z}_3)$, gde je $(1)\Psi_1 = \Phi_1$:

$$(1,(0,0))^{-1} \star (0,(1,0)) \star (1,(0,0)) = (0,(1,0)\Phi_1) = (0,(2,0)) = (0,(1,0))^2,$$

$$(1,(0,0))^{-1} \star (0,(0,1)) \star (1,(0,0)) = (0,(0,1)\Phi_1) = (0,(0,2)) = (0,(0,1))^2,$$

odnosno,

$$(0,(1,0)) \star (1,(0,0)) = (1,(0,0)) \star (0,(1,0))^2,$$

$$(0,(0,1)) \star (1,(0,0)) = (1,(0,0)) \star (0,(0,1))^2.$$

Ovim je, uz već poznate relacije

$$(1,(0,0))^2 = (0,(1,0))^3 = (0,(0,1))^3 = (0,(0,0))$$

i

$$(0,(1,0)) \star (0,(0,1)) = (0,(0,1)) \star (0,(1,0)),$$

potpuno određena grupa $(\mathbf{Z}_3 \times \mathbf{Z}_3) \times_{\Psi_1} \mathbf{Z}_2$. Indukcijom se lako proverava da je

$$(0,(1,0))^m \star (1,(0,0))^k = (1,(0,0))^k \star (0,(1,0))^{m\cdot_3 2^k}$$

(analogan rezultat važi i za proizvod stepena elemenata $(0,(0,1))$ i $(1,(0,0))$), pa je (za $k, k_1 \in 2$, $m, m_1, n, n_1 \in 3$):

$$(k,(m,n)) \star (k_1,(m_1,n_1)) = (k +_2 k_1, (m \cdot_3 2^{k_1} +_3 m_1, n \cdot_3 2^{k_1} +_3 n_1)).$$

Ova grupa ima devet elemenata reda 2, jer iz $k +_2 k = 0$ i $m \cdot_3 2^k +_3 m = 0$, $n \cdot_3 2^k +_3 n = 0$ sledi $k = 0$ ili $k = 1$, a za $k = 0$ mora biti i $m = n = 0$ (te taj slučaj daje jedinični element), dok su za $k = 1$, $m, n$ prozvoljni.

Matrici $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ odgovara automorfizam $\Phi_2$: $(1,0)\Phi_2 = (1,0)$, $(0,1)\Phi_2 = (0,2)$, te utapanju $\Psi_2 : Z_2 \longrightarrow Aut(\mathbf{Z}_3 \times \mathbf{Z}_3)$, gde je $(1)\Psi_2 = \Phi_2$, odgovara poludirektni proizvod u kome je:

$$(1,(0,0))^{-1} \star (0,(1,0)) \star (1,(0,0)) = (0,(1,0)\Phi_2) = (0,(1,0)),$$

$$(1,(0,0))^{-1} \star (0,(0,1)) \star (1,(0,0)) = (0,(0,1)\Phi_2) = (0,(0,2)) = (0,(0,1))^2,$$

odnosno,

$$(0,(1,0)) \star (1,(0,0)) = (1,(0,0)) \star (0,(1,0)),$$

$$(0,(0,1)) \star (1,(0,0)) = (1,(0,0)) \star (0,(0,1))^2.$$

Imajući u vidu i gore navedene relacije koje uvek važe zaključujemo da se radi o grupi (izomorfnoj grupi) $\mathbf{Z}_3 \times \mathbf{S}_3$ (videti i naredno poglavlje). "Množenje" je dato sa (za $k, k_1 \in 2$, $m, m_1, n, n_1 \in 3$):

$$(k,(m,n)) \star (k_1,(m_1,n_1)) = (k +_2 k_1, (m +_3 m_1, n \cdot_3 2^{k_1} +_3 n_1)).$$

Ova grupa ima tri elementa reda 2, jer se iz $k +_2 k = 0$, $m +_3 m = 0$, $n \cdot_3 2^k +_3 n = 0$ dobija: $m = 0$; $k = 0$ daje i $n = 0$ (dakle jedinični element) dok je, u slučaju da je $k = 1$, $n$ proizvoljno.

Sve ostale matrice reda 2 su konjugovane sa nekom od ove dve, te prema 13.10($b$) drugih grupa i nemamo. Iz linearne algebre je poznato da je svaka od datih matrica konjugovana sa nekom regularnom dijagonalnom, a ovde je izbor doista ograničen. Trivijalno, matrice $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ i $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ su konjugovane (a jedinična ne dolazi u obzir). Čitalac koji nije upoznat sa elementima linearne algebre može se i prostim računom uveriti u navedeno. Tako je npr.

$$\begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}^{-1} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2 & 2 \end{bmatrix}$$

ili

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}^{-1} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}.$$

Kasnije ćemo, vežbe radi, pokazati i na drugi način, koristeći prezentaciju grupa, da su poludirektni proizvodi koji odgovaraju ovde navedenim konjugovanim matricama izomorfni.□

**Lema 18.4** *Postoji pet grupa reda* 20.



**Dokaz**. Neka je $\mathbf{G}$ grupa reda $20 (= 2^2 \cdot 5)$. Očigledno, $s_5 = 1$, a $s_2$ je ili 1 ili 5. U svakom slučaju, s obzirom da je presek Sylowe 5-podgrupe i (ma koje) Sylowe 2-podgrupe jedinična podgrupa, $\mathbf{G}$ je poludirektni proizvod normalne Sylowe 5-podgrupe i (ma koje) Sylowe 2-podgrupe.

Pretpostavimo prvo da je (jedna, a onda i sve ostale, ukoliko ih ima više) Sylowa 2-podgrupa ciklična grupa – $\mathbf{Z}_4$; Sylowe 5-podgrupa će, naravno, biti $\mathbf{Z}_5$. Kako je $\mathbf{Aut}(\mathbf{Z}_5) = \langle\{\imath, \varphi_2, \varphi_3, \varphi_4\}, \circ\rangle$, gde je, ponavljamo, $(m)\varphi_k = m \cdot_5 k$ i $\varphi_k \circ \varphi_l = \varphi_{k \cdot_5 l}$, na raspolaganju su nam sledeća homomorfna preslikavanja grupe $\mathbf{Z}_4$ u $\mathbf{Aut}(\mathbf{Z}_5)$, određena, jasno, slikom generatornog elementa: (trivijalan homomorfizam) $(1)\psi_0 = \imath$, $(1)\psi_1 = \varphi_4$, $(1)\psi_2 = \varphi_2$ i $(1)\psi_4 = \varphi_3$. Homomorfizmi $\psi_2$ i $\psi_3$ su bijektivni, te uzimamo u obzir samo jedan od njih. Već nam je poznato: $\mathbf{Z}_5 \times_{\psi_0} \mathbf{Z}_4 \cong \mathbf{Z}_5 \times \mathbf{Z}_4 \cong \mathbf{Z}_{20}$. U grupi $\mathbf{Z}_5 \times_{\psi_1} \mathbf{Z}_4$ važi:

$$(1,0)^{-1} \star (0,1) \star (1,0) = (3,0) \star (0,1) \star (1,0) = (0,(1)\varphi_4) = (0,4) = (0,1)^4,$$

tj.

$$(0,1) \star (1,0) = (1,0) \star (0,1)^4.$$

Lako se indukcijom (po $k$) pokazuje da je

$$(0,1)^m \star (0,1)^k = (1,0)^k \star (0,1)^{m \cdot_5 (\overbrace{4 \cdot_5 \ldots \cdot_5 4}^{k-puta})},$$

te je, u opštem (za $k, k_1 \in 4$, $m, m_1 \in 5$):

$$(k,m) \star (k_1,m_1) = (k +_4 k_1, m \cdot_5 (\overbrace{4 \cdot_5 \ldots \cdot_5 4}^{k_1-puta}) +_5 m_1).$$

U grupi $\mathbf{Z}_5 \times_{\psi_2} \mathbf{Z}_4$ važi:

$$(1,0)^{-1} \star (0,1) \star (1,0) = (3,0) \star (0,1) \star (1,0) = (0,(1)\varphi_2) = (0,2) = (0,1)^2,$$

odnosno

$$(0,1) \star (1,0) = (1,0) \star (0,1)^2.$$

Stoga je, generalno, (za $k, k_1 \in 4$, $m, m_1 \in 5$):

$$(k,m) \star (k_1,m_1) = (k +_4 k_1, m \cdot_5 (\overbrace{2 \cdot_5 \ldots \cdot_5 2}^{k_1-puta}) +_5 m_1).$$

Određivanjem elemenata reda 2 lako se pokazuje da date grupe nisu izomorfne. U grupi $\mathbf{Z}_5 \times_{\psi_1} \mathbf{Z}_4$ samo je $(2,0)$ element reda 2. Iz $k +_4 k = 0$ i $m \cdot_5 (\overbrace{4 \cdot_5 \ldots \cdot_5 4}^{k-puta}) +_5 m = 0$ sledi $k = 0$ ili $k = 2$ i $m = 0$. U grupi $\mathbf{Z}_5 \times_{\psi_2} \mathbf{Z}_4$ pet elemenata su reda 2: $(2,m)$, $m \in 5$ (provera je analogna).

Neka je sada Sylowa 2-podgrupa Kleinova grupa – $\mathbf{Z}_2 \times \mathbf{Z}_2$. Pored trivijalnog homomorfnog preslikavanja grupe $\mathbf{Z}_2 \times \mathbf{Z}_2$ u grupu $\mathbf{Aut}(\mathbf{Z}_5)$ koji daje direktan proizvod $\mathbf{Z}_5 \times (\mathbf{Z}_2 \times \mathbf{Z}_2)$ ($\cong \mathbf{Z}_{10} \times \mathbf{Z}_2$), postoji u osnovi još jedan: dva se nejedinična elementa preslikavaju u $\varphi_4$ (element reda 2), a treći (nejedinični) u $\imath$. Zbog simetrije stvari možemo uzeti da je preslikavanje $\psi : Z_2 \times Z_2 \longrightarrow Aut(\mathbf{Z}_5)$ dato sa $(1,0)\psi = \varphi_4$, $(0,1)\psi = \imath$ (jasno, $(1,1)\psi = \varphi_4 \circ \imath = \varphi_4$). U grupi $\mathbf{Z}_5 \times_\psi (\mathbf{Z}_2 \times \mathbf{Z}_2)$ imaćemo:

$$((1,0),0)^{-1} \star ((0,0),1) \star ((1,0),0) =$$

$$((1,0),0) \star ((0,0),1) \star ((1,0),0) = ((0,0),(1)\varphi_4) = ((0,0),1)^4,$$

tj.

$$((0,0),1) \star ((1,0),0) = ((1,0),0) \star ((0,0),1)^4,$$

kao i

$$((0,0),1) \star ((0,1),0) = ((0,1),0) \star ((0,0),1).$$

Stoga je (za $k, k_1, l, l_1 \in 2$, $m, m_1 \in 5$)

$$((k,l),m) \star ((k_1,l_1),m_1) = ((k +_2 k_1, l +_2 l_1), m \cdot_5 \underbrace{(4 \cdot_5 \ldots \cdot_5 4)}_{k_1-puta} +_5 m_1).$$

Elemenata reda 2, kad smo već kod njih, sada ima sedam: $((1,0),m)$, $m \in 5$, $((0,1),0)$ i $((1,1),0)$.□

Pažljiviji čitalac je primetio da su nam sada poznate (do na izomorfizam) sve grupe reda manjeg od ili jednakog 20 (i ne samo one). Posebno primer sa grupama reda 16 pokazuje da je "otkrivanje" svih grupa datog reda u osnovi nezahvalan, da ne kažemo težak posao. Konačno, nije ni poznata formula koja bi za proizvoljno dati prirodan broj $n$ dala broj neizomorfnih grupa reda $n$. Određujemo još, prakse radi, sve grupe reda 30 (ako je nekome "simpatičniji" broj 32 trebalo bi da zna da grupa tog reda ima 51) i jedan opšti slučaj, sve grupe reda $p^3$, gde je $p$ prost broj.

**Lema 18.5** *Grupa reda* 30 *ima četiri.*

**Dokaz.** Neka je $\mathbf{G}$ grupa reda $30 = 2 \cdot 3 \cdot 5$. Odmah možemo zaključiti da je bilo $s_3 = 1$ bilo $s_5 = 1$. Jer, ako bi bilo $s_3 = 10$ i $s_5 = 6$, onda bi unija Sylowih 5-podgrupa imala $6 \cdot 4 + 1 = 25$ elemenata, pa definitivno, ne bi bilo "mesta" za 10 Sylowih 3-podgrupa. Neka je, recimo, $s_3 = 1$ i neka je $\mathbf{A}$ jedinstvena Sylowa 3-podgrupa, a $\mathbf{B}$ (jedna od) Sylowih 5-podgrupa. Kako je $\mathbf{A} \lhd \mathbf{G}$, to je $\mathbf{C} = \mathbf{AB}$ podgrupa reda 15 (jer $\mathbf{A} \cap \mathbf{B} = \mathbf{E}$). $\mathbf{B}$ je karakteristična podgrupa (automorfizam očuvava red elementa) normalne podgrupe $\mathbf{C}$ grupe $\mathbf{G}$, te je, prema 4.34, i sama normalna podgrupa. Dakle, i $s_5 = 1$ (analogno bismo dobili da $s_5 = 1$ implicira $s_3 = 1$). $\mathbf{C}$ je, znači, ciklična grupa reda 15,



a $\mathbf{G}$ je poludirektni proizvod podgrupe $\mathbf{C}$ i jedne Sylowe 2-podgrupe. Neka je $\mathbf{C}$ baš $\mathbf{Z}_{15}$ i neka je $\mathbf{Z}_2$ jedna Sylowa 2-podgrupa. U grupi $\mathbf{Aut}(\mathbf{Z}_{15}) = \langle\{\imath, \varphi_2, \varphi_4, \varphi_7, \varphi_8, \varphi_{11}, \varphi_{13}, \varphi_{14}\}, \circ\rangle$ (gde je $\varphi_k \circ \varphi_l = \varphi_{k \cdot_{15} l}$ i $(m)\varphi_k = m \cdot_{15} k$ – 8.24), izomorfnoj sa $\mathbf{Aut}(\mathbf{Z}_3) \times \mathbf{Aut}(\mathbf{Z}_5)$, imamo tri elementa reda 2 ($\varphi_4$, $\varphi_{11}$, $\varphi_{14}$), pa postoje svega tri netrivijalna homomorfna preslikavanja grupe $\mathbf{Z}_2$ u grupu $\mathbf{Aut}(\mathbf{Z}_{15})$ (određena slikom generatornog elementa – 1):

$$(1)\theta_1 = \varphi_4, \quad (1)\theta_2 = \varphi_{11}, \quad (1)\theta_3 = \varphi_{15}.$$

Kako je $\varphi_4|_{\langle 5\rangle} = \imath_{\langle 5\rangle}$, prema 13.10 je $\mathbf{Z}_{15} \times \mathbf{Z}_2 \cong \langle 5\rangle \times (\langle 3\rangle \times_{\psi_1} \mathbf{Z}_2)$, gde je $\psi_1 = \theta_1|_{\langle 3\rangle}$. S obzirom da je

$$(1,0)^{-1} \star (0,3) \star (1,0) = (1,0) \star (0,3) \star (1,0) = (0,(3)\varphi_4) = (0,12) = (0,3)^4,$$

dobijamo $(0,3) \star (1,0) = (1,0) \star (0,3)^4$ i $\langle 3\rangle \times_{\psi_1} \mathbf{Z}_2 = \mathbf{D}_5$ (dijedarska grupa stepena 5). Dakle: $\mathbf{Z}_{15} \times_{\theta_1} \mathbf{Z}_2 \cong \mathbf{Z}_3 \times \mathbf{D}_5$.

$\varphi_{11}$ ostavlja fiksnim sve elemente ciklične podgrupe $\langle 3\rangle$ (reda 5), pa je $\mathbf{Z}_{15} \times_{\theta_2} \mathbf{Z}_2 \cong \langle 3\rangle \times (\langle 5\rangle \times_{\psi_2} \mathbf{Z}_2)$. Sada je, naravno, $\psi_2 = \theta_2|_{\langle 5\rangle}$ i

$$(1,0)^{-1} \star (0,5) \star (1,0) = (0,(5)\varphi_{11}) = (0,10) = (0,5)^2,$$

tj. $(0,5) \star (1,0) = (1,0) \star (0,5)^2$. Stoga je $\mathbf{Z}_{15} \times_{\theta_2} \mathbf{Z}_2 \cong \mathbf{Z}_5 \times \mathbf{D}_3$.

$\varphi_{14}$ ne ostavlja fiksnim sve elemente nijedne od podgrupa $\langle 3\rangle$, $\langle 5\rangle$. Ovog puta je:

$$(1,0)^{-1} \star (0,1) \star (1,0) = (0,(1)\varphi_{14}) = (0,14) = (0,1)^{14},$$

odnosno $(0,1) \star (1,0) = (1,0) \star (0,1)^{14}$, i grupa $\mathbf{G}$ je dijedarska grupa stepena 15 – $\mathbf{D}_{15}$.

Trivijalno homomorfno preslikavanje nam daje direktan proizvod: $\mathbf{Z}_{15} \times \mathbf{Z}_2 \cong \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$.□

**Korolar 18.6** *Za svaki prost broj $p$ postoji svega pet grupa reda $p^3$.*

**Dokaz.** U 12.5 smo dokazali ovo tvrđenje za $p = 2$. Diskusija u slučaju Abelovih grupa je (gotovo) identična no, vežbe radi, ponovićemo je.

Neka je $\mathbf{G}$ neciklična Abelova grupa reda $p^3$. Ako su joj svi elementi reda $p$, onda je, prema 10.33, $\mathbf{G} \cong \mathbf{C}_p \times \mathbf{C}_p \times \mathbf{C}_p$. Pretpostavimo sada da ima jedan element reda $p^2$, recimo $a$, i neka $b \notin \langle a\rangle$. Ako je $b$ element reda $p$, tada je $\langle a\rangle \cap \langle b\rangle = \{e\}$ i $\mathbf{G} = \langle a\rangle \times \langle b\rangle$. Ukoliko je i $b$ reda $p^2$, onda je podgrupa $\langle a\rangle \cap \langle b\rangle$ reda $p$, pa je $b^p \in \langle a\rangle$. Možemo pretpostaviti da je $b^p = a^p$, u suprotnom bismo izabrali drugi adekvatni generatorni element grupe $\langle a\rangle$, te je element $c = a^{p-1}b$ ($\notin \langle a\rangle$) reda $p$ i opet je $\mathbf{G} \cong \mathbf{C}_{p^2} \times \mathbf{C}_p$. Dakle, Abelove grupe reda $p^3$ su: $\mathbf{C}_{p^3}$, $\mathbf{C}_{p^2} \times \mathbf{C}_p$ i $\mathbf{C}_p \times \mathbf{C}_p \times \mathbf{C}_p$.

Neka je, dalje, $\mathbf{G}$ neabelova grupa i neka je $p > 2$. Prema 4.13 i 8.19, $\mathbf{Z(G)}$ je reda $p$, a zbog 6.8 i 8.20 važi i $\mathbf{Z(G)} = \mathbf{G}'$. Prema 6.3($b$), preslikavanje $\phi$ dato sa $(a)\phi = a^p$ homomorfno je preslikavanje grupe $\mathbf{G}$ u $\mathbf{Z(G)}$ (podsetimo se: $(ab)^p = [b,a]^{\frac{1}{2}p(p-1)}a^pb^p = a^pb^p$ – koristimo da je $p > 2$). $\mathbf{Ker}(\phi)$ je reda $p^2$ ili $p^3$. Ako je $|Ker(\phi)| = p^2$, preslikavanje $\phi$ je surjektivno i postoji element reda $p^2$ – neka je to $a$. Prema 16.16, $\langle a\rangle$ je normalna podgrupa grupe $\mathbf{G}$. Kako su nejedinični elementi jezgra reda $p$, to je jezgro direktni proizvod cikličnih grupa reda $p$, recimo $\mathbf{Ker}(\phi) = \langle b\rangle \times \langle c\rangle$ i $Ker(\phi) \cap \langle a\rangle = \langle a^p\rangle$. Ako je npr. $b \in Ker(\phi)\setminus\langle a\rangle$, $\mathbf{G}$ je poludirektni proizvod (normalne) podgrupe $\langle a\rangle$ i grupe $\langle c\rangle$. Prema 8.25($b$), $\mathbf{Aut}(\langle a\rangle) = \langle\{\varphi_k \mid 0 < k < p^2, (k,p) = 1\}, \circ\rangle$, gde je $(a)\varphi_k = a^k$ i $\varphi_k \circ \varphi_l = \varphi_{k+_{p^2}l}$, ciklična je grupa reda $p(p-1)$. Trivijalno homomorfno preslikavanje grupe $\langle b\rangle$ u $\mathbf{Aut}(\langle a\rangle)$ je isključeno jer bi to dalo direktni proizvod i $\mathbf{G}$ bi bila Abelova grupa. Svi drugi homomorfizmi (radi se zapravo o utapanjima) preslikavaju grupu $\langle b\rangle$ na jedinstvenu podgrupu reda $p$ grupe $\mathbf{Aut}(\langle a\rangle)$. Ta grupa je generisana elementom $\varphi_{1+p}$ (lako se proverava da je $(1+p)^p - [\frac{(1+p)^p}{p^2}]p^2 = 1$), te uzimamo u obzir samo jedan od njih, npr. $\psi$ dat sa $(b)\psi = \varphi_{1+p}$. U grupi $\langle a\rangle \times_\psi \langle b\rangle$ važi:

$$(b,e)^{-1} \star (e,a) \star (b,e) = (b^{-1},e) \star (e,a) \star (b,e) = (e,(a)\varphi_{1+p}) =$$

$$(e,a^{1+p}) = (e,a)^{1+p},$$

tj.

$$(e,a) \star (b,e) = (b,e) \star (e,a)^{1+p}.$$

Odatle izvodimo, indukcijom po $m$:

$$(e,a)^n \star (b,e)^m = (b,e)^m \star (e,a)^{n\cdot_{p^2}\overbrace{[(1+p)\cdot_{p^2}\cdots\cdot_{p^2}(1+p)]}^{m-puta}},$$

što determiniše množenje (proizvoljnih elemenata, $m, m_1 \in p$, $n, n_1 \in p^2$)

$$(b^m,a^n) \star (b^{m_1},a^{n_1}) = (b,e)^m \star (e,a)^n \star (b,e)^{m_1} \star (e,a)^{n_1} =$$

$$(b,e)^{m+_pm_1} \star (e,a)^{n\cdot_{p^2}\overbrace{[(1+p)\cdot_{p^2}\cdots\cdot_{p^2}(1+p)]}^{m_1-puta}+_{p^2}n_1} =$$

$$(b^{m+_pm_1},a^{n\cdot_{p^2}\overbrace{[(1+p)\cdot_{p^2}\cdots\cdot_{p^2}(1+p)]}^{m_1-puta}+_{p^2}n_1}).$$

Ako je $|Ker(\phi)| = p^3$, tj. $Ker(\phi) = G$, svi elementi su reda $p$. Neka je $\mathbf{H}$ (jedna) normalna podgrupa reda $p^2$ (videti 16.16). $\mathbf{H}$ je direktni proizvod dve ciklične grupe reda $p$, recimo $\mathbf{H} = \langle a\rangle \times \langle b\rangle$. Ako $c \notin H$, onda $H \cap \langle c\rangle = \{e\}$ i $\mathbf{G}$ je poludirektni proizvod normalne podgrupe $\mathbf{H}$ i grupe $\langle c\rangle$. Prema 10.45($f$), 10.46, $\mathbf{Aut(H)} \cong \mathbf{GL}_2(Z_p)$ je reda $(p^2-p)(p^2-1)$, pa su njene Sylowe



$p$-podgrupe reda $p$. Trivijalno homomorfno preslikavanje opet ne dolazi u obzir (dobijamo Abelovu grupu). Svaki drugi homomorfizam je izomorfno preslikavanje grupe $\langle c\rangle$ na neku od Sylowih $p$-podgrupa grupe $\mathbf{Aut(H)}$, a kako su ove sve međusobno konjugovane, biće, prema 13.10($b$), svi odgovarajući poludirektni proizvodi izomorfni, te smo slobodni u izboru jedne od njih. Lako se uočava da je u $\mathbf{GL}_2(Z_p)$ jedan element reda $p$ matrica $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, a njoj odgovara automorfizam $\varphi$ grupe $\mathbf{H}$ koji preslikava $a$ u $ab$ i $b$ ostavlja fiksnim. Stoga je za utapanje $\theta$ grupe $\langle c\rangle$ u $\mathbf{Aut(H)}$, gde je $(c)\theta = \varphi$, u grupi $\mathbf{H} \times_\theta \langle c\rangle$:

$$(c,e)^{-1} \star (e,a) \star (c,e) = (e,(a)\varphi) = (e,ab) = (e,a) \star (e,b),$$

tj.

$$(e,a) \star (c,e) = (c,e) \star (e,a) \star (e,b),$$

i

$$(c,e)^{-1} \star (e,b) \star (c,e) = (e,(b)\varphi) = (e,b),$$

odnosno

$$(e,b) \star (c,e) = (c,e) \star (e,b).$$

Ovim je relacijama (uz već poznate: $(e,a)^p = (e,b)^p = (c,e)^p = (e,e)$ i $(e,a) \star (e,b) = (e,b) \star (e,a)$) potpuno određena grupa. "Množenje" je dato sa

$$(c^k,a^mb^n) \star (c^{k_1},a^{m_1}b^{n_1}) = (c^{k+_pk_1},a^{m+_pm_1}b^{k\cdot_pm+_pn+_pn_1}).\square$$

## 19 Neke familije prostih grupa

U ovom paragrafu koristićemo nešto više elementarnog poznavanja linearne algebre i teorije prstena i polja, ali i to ćemo da svedemo na najmanju moguću meru. Zbog koherentnosti teksta izložićemo u najkraćim crtama, koji put bez kompletnih dokaza, neke od definicija i stavova (iz datih oblasti) relevantnih za ovu priču; druge ćemo pak smatrati poznatim (kao npr. definicije potprstena, potpolja, homomorfizma prstena, zatim matrični račun i tako dalje).

Nas će prevashodno interesovati komutativni prsteni sa jedinicom ili polja. Napominjemo da se mnogi od datih rezultata odnose na sve ili širu klasu prstena. Po pravilu, neutralni element aditivne operacije prstena $\mathbf{R} = \langle R,+,\cdot\rangle$ obeležava se sa 0, neutralni element multiplikativne operacije, ukoliko postoji, sa 1. Kada se govori o inverzibilnom elementu prstena sa jedinicom, misli se na element koji ima inverzni u odnosu na operaciju "množenja" (jer, $\langle R,+\rangle$ je Abelova grupa i, naravno, svaki element je inverzibilan s obzirom na aditivnu operaciju).

**Lema 19.1** *Svaki integralni domen* $\mathbf{R}$ *se može utopiti u, do na izomorfizam, jedinstveno minimalno polje, tzv. količničko polje domena* $\mathbf{R}$.

**Dokaz.** Na skupu $R \times (R \setminus \{0\})$ definišimo relaciju $\sim$ sa: $(a,b) \sim (c,d)$ akko $ad = bc$. Relacija $\sim$ je relacija ekvivalencije. Svojstva refleksivnosti i simetričnosti su očigledna. Ako je $(a,b) \sim (c,d)$ i $(c,d) \sim (e,f)$, tj. $ad = bc$ i $cf = de$, tada je $adcf = bcde$, dakle, $cd(af - be) = 0$, pa ako je $c = 0$, onda je i $a = e = 0$, a ako je $c \neq 0$ (stoga i $cd \neq 0$), onda je $af = be$; u svakom slučaju $(a,b) \sim (e,f)$. Neka je $[(a,b)]$ klasa ekvivalencije relacije $\sim$ čiji je reprezent $(a,b)$. Na skupu svih klasa ekvivalencije, u oznaci $(R \times (R \setminus \{0\}))/\sim$, definišemo operacije $+$ i $\cdot$ (korišćenje istih oznaka za različite operacije ustaljena je praksa jer kontekst isključuje mogućnost zabune) sa:

$$[(a,b)] + [(c,d)] \stackrel{\text{def}}{=} [(ad + bc, bd)],$$

$$[(a,b)] \cdot [(c,d)] \stackrel{\text{def}}{=} [(ac, bd)].$$

Lako se proverava da su operacije dobro definisane, tj. da su definicije nezavisne od predstavnika klasa ekvivalencija, kao i da je $\overline{\mathbf{R}} = \langle (R \times (R \setminus \{0\}))/\sim, +, \cdot \rangle$ polje; neutralni element za sabiranje je $[(0,1)]$, za množenje $[(1,1)]$, inverzni element elementa $[(a,b)]$, $a \neq 0$, je $[(b,a)]$. Preslikavanja $\varphi : R \longrightarrow \overline{R}$ dato sa $(a)\varphi = [(a,1)]$ utapanje je integralnog domena $\mathbf{R}$ u polje $\overline{\mathbf{R}}$.

Neka je, dalje, $\mathbf{F}$ polje koje sadrži domen $\mathbf{R}$. Tada je polje $\overline{\mathbf{R}}$ izomorfno potpolju polja $\mathbf{F}$ sa domenom $\{ab^{-1} \mid a \in R, b \in R \setminus \{0\}\}$ (primetimo samo: $ab^{-1} + cd^{-1} = (ad + bc)(bd)^{-1}$, $(ab^{-1})(cd^{-1}) = (ac)(bd)^{-1}$). Korespondencija je data sa $[(a,b)] \longleftrightarrow ab^{-1}$ (ako je $[(a,b)] = [(c,d)]$, odnosno $ad = bc$, onda je $ab^{-1} = cd^{-1}$).□

**Definicija 19.2** *Karakteristika prstena* $\mathbf{R}$ *je najmanji pozitivan prirodan broj* $n$ *takav da je, za svako* $a \in R$, $na = \underbrace{a + \cdots + a}_{n-puta} = 0$, *ukoliko takav postoji, u suprotnom prsten je karakteristike* 0 *ili* $\infty$.

**Lema 19.3** (*a*) *Ako je* $a$ *nenula element polja* $\mathbf{F}$, *onda je, za prirodan broj* $n$, $na = 0$ *akko je* $n1 = 0$;

(*b*) *Karakteristika polja je ili* 0 *ili prost broj;*

(*c*) *Presek familije potpolja datog polja je potpolje;*

(*d*) *Svako polje sadrži minimalno (s obzirom na inkluziju) potpolje. Ako je polje karakteristike* 0, *njegovo minimalno potpolje je izomorfno polju racionalnih brojeva; ako je karakteristike* $p$ ($p$ - *prost broj*), *onda polju* $\langle Z_p, +_p, \cdot_p \rangle$.

**Dokaz.** (*a*) $na = \underbrace{a + \cdots + a}_{n-puta} = 0$ akko $na \cdot a^{-1} = 0$ akko $n1 = 0$.

(*b*) Neka je $n$ konačna karakteristika polja. Ako bi $n$ bio složen broj, $n = kl$, $k, l > 1$, sledilo bi: $n1 = \underbrace{(1 + \cdots + 1)}_{k-puta} \cdot \underbrace{(1 + \cdots + 1)}_{l-puta} = 0$, pa bi bilo ili $k1 = 0$ ili $l1 = 0$, kontradikcija.



(*c*) Direktna (i trivijalna) provera.

(*d*) Minimalno potpolje polja $\mathbf{F}$ je presek svih njegovih potpolja. Kako je 1 (neutralni element grupe $\langle F \setminus \{0\}, \cdot \rangle$) svakako njegov element, to ono, već u zavisnosti od karakteristike polja, sadrži ili izomorfnu kopiju prstena celih brojeva ili prstena $\langle p, +_p, \cdot_p \rangle$. Količničko polje prstena celih brojeva je polje racionalnih brojeva, a prsten $\langle p, +_p, \cdot_p \rangle$ je i polje (2.13).□

**Korolar 19.4** *Ako je karakteristika polja* $\mathbf{F} = \langle F, +, \cdot \rangle$ *prost broj* $p$, *onda je* $\langle F, + \rangle$ *direktna suma cikličnih grupa reda* $p$.

**Dokaz.** Već dat - 10.33.

Adekvatno tvrđenje za slučaj kada je polje karakteristike 0 dato je u 33.22.□

**Definicija 19.5** *Potprsten* $\mathbf{I}$ *prstena* $\mathbf{R}$ *je ideal (prstena* $\mathbf{R}$*), piše se* $\mathbf{I} \lhd \mathbf{R}$, *akko je zatvoren za množenje "spolja", tj. akko je, za svako* $a \in I$ *i svako* $r \in R$, $ar, ra \in I$. *Ideal je pravi akko je njegov domen pravi podskup domena prstena* ($I \subset R$).

*Pravi ideal je maksimalan akko nije strogo sadržan ni u jednom drugom pravom idealu.*

**Lema 19.6** (*a*) *Neprazan podskup* $I$ *domena* $R$ *prstena* $\mathbf{R}$ *je domen ideala akko za svako* $a, b \in I$ *i svako* $r \in R$ *važi:* $a - b$, $ra$, $ar \in I$;

(*b*) *Ideal* $\mathbf{I}$ *prstena* $\mathbf{R}$ *sa jedinicom je pravi akko* $1 \notin I$;

(*c*) *Presek familije ideala (datog prstena) je ideal;*

(*d*) *Za svaki podskup* $A$ *domena prstena* $\mathbf{R}$ *postoji jedinstven najmanji ideal* $\mathbf{I}$ *takav da je* $A \subseteq I$ - *ideal generisan skupom* $A$; *kao i kod grupa, pisaćemo* $\mathbf{I} = \langle A \rangle$;

(*e*) *Ako je* $\mathbf{R}$ *komutativan prsten sa jedinicom i* $a \in R$, *onda je* $\langle a \rangle = aR \stackrel{\text{def}}{=} \{ar \mid r \in R\}$. *Uopšte:*

$$\langle A \rangle = \{r_1 a_{i_1} + \cdots + r_n a_{i_n} \mid r_j \in R,\ a_{i_j} \in A,\ j \in \{1, \ldots, n\},\ n \in N\}.$$

(*f*) *Pravi ideal* $\mathbf{I}$ *komutativnog prstena sa jedinicom* $\mathbf{R}$ *je maksimalan akko za svako* $x$ *koje nije u* $I$ *postoji element* $y$ ($\in R$) *takav da je* $1 - xy \in I$;

(*g*) *Integralni domen je polje akko nema netrivijalnih ideala (trivijalni ideali su sam prsten i nula ideal - ideal čija je jedini element nula).*

**Dokaz.** (*a*) i (*c*) je trivijalno, (*d*) je direktna posledica tačke (*c*).

(*b*) Pokazaćemo: $\mathbf{I} = \mathbf{R}$ akko $1 \in I$. Neka $1 \in I$. Onda je, za svako $r \in R$, $r = 1 \cdot r \in I$, pa $I = R$.

(*e*) Jasno, $aR \subseteq \langle a \rangle$, dok se, s druge strane, lako proverava da je i sam skup $aR$ domen ideala. Jednako se rezonuje i u opštem slučaju.

($f$) Neka je $\mathbf{I}$ maksimalan ideal i $x \notin I$. Tada je ideal $\mathbf{I}$ strogo sadržan u idealu $\langle I, x\rangle$, pa je $\langle I, x\rangle = \mathbf{R}$. S obzirom na komutativnost prstena i egzistenciju jedinice, elementi ideala (prstena) su oblika $i + xr$, $i \in I$, $r \in R$. Posebno je, za neko $y\ (\in R)$ i neko $i_0 \in I$, $1 = i_0 + xy$, tj. $1 - xy = i_0 \in I$.

Neka je sada ispunjen uslov iz tačke ($f$) i neka je ideal $\mathbf{I}$ strogo sadržan u idealu $\mathbf{J}$. Onda postoji neko $x \in J \setminus I$, pa za $y \in R$ i $i \in I$ takve da je $1 - xy = i \in I$ imamo $1 = xy + i \in J$, stoga i $\mathbf{J} = \mathbf{R}$.

($g$) Neka je integralni domen $\mathbf{R}$ polje i neka je $\mathbf{I}$ njegov nenula ideal. Ako $0 \neq a \in I$, onda i $1 = a^{-1} \cdot a \in I$, pa je, prema tački ($b$), $\mathbf{I} = \mathbf{R}$.

Ako je pak $\mathbf{R}$ integralni domen bez netrivijalnih ideala i $a \neq 0$, tada je $a\mathbf{R}$ nenula ideal; stoga je $a\mathbf{R} = \mathbf{R}$, te je, za neko $r \in R$, $ra = 1$. Dakle, svaki nenula element je inverzibilan i $\mathbf{R}$ je polje.□

**Napomena.** Ideal generisan jednoelementnim skupom zove se *glavni ideal* (eng. *principal ideal*). Prsten čiji su svi ideali glavni zove se *prsten glavnih ideala.*

**Lema 19.7** *Neka je* $\mathbf{R} = \langle R, +, \cdot\rangle$ *prsten (s jedinicom, integralni domen) i* $\mathbf{I}$ *njegov pravi ideal. Ako na skupu koseta faktor grupe* $\langle R, +\rangle/\langle I, +\rangle = \{a + I \mid a \in R\}$ *definišimo operacije* $+$ *i* $\cdot$ *(praksa je da se ne menjaju oznake) sa:*

$$(a + I) + (b + I) \stackrel{\text{def}}{=} (a + b) + I,$$

$$(a + I) \cdot (b + I) \stackrel{\text{def}}{=} (ab) + I,$$

*opet dobijamo prsten (s jedinicom, integralni domen), tzv. faktor prsten prstena* $\mathbf{R}$ *po idealu* $\mathbf{I}$*, u oznaci* $\mathbf{R/I}$.

*Homomorfno preslikavanje* $\varphi : R \longrightarrow R/I$ *dato sa* $(a)\varphi = a + I$ *kanoničko je (ili prirodno) homomorfno preslikavanje pstena* $\mathbf{R}$ *na faktor prsten* $\mathbf{R/I}$.

**Dokaz.** Lako se proverava da su definicije korektne, tj. da ne zavise od izbora predstavnika koseta. Tako npr. ako je $a + I = a_1 + I$, $b + I = b_1 + I$, onda je, za neke elemente $i, j$ ideala $\mathbf{I}$, $a = a_1 + i$, $b = b_1 + j$, pa je $ab - a_1b_1 = ib_1 + a_1j + ij \in I$, odnosno $(ab) + I = (a_1b_1) + I$. Ostalo se jednako lako dokazuje. Recimo još samo da smo uslov da je $\mathbf{I}$ pravi ideal uveli samo zbog očuvanja jedinice ($1 + I$ je jedinica faktor prstena $\mathbf{R/I}$; za $\mathbf{I} = \mathbf{R}$ faktor prsten $\mathbf{R/I}$ je nula prsten – prsten sa samo jednim elementom).□

**Teorema 19.8** *Neka je* $\mathbf{R}$ *prsten i* $\mathbf{I}$ *njegov pravi ideal. Tada postoji uzajamno jednoznačna korespondencija između svih ideala prstena* $\overline{\mathbf{R}} = \mathbf{R/I}$ *i svih ideala prstena* $\mathbf{R}$ *koji sadrže* $\mathbf{I}$*, takva da ako su* $\overline{\mathbf{J}} \lhd \overline{\mathbf{R}}$ *i* $(\mathbf{I} \leq)\ \mathbf{J} \lhd \mathbf{R}$ *korespondentni ideali, onda su faktor prsteni* $\overline{\mathbf{R}}/\overline{\mathbf{J}}$ *i* $\mathbf{R/I}$ *izomorfni.*

**Dokaz.** Korespondencija je data sa $\overline{\mathbf{J}} \longleftrightarrow (\overline{\mathbf{J}})\varphi^{-1}$, $\overline{\mathbf{J}} \lhd \overline{\mathbf{R}}$, gde je $\varphi$ kanoničko homomorfno preslikavanje prstena $\mathbf{R}$ na faktor prsten $\overline{\mathbf{R}}$. Trivijalna je provera



da je $(\overline{J})\varphi^{-1} \stackrel{\text{def}}{=} \{a \in R \mid (a)\varphi \in \overline{J}\}$ domen ideala ($\mathbf{J}$) koji sadrži ideal $\mathbf{I}$, a preslikavanje $\psi : R/J \longrightarrow \overline{R}/\overline{J}$ dato sa $(a + J)\psi = (a)\varphi + \overline{J}\ (= (a + I) + \overline{J})$ izomorfno je preslikavanje prstena $\mathbf{R/J} = \mathbf{R}/(\overline{\mathbf{J}})\varphi^{-1}$ na prsten $\overline{\mathbf{R}}/\overline{\mathbf{J}}$. Ova teorema se direktno "oslanja" na 8.7, te je i dokaz u mnogome kopija dokaza teoreme 8.7.■

**Korolar 19.9** *Neka je* $\mathbf{R}$ *integralni domen i* $\mathbf{I}$ *njegov ideal. Tada važi: faktor prsten* $\mathbf{R/I}$ *je polje akko je* $\mathbf{I}$ *maksimalan ideal.*

**Dokaz.** Direktna posledica prethodne teoreme i tačke ($g$) leme 19.6.□

**Lema 19.10** *Neka je* $\mathbf{F}$ *polje i* $\mathbf{F}[x] = \langle\{f(x) \mid f(x)$ *– polinom s koeficijentima iz* $F\}, +, \cdot\rangle$ *($+$ i $\cdot$ su "standardne" operacije sabiranja i množenja polinoma). Tada je* $\mathbf{F}[x]$ *integralni domen čiji je skup inverzibilnih elemenata* $F \setminus \{0\}$.

**Dokaz.** Trivijalan.□

**Lema 19.11** *Neka je* $\mathbf{F}$ *potpolje polja* $\mathbf{K}$*, tj. neka je* $\mathbf{K}$ *proširenje (ekstenzija) polja* $\mathbf{F}$*; piše se* $\mathbf{K/F}$ *(ne mešati sa istom oznakom za faktor prstene) ili* $\mathbf{F} \leq \mathbf{K}$*. Tada je* $\langle K, +\rangle$ *vektorski prostor nad poljem* $\mathbf{F}$.

**Dokaz.** Očigledan.□

**Definicija 19.12** *Neka je* $\mathbf{F}$ *potpolje polja* $\mathbf{K}$*. Dimenzija vektorskog prostora* $\langle K, +\rangle$ *nad poljem* $\mathbf{F}$ *je stepen proširenja (ekstenzije) polja* $\mathbf{K}$ *nad poljem* $\mathbf{F}$*, u oznaci* $[\mathbf{K} : \mathbf{F}]$*. Ako je* $[\mathbf{K} : \mathbf{F}] < \infty$*,* $\mathbf{K}$ *je konačna ekstenzija polja* $\mathbf{F}$*, u suprotnom je beskonačna.*

**Lema 19.13** *Neka je* $\mathbf{L}$ *ekstenzija polja* $\mathbf{K}$*, a* $\mathbf{K}$ *ekstenzija polja* $\mathbf{F}$*. Tada važi:*

$$[\mathbf{L} : \mathbf{F}] = [\mathbf{L} : \mathbf{K}] \cdot [\mathbf{K} : \mathbf{F}].$$

*Posebno, konačna ekstenzija konačne ekstenzije je konačna ekstenzija.*

**Dokaz.** Neka je $\{c_j \mid j \in J\}$ baza vektorskog prostora $\langle L, +\rangle$ nad poljem $\mathbf{K}$ i $\{b_i \mid i \in I\}$ baza vektorskog prostora $\langle K, +\rangle$ nad poljem $\mathbf{F}$. Direktno se proverava da je $\{b_ic_j \mid i \in I,\ j \in J\}$ baza vektorskog prostora $\langle L, +\rangle$ nad poljem $\mathbf{F}$.□

**Lema 19.14** *Neka je* $\psi$ *homomorfno preslikavanje prstena* $\mathbf{R}$ *u (na) prsten* $\mathbf{S}$*. Tada je* $\overline{\psi} : R[x] \longrightarrow S[y]$*, gde je, za* $p(x) = a_nx^n + \cdots + a_1x + a_0 \in R[x]$*,* $(p(x))\overline{\psi} = (a_n)\psi y^n + \cdots + (a_1)\psi y + (a_0)\psi$*, homomorfno preslikavanje prstena* $\mathbf{R}[x]$ *u (na) prsten* $\mathbf{S}[y]$.

**Dokaz**. Jednostavna provera.□

**Definicija 19.15** *Neka je* **F** *potpolje polja* **K**. *Element* $a \in K$ *je algebarski nad poljem* **F** *akko postoji nenula polinom* $f(x) \in F[x]$ *čija je nula* $a$ $(f(a) = 0)$, *u suprotnom je transcedentan nad* **F**. *Ako su svi elementi polja* **K** *algebarski nad* **F**, *onda je* **K** *algebarsko proširenje polja* **F**.

*Ako je* $a$ *algebarski nad* **F**, *jedinstveni normirani polinom (koeficijent uz najviši stepen od* $x$ *je jedinica) najnižeg stepena iz* $F[x]$ *čija je nula* $a$ *zove se minimalni polinom elementa* $a$ *s obzirom na* **F**.

**Lema 19.16** *Neka je* **F** *potpolje polja* **K**. *Onda važi:*

*(a) Ako je* **K** *konačna ekstenzija polja* **F**, *onda je i algebarska;*

*(b) Ako je* $b \in K$ *algebarski element nad poljem* **F**, *tada je minimalni polinom elementa* $b$, $p(x) \in F[x]$ *(s obzirom na* **F***) nesvodljiv ili ireducibilan polinom (tj. polinom pozitivnog stepena koji se ne može predstaviti kao proizvod dva polinoma pozitivnog stepena), deljiv sa* $x - b$ *u prstenu* $K[x]$ *i koji deli svaki drugi polinom* $q(x)$ *iz* $F[x]$ *čija je jedna nula* $b$.

**Dokaz**. *(a)* Neka je $[\mathbf{K} : \mathbf{F}] = n$ $(\in N)$ i neka je $b \in K$. Tada su vektori $1 = b^0, b, \ldots, b^n$ linearno zavisni vektori vektorskog prostora $\langle K, + \rangle$ nad poljem **F** (ima ih više od $n$), pa je, za neke elemente $a_0, a_1, \ldots, a_n$ iz $F$, koji nisu svi jednaki nuli: $a_0 + a_1 b + \cdots + a_n b^n = 0$, tj. $b$ je nula (nenula) polinoma $a_n x^n + \cdots + a_1 x + a_0 \in F[x]$.

Napomenimo još da obrat ovog tvrđenja ne važi; algebarska ekstenzija nije nužno i konačna.

*(b)* Iz srednje škole nam je poznato da za svaka dva polinoma $f(x), g(x) \in F[x]$, gde je $g(x) \neq 0$ (i **F** ma kakvo polje), postoje polinomi $u(x), v(x) \in F[x]$ takvi da je $f(x) = u(x)g(x) + v(x)$ i $v(x)$ je ili nula polinom ili polinom nižeg stepena od $g(x)$. Drugim rečima, $\mathbf{F}[x]$ je Euklidov domen, a stoga i domen glavnih ideala, dakle i Gausov prsten. Prema tome, na raspolaganju su nam Euklidov algoritam za iznalaženje najvećeg zajedničkog delioca (najveće zajedničke mere) i mogućnost rastavljanja polinoma na proizvod nesvodljivih faktora, jednoznačnog do na raspored faktora i množenje konstantama (elementima polja **F**).

Ako bismo pretpostavili da je $p(x) = q(x)r(x)$, gde su $q(x)$ i $r(x)$ (iz $F[x]$) polinomi pozitivnog stepena, onda bi bilo (u polju **K**): $0 = p(b) = q(b)r(b)$, i kako je polje bez delioca nule, to bi bilo ili $q(b) = 0$ ili $r(b) = 0$, kontradikcija (polinomi $q(x)$ i $r(x)$ su, po pretpostavci, nižeg stepena od $p(x)$). Ostalo sledi prema uvodnom delu.

Konstatujmo uzgred: polinom nad datim poljem ima u tom polju najviše onoliko nula koliki je njegov stepen.□

**Lema 19.17** *Konačna podgrupa multiplikativne grupe ma kog polja je ciklična.*



**Dokaz**. Neka je **G** podgrupa reda $n$ $(\in N)$ multiplikativne grupe $\langle F \setminus \{0\}, \cdot \rangle$ polja **F** i neka je $a \in G$ element takav da je $n \geq m = red(a) = max\{red(g) \mid g \in G\}$ (jasno, $a$ ne mora biti jedinstveno). Tada red svakog elementa iz **G** deli red elementa $a$. Zaista, pretpostavimo suprotno. Neka je, za neki prost broj $p$ i neki element $b \in G$, $m = p^\alpha k$, $red(b) = p^\beta l$, $(k, p) = (l, p) = 1$ i $\beta > \alpha$ $(\geq 0)$. Onda je $red(a^{p^\alpha}) = k$, $red(b^l) = p^\beta$, te je $red(a^{p^\alpha} \cdot b^l) = p^\beta k > m$, kontradikcija. Proizilazi da je, za svako $c \in G$, $c^m = 1$, dakle jednačina $x^m - 1 = 0$ ima (barem) $n$ rešenja. Stoga $n \leq m$ i, zapravo, $m = n$.□

**Teorema 19.18** *(Teorema Kroneckera (Leopold Kronecker,* 1823-1891)). Neka je **F** polje i $p(x) \in F[x]$ nesvodljiv polinom (nad $\mathbf{F}[x]$). Tada postoji proširenje (ekstenzija) **K** polja **F** u kome polinom $p(x)$ ima (bar) jednu nulu.

**Dokaz**. Neka je $\mathbf{I} = \langle p(x) \rangle = p(x)\mathbf{F}[x]$. Jasno, **I** je pravi ideal – njegov domen je skup polinoma iz $F[x]$ deljivih sa $p(x)$, pa npr. $1 \notin I$. Radi se, zapravo, o maksimalnom idealu. Jer, ako je $g(x) \in F[x]$ polinom koji nije deljiv sa $p(x)$, onda je, prema Euklidovom algoritmu, za neke polinome $u(x), v(x) \in F[x]$, $u(x)p(x) + v(x)g(x) = 1$ (polinomi $p(x)$ i $g(x)$ su uzajamno prosti pošto je $p(x)$ nesvodljiv polinom), dakle, $1 - v(x)g(x) = u(x)p(x) \in I$ i **I** je maksimalan ideal (19.6($f$)). Prema 19.9, faktor prsten $\mathbf{F}[x]/\mathbf{I}$ je polje koje sadrži izomorfnu kopiju polja **F** (preslikavanje $\varphi : F \longrightarrow F[x]/I$ dato sa $(a)\varphi = a + I$ utapanje je polja **F** u polje $\mathbf{F}[x]/\mathbf{I}$). Ako je $p(x) = a_n x^n + \cdots + a_1 x + a_0$, njegova "slika" u $(\mathbf{F}[x]/\mathbf{I})[y]$ je $(a_n + I)y^n + \cdots + (a_1 + I)y + (a_0 + I)$, a jedna nula ovog polinoma je, evidentno, $x + I$. Uočimo da je $[\mathbf{F}[x]/\mathbf{I} : (\mathbf{F})\varphi] = deg(p(x))$ – stepen polinoma $p(x)$.■

**Korolar 19.19** *Neka je* **K** *ekstenzija polja* **F** *i neka je* $b \in K$ *algebarski nad* **F**. *Ako je* $p(x) \in F[x]$ *minimalni polinom elementa* $b$, *onda je minimalni potprsten polja* **K** *(s obzirom na inkluziju) čiji domen sadrži* $F \cup \{b\}$ – $\mathbf{F}[b] = \langle \{q(b) \mid q(x) \in F[x]\}, +, \cdot \rangle$ – *polje izomorfnu polju* $\mathbf{F}[x]/\langle p(x) \rangle$.

**Dokaz**. Preslikavanje $\psi : F[b] \longrightarrow F[x]/\langle p(x) \rangle$ dato sa $(q(b))\psi = q(x) + \langle p(x) \rangle$ izomorfno je preslikavanje prstena $\mathbf{F}[b]$ na polje $\mathbf{F}[x]/\langle p(x) \rangle$; na primer, ako je $q(b) = r(b)$, $q(x), r(x) \in F[x]$, onda $p(x)$ deli $q(x) - r(x)$ i zato $q(x) + \langle p(x) \rangle = r(x) + \langle p(x) \rangle$ (ostalo se jednako lako proverava).

S obzirom da je $\mathbf{F}[b]$ polje piše se i $\mathbf{F}(b)$ (obratiti pažnju na drugu vrstu zagrada).□

**Napomena**. Ako je $b \in K$ transcedentan nad **F**, onda je $\mathbf{F}[b]$ prsten izomorfan prstenu polinoma nad poljem **F** ($\mathbf{F}[b] \cong \mathbf{F}[x]$), a domen polja $\mathbf{F}(b)$, minimalnog međupolja (polja između **F** i **K**), koje sadrži $F \cup \{b\}$, je $\{u(b)/v(b) \mid u(x), v(x) \in F[x],\ v(x) \neq 0\}$.

**Korolar 19.20** *Neka je* $\mathbf{K}$ *ekstenzija polja* $\mathbf{F}$ *i neka je* $B$ *skup elemenata iz* $\mathbf{K}$ *algebarskih nad* $\mathbf{F}$. *Tada je* $\mathbf{F}[B] = \langle \{q(b_{i_1}, \ldots, b_{i_n}) \mid q(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n],\ b_{i_j} \in B\}, +, \cdot \rangle$ *(minimalni potprsten polja* $\mathbf{K}$ *čiji domen sadrži* $F \cup B$*) polje, u oznaci* $\mathbf{F}(B)$.

**Dokaz.** Ako je $B$ konačan skup, dokaz je indukcijom po njegovoj kardinalnosti. Ako je $|B| = 1$ u pitanju je prethodni korolar. Pretpostavimo da je tvrđenje tačno za svaki skup algebarskih elemenata kardinalnosti manje od $n\ (> 1)$ i neka je $|B| = n$, recimo $B = \{b_1, \ldots, b_n\}$. No tada: $\mathbf{F}[b_1, \ldots, b_{n-1}, b_n] = (\mathbf{F}[b_1, \ldots, b_{n-1}])[b_n] = (\mathbf{F}(b_1, \ldots, b_{n-1}))[b_n]$ (po induktivnoj pretpostavci) $= (\mathbf{F}(b_1, \ldots, b_{n-1}))(b_n)$ (prema prethodnom korolaru) $= \mathbf{F}(b_1, \ldots, b_{n-1}, b_n)$.

Neka je sada $B$ beskonačan skup i neka $0 \neq c \in F[B]$. Kako je, za neki konačan podskup $B_1$ od $B$, $c \in F[B_1] = F(B_1)$, to je $c^{-1} \in F[B_1]\ (\subseteq F[B])$.

Primetimo na kraju da je, prema 19.13 i 19.19, za konačan skup algebarskih elemenata $B$, polje $\mathbf{F}[B] = \mathbf{F}(B)$ konačne ekstenzije nad $\mathbf{F}$.□

**Lema 19.21** *Ako je* $\mathbf{L}$ *algebarska ekstenzija polja* $\mathbf{K}$, *a* $\mathbf{K}$ *algebarska ekstenzija polja* $\mathbf{F}$, *onda je* $\mathbf{L}$ *algebarska ekstenzija i polja* $\mathbf{F}$ *(sažeto: algebarska ekstenzija algebarske ekstenzije je algebarska ekstenzija).*

**Dokaz.** Neka je $b_n x^n + \cdots + b_1 x + b_0 \in K[x]$ minimalni polinom elementa $c \in L$ (nad $\mathbf{K}$). No onda je $c$ algebarski i nad poljem $\mathbf{F}(b_0, \ldots, b_n)$, pa je, prema prethodnom korolaru i 19.16$(a)$, $(\mathbf{F}(b_0, \ldots, b_n))[c] = \mathbf{F}(b_0, \ldots, b_n, c)$ algebarska ekstenzija polja $\mathbf{F}$, posebno, $c$ je algebarski element nad $\mathbf{F}$.□

**Korolar 19.22** *Neka je* $f(x)$ *polinom nad poljem* $\mathbf{F}$. *Tada postoji algebarsko proširenje polja* $\mathbf{F}$ *koje sadrži sve nule polinoma* $f(x)$.

**Dokaz.** Neka je $f(x) = p_1(x) \cdot \ldots \cdot p_m(x)$, $m \geq 1$, gde je $p_i(x)$, $i = 1, \ldots, m$, nesvodljivi polinom. Prema Kroneckerovoj teoremi postoji algebarska ekstenzija polja $\mathbf{F}$, neka je to $\mathbf{F}_1$, u kojoj polinom $p_1(x)$ ima (bar) jednu nulu – neka je to $b$. Polinom $p_1(x)$, a onda i $f(x)$, deljiv je sa $x - b$ (u $\mathbf{F}_1[x]$). Ako su sve ostale nule polinoma $f(x)$ u $\mathbf{F}_1$ stajemo – posao je gotov. Ako nisu, onda polinom $\frac{f(x)}{x-b} \in F_1[x]$ rastavljamo na proste faktore i nastavljamo postupak. Očigledno, posle konačno mnogo koraka (ako je $f(x)$ stepena $n$ učinićemo najviše $n - 1$ takvih koraka) stići ćemo do polja, algebarske ekstenzije polaznog polja $\mathbf{F}$, koje sadrži sve nule polinoma $f(x)$, znači polja u kojem se polinom $f(x)$ razlaže na proizvod linearnih faktora.□

**Definicija 19.23** *Polje* $\mathbf{F}$ *je algebarski zatvoreno akko nema pravih algebarskih proširenja.*

**Lema 19.24** *Neka je* $\mathbf{F}$ *polje. Tada su sledeći uslovi ekvivalentni:*

$(a)$ $\mathbf{F}$ *je algebarski zatvoreno polje;*



$(b)$ *svaki polinom* $f(x)$ *iz* $F[x]$ *stepena većeg od* 1 *ima u* $\mathbf{F}$ *bar jednu nulu;*

$(c)$ *svaki nesvodljiv polinom* $p(x)$ *iz* $F[x]$ *je linearan;*

$(d)$ *svaki polinom* $g(x)$ *iz* $F[x]$ *stepena većeg od* 1 *proizvod je linearnih faktora (u* $\mathbf{F}[x]$*).*

**Dokaz.** $(a) \Longrightarrow (b)$ Neka je $\mathbf{F}$ algebarski zatvoreno polje i neka je $f(x) \in F[x]$ polinom stepena većeg od 1. Ako polinom $f(x)$ ne bi imao nijednu nulu u $\mathbf{F}$, onda, naravno, ni njegovi nesvodljivi faktori ne bi imali nula u $\mathbf{F}$; ponavljamo: koristimo, premda to nismo dokazali, da je $\mathbf{F}[x]$ tzv. Gausov prsten i da se prema tome svaki polinom može razložiti na proizvod nesvodljivih (ireducibilnih) polinoma. Neka je $p(x)$, stepena većeg od 1, jedan od njih. Prema Kroneckerovoj teoremi je $\mathbf{F}[x]/\langle p(x) \rangle$ prava algebarska ekstenzija (izomorfne kopije) polja $\mathbf{F}$, kontradikcija.

Implikacije $(b) \Longrightarrow (c) \Longrightarrow (d) \Longrightarrow (d)$ slede trivijalno.□

**Lema 19.25** *Svako polje* $\mathbf{F}$ *se može utopiti u algebarski zatvoreno polje koje je algebarsko proširenje polja* $\mathbf{F}$.

**Dokaz.** Neka je $\{f_\alpha(x) \in F[x] \mid \alpha < \lambda,\ deg((f_\alpha(x)) \geq 1\}$ skup svih nekonstantnih polinoma nad poljem $\mathbf{F}$; uzimamo da je $\lambda$ kardinal (jasno, ako je polje $\mathbf{F}$ beskonačno, onda je $\lambda = |F|$, u suprotnom je $\lambda = \aleph_0$). Definišimo polja $\mathbf{F}_\alpha$, $\alpha < \lambda$, rekurzivno. $\mathbf{F}_0$ je algebarska ekstenzija polja $\mathbf{F}$ u kome se polinom $f_0(x)$ razlaže na proizvod linearnih faktora. Pretpostavimo da su već određena sva polja $\mathbf{F}_\gamma$, $\gamma < \alpha$, koja su algebarska proširenja polja $\mathbf{F}$. Ako je $\alpha = \beta + 1$, onda je $\mathbf{F}_\alpha$ algebarsko proširenje polja $\mathbf{F}_\beta$ koje sadrži sve nule polinoma $f_\alpha(x)$. Ako je $\alpha$ granični ordinal, tada je $\mathbf{F}_\alpha$ algebarska ekstenzija polja $\bigcup_{\gamma<\alpha} \mathbf{F}_\gamma$ koje sadrži sve nule polinoma $f_\alpha(x)$. Konačno, $\mathbf{K} = \bigcup_{\alpha<\lambda} \mathbf{F}_\alpha$ je algebarsko proširenje polja $\mathbf{F}$; evidentno, unija algebarskih proširenja je algebarsko proširenje, a videli smo, svojstvo "biti algebarsko proširenje" je tranzitivno. $\mathbf{K}$ je i algebarski zatvoreno polje. Jer, pretpostavimo da je $\mathbf{L}$ algebarska ekstenzija polja $\mathbf{K}$, dakle i polja $\mathbf{F}$ i neka je $b$ proizvoljni element iz $L$. Kao algebarski element nad $\mathbf{F}$, $b$ je nula nekog polinoma iz $F[x]$, recimo $f_\delta(x)$. Ali tada $b \in F_\delta \subseteq K$; znači $\mathbf{K} = \mathbf{L}$.□

**Napomena.** Pokazuje se da je za dato polje $\mathbf{F}$, algebarski zatvoreno algebarsko proširenje polja $\mathbf{F}$ jedinstveno do na izomorfizam. U osnovi ovog tvrđenja je stav koji kaže: ako je $\mathbf{K}$ algebarsko proširenje polja $\mathbf{F}$ i $\mathbf{L}$ algebarski zatvorena ekstenzija polja $\mathbf{F}$, onda postoji utapanje polja $\mathbf{K}$ u polje $\mathbf{L}$ koje ostavlja sve elemente iz $\mathbf{F}$ fiksnim. Dokaz se bazira na teoremi Kroneckera i lemi Zorna. Ovo nam pak daje za pravo da uvedemo posebno ime za polje $\mathbf{K}$ iz prethodne leme: *algebarsko zatvorenje polja* $\mathbf{F}$, obično u oznaci $\overline{\mathbf{F}}$.

**Korolar 19.26** *Neka je* $\mathbf{F}$ *polje i* $f(x) \in F[x]$ *polinom pozitivnog stepena* $n$. *Tada postoji jedinstveno do na izomorfizam minimalno algebarsko proširenje polja* $\mathbf{F}$ *koje sadrži sve nule polinoma* $f(x)$, *tzv. polje razlaganja polinoma* $f(x)$.

**Dokaz.** Neka je $\mathbf{K}$ ekstenzija polja $\mathbf{F}$ koje sadrži sve nule polinoma $f(x)$, neka su to $b_1, \ldots, b_n$. No tada je $\mathbf{F}[b_1, \ldots, b_n]$ očigledno minimalno međupolje koje sadrži (sve) nule polinoma $f(x)$ (pokazali smo da je to i algebarsko proširenje polja $\mathbf{F}$). Ako su dva takva polja, $\mathbf{K}_1$ i $\mathbf{K}_2$, potpolja istog algebarskog zatvorenja polja $\mathbf{F}$ – $\overline{\mathbf{F}}$, onda su i jednaka, zbog jedinstvenosti razlaganja polinoma $f(x)$ u $\overline{\mathbf{F}}$ na proizvod konstante iz $\mathbf{F}$ i normiranih polinoma prvog stepena. Ako nisu, onda je, za utapanje $\varphi$ polja $\mathbf{K}_1$ u polje $\overline{\mathbf{K}_2}$, koje ostavlja elemente iz $\mathbf{F}$ fiksnim (videti prethodnu napomenu), $\mathbf{K}_1 \cong (\mathbf{K}_1)\varphi = \mathbf{K}_2$.□

**Lema 19.27** (*a*) *U komutativnom prstenu sa jedinicom važi binomna formula; za* $n \geq 1$ *je:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k;$$

(*b*) *U polju* $\mathbf{F}$ *konačne karakteristike* $p$ *važi (za svako* $a, b \in F$ *i svako* $n \geq 0$*):*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

**Dokaz.** (*a*) se dokazuje indukcijom po $n$, a (*b*) je direktna posledica tačke (*a*) (binomni koeficijent $\binom{p^n}{k}$ deljiv je sa $p$ za svako $k \in \{1, \ldots, p^n - 1\}$).□

**Lema 19.28** *Red konačnog polja je broj oblika* $p^n$, *gde je* $p$ *prost broj i* $n$ *pozitivan prirodan broj.*

**Dokaz.** Neka je $\mathbf{F}$ konačno polje čije je minimalno potpolje $\langle Z_p, +_p, \cdot_p \rangle$, koje ćemo za ovu priliku obeležiti, kao i odgovarajuću cikličnu grupa, sa $\mathbf{Z}_p$ ($\mathbf{F}$ je, dakle, karakteristike $p$), i neka je $[\mathbf{F} : \mathbf{Z}_p] = n$. Ako je $\{1, a_1, \ldots, a_{n-1}\}$ baza vektorskog prostora $\langle F, + \rangle$ nad poljem $\mathbf{Z}_p$, onda se svaki element iz $\mathbf{F}$ na jedinstven način predstavlja kao linearna kombinacija:

$$m_0 1 + m_1 a_1 + \cdots + m_{n-1} a_{n-1},$$

gde, za $i = 0, \ldots, n-1$, $m_i \in Z_p$, te je $|F| = \overline{V}_n^p = p^n$ ($\overline{V}_n^p$ – broj varijacija s ponavljanjem od $p$ elemenata $n$-te klase).□

**Lema 19.29** *Neka je, za* $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$, *gde je* $\mathbf{F}$ *polje,* $f'(x) \stackrel{\text{def}}{=} n a_n x^{n-1} + \cdots + a_1 = \sum_{i=1}^{n} i a_i x^{i-1}$. *Tada važi:*



(*a*) $(f(x)+g(x))' = f'(x)+g'(x)$, $(f(x)\cdot g(x))' = f'(x)\cdot g(x) + f(x)\cdot g'(x)$;

(*b*) *Polinom* $f(x) \in F[x]$ *pozitivnog stepena* $n$ *ima samo jednostruke nule (u adekvatnom proširenju polja* $\mathbf{F}$*) akko je* $(f(x), f'(x)) = 1$.

**Dokaz.** (*a*) Trivijalno.

(*b*) Neka je $\mathbf{K}$ polje razlaganja polinoma $f(x)$. Ako $f(x)$ ima nulu $b$ višestrukosti $m > 1$ u $\mathbf{K}$ onda je, u $\mathbf{K}[x]$, $f(x) = (x-b)^m f_1(x)$ (za neki polinom $f_1(x) \in K[x]$), te je, u $\mathbf{K}[x]$, $f'(x) = m(x-b)^{m-1} f_1(x) + (x-b)^m f_1'(x)$ i stoga, opet u $\mathbf{K}[x]$, $(f(x), f'(x)) \neq 1$. No onda $(f(x), f'(x)) \neq 1$ i u $\mathbf{F}[x]$, jer se najveći zajednički delilac dobija Euklidovim algoritmom.

S druge strane, neka je $(f(x), f'(x)) = g(x)$, $deg(g(x)) \geq 1$. U prstenu $\mathbf{K}[x]$ ($\mathbf{K}$ ostaje polje razlaganja polinoma $f(x)$) imamo: $f(x) = a(x-b_1)\cdots(x-b_n)$, gde je $a$ koeficijent uz najviši stepen polinoma $f(x)$, pa je $f'(x) = a\sum_{i=1}^{n}(\prod_{j\neq i}(x-b_j))$. Ako je $b_k$ nula polinoma $g(x)$, dakle i polinoma $f'(x)$, onda je, zbog $\prod_{j\neq k}(b_k - b_j) = 0$, za neko $j$ ($\neq k$), $b_k = b_j$; znači, $f(x)$ ima višestrukih nula.□

**Lema 19.30** *Za svaki prost broj* $p$ *i svaki pozitivan prirodan broj* $n$ *postoji polje reda* $p^n$, *jedinstveno do na izomorfizam.*

**Dokaz.** Neka je $\overline{\mathbf{Z}}_p$ algebarsko zatvorenje polja $\mathbf{Z}_p = \langle p, +_p, \cdot_p \rangle$. Skup nula polinoma $x^{p^n} - x \in Z_p[x]$, a takvih je $p^n$ (jer $(x^{p^n} - x)' = -1$, te su sve nule različite), domen je potpolja $\mathbf{F}$ polja $\overline{\mathbf{Z}}_p$; ako su $a, b$, $a \neq 0$, nule datog polinoma, onda je i: $(a-b)^{p^n} - (a-b) = (a^{p^n} - a) - (b^{p^n} - b) = 0$, $(ab)^{p^n} - (ab) = a^{p^n} b^{p^n} - ab = ab - ab = 0$, $(a^{-1})^{p^n} - a^{-1} = (a^{p^n})^{-1} - a^{-1} = a^{-1} - a^{-1} = 0$. Jasno, $\mathbf{F}$ je polje razlaganja polinoma $x^{p^n} - x$.□

**Napomena.** Konačna polja zovu se i polja Galois, jer ih je ovaj prvi i "otkrio" u okviru svoje čuvene teorije o rešavanju algebarskih jednačina pomoću radikala koju je stvorio sa devetnaest godina. Jedinstveno konačno polje reda $q$ označava se stoga sa $\mathbf{GF}(q)$ ($\mathbf{GF}$ – *Galois field*).

**Lema 19.31** *Neka je* $\mathbf{K}$ *polje sa* $p^n$ *elemenata,* $p$*-prost broj. Tada je svako potpolje polja* $\mathbf{K}$ *reda* $p^m$, *gde je* $m$ *pozitivan delilac broja* $n$ *i za svaki pozitivan delilac* $k$ *broja* $n$ *postoji potpolje polja* $\mathbf{K}$ *reda* $p^k$.

**Dokaz.** Neka je $\mathbf{F}$ potpolje polja $\mathbf{K}$ i neka je $[\mathbf{K} : \mathbf{F}] = l$. Onda je $p^n = |K| = |F|^l$, pa ako je red polja $\mathbf{F}$ recimo $p^m$, imamo $p^n = p^{ml}$ i $m$ deli $n$.

Pretpostavimo sada da je $n = k \cdot r$. Tada je

$$p^n - 1 = (p^k)^r - 1 = (p^k - 1)\cdot((p^k)^{r-1} + (p^k)^{r-2} + \cdots + p^k + 1)$$

i stoga polinom $x^{p^k-1} - 1$ deli polinom $x^{p^n-1} - 1$, a onda i polinom $x^{p^k} - x$ deli $x^{p^n} - x$. Polje $\mathbf{K}$ je polje razlaganja polinoma $x^{p^n} - x$ (štaviše, konstatovali smo, svaki element polja $\mathbf{K}$ je nula ovog polinoma), a skup nula polinoma $x^{p^k} - x$ je domen potpolja reda $p^k$ (polja $\mathbf{K}$).□

**Lema 19.32** *Neka je $p(x) \in F[x]$ nesvodljiv polinom stepena $m$ nad poljem $\mathbf{F}$ konačnog reda $q = p^k$. Tada $p(x)$ deli polinom $x^{q^n} - x$ akko $m$ deli $n$.*

**Dokaz.** Neka $p(x)$ deli $x^{q^n} - x$ i neka je $\mathbf{K}$ polje razlaganja polinoma $x^{q^n} - x$ nad $\mathbf{F}$; $\mathbf{K}$ je, ponavljamo, reda $q^n$. Ako je $a \in K$ nula polinoma $p(x)$, onda je $[\mathbf{F}[a] : \mathbf{F}] = m$ ($\mathbf{F}[a]$ je potpolje reda $q^m$ polja $\mathbf{K}$). Sledi:

$$n = [\mathbf{K} : \mathbf{F}] = [\mathbf{K} : \mathbf{F}[a]] \cdot [\mathbf{F}[a] : \mathbf{F}] = [\mathbf{K} : \mathbf{F}[a]] \cdot m.$$

Ako pak $m$ deli $n$, tada, prema prethodnoj lemi, polje $\mathbf{K}$ ima potpolje $\mathbf{L}$ reda $q^m$ ($mk$ deli $nk$, te postoji potpolje, polja $\mathbf{K}$, reda $p^{mk} = q^m$). Polje $\mathbf{F}[x]/\langle p(x)\rangle$ je reda $q^m$, znači izomorfno sa $\mathbf{L}$. Polje $\mathbf{K}$ sadrži, dakle, bar jednu nulu polinoma $p(x)$, neka je to $b$. Ali $b$ je nula i polinoma $x^{q^n} - x$, te $p(x)$ deli $x^{q^n} - x$ (19.16($b$)).□

**Korolar 19.33** *Neka je $\mathbf{F}$ potpolje reda $q$ polja $\mathbf{K}$ i neka je polinom $p(x) \in F[x]$, stepena $m$, nesvodljiv nad $\mathbf{F}$. Ako je $a \in K$ jedna nula polinoma $p(x)$, onda je $a^{q^m} = a$, a nule polinoma $p(x)$ su: $a$, $a^q$, $a^{q^2}$, ..., $a^{q^{m-1}}$.*

**Dokaz.** $\mathbf{F}[a]$ je potpolje (polja $\mathbf{K}$) reda $q^m$, pa je, za svaki njegov element $b$, $b^{q^m} = b$. Isto tako je, za svaki element $c \in F$, $c^q = c$. Odatle, prema 19.27($b$), sledi: $p(x^{q^i}) = (p(x))^{q^i}$, posebno $p(a^{q^i}) = (p(a))^{q^i} = 0$. Preostaje još da se pokaže da među elementima $a$, $a^q$, ..., $a^{q^{m-1}}$ nema jednakih. Ali to je direktna posledica prethodne leme: $a^{q^i} = a^{q^j}$, za $0 \le j < i \le m-1$, dalo bi: $a^{q^j(q^{i-j}-1)} - 1 = 0$, odnosno $(a^{q^{i-j}-1})^{q^j} = 1$; prema tome, $a^{q^{i-j}} - a = 0$, što će reći da polinom $p(x)$ deli $x^{q^{i-j}} - x$, tj. da $m$ deli $i - j$, kontradikcija.□

Grupa regularnih matrica formata $m \times m$ sa elementima iz polja $\mathbf{F}$ (i s obzirom na matrično množenje) označava se sa $\mathbf{GL}_m(\mathbf{F})$ (videti 2.4($d$), 10.45($e$); koristi se i oznaka $\mathbf{GL}(m, \mathbf{F})$) i zove se *generalna linearna grupa*. Ako je $\mathbf{F}$ konačno polje reda $q$, piše se kratko $\mathbf{GL}_m(q)$ ili $\mathbf{GL}(m, q)$. Prema 10.46 važi (ništa se ne menja u dokazu te leme ako umesto polja sa $p$ elemenata posmatramo, generalno, polje sa $p^n$ elemenata ($n > 1$)):

$$|GL_m(q)| = (q^m - 1) \cdot (q^m - q) \cdot \ldots \cdot (q^m - q^{m-1}) = \prod_{i=0}^{m-1} (q^m - q^i).$$

Već smo videli da je $\mathbf{GF}^*(q) = \langle GF(q) \setminus \{0\}, \cdot\rangle$ ciklična grupa (19.17). Njene generatorne elemente (a ima ih $\varphi(q-1)$, gde je $\varphi$ Eulerova funkcija) zovemo *primitivnim elementima* polja $\mathbf{GF}(q)$. Fiksirajmo jedan – $a$, i neka je

$$M(t) \stackrel{\text{def}}{=} \{A \in GL_m(q) \mid det(A) \text{ je stepen od } a^t\}.$$

Tada važi

**Lema 19.34** *Neka je $t$ delilac broja $q-1$. Tada je $M(t)$ domen normalne podgrupe grupe $\mathbf{GL}_m(q)$ reda $\frac{|GL_m(q)|}{t}$.*



**Dokaz.** Preslikavanje $det : GL_m(q) \longrightarrow GF^*(q)$, gde je, jasno, $(A)det$ determinanta matrice $A$ (koju opet obeležavamo sa $det(A)$), homomorfno je preslikavanje grupe $\mathbf{GL}_m(q)$ na grupu $\mathbf{GF}^*(q)$. Normalna podgrupa $\langle a^t\rangle$ grupe $\mathbf{GF}^*(q)$ ($\mathbf{GF}^*(q)$ je Abelova grupa pa su joj sve podgrupe normalne) reda je $\frac{q-1}{t}$, znači, indeksa $t$, a $(\langle a^t\rangle)det^{-1} = M(t)$. Stoga je $\mathbf{M}(t) = \langle M(t), \cdot\rangle$ normalna podgrupa grupe $\mathbf{GL}_m(q)$ indeksa $t$, odnosno reda $\frac{|GL_m(q)|}{t}$.□

**Korolar 19.35** *Neka je $q - 1 = p_1 \cdot \ldots \cdot p_k$, gde $p_i$, $i = 1, \ldots, k$, nisu nužno različiti prosti brojevi, i neka je $a$ primitivni element polja $\mathbf{GF}(q)$. Tada su faktori invarijantnog lanca (– opadajući lanac normalnih podgrupa – 46.12):*

$$\mathbf{GL}_m(q) = \mathbf{M}(1) > \mathbf{M}(p_1) > \mathbf{M}(p_1p_2) > \cdots > \mathbf{M}(q-1),$$

*tj. faktor grupe $\mathbf{M}(p_1 \cdots p_i)/\mathbf{M}(p_1 \cdots p_{i+1})$, ciklične grupe prostog reda.*

**Dokaz.**

$$|M(p_1 \ldots p_i)/M(p_1 \ldots p_{i+1})| = \frac{|M(p_1 \ldots p_i)|}{M(p_1 \cdots p_{i+1})|} = \frac{\frac{|GL_m(q)|}{p_1 \cdots p_i}}{\frac{|GL_m(q)|}{p_1 \cdots p_{i+1}}} = p_{i+1}.\square$$

**Definicija 19.36** *Normalna podgrupa grupe $\mathbf{GL}_m(\mathbf{F})$ sa domenom*

$$\{A \in GL_m(\mathbf{F}) \mid A \text{ je unimodularna matrica, tj. } det(A) = 1\},$$

*u oznaci $\mathbf{SL}_m(\mathbf{F})$ (koristi se i $\mathbf{SL}(m, \mathbf{F})$), zove se specijalna linearna grupa.*

*Kao i u slučaju generalnih linearnih grupa, ako je $\mathbf{F}$ polje Galois reda $q$, umesto $\mathbf{SL}_m(\mathbf{F})$ pišemo kratko $\mathbf{SL}_m(q)$ ili $\mathbf{SL}(m, q)$.*

Prema oznakama iz prethodnog korolara, $\mathbf{SL}_m(q) = \mathbf{M}(q-1)$ ($M(q-1) = \{A \in GL_m(q) \mid det(A)$ je stepen elementa $a^{q-1}$ ($= 1$), tj. $A$ je unimodularna matrica $\}$), pa je

$$|SL_m(q)| = \frac{|M(p_1 \cdots p_{k-1})|}{p_k} = \frac{|M(p_1 \cdots p_{k-2})|}{p_{k-1}p_k} = \cdots = \frac{|GL_m(q)|}{q-1}.$$

Neka je $I_{ij}$ matrica (formata $m \times m$) čiji su svi elementi 0, osim elementa na $ij$-toj poziciji (presek $i$-te vrste i $j$-te kolone) koji je jedinica. Za $i \neq j$ i $a \in F^*$ ($= F \setminus \{0\}$), matrica $T_{ij}(a) = I + aI_{ij}$ ($I$ je, jasno, jedinična matrica odgovarajućeg formata) je tzv. *transvekcija* (eng. *transvection*). Očigledno, svaka transvekcija je element grupe $\mathbf{SL}_m(\mathbf{F})$.

**Lema 19.37** *Za $A \in GL_m(\mathbf{F})$ važi: $A = B \cdot D(a)$, gde je $B$ proizvod (nekih) transvekcija, a neki element iz $F^*$ i $D(a) = diag[1, \ldots, 1, a]$ (dijagonalna matrica sa naznačenim, po redu, dijagonalnim elementima).*

**Dokaz.** Kako je $A = [a_{ij}]_{1 \leq i,j \leq m}$ regularna matrica, ne mogu svi elementi njene prve kolone biti nula. Neka je npr. $a_{i1} \neq 0$. Dodajemo $i$-tu vrstu pomnoženu sa $a_{i1}^{-1}(1 - a_{11})$ prvoj, pa na poziciji 11 dobijamo jedinicu. Ovo se ostvaruje zapravo množenjem matrice $A$ sleva matricom $T_{1i}(a_{i1}^{-1}(1 - a_{11}))$. Iskoristimo sada prvu vrstu i jedinicu na 11-poziciji da adekvatnim elementarnim transformacijama sve ostale elemente u prvoj koloni "učinimo" nulom. Prelazimo onda na drugu kolonu – pravimo na 22-poziciji jedinicu i sve ostale elemente druge kolone "pretvaramo" u nulu. Ako se nešto pokvarilo u prvoj koloni (recimo, ako smo koristili element na 12-poziciji da napravimo jedinicu na 22-poziciji), tada to, pošto smo "očistili" drugu kolonu, naknadno doterujemo. Postupak se tako nastavlja dok ne dođemo do dijagonalne matrice $D(a)$, za neko $a \in F^*$. Sve transformacije su, rekli smo, izvedene množenjem sleva odgovarajućim transvekcijama, pa ako je $C$ njihov proizvod, imamo: $CA = D(a)$, odnosno $A = C^{-1}D(a)$. No matrica inverzna transvekciji i sama je transvekcija ($T_{ij}(b)^{-1} = T_{ij}(-b)$), te je $B = C^{-1}$ opet proizvod transvekcija.□

**Korolar 19.38** *Grupa* $\mathbf{SL}_m(\mathbf{F})$ *je generisana skupom transvekcija.*

**Dokaz.** Neka $A = BD(a) \in SL_m(\mathbf{F})$, gde je $B$ proizvod nekih transvekcija i $D(a) = diag[1, \ldots, 1, a]$, $a \in F^*$. Kako je $1 = det(A) = det(B) \cdot det(D(a)) = a$, sledi $D(a) = D(1) = I$, dakle $A$ proizvod transvekcija.□

Uočimo da je skup $\{D(a) \mid a \in F^*\}$ domen podgrupe, označimo je sa $\mathbf{D}$, grupe $\mathbf{GL}_m(\mathbf{F})$, izomorfne multiplikativnoj grupi polja $\mathbf{F} - \mathbf{F}^*$. Odatle (i prema prethodnoj lemi) sledi

**Korolar 19.39** *Grupa* $\mathbf{GL}_m(\mathbf{F})$ *je poludirektni proizvod normalne podgrupe* $\mathbf{SL}_m(\mathbf{F})$ *i podgrupe* $\mathbf{D}$ $(\cong \mathbf{F}^*)$.

**Lema 19.40** *Neka je* $\mathbf{H}$ *normalna podgrupa grupe* $\mathbf{SL}_m(\mathbf{F})$ *i neka je matrica* $A$ *iz* $\mathbf{H}$ *slična matrici*

$$C = \begin{bmatrix} c_{11} & \ldots & c_{1,m-1} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ c_{m-1,1} & \ldots & c_{m-1,m-1} & b_{m-1} \\ a_1 & \ldots & a_{m-1} & d \end{bmatrix}.$$

*Tada je, za neko* $u \in F^*$, *i matrica*

$$C_1 = \begin{bmatrix} c_{11} & \ldots & c_{1,m-1} & u^{-1}b_1 \\ \vdots & \ddots & \vdots & \vdots \\ c_{m-1,1} & \ldots & c_{m-1,m-1} & u^{-1}b_{m-1} \\ ua_1 & \ldots & ua_{m-1} & d \end{bmatrix}$$

*u* $\mathbf{H}$.



**Dokaz.** Neka je, za $P$ $(\in GL_m(\mathbf{F}))$, $P^{-1}AP = C$ $(\in H)$ (podsećamo: matrice $K$ i $M$ su slične akko je $Q^{-1}KQ = M$ za neku regularnu matricu $Q$; dve matrice su ekvivalentne akko se mogu elementarnim transformacijama "prevesti" jedna u drugu). Prema prethodnoj lemi je $P = BD(u)$, gde je $B$ proizvod (nekih) transvekcija i $u$ (neki) element iz $F^*$, te iz $C = D(u)^{-1}B^{-1}ABD(u)$ sledi $B^{-1}AB = D(u)CD(u)^{-1} = D(u)CD(u^{-1}) = C_1 \in H$.□

**Lema 19.41** *Centar grupe* $\mathbf{SL}_m(q)$ *je reda* $(m, q-1)$ *(najveći zajednički delilac brojeva* $m$ *i* $q-1$*).*

**Dokaz.** Lako se pokazuje da iz permutabilnosti matrice $A \in GL_m(\mathbf{F})$ sa matricama $T_{ij}(1)$, $i \neq j$, $1 \leq i,j \leq m$, proizilazi da je $A$ skalarna matrica, dakle, za neko $a \in F^*$, $A = aI$, a trivijalno, skalarne matrice su u centru grupe $\mathbf{GL}_m(\mathbf{F})$. Prema tome, $Z(\mathbf{GL}_m(\mathbf{F})) = \{aI \mid a \in F^*\}$. Posebno, $Z(\mathbf{SL}_m(\mathbf{F})) = \{aI \mid a \in F^*, a^m = 1\}$, te je $|Z(\mathbf{SL}_m(q))| = |\{b \in F^* \mid b^m = 1\}|$.

Neka je $a$ primitivni element polja $\mathbf{F} = \mathbf{GF}(q)$ (tj. generatorni element grupe $\mathbf{F}^*$, dakle reda $q-1$). Neka je $(a^t)^m = 1$, odnosno $a^{t \cdot q-1 m} = 1$. Odatle, $tm - [\frac{tm}{q-1}](q-1) = 0$, pa ako je $d = (m, q-1)$ i, recimo, $m = dm_1$, $q-1 = dr$ $((m_1, r) = 1)$, onda je $tdm_1 - [\frac{tdm_1}{dr}]dr = 0$ i, dalje, $tm_1 - [\frac{tm_1}{r}]r = 0$, te $r$ deli $t$. Stoga je, za neko $s$, $0 \leq s < d$, $a^t = (a^{\frac{q-1}{d}})^s$. S druge strane je, za svako $t$, $0 \leq t < d$:

$$(a^{\frac{q-1}{d}t})^m = (a^{rt})^m = (a^{rd})^{tm_1} = (a^{q-1})^{t\acute{m}_1} = 1.$$

Zaključujemo: $\{b \in F^* \mid b^m = 1\} = \{a^{\frac{q-1}{d}t} \mid 0 \leq t < d\}$.□

**Definicija 19.42** *Projektivna unimodularna grupa je faktor grupa*

$$\mathbf{SL}_m(\mathbf{F})/\mathbf{Z}(\mathbf{SL}_m(\mathbf{F})).$$

*Označava se sa* $\mathbf{PSL}_m(\mathbf{F})$ *(ili* $\mathbf{PSL}(m, \mathbf{F})$*), odnosno, ako je* $\mathbf{F}$ *konačno polje reda* $q$*, kraće sa* $\mathbf{PSL}_m(q)$ *(*$\mathbf{PSL}(m, q)$*).*

**Korolar 19.43** *Grupa* $\mathbf{PSL}_m(q)$ *je reda* $\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{m-1})}{(m,q-1)\cdot(q-1)}$.

**Dokaz.** Prema komentaru uz definiciju 19.36 i prethodnoj lemi imamo:

$$|PSL_m(q)| = \frac{|SL_m(q)|}{|Z(\mathbf{SL}_m(q))|} = \frac{\frac{|GL_m(q)|}{(q-1)}}{(m, q-1)} =$$

$$\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{m-1})}{(m,q-1)\cdot(q-1)} = \frac{\prod_{i=0}^{m-1}(q^m-q^i)}{(m,q-1)\cdot(q-1)}.$$□

**Lema 19.44** *Ako normalna podgrupa* $\mathbf{H}$ *grupe* $\mathbf{SL}_2(\mathbf{F})$, *gde je* $\mathbf{F}$ *ili konačno polje ili beskonačno polje karakteristike različite od* 2, *sadrži jednu transvekciju, onda je* $\mathbf{H} = \mathbf{SL}_2(\mathbf{F})$.

**Dokaz**. Neka je, za $a \in F^*$, $T_{12}(a) \in H$. Onda je i za svako $b \in F^*$:

$$\begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} b^{-1} & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} 1 & ab^2 \\ 0 & 1 \end{bmatrix} \in H,$$

kao i

$$\begin{bmatrix} 0 & b^{-1} \\ -b & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -b^{-1} \\ b & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -ab^2 & 1 \end{bmatrix} \in H.$$

Pretpostavimo prvo da je $\mathbf{F}$ konačno polje. Preslikavanje $\psi : F^* \longrightarrow F^*$, dato sa $(c)\psi = c^2$, endomorfizam je multiplikativne grupe $\mathbf{F}^*$ (polja $\mathbf{F}$) (2.16). Jasno, $Ker(\psi) = \{c \in F^* \mid c^2 = 1\}$, pa s obzirom da jednačina $x^2 - 1$ ima najviše dve različite nule u polju (tj. jednu, višestrukosti dva, ako je karakteristika polja 2, inače dve), najmanje polovina elemenata iz $F^*$ je kvadrat. Neka je $\Gamma = \{c \in F^* \mid T_{12}(c) \in H\} \cup \{0\}$. $\Gamma$ je domen podgrupe grupe $\langle F, + \rangle$ jer je $T_{12}(c) \cdot T_{12}(d) = T_{12}(c+d)$, $T_{12}(c)^{-1} = T_{12}(-c)$. Pošto $\Gamma$ sadrži sve elemente $ac^2$, $c \in F$, to je $|\Gamma| > \frac{|F|}{2}$, pa je $\Gamma = F$ i sve su transvekcije $T_{12}(a)$, $a \in F^*$, u $\mathbf{H}$. Po istom rezonu su i sve transvekcije $T_{21}(a)$, $a \in F^*$, u $\mathbf{H}$ i (prema 19.38) $\mathbf{H} = \mathbf{SL}_2(\mathbf{F})$.

Ako je $\mathbf{F}$ beskonačno polje karakteristike različite od 2, onda koristimo činjenicu da je svaki element tog polja razlika dva kvadrata:

$$b = (2^{-1}(b+1))^2 - (2^{-1}(b-1))^2$$

(uočimo da su oba kvadrata različita od nule ako je $b \neq \pm 1$). Sada, ako je $T_{12}(a) \in H$, tada su, prema navedenom, za svako $b, c \in F^*$, i matrice $(T_{12}(a))^{-1} = T_{12}(-a)$, $T_{12}(ab^2)$, $T_{12}(-ac^2)$ u $\mathbf{H}$, dakle i matrica $T_{12}(a(b^2 - c^2))$ $(= T_{12}(ab^2) \cdot T_{12}(-ac^2))$, te su ponovo sve transvekcije $T_{12}(a)$, $a \in F^*$, u $\mathbf{H}$. Po simetriji stvari su i transvekcije $T_{21}(a)$, $a \in F^*$, u $\mathbf{H}$.□

**Teorema 19.45** *Ako je polje* $\mathbf{F}$ *konačno, reda većeg od* 3, *ili beskonačno, karakteristike različite od* 2, *onda je grupa* $\mathbf{PSL}_2(\mathbf{F})$ *prosta.*

**Dokaz**. Posmatraćemo konačna polja; dokaz za njih, videće se, odnosi se i na beskonačna polja (karakteristike različite od 2). Neka je $\mathbf{F}$ polje reda $q$. Prema 19.43 je

$$|PSL_2(q)| = \frac{(q^2-1)\cdot(q^2-q)}{(2, q-1)\cdot(q-1)} = \begin{cases} (q+1)\cdot(q^2-q) & q \text{ parno} \\ \frac{1}{2}\cdot(q+1)\cdot(q^2-q) & q \text{ neparno} \end{cases}.$$



Posebno, $|PSL_2(2)| = 6$ i $|PSL_2(3)| = 12$, a znamo da nema prostih grupa reda 6 i 12 (16.53($a$),($b$)). Zapravo važi: $\mathbf{PSL}_2(3) \cong \mathbf{S}_3$, $\mathbf{PSL}_2(3) \cong \mathbf{A}_4$ – videti 18.1. Neka je, stoga, $q > 3$ i neka je $\overline{\mathbf{H}}$ nejedinična normalna podgrupa grupe $\mathbf{PSL}_2(q) = \mathbf{SL}_2(q)/\mathbf{Z}(\mathbf{SL}_2(q))$. Onda je, za neku normalnu podgrupu $\mathbf{H}$ grupe $\mathbf{SL}_2(q)$ koja strogo sadrži centar $\mathbf{Z}(\mathbf{SL}_2(q)) = \mathbf{Z}_0$ (pojednostavljujemo notaciju), $\overline{\mathbf{H}} = \mathbf{H}/\mathbf{Z}_0$. Dokazaćemo da je $\mathbf{H} = \mathbf{SL}_2(q)$. Prema prethodnoj lemi treba nam (samo) jedna transvekcija u $\mathbf{H}$. Uočimo prvo da ako je matrica $A = \begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$, gde je $a \neq \pm 1$ (a tada i $c \neq \pm 1$, jer je $ac = 1$), u $\mathbf{H}$, sledi:

$$[T_{21}(1), A] = T_{21}(-1)A^{-1}T_{21}(1)A = \begin{bmatrix} 1 & 0 \\ a^2 - 1 & 1 \end{bmatrix} \in H,$$

pa je, zbog $a^2 - 1 \neq 0$, $\mathbf{H} = \mathbf{SL}_2(q)$. Problem se, znači, sveo na to da pokažemo da podgrupa $\mathbf{H}$ sadrži ili matricu oblika $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$, gde je $a \neq \pm 1$, ili (nekim drugim putem) jednu transvekciju. Neka je matrica $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ u $H \setminus Z_0$. Prema poznatoj teoriji matričnog računa, matrica $M$ je slična ili dijagonalnoj matrici ili matrici $\begin{bmatrix} a+d & 1 \\ -1 & 0 \end{bmatrix}$ (govorimo o racionalnoj ili drugoj kanoničkoj formi matrice). U prvom slučaju su nule karakterističnog polinoma matrice $M$ ($det(\lambda I - M) = \lambda^2 - (a+d)\lambda + 1$) u polju $\mathbf{F}$ i pošto su to uzajamno inverzni elementi ($det(M) = 1$), a $M$ nije u centru (dakle nije skalarna matrica), različite su, pa su različite i od $\pm 1$. U drugom slučaju karakteristični polinom je nesvodljiv (u $\mathbf{F}[x]$) i matrica $B = \begin{bmatrix} a+d & 1 \\ -1 & 0 \end{bmatrix}$ je njegova tzv. prateća matrica. Prema 19.40 i matrica $\begin{bmatrix} a+d & g^{-1} \\ -g & 0 \end{bmatrix}$ $(g \in F^*)$ je u $\mathbf{H}$, a tada je i, za $C = \begin{bmatrix} h & 0 \\ 0 & h^{-1} \end{bmatrix}$, $h \in F^*$:

$$[C, B] = C^{-1}B^{-1}CB = \begin{bmatrix} h^{-2} & 0 \\ g(a+d)(h^2-1) & h^2 \end{bmatrix} \in H.$$

Pitanje je sada da li imamo na raspolaganju element iz $F^*$ takav da je $h^2 \neq \pm 1$ ($\Longleftrightarrow$ $h^{-2} \neq \pm 1$). Ako je $\mathbf{F}$ karakteristike 2 i $|F| = q \geq 4$, grupa $\mathbf{F}^*$ je neparnog reda (većeg od ili jednakog 3) i kvadrat svakog elementa $h$ iz $F^* \setminus \{1\}$ je različit od 1 ($= -1$). Ako je $\mathbf{F}$ karakteristike $p \neq 2$, možemo odmah pretpostaviti da je trag matrice $M$ (zbir dijagonalnih elemenata – $a+d$), u oznaci $tr(M)$, različit od nule. U suprotnom ($a+d=0$), pošli bismo od matrice $M^2 = \begin{bmatrix} a^2+bc & b(a+d) \\ c(a+d) & bc+d^2 \end{bmatrix} = \begin{bmatrix} a^2+bc & 0 \\ 0 & bc+d^2 \end{bmatrix}$; $tr(M^2) =$

$a^2 + d^2 + 2bc = a^2 + d^2 + 2(ad - 1) = (a + d)^2 - 2 = -2$. Ako je $q > 5$, imamo, naravno, na raspolaganju $h$ za koje je $h^4 \neq 1$, stoga i $h^2 \neq \pm 1$ (ponavljamo se: polinom $x^4 - 1 \in F[x]$ ima najviše četiri različite nule). Ako je $q = 5$, možemo uzeti za $\mathbf{F}$ baš polje $\langle 5, +_5, \cdot_5 \rangle$, te, za $h = 2$, dobijamo matricu $C = \begin{bmatrix} 4 & 0 \\ 3g(a+d) & 4 \end{bmatrix} (\in H)$, a $C^2 = \begin{bmatrix} 1 & 0 \\ 4g(a+d) & 1 \end{bmatrix} = T_{21}(4g(a+d))$.■

**Napomena**. Navedimo bez dokaza i sledeći "amandman" na prethodnu teoremu:

*Grupa* $\mathbf{PSL}_2(\mathbf{F})$ *je prosta za svako beskonačno polje.*

**Primer 19.46** (*a*) $\mathbf{PSL}_2(2) \cong \mathbf{S}_3$, $\mathbf{PSL}_2(3) \cong \mathbf{A}_4$.

**Dokaz**. Postoje samo dve grupe reda 6 (16.53): jedna je ciklična a druga je $\mathbf{S}_3$ ($\cong \mathbf{D}_3$). Očigledno, $\mathbf{PSL}_2(2) \cong \mathbf{SL}_2(2)$ ($Z(\mathbf{SL}_2(2)) = \{I\}$), a $\mathbf{SL}_2(2)$ nije Abelova grupa. Na primer:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

No, $Z_0 = Z(\mathbf{SL}_3(3)) = \{I, 2I\}$, i opet se trivijalno proverava da $\mathbf{PSL}_2(3) = \mathbf{SL}_2(3)/\mathbf{Z}_0$ nije Abelova grupa. Samo jedna neabelova grupa reda 12, baš $\mathbf{A}_4$, nema element reda 6 (videti 18.1). U prethodnoj teoremi smo konstatovali da je svaka matrica $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(3)$ slična ili (regularnoj) dijagonalnoj matrici ili matrici $B = \begin{bmatrix} a+d & 1 \\ -1 & 0 \end{bmatrix}$. Dijagonalne matrice su reda najviše 2 ($1^2 = 2^2 = 1$). Ako je, u drugom slučaju, $a + d = 0$, onda je $B^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = 2I$ (tj. $(BZ_0)^2 = Z_0$). Ako je pak $a + d$ ili 1 ili 2, pokazuje se da je $(BZ_0)^3 = Z_0$.

Primetimo da grupa $\mathbf{SL}_2(3)$ nije izomorfna grupi $\mathbf{S}_4$ ($\mathbf{S}_4$ je grupa bez centra – videti dokaz korolara 9.24).

(*b*) *Grupe* $\mathbf{PSL}_2(4)$ *i* $\mathbf{PSL}_2(5)$ *su izomorfne.*

**Dokaz**. Obe grupe su proste grupe reda 60 (19.43 i prethodna teorema), a znamo da postoji samo jedna takva – 16.53($f$). Prema tome:

$$\mathbf{PSL}_2(4) \cong \mathbf{A}_5 \cong \mathbf{PSL}_2(5).$$

(*c*) *Neka normalna podgrupa* $\mathbf{H}$ *grupe* $\mathbf{SL}_m(\mathbf{F})$ *sadrži matricu* $\begin{bmatrix} A & O \\ O & B \end{bmatrix}$, *obeležimo je sa* $M$, *gde je* $B$ *matrica formata* $k \times k$, $k < m$, *koja nije skalarna. Onda je u* $\mathbf{H}$ *i matrica* $\begin{bmatrix} I_{m-k} & O \\ O & D \end{bmatrix}$ *za neku matricu* $D$ *koja takođe nije skalarna.*



**Dokaz**. Opšta ideja je da pokažemo da je, za neku matricu $L$, $[L^{-1}, M^{-1}] = LML^{-1}M^{-1}$ matrica traženog oblika.

Pretpostavimo prvo da je $B$ dijagonalna matrica $diag[b_1, \ldots, b_k]$. Kako $B$ nije skalarna, možemo pretpostaviti da je $b_1 \neq b_2$ (U suprotnom bismo na poziciju 22 mogli dovesti odgovarajući element razmenom mesta druge vrste i odgovarajuće $i$-te vrste i druge i $i$-te kolone, odnosno množenjem matrice $M$ sleva matricom $K = \begin{bmatrix} I & O \\ O & K_1 \end{bmatrix}$, gde je $K_1$ matrica (formata $k \times k$) nastala od jedinične razmenom mesta druge i $i$-te vrste i množenjem, nakon zamene vrsta, $i$-te vrste sa $-1$, i zdesna matricom $K^{-1} = \begin{bmatrix} I & O \\ O & K_1^{-1} \end{bmatrix}$; jasno, $M_1 = KMK^{-1} = \begin{bmatrix} A & O \\ O & B_1 \end{bmatrix} \in H$ i $B_1 = diag[b_1, b_i, \ldots]$.) Tada je, za matricu

$$L_1 = \begin{bmatrix} I_{m-k} & O & O \\ O & C_1 & O \\ O & O & I_{k-2} \end{bmatrix},$$

gde je $C_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$,

$$[L_1^{-1}, M^{-1}] = L_1 M L_1^{-1} M_{-1} = \begin{bmatrix} I_{m-k} & O & O \\ O & D_1 & O \\ O & O & I_{k-2} \end{bmatrix} \in H,$$

i $D_1 = \begin{bmatrix} 1 & b_2^{-1}(b_2 - b_1) \\ 0 & 1 \end{bmatrix}$.

Ako je $det(A) \neq \pm 1$ i $B$ nije dijagonalna matrica, recimo, za $i \neq j$, $1 \leq i, j \leq k$, $b_{ij} \neq 0$, tada je za matricu

$$L_2 = \begin{bmatrix} A & O \\ O & diag[1, \ldots, det(A)^{-1}, \ldots, 1] \end{bmatrix},$$

gde je $det(A)^{-1}$ na poziciji $jj$ dijagonalne submatrice,

$$[L_2^{-1}, M^{-1}] = \begin{bmatrix} I & O \\ O & D_2 \end{bmatrix} \in H;$$

i $D_2 = diag[1, \ldots, det(A), \ldots, 1] \cdot B \cdot diag[1, \ldots, det(A)^{-1}, \ldots, 1] \cdot B^{-1}$ nije skalarna matrica – lako se proverava da je, za svako $a \in F^*$:

$$diag[1, \ldots, det(A), \ldots, 1] \cdot B \cdot diag[1, \ldots, det(A)^{-1}, \ldots, 1] \neq aB.$$

Ako je $k \geq 3$, ne smeta ako je $det(A) = -1$. Ako je $k = 2$, slučaj je generalno trivijalan (uzimamo za prvi blok matrice $L$ jediničnu matricu $I_{m-k}$, drugi "udešavamo", s tim da bude unimodularna matrica). Ako je $\mathbf{F}$ polje sa svega dva elementa, opet je lako: prvi blok je jedinična matrica, drugi regularna matrica koja nije permutabilna sa $B$ – sada je jedina skalarna matrica jedinična. Ako je $det(A) = 1$, $k \geq 3$ i, za $i \neq j$, $b_{ij} \neq 0$, stavljamo na mesto prvog bloka jediničnu matricu, na mesto drugog dijagonalnu matricu $diag[1, \ldots, a, \ldots, a^{-1}, \ldots, 1]$, gde je $a$ na $ii$-toj poziciji, $a^{-1}$ na $jj$-toj poziciji i $a$ ($\in F^*$) takav element da je $a^3 \neq 1$. Ako takvog elementa nemamo, a to je slučaj samo ako polje $\mathbf{F}$ ima (tačno) četiri elementa (znači karakteristike je 2), razmatramo moguće slučajeve; ako je $b_{ij} \neq 0$ i $b_{ji} = 0$ ($i \neq j$), koristimo za drugi blok istu matricu (sada je dovoljno da je $a^2 \neq 1$); ako je i $b_{ji} \neq 0$, razmatramo podslučajeve: (1) $b_{ij} = b_{ji}$ i (2) $b_{ij} \neq b_{ji}$. U prvom, za drugi blok uzimamo dijagonalnu matricu u kojoj je na poziciji $ii$ (nenula) element $a \neq 1$, na poziciji $kk$, $k \neq i, j$, $a^2$, dok su ostali elementi na dijagonali jedinica; u drugom, drugi blok je matrica nastala od jedinične zamenom mesta $i$-te i $j$-te vrste i množenjem, nakon toga, $i$-te vrste sa $a$ ($\neq 0, 1$) i $k$-te vrste ($k \neq i, j$) sa $a^2$.

(*d*) *Neka je* $\mathbf{F}$ *potpolje polja* $\mathbf{K}$ *i neka* $A \in GL_m(\mathbf{F})$. *Ako je, za neku matricu* $P \in GL_m(\mathbf{K})$, $P^{-1}AP = B$ *(*$B$ *je, generalno, element grupe* $\mathbf{GL}_m(\mathbf{K})$*), onda je, za neki pozitivan prirodan broj* $n$, $A^n$ *skalarna matrica akko je matrica* $B^n$ *skalarna matrica.*

**Dokaz.** Očigledno, skalarna matrica je element centra grupe $\mathbf{GL}_m(\mathbf{K})$. Primetimo da ako je $B^n$ skalarna matrica, onda je $B^n \in GL_m(\mathbf{F})$.□

**Lema 19.47** *Ako za prirodan broj* $m$ *veći od* 2 *i ma kakvo polje* $\mathbf{F}$ *normalna podgrupa* $\mathbf{H}$ *grupe* $\mathbf{SL}_m(\mathbf{F})$ *sadrži jednu transvekciju, onda je* $\mathbf{H} = \mathbf{SL}_m(\mathbf{F})$.

**Dokaz.** Neka je, za $i \neq j$, $1 \leq i, j \leq m$ i $a \in F^*$, $T_{ij}(a) \in H$. Za (indeks) $k$, različit od $i$ i $j$, i $b \in F^*$ imamo:

$$[T_{ij}(a)^{-1}, T_{jk}(b)^{-1}] = T_{ij}(a)T_{jk}(b)T_{ij}(-a)T_{jk}(-b) =$$

$$(I + aI_{ij}) \cdot (I + bI_{jk}) \cdot (I - aI_{ij}) \cdot (I - bI_{jk}) =$$

$$(I + aI_{ij} + bI_{jk} + abI_{ik}) \cdot (I - aI_{ij} - bI_{jk} + abI_{ik}) =$$

$$I + aI_{ij} + bI_{jk} + abI_{ik} - aI_{ij} - bI_{jk} - abI_{ik} + abI_{ik} =$$

$$I + abI_{ik} = T_{ik}(ab) \in H;$$

koristili smo:

$$I_{rs} \cdot I_{uv} = \begin{cases} O & s \neq u \\ I_{rv} & s = u \end{cases}$$



($O$ – nula matrica). Prema tome, za $k \neq j$, $\mathbf{H}$ sadrži sve transvekcije $T_{ik}(c)$, $c \in F^*$ (s obzirom da je $b$ bio proizvoljan element grupe $\mathbf{F}^*$). Slično:

$$[T_{ki}(b)^{-1}, T_{ij}(a)^{-1}] = T_{ki}(b)T_{ij}(a)T_{ki}(-b)T_{ij}(-a) = T_{kj}(ab) \in H,$$

pa $\mathbf{H}$ sadrži i sve transvekcije $T_{kj}(c)$, $k \neq i$, $c \in F^*$, odnosno, sumiramo li, sve transvekcije, osim možda transvekcije $T_{ij}(c)$ za $c \neq a$. Ali onda bismo, analogno, transvekciju $T_{ij}(c)$ (za $c \neq a$) dobili polazeći od transvekcije $T_{ik}(d)$, $k \neq j$, $d$ proizvoljan element iz $F^*$.□

**Lema 19.48** *Ako je za* $m$ *veće od* 2 *i ma kakvo polje* $\mathbf{F}$ *grupa* $\mathbf{PSL}_m(\mathbf{F})$ *prosta i* $\mathbf{H}$ *normalna podgrupa grupe* $\mathbf{SL}_m(\mathbf{F})$ *koja sadrži matricu koja nije skalarna, onda je* $\mathbf{H} = \mathbf{SL}_m(\mathbf{F})$.

**Dokaz.** Naravno, nije interesantan slučaj kada je $\mathbf{Z}_0 = \mathbf{Z}(\mathbf{SL}_m(\mathbf{F})) \leq \mathbf{H}$ (onda je $\overline{\mathbf{H}} = \mathbf{H}/\mathbf{Z}_0$ nejedinična normalna podgrupa grupe $\mathbf{PSL}_m(\mathbf{F})$, dakle, $\overline{\mathbf{H}} = \mathbf{PSL}_m(\mathbf{F})$ i $\mathbf{H} = \mathbf{SL}_m(\mathbf{F})$). Tretiramo stoga opšti slučaj ($\mathbf{Z}_0 \not\leq \mathbf{H}$). Treba nam, kao što smo videli, jedna transvekcija u $\mathbf{H}$. Prema uslovu leme i 8.7, $\mathbf{Z}_0$ je maksimalna normalna podgrupa grupe $\mathbf{SL}_m(\mathbf{F})$, pa je $\mathbf{Z}_0\mathbf{H} = \mathbf{SL}_m(\mathbf{F})$. Stoga je za dato $a \in F^*$, za neko $b \in F^*$ za koje je $b^m = 1$ i za neku matricu $A \in H$: $bI \cdot A = T_{12}(a)$, tj.

$$A = b^{-1}I \cdot T_{12}(a) = \begin{bmatrix} b^{-1} & b^{-1}a & \ldots & 0 \\ 0 & b^{-1} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & b^{-1} \end{bmatrix}.$$

Ako je $\mathbf{F}$ polje sa svega dva elementa, $A$ je transvekcija i mi smo gotovi. Ako je $|F| > 2$, nastavljamo razmatranje. $A^{-1}$ je matrica

$$\begin{bmatrix} b & -ab & 0 & \ldots & 0 \\ 0 & b & 0 & \ldots & 0 \\ 0 & 0 & b & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & b \end{bmatrix}.$$

($A^{-1}$ se najlakše nalazi ako $A$ posmatramo kao blok matricu $\begin{bmatrix} C & O \\ O & D \end{bmatrix}$, gde je $C = \begin{bmatrix} b^{-1} & b^{-1}a \\ 0 & b^{-1} \end{bmatrix}$ i $D = b^{-1}I_{m-2}$; $I_{m-2}$ je jedinična matrica formata $(m-2) \times (m-2)$). Neka je element $c$ iz $F^*$ takav da je $-ab + c \neq 0$. Matrice $\begin{bmatrix} b & -ab \\ 0 & b \end{bmatrix}$ i $\begin{bmatrix} b & -ab + c \\ 0 & b \end{bmatrix}$ su slične. (U proveri ovoga uputno je pozvati se

na stav: *kvadratne matrice istog formata $K$ i $M$, nad datim poljem* $\mathbf{F}$, *slične su akko su matrice* $\lambda I - K$ *i* $\lambda I - M$ *ekvivalentne.*) Ali tada su i matrice $A^{-1}$ i

$$B = \begin{bmatrix} b & -ab+c & 0 & \dots & 0 \\ 0 & b & 0 & \dots & 0 \\ 0 & 0 & b & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & b \end{bmatrix}$$

slične. Koristimo: ako su $C$ i $C_1$, kao i $D$ i $D_1$, parovi sličnih matrica, tada su i matrice $\begin{bmatrix} C & O \\ O & D \end{bmatrix}$ i $\begin{bmatrix} C_1 & O \\ O & D_1 \end{bmatrix}$ slične. Ovde samo moramo voditi računa da je matrica $M$, za koju je $B = M^{-1}A^{-1}M$, unimodularna; no kako je drugi blok matrica $A^{-1}$ i $B$ ista skalarna matrica – $bI_{m-2}$, ako je $M_1$ matrica za koju je $M_1^{-1}\begin{bmatrix} b & -ab \\ 0 & b \end{bmatrix} M_1 = \begin{bmatrix} b & -ab+c \\ 0 & b \end{bmatrix}$, možemo za $M$ uzeti matricu

$$\begin{bmatrix} M_1 & O \\ O & diag[1,\dots,1,(det(M_1))^{-1}] \end{bmatrix}.$$

Konačno, $AB$ $(\in H)$ je transvekcija $T_{12}(b^{-1}c)$.□

**Teorema 19.49** *Grupa* $\mathbf{PSL}_m(\mathbf{F})$ *je prosta za svako* $m$ *veće od* 2 *i svako polje* $\mathbf{F}$.

**Dokaz.** Indukcijom po $m$ $(\geq 3)$.

Neka je $m = 3$, $\mathbf{H}$ normalna podgrupa grupe $\mathbf{SL}_3(\mathbf{F})$ koja strogo sadrži centar $\mathbf{Z}_0 = \mathbf{Z}(\mathbf{SL}_3(\mathbf{F}))$ (dakle, $\overline{\mathbf{H}} = \mathbf{H}/\mathbf{Z}_0$ je nejedinična normalna podgrupa grupe $\mathbf{PSL}_3(\mathbf{F})$) i neka je $A \in H \setminus Z_0$. Racionalna kanonička forma matrice $A$ (koja je, kao matrica slična matrici $A$, takođe u $\mathbf{H}$) je ili

(I) dijagonalna matrica:

$$A_1 = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix},$$

gde je npr. $ab^{-1} \neq 1$ (jer $A$ nije skalarna matrica),
ili

(II) matrica oblika:

$$A_2 = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 0 \\ 0 & 0 & c \end{bmatrix},$$

ili



(III) matrica oblika:

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \\ c & 0 & 0 \end{bmatrix},$$

odnosno matrica oblika:

$$A_3 = \begin{bmatrix} 0 & 0 & c \\ 1 & 0 & b \\ 0 & 1 & a \end{bmatrix}.$$

Razmotrimo svaki od ovih slučajeva. Jasno, ideja je da se pokaže da $\mathbf{H}$ sadrži jednu transvekciju.

(I)

$$[T_{12}(1)^{-1}, A_1^{-1}] = T_{12}(1)A_1T_{12}(-1)A_1^{-1} =$$

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a^{-1} & 0 & 0 \\ 0 & b^{-1} & 0 \\ 0 & 0 & c^{-1} \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 1-ab^{-1} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = T_{12}(1-ab^{-1}) \in H.$$

(II)

$$M = [T_{23}(1)^{-1}, A_2^{-1}] = T_{23}(1)A_2T_{23}(-1)A_2^{-1} =$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & 1 & 0 \\ b & 0 & 0 \\ 0 & 0 & c \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & b^{-1} & 0 \\ 1 & -ab^{-1} & 0 \\ 0 & 0 & c^{-1} \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 0 & -c^{-1} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = T_{13}(c^{-1}).$$

Matrica $M$ nije skalarna ($T_{23}(1)A_2T_{23}(-1) \neq cA$ za svako $c \in F^*$), a njen karakteristični polinom – $det(\lambda I - M)$ – je $(\lambda - 1)^3$. Direktno proveravamo da je $M^2 = 2M - I$, tj. $(M - I)^2 = O$, što će reći da je $(\lambda - 1)^2$ minimalni polinom matrice $M$. Stoga su elementarni delitelji matrice $M$: $\lambda - 1$, $(\lambda - 1)^2$, i njena racionalna kanonička forma je

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = B_{12}(1)\,(\in H).$$

(III) Sada su karakteristični i minimalni polinom matrice $A$ isti – u pitanju je nesvodljivi polinom (nad poljem $\mathbf{F}$) trećeg stepena $x^3 - ax^2 - bx - c$, gde je

$c = det(A) = 1$; znači:

$$A_3 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & b \\ 0 & 1 & a \end{bmatrix}.$$

Onda je:

$$D = [A_3, T_{21}(1)] = A_3^{-1}T_{21}(-1)A_3T_{21}(1) =$$

$$\begin{bmatrix} -b & 1 & 0 \\ -a & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & b \\ 0 & 1 & a \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 0 & -1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} (\in H),$$

i

$$[T_{21}(1)^{-1}, D^{-1}] = T_{21}(1)DT_{21}(-1)D^{-1} =$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & -1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 \\ -1 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} = T_{23}(-1) \in H.$$

Pretpostavimo dalje da je grupa $\mathbf{PSL}_k(\mathbf{F})$ prosta za svako polje $\mathbf{F}$ i svako $k < m\ (> 3)$. Neka je opet $\mathbf{H}$ normalna podgrupa grupe $\mathbf{SL}_m(\mathbf{F})$ koja strogo sadrži centar, koji opet označavamo sa $\mathbf{Z_0}$, i neka je opet $A \in H \setminus Z_0$. Recimo da je racionalna kanonička forma matrice $A$ matrica

$$B = \begin{bmatrix} A_1 & O & \dots & O \\ O & A_2 & \dots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \dots & A_r \end{bmatrix},$$

gde su $A_1, \dots, A_r$ kvadratne (sub)matrice, ne nužno istog formata (tzv. hiperprateće matrice elementarnih delitelja matrice $A$); uzimamo da je $m_i \times m_i$ format matrice $A_i$ $(i = 1, \dots, r)$.

Ako je $r \geq 2$, prema 19.46$(c)$ $\mathbf{H}$ sadrži i matricu $\begin{bmatrix} I_{m-m_r} & O \\ O & D \end{bmatrix}$, gde $D$ (formata $m_r \times m_r$) nije skalarna matrica. Pretpostavićemo da je $m_r \geq 3$ (u suprotnom – $m_r = 2$, posmatrali bismo blok $\begin{bmatrix} 1 & O \\ O & D \end{bmatrix}$). Podgrupa $\mathbf{G}$ grupe



$\mathbf{SL}_m(\mathbf{F})$ sa domenom $\{\begin{bmatrix} I_{m-m_r} & O \\ O & M \end{bmatrix} \mid M \in SL_{m_r}(\mathbf{F})\}$ izomorfna je (po induktivnoj pretpostavci) prostoj grupi $\mathbf{SL}_{m_r}(\mathbf{F})$. Kako je $\mathbf{H} \cap \mathbf{G} \lhd \mathbf{G}$ i $I \neq \begin{bmatrix} I_{m-m_r} & O \\ O & D \end{bmatrix} \in H \cap G$, sledi $\mathbf{G} \cap \mathbf{H} = \mathbf{G}$, odnosno $\mathbf{G} \leq \mathbf{H}$; odatle, $\mathbf{H}$ sadrži transvekciju i stoga je $\mathbf{H} = \mathbf{SL}_m(\mathbf{F})$ (19.47).

Ako je $r = 1$, karakteristični polinom matrice $A - \lambda^m - a'_{m-1}\lambda^{m-1} - a'_{m-2}\lambda^{m-2} - \dots - a'_1\lambda - a'_0$ – je nesvodljiv. Znamo da je $-a'_0 = (-1)^m det(A) = (-1)^m$, tj. $a'_0 = (-1)^{m+1}$. Racionalna kanonička forma matrice $A$ je

$$B = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & a'_0 \\ 1 & 0 & 0 & \dots & 0 & a'_1 \\ 0 & 1 & 0 & \dots & 0 & a'_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & a'_{m-2} \\ 0 & 0 & 0 & \dots & 1 & a'_{m-1} \end{bmatrix},$$

pa je u $\mathbf{H}$ i "adaptirana" matrica (matrica slična, u $\mathbf{SL}_m(\mathbf{F})$, racionalnoj kanoničkoj formi matrice $A$):

$$A_1 = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & a_1 \\ 0 & 1 & 0 & \dots & 0 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & a_{m-2} \\ 0 & 0 & 0 & \dots & (-1)^{m+1} & a_{m-1} \end{bmatrix}.$$

Izbor matrice $A_1$ nije jedinstven (zato se i nismo opredeljivali za elemente $a_1$, $\dots$, $a_{m-1}$); jedan je, recimo:

$$diag[1, (-1)^{m+1}, 1, \dots, 1, (-1)^{m+1}] \cdot B \cdot diag[1, (-1)^{m+1}, 1, \dots, 1, (-1)^{m+1}]$$

(osnovna namera da na poziciju $1m$ dobijemo jedinicu time je ispunjena).

Ako je $\{\alpha_1, \dots, \alpha_m\}$ baza vektorskog prostora $\mathbf{F}^m$ nad poljem $\mathbf{F}$, onda je za odgovarajuću transformaciju $A_1$:

$A_1(\alpha_1) = \alpha_2$
$A_1(\alpha_2) = \alpha_3$
$\vdots$
$A_1(\alpha_{m-1}) = (-1)^{m-1}\alpha_m$
$A_1(\alpha_m) = \alpha_1 + a_1\alpha_2 + \dots + a_{m-2}\alpha_{m-1} + a_{m-1}\alpha_m.$

Odatle je:

$A_1^{-1}(\alpha_2) = \alpha_1$
$A_1^{-1}(\alpha_3) = \alpha_2$

$$\vdots$$

$A_1^{-1}(\alpha_m) = (-1)^{m-1}\alpha_{m-1}$

$A_1^{-1}(\alpha_1) = -a_1\alpha_1 - a_2\alpha_2 - \cdots - a_{m-2}\alpha_{m-2} - (-1)^{m-1}\alpha_{m-1} + \alpha_m,$

te je:

$$A_1^{-1} = \begin{bmatrix} -a_1 & 1 & 0 & \dots & 0 & 0 \\ -a_2 & 0 & 1 & \dots & 0 & 0 \\ -a_3 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (-1)^m a_{m-1} & 0 & 0 & \dots & 0 & (-1)^{m-1} \\ 1 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}.$$

Sada je $[T_{21}(1)^{-1}, A_1^{-1}] = T_{21}(1)A_1T_{21}(-1)A_1^{-1} = \begin{bmatrix} D & O \\ O & I_{m-3} \end{bmatrix}$, gde je $D = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ a_1 & -1 & 1 \end{bmatrix}$. Umesto direktnog množenja, mišljenja smo, jednostavnije je ispitati slike vektora baze. Tako je npr.

$$T_{21}(1)A_1T_{21}(-1)A_1^{-1}\begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{bmatrix} = T_{21}(1)A_1T_{21}(-1)\begin{bmatrix} -a_1 \\ -a_2 \\ -a_3 \\ \vdots \\ -a_{m-2} \\ (-1)^m a_{m-1} \\ 1 \end{bmatrix} =$$

$$T_{21}(1)A_1\begin{bmatrix} -a_1 \\ a_1 - a_2 \\ -a_3 \\ \vdots \\ -a_{m-3} \\ -a_{m-2} \\ (-1)^m a_{m-1} \end{bmatrix} = T_{21}(1)\begin{bmatrix} 1 \\ 0 \\ a_1 \\ \vdots \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ a_1 \\ \vdots \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Po analogiji sa prethodnim slučajem koristimo ovog puta podgrupu $\mathbf{K}$ grupe $\mathbf{SL}_m(\mathbf{F})$ sa domenom $\{\begin{bmatrix} M & O \\ O & I \end{bmatrix} \mid M \in SL_3(\mathbf{F})\}$, izomorfnu prostoj grupi $\mathbf{SL}_3(\mathbf{F})$. Opet, $\mathbf{H} \cap \mathbf{K} \lhd \mathbf{K}$ i $I \neq [T_{21}(1)^{-1}, A_1^{-1}] \in H \cap K$, pa je $\mathbf{K} \leq \mathbf{H}$ i (ponovo zbog 19.47) $\mathbf{H} = \mathbf{SL}_m(\mathbf{F})$.■

**Lema 19.50** *Postoje proste grupe istog konačnog reda koje nisu izomorfne.*



**Dokaz.** Kao (kontra)primer poslužiće nam grupe $\mathbf{A}_8$ i $\mathbf{PSL}_3(4)$ reda 20.160 ($= \frac{8!}{2} = \frac{(4^3-1)\cdot(4^3-4)\cdot(4^3-4^2)}{(3,3)\cdot(4-1)}$). Grupa $\mathbf{A}_8$ ima elemenata reda 15; jedan takav je permutacija $(0\ 1\ 2)\cdot(3\ 4\ 5\ 6\ 7)$. Pokazaćemo da u grupi $\mathbf{PSL}_3(\mathbf{F})$, $|F| = 4$, nema elemenata reda 15. Neka je $AZ_0 \in PSL_3(\mathbf{F})$, gde je $A \in SL_3(\mathbf{F})$ i $\mathbf{Z}_0 = \mathbf{Z}(\mathbf{SL}_3(\mathbf{F}))$, i neka je $p(x) = det(xI - A)$ karakteristični polinom matrice $A$. Prema 19.26 postoji minimalna ekstenzija $\mathbf{K}$ polja $\mathbf{F}$ koja sadrži sve nule polinoma $p(x)$ (polje razlaganja polinoma $p(x)$). Ako je $A_1$ racionalna kanonička forma matrice $A$ nad poljem $\mathbf{K}$ i $\mathbf{Z}_1 = \mathbf{Z}(\mathbf{SL}_3(\mathbf{K}))$, onda su, prema 19.46($c$), elementi $AZ_0$ i $A_1Z_1 \in PSL_3(\mathbf{K})$ istog reda (jer je matrica $A_1$ slična matrici $A$). U zavisnosti od nula polinoma $p(x)$, matrica $A_1$ je jednog od oblika:

(I)

$$\begin{bmatrix} a & 0 & 0 \\ 1 & a & 0 \\ 0 & 1 & a \end{bmatrix},$$

kada $p(x)$ ima samo jednu nulu – $a$, višestrukosti tri;

(II)

$$\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 1 & b \end{bmatrix},$$

kada $p(x)$ ima jednu dvostruku nulu – $b$;

(III)

$$\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix},$$

kada su nule polinoma $p(x)$ različite.

Ako bi bilo $(AZ_0)^{15} = Z_0$ (smatramo, jasno: $A \notin Z_0$), tj. ako bi $A^{15}$ bila skalarna matrica $aI$ za neko $a \in F^*$, sledilo bi $A^{45} = I$ (pošto je svakako $a^3 = 1$), a onda i $A_1^{45} = I$. No ako je $A_1$ bilo oblika (I) bilo oblika (II) to, gotovo očigledno, nije tačno. Indukcijom se, naime, pokazuje da je

$$\begin{bmatrix} a & 0 & 0 \\ 1 & a & 0 \\ 0 & 1 & a \end{bmatrix}^n = \begin{bmatrix} a^n & 0 & 0 \\ na^{n-1} & a^n & 0 \\ s(n)a^{n-2} & na^{n-1} & a^n \end{bmatrix},$$

gde je $s(1) = 0$ i, za $n > 1$, $s(n) = \binom{n}{2}$, kao i

$$\begin{bmatrix} b & 0 \\ 1 & b \end{bmatrix}^n = \begin{bmatrix} b^n & 0 \\ nb^{n-1} & b^n \end{bmatrix}.$$

Ako je pak $A_1$ matrica oblika (III), može se desiti da je $(A_1Z_1)^{15} = Z_1$ ali, svejedno, onda će red elementa $A_1Z_1$ biti 5. Dokažimo i to.

Pretpostavimo prvo da je polinom $p(x)$ nesvodljiv nad $\mathbf{F}$. Ako je $a$ (jedna) nula ovog polinoma u $\mathbf{K}$, onda su, prema 19.33, preostale dve $a^4$ i $a^{16}$. Kako je $|F[a]| = 4^3 = 64$ (jer, $[\mathbf{F}[a] : \mathbf{F}] = 3$), to je $a^{63} = 1$. S druge strane, iz $(diag[a, a^4, a^{16}])^{45} = I$, sledi $a^{45} = 1$, te je $red(a) = 9$ (dobili smo $a^{18} = 1$, a parni delioci broja 18 i 3 su isključeni; parni delioci ne dele 45, tri ne dolazi u obzir pošto je $a$ nula nesvodljivog polinoma trećeg stepena nad $\mathbf{F}$). Ali tada je $(diag[a, a^4, a^{16}])^9 = I$.

Ako je polinom $p(x)$ razloživ u proizvod linearnih faktora u $\mathbf{F}[x]$ (odnosno ako su mu sve nule u $\mathbf{F}$), onda, trivijalno, $(diag[a, b, c])^3 = I$.

Preostaje slučaj: $p(x)$ ima samo jednu nulu u $\mathbf{F}$, recimo $a$; znači, $p(x) = (x - a) \cdot q(x)$, gde je $q(x) \in F[x]$ nesvodljiv nad $\mathbf{F}$. Ako je $b$ nula polinoma $q(x)$ u $\mathbf{K}$, druga je, ponovo prema 19.33, $b^4$. Sada je $\mathbf{K} = \mathbf{F}[b]$ i $|K| = 4^2 = 16$; drugim rečima, $\mathbf{K}$ je polje razlaganja i polinoma $x^{16} - x = x(x^{15} - 1)$. Neka je $d$ generatorni element (multiplikativne) grupe $\mathbf{K}^*$ (polja $\mathbf{K}$), tj. jedan od primitivnih petnaestih korena iz jedinice (videti 19.17) i neka je $b = d^m$. Nenula elementi polja $\mathbf{F}$ su 1 $(= d^0)$, $d^5$, $d^{10}$ i bez obzira koji od njih je $a$, važi: $(diag[a, b, b^4])^5 \in Z(\mathbf{SL}_3(\mathbf{K}))$ (štaviše, $(diag[a, b, b^4])^5 \in Z(\mathbf{SL}_3(\mathbf{F}))$), pa je $red(A_1Z_1) = 5$. Jer, neka je na primer $a = d^{10}$. Pošto je $diag[a, b, b^4]$ unimodularna matrica, imamo $a \cdot b^5 = d^{10} \cdot d^{5m} = d^{10+15m} = 1$ i dalje (posle množenja sa $d^5$) $d^{5m} = d^5$. Odatle, $(diag[a, b, b^4])^5 = (diag[ad^{10}, d^m, d^{4m}])^5 = diag[d^5, d^5, d^5] = d^5I = a^2I$ (očigledno, $(d^{4m})^5 = d^{4\cdot 15 5\cdot 15 m} d^{5\cdot 15 m} = d^5$).□

## 20 Grupe Hamiltona

Hamiltonove grupe spadaju u one familije grupa, danas već sve brojnije, koje su potpuno okarakterisane. Uostalom tu je

**Teorema 20.1** *Grupa je grupa Hamiltona akko je direktni proizvod jedne grupe kvaterniona sa Abelovom grupom čiji su elementi neparnog reda i Abelovom grupom čiji su elementi reda najviše 2.*

**Dokaz.** Primetimo odmah da dozvoljavamo datom formulacijom da su obe pomenute Abelove grupe ili pak samo jedna od njih jedinična grupa.

($\Longrightarrow$) Neka je $\mathbf{G}$ Hamiltonova grupa. Kako je neabelova, postoje elementi $a$ i $b$ koji nisu permutabilni. Nejedinični element $c = [a, b] = a^{-1}b^{-1}ab$ je u preseku cikličnih grupa $\mathbf{A} = \langle a \rangle$ i $\mathbf{B} = \langle b \rangle$ jer su one, kao uostalom i sve druge podgrupe, normalne, a pošto su i Abelove, $c$ je i element centra podgrupe $\mathbf{D} = \langle a, b \rangle$ (jasno, $\mathbf{A} \cap \mathbf{B} \leq \mathbf{Z}(\mathbf{D})$). Proizilazi da je $\mathbf{D}'$ ciklična grupa generisana elementom $c$. Trivijalno, $\langle c \rangle \subseteq D'$. S druge strane, $\mathbf{D}/\mathbf{A}$ i $\mathbf{D}/\mathbf{B}$ su Abelove grupe (uočimo da su npr. elementi grupe $\mathbf{D}/\mathbf{A}$ oblika $b^\beta A$, $\beta \in Z$), pa je $\mathbf{D}' \leq \mathbf{A} \cap \mathbf{B} \leq \mathbf{Z}(\mathbf{D})$, a tada sledi, imajući u vidu 6.3, da je svaki



element podgrupe $\mathbf{D}'$ stepen elementa $c$. Ako je $c = a^r = b^s$, $r, s \neq 0$, prema istom korolaru je $c^r = [a, b]^r = [a^r, b] = e$, te su elementi $a$ i $b$ konačnog reda. S obzirom da u njihovom izboru nije bilo nikakvih ograničenja, zaključujemo generalno da uzajamno nepermutabilni elementi moraju biti konačnog reda. Učinićemo sada jedan "poseban" izbor.

Neka je $a_1$ jedan element van centra grupe najmanjeg reda, recimo $m$ (naravno, taj izbor ne mora biti jedinstven), i neka je $b_1$ jedan element van $C(a_1)$ najmanjeg reda, neka to bude $n$. Ako je $p$ prost faktor broja $m$, po učinjenom izboru je $a_1^p \in Z(\mathbf{G})$, a onda i $c_1^p = [a_1, b_1]^p = [a_1^p, b_1] = e$ (stavili smo $c_1 = [a_1, b_1]$). Analogno, za bilo koji prost faktor $q$ broja $n$ je $c_1^q = e$ (zbog $b_1^q \in C(a)$). Stoga su redovi elemenata $a_1$ i $b_1$ stepeni većeg od 1 istog prostog broja (ako bismo imali npr. $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $k \geq 2$, sledilo bi: $c_1^{p_1} = c_1^{p_2} = e$, a zbog $(p_1, p_2) = 1$ i $c_1 = e$, kontradikcija; slično bismo rezonovali i u slučaju pretpostavke da $m$ i $n$ imaju neke različite proste faktore; isključeno je i da je upravo $m = p$ ili $n = p$, jer je $(e \neq) c_1$ stepen elemenata $a_1$ i $b_1$, a $\mathbf{C}_1 = \langle c_1 \rangle$ je prava podgrupa grupa $\mathbf{A}_1 = \langle a_1 \rangle$ i $\mathbf{B}_1 = \langle b_1 \rangle$. Neka je $m = p^k$, $n = p^l$, $k, l \geq 2$. Pošto je $c_1 \in A_1$ i $C_1 \subset A_1$, $c_1$ je oblika $a_1^{up^{k-1}}$ za neki (ceo) broj $u$ uzajamno prost sa $p$. Prema Euklidovoj teoremi je, za neke cele brojeve $v$, $v_1$, $uv + v_1 p = 1$ (naravno, i $(v, p) = 1$), a odatle je $c_1^v = a_1^{uvp^{k-1}} = a_1^{(1-v_1 p)p^{k-1}} = a_1^{p^{k-1}}$. Iz istih razloga dobijamo i $c_1^w = b_1^{p^{l-1}}$ za neki ceo broj $w$ uzajamno prost sa $p$. Ako je $a_2 = a_1^w$, $b_2 = b_1^v$ i $c_2 = [a_2, b_2]$ imamo:

$$a_2^{p^{k-1}} = b_2^{p^{l-1}} = c_1^{vw} = [a_1, b_1]^{vw} = [a_1^w, b_1^v] = [a_2, b_2] = c_2 \qquad (I)$$

i $\langle a_1 \rangle = \langle a_2 \rangle$, $\langle b_1 \rangle = \langle b_2 \rangle$, $\langle c_1 \rangle = \langle c_2 \rangle = Q' = \langle a_1, b_1 \rangle' = \langle a_2, b_2 \rangle'$. Ostaje, razumljivo, s obzirom na izbor elemenata $a_1$, $b_1$, i $c_2^p = e$. Pretpostavićemo nadalje da je $k \geq l$ $(> 2)$. Ako je $b_3 = a_2^{-p^{k-l}} b_2$, onda je $\mathbf{Q} = \langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle = \langle a_2, b_3 \rangle$, $b_3$ nije permutabilno sa $a_2$, dakle ni sa $a_1$, i stoga je red elementa $b_3$ veći od ili jednak redu elementa $b_2$, koji je pak jednak redu elementa $b_1$ $(p^l)$. Prema 6.3 važi:

$$b_3^{p^{l-1}} = (a_2^{-p^{k-l}} b_2)^{p^{l-1}} = [a_2^{-p^{k-l}}, b_2]^{-\frac{1}{2}p^{l-1}(p^{l-1}-1)} (a_2^{-p^{k-l}})^{p^{l-1}} b_2^{p^{l-1}} = c_2^{p^{k-1}\frac{p^{l-1}-1}{2}} \qquad (II).$$

Iz $(II)$ sledi $p = 2$ i $k = l = 2$. Jer, $p > 2$ bi dalo $b_3^{p^{l-1}} = e$, pošto bi $p$ delilo $p^{k-1}\frac{p^{l-1}-1}{2}$, a $c_2^p = e$. Kada znamo da je $p = 2$, zaključujemo, rezonujući na sličan način, i da mora biti $k = l = 2$. Prema $(I)$ je $a_2^2 = b_2^2 = [a_2, b_2] = c_2$, a već nam je poznato $c_2^2 = e$. Prema tome je $a_2^4 = e$, a odatle se lako izvodi i $b_2 a_2 = a_2^3 b_2$. Grupa $\mathbf{Q} = \langle a_2, b_2 \rangle$ je, dakle, grupa kvaterniona (videti 5.7(a)).

Tvrdimo dalje da je $\mathbf{G} = \mathbf{Q} \cdot \mathbf{C}(\mathbf{Q})$ ($\mathbf{C}(\mathbf{Q})$ - centralizator grupe $\mathbf{Q}$). Zaista, neka je $g \in G$ i pretpostavimo $g \notin Q \cup C(\mathbf{Q})$. Recimo da $g$ nije komutativan sa $a_2$, znači $g^{-1}a_2 g \in \langle a_2 \rangle$ i $g^{-1}a_2 g \neq a_2$. Stoga je $g^{-1}a_2 g = a_2^3 = a_2^{-1}$

(elementi $a_2$ i $g^{-1}a_2g$ su istog reda $-4$), stoga je i $b_2^{-1}g^{-1}a_2gb_2 = b_2^{-1}a_2^3b_2 = a_2$, tj. $a_2 \cdot (gb_2) = (gb_2) \cdot a_2$, pa je $gb_2 \in C(a_2)$. Ako je $gb_2$ komutativan i sa $b_2$, sledi $gb_2 \in C(\mathbf{Q})$ i $g \in Q \cdot C(\mathbf{Q})$ $(= C(\mathbf{Q}) \cdot Q)$. U protivnom, ponavljajući prethodno razmatranje, dobijamo redom:

$$(gb_2)^{-1}b_2(gb_2) = b_2^3 = a_2^2b_2,$$

$$(gb_2a_2)^{-1}b_2(gb_2a_2) = a_2^{-1}a_2^2b_2a_2 = a_2b_2a_2 = b_2,$$

$$b_2 \cdot (gb_2a_2) = (gb_2a_2) \cdot b_2;$$

i zaključujemo: $gb_2a_2 \in C(b_2)$, a onda i $gb_2a_2 \in C(\mathbf{Q})$ (jasno, $gb_2a_2 \in C(a_2)$), i ponovo je $g \in Q \cdot C(\mathbf{Q})$, kontradikcija.

Svi elementi iz $C(\mathbf{Q})$ su konačnog reda, jer ako $(e \neq)\ d \in C(\mathbf{Q})$, onda $b_2d$ ne komutira sa $a_2$ (inače bi i $a_2$ i $b_2$ bili permutabilni), a ranije smo konstatovali da su uzajamno nepermutabilni elementi konačnog reda. U svakom slučaju $d$ ne može biti reda 4 jer bi to dalo $(b_2d)^4 = b_2^4d^4 = e$, a tada, ako je $red(b_2d) = 4$, dobijamo:

$$[b_2d, a_2] = (b_2d)^{-1}(a_2^{-1}b_2da_2) = (b_2d)^{-1}(b_2d)^3 = (b_2d)^2 = b_2^2d^2,$$

ali i

$$[b_2d, a_2] = ((b_2d)^{-1}a_2^{-1}(b_2d)a_2 = ((b_2d)^{-1}a_2(b_2d))^{-1}a_2 = a_2^{-3}a_2 = a_2^2 = b_2^2.$$

Sledilo bi $b_2^2d^2 = b_2^2$, tj. $d^2 = e$, kontradikcija. No red elementa $b_2d$ ne može biti ni 2, jer $a_2^{-1}b_2da_2 \in \langle b_2d\rangle$ (sve su podgrupe normalne), a svaka od relacija $a_2^{-1}b_2da_2 = e$, $a_2^{-1}b_2da_2 = b_2d$ vodi u protivurečnost.

Iz prethodnog proizilazi da $\mathbf{C(Q)}$ ne može sadržati kao podgrupu grupu kvaterniona, a kako su joj sve podgrupe normalne mora biti Abelova (inače bismo na gore opisan način, uz pretpostavku o egzistenciji nepermutabilnih elemenata, našli u njoj jednu grupu kvaterniona). Neka je $\mathbf{N}$ podgrupa grupe $\mathbf{C(Q)}$ generisana elementima neparnog reda (nije isključeno da je $\mathbf{N} = \mathbf{E}$), a $\mathbf{P}_1$ podgrupa generisana elementima reda 2 (jedan takav uvek postoji: $c_2 = [a_2, b_2]$). U $\mathbf{C(Q)}$, videli smo, ne postoji element čiji bi red bio deljiv sa 4, pa ako je red nekog elementa $2p_1^{\alpha_1}\dots p_k^{\alpha_k}$, on se može predstaviti (na jedinstven način) kao proizvod elemenata redova, respektivno, 2 i $p_1^{\alpha_1}\dots p_k^{\alpha_k}$. Ako je $\mathbf{P}$ maksimalna podgrupa grupe $\mathbf{P}_1$ takva da je $\mathbf{P} \cap \langle c_2\rangle = \mathbf{E}$, onda je $\mathbf{P}_1 = \mathbf{P} \times \langle c_2\rangle$, te je, sumiramo: $\mathbf{C(Q)} = \mathbf{N} \times \mathbf{P} \times \langle c_2\rangle$. Kako je $\mathbf{Q} \cap \mathbf{C(Q)} = \langle c_2\rangle$, to je $\mathbf{Q} \cap (\mathbf{N} \times \mathbf{P}) = \mathbf{E}$ i $\mathbf{G} = \mathbf{Q} \cdot \mathbf{C(Q)} = \mathbf{Q} \times \mathbf{N} \times \mathbf{P}$.

($\Longleftarrow$) Pretpostavimo sada da je $\mathbf{G} = \mathbf{Q} \times \mathbf{N} \times \mathbf{P}$, gde je $\mathbf{Q}$ grupa kvaterniona, $\mathbf{N}$ Abelova grupa čiji su svi elementi neparnog reda i $\mathbf{P}$ grupa čiji su elementi, osim jediničnog (ukoliko takvih ima), reda 2 ($\mathbf{P}$ je, prema 2.7($f$), Abelova grupa). $\mathbf{G}$ je, zbog $\mathbf{Q}$, neabelova grupa. Pokazaćemo i da su sve ciklične podgrupe, a samim tim i sve podgrupe, grupe $\mathbf{G}$ normalne. Neka je



$qcd$, gde je $q \in Q$ element reda 4, $c \in N$, $d \in P$, jedan element grupe $\mathbf{G}$. Naravno, dovoljno je samo proveriti $a^{-1}\langle qcd\rangle a = \langle qcd\rangle$ i $b^{-1}\langle qcd\rangle b = \langle qcd\rangle$, gde su $a$ i $b$ generatorni elementi grupe $\mathbf{Q}$ ($a^4 = e$, $a^2 = b^2 = (ab)^2$). Za $a$ imamo:

$$a^{-1}\langle qcd\rangle a = \langle a^{-1}(qcd)a\rangle = \langle a^{-1}qa \cdot cd\rangle = \langle q^rcd\rangle,$$

gde je r ili 1 ili 3. Ali i elementi $qcd$ i $q^3cd$ generišu istu podgrupu. Tako se na primer, ako je red elementa $c$ neparan broj $m$, odmah uočava da sistem jednačina $3x + 4y = 1$, $x + mz = 1$ ima celobrojna rešenja, i ako je $n$ (jedno) rešenje za $x$ (to je, jasno, neparan broj), onda je $(q^3cd)^n = qcd$, te je $\langle qcd\rangle \subseteq \langle q^3cd\rangle$. Slično se dokazuje i obrnuta inkluzija.■

**Korolar 20.2** ($a$) *Osim grupe kvaterniona, svaka Hamiltonova grupa je razloživa.*

($b$) *Direktni proizvod dve (ili više) Hamiltonove grupe nije Hamiltonova grupa.*

($c$) *U Hamiltonovoj grupi su elementi uzajamno prostih redova permutabilni.*

# Glava 2

# Kombinatorna teorija grupa

## 21 Prezentacija grupa

Neka je $A = \{a_i \mid i \in I\}$ neprazan skup takav da $1 \notin A$. Sa $A^{-1}$ obeležićemo skup $\{a_i^{-1} \mid i \in I\}$. Ovde $^{-1}$ nije nikakva unarna operacija. Jednostavno, svakom elementu iz $A$ pridružili smo jedan novi element (shodno tome mogli smo umesto $a_i^{-1}$ koristiti i $b_i$, no iz onoga što sledi biće već jasna prednost prve oznake). Elemente skupova $A$ i $A^{-1}$ posmatramo (isključivo) kao simbole, stoga je $A \cap A^{-1} = \emptyset$. Skup $A \cup A^{-1}$ biće naša azbuka. Reč je svaki konačan niz simbola iz $A \cup A^{-1}$, npr. $a_{i_1} a_{i_2} a_{i_3}^{-1}$ (nije uobičajeno da se između elemenata niza stavlja zarez). Dužina reči je broj elemenata niza (u prethodnom slučaju to je 3). U skup reči je uključena i prazna reč – reč dužine nula; nju ćemo, baš kad bude neophodno, obeležavati sa 1 – do zabune ne može doći jer 1 nije element naše azbuke. Reči ćemo generalno obeležavati sa $u, v, w, \ldots$. Neki put ćemo reč predstaviti i sa npr. $b_1 \ldots b_n$, gde onda podrazumevamo: za svako $j = 1, \ldots, n$, $b_j$ je, za neko $i_j \in I$, ili $a_{i_j}$ ili $a_{i_j}^{-1}$. $l(u)$ će označavati dužinu reči $u$ (tako je $l(1) = 0$). Iz praktičnih razloga koriste se skraćenice: $a_i^n \equiv \underbrace{a_i \ldots a_i}_{n-slova}$; $a_i^{-n} \equiv \underbrace{a_i^{-1} \ldots a_i^{-1}}_{n-slova}$. Tako ćemo umesto $a_i a_i^{-1} a_i^{-1} a_j a_j a_j$ češće pisati $a_i a_i^{-2} a_j^3$ (ostaje, naravno, $l(a_i a_i^{-2} a_j^3) = 6$). Dalje, $a_i^\alpha$, $\alpha \in \{1, -1\}$, biće $a_i$ za $\alpha = 1$ i $a_i^{-1}$ za $\alpha = -1$. Koristićemo i $a^0 \equiv 1$. Ako je $u \equiv a_{i_1}^{\alpha_1} \ldots a_{i_k}^{\alpha_k}$, $u^{-1}$ će označavati reč $a_{i_k}^{-\alpha_k} \ldots a_{i_1}^{-\alpha_1}$; npr. $(a_{i_1} a_{i_2} a_{i_3}^{-1})^{-1}$ je reč $a_{i_3} a_{i_2}^{-1} a_{i_1}^{-1}$ (posebno, $1^{-1} \equiv 1$). Reč $u$ je podreč reči $v$ ako je $v$ oblika $v_1 u v_2$, gde dozvoljavamo da su obe ili samo jedna od reči $v_1$, $v_2$ prazna reč; prazna reč je podreč svake reči.

Neka je $W$ skup svih reči azbuke $A \cup A^{-1}$. Definišimo na tom skupu (binarnu) operaciju (u oznaci, već standardno, $\cdot$) na sledeći način: $u \cdot v = uv$ – jednostavno, "proizvod" dve reči $u$ i $v$ je reč dobijena dopisivanjem reči $v$





zdesna reči $u$ (tj. dopisivanjem reči $u$ sleva reči $v$, stvar gledanja); npr.

$$a_{i_1} a_{i_2} a_{i_2} a_{i_3}^{-1} \cdot a_{i_3} a_{i_1} = a_{i_1} a_{i_2} a_{i_2} a_{i_3}^{-1} a_{i_3} a_{i_1},$$

(nikakvih "skraćivanja"). Naravno, kao i ranije, kad god je to moguće izostavljaćemo znak operacije, pa ćemo jednostavno u takvim slučajevima pisati $uv$ umesto $u \cdot v$.

**Lema 21.1** $\mathbf{W} = \langle W, \cdot \rangle$ *je polugrupa sa jediničnim elementom.*

**Dokaz.** Jasno, prazna reč je jedinični element: $1 \cdot u = u \cdot 1 = u$ (ništa ne dopisujemo reči $u$). Asocijativnost je očigledna.□

Do daljnjega smatraćemo fiksiranom našu azbuku $A \cup A^{-1}$; $W$ je skup reči te azbuke.

Za ma kakvo preslikavanje $\varphi$ skupa $A$ u domen $G$ (proizvoljne) grupe $\mathbf{G}$ definišimo preslikavanje $\overline{\varphi} : W \longrightarrow G$ na sledeći način: ako je $u \equiv a_{i_1}^{\alpha_1} \ldots a_{i_k}^{\alpha_k}$, $\alpha_i \in \{1, -1\}$ (dozvoljavamo mogućnost da je za neko $r, s$, $1 \leq r, s \leq k$, $i_r = i_s$), tada je $(u)\overline{\varphi} \stackrel{\text{def}}{=} ((a_{i_1})\varphi)^{\alpha_1} \ldots ((a_{ik})\varphi)^{\alpha_k}$; tako je npr. $(a_i^{-1})\overline{\varphi} = ((a_i)\varphi)^{-1}$, gde je sada $((a_i)\varphi)^{-1}$ inverzni element elementa $(a_i)\varphi$. Praznu reč $\overline{\varphi}$ preslikava u jedinični element grupe ($(1)\overline{\varphi} = e_G$). Za $\overline{\varphi}$ važi

**Lema 21.2** $\overline{\varphi}$ *je homomorfno preslikavanje polugrupe* $\mathbf{W}$ *u grupu* $\mathbf{G}$ *i* $\overline{\varphi}|_A = \varphi$. $(W)\overline{\varphi}$ *je domen podgrupe grupe* $\mathbf{G}$ *generisane skupom* $(A)\varphi$.

**Dokaz.** Ako je $g = (u)\overline{\varphi} \in (W)\overline{\varphi}$, onda je $g^{-1} = (u^{-1})\overline{\varphi}$. Ostalo se takođe lako proverava.□

U daljem razmatranju pretpostavićemo da su i grupa $\mathbf{G}$ i preslikavanja $\varphi$, $\overline{\varphi}$ fiksna.

Ako je $(u)\overline{\varphi} = g$ kažemo da reč $u$ definiše element $g$ (za preslikavanje $\varphi$). Reči polugrupe $\mathbf{W}$ koje definišu jedinični element (tj. elemente jezgra preslikavanja $\overline{\varphi}$) zovemo *odrednicama* (eng. *relators*). Prazna reč i reči oblika $a_i a_i^{-1}$, $a_i^{-1} a_i$ su tzv. *trivijalne odrednice*.

Na skupu $W$ definišemo relaciju $\sim$ sa: $u \sim v$ ako i samo ako definišu isti element grupe, dakle, ako i samo ako je $(u)\overline{\varphi} = (v)\overline{\varphi}$ ili, što je ekvivalentno, ako i samo ako je $uv^{-1}$ odrednica (često je u upotrebi i $u = v$, no to može da izazove konfuziju – u $\mathbf{W}$ dve reči su jednake akko su identične, tj. akko su isti niz simbola). Prema tome, $u$ je odrednica akko je $u \sim 1$. Očigledno, $\sim$ je relacija kongruencije polugrupe $\mathbf{W}$.

Ako je $(W)\overline{\varphi}$ baš $G$, skup $A$ je skup *izvodnih simbola*.

U daljem pretpostavljamo da je $\overline{\varphi}$ surjektivno preslikavanje. Skup svih odrednica obeležićemo sa $O$.

**Definicija 21.3** *Neka je $P$ podskup skupa $O$. Reč $u$ je određena skupom $P$ (izvediva iz skupa $P$) akko postoji konačan niz reči $u \equiv u_0, u_1, \ldots, u_n \equiv 1$, takav da je za svako $i$, $0 < i \leq n$, $u_i$ dobijeno od $u_{i-1}$ nekom od operacija:*

*(i) umetanjem u $u_{i-1}$ (kao podreč) neke reči iz $P$ ili neke trivijalne odrednice;*

*(ii) brisanjem u $u_{i-1}$ (uz uslov da je to njena podreč) neke reči iz $P$ ili neke trivijalne odrednice.*

*Relacija $u \sim v$ je određena skupom $P$ akko je reč $uv^{-1}$ određena skupom $P$.*

Uočimo odmah da je svaka reč izvediva iz skupa odrednica $P$ i sama odrednica (sve reči u nizu imaju istu homomorfnu sliku – $e_G$). Takođe je svaka reč oblika $uu^{-1}$, $u^{-1}u$ izvediva iz skupa trivijalnih odrednica – u opštem, brisanjem jedne pojavljuje se nova koju opet brišemo i tako redom dok ne dobijemo praznu reč. Isto tako, ako je reč $u$ određena skupom $P$, onda je možemo dobiti od prazne reči konačnom primenom $(i)$ i $(ii)$, jer dat je niz $u \equiv u_0, u_1, \ldots, u_n \equiv 1$, gde je $u_i$ dobijeno od $u_{i-1}$ primenom $(i)$ ili $(ii)$. Sada, u obrnutom redu poteza, startujući od prazne reči, imamo niz $1 \equiv u'_0, u'_1, \ldots, u'_n \equiv u$, gde je $u'_i \equiv u_{n-i}$, pa ako je $u_{n-i+1}$ dobijeno od $u_{n-i}$ umetanjem (brisanjem) reči $v$ (gde je $v$ element iz $P$ ili trivijalna odrednica), onda $u'_i$ nastaje od $u'_{i-1}$ brisanjem (umetanjem) reči $v$.

$(i)$ i $(ii)$ nam dozvoljavaju i umetanje odnosno brisanje reči $v^{-1}$ za $v \in P$. Recimo, želimo da umetnemo reč $v^{-1}$. Tada bismo, korišćenjem trivijalnih odrednica, prvo umetnuli $vv^{-1}$, a onda izbrisali $v$. Ovo ćemo nadalje (bez posebnog naglašavanja) koristiti.

**Napomena.** S obzirom na upravo rečeno, a u cilju izbegavanja razmatranja nekih trivijalnih slučajeva, u daljem tekstu $P$ će uvek biti podskup skupa odrednica, moguće prazan skup (videti 21.8), ili uopšte, skup reči (date azbuke) koji ne sadrži reči oblika $uu^{-1}$, $u^{-1}u$.

**Lema 21.4** *Neka je $P$ skup odrednica. Tada važi:*

*(a) Ako je $u$ izvedivo iz $P$, onda je i $u^{-1}$ izvedivo iz $P$;*

*(b) Ako su reči $uv$ i $w$ izvedive iz $P$, onda je i reč $uwv$ izvediva iz $P$; za $v \equiv 1$ ili $u \equiv 1$ imamo da je proizvod izvedivih reči izvediv;*

*(c) Ako su reči $u_1, u_2, \ldots, u_n$ izvedive iz $P$, onda je i*

$$v_1^{-1}u_1v_1v_2^{-1}u_2v_2 \ldots v_n^{-1}u_nv_n$$

*izvedivo iz $P$, gde su $v_i$, $1 \leq i \leq n$, proizvoljne reči;*

*(d) $u \sim v$ je izvedivo iz $P$ akko se reč $u$ konačnom primenom operacija $(i)$ i $(ii)$ (definicije 21.3) može svesti na (transformisati u) $v$;*



*(e) Ako su relacije $u \sim v$ i $v \sim w$ izvedive iz $P$, onda su i relacije $u \sim w$, $u^{-1} \sim v^{-1}$ izvedive iz $P$;*

*(f) Ako su relacije $u_1 \sim v_1$ i $u_2 \sim v_2$ izvedive iz $P$, tada su i relacije $u_1u_2 \sim v_1v_2$, $w_1u_1w_2 \sim w_1v_1w_2$ (gde su $w_1$, $w_2$ proizvoljne reči) izvedive iz $P$.*

**Dokaz.** $(a)$ S obzirom na gornje primedbe imamo

$$u^{-1}, \ldots, uu^{-1}, \ldots, 1;$$

$(b)$ Polazeći od reči $uwv$ prvo $w$ svedemo na praznu reč; ostaje nam reč $uv$ koja se i sama svodi na praznu reč. Nešto formalnije: neka su nam dati nizovi $w \equiv w_0, \ldots, w_n \equiv 1$ i $uv \equiv z_0, \ldots, z_k \equiv 1$; onda niz

$$uwv,\ uw_1v, \ldots, uw_nv \equiv uv,\ z_1, \ldots, z_k \equiv 1$$

dokazuje određenost reči $uwv$ (skupom $P$);

$(c)$ S obzirom da je $v_i^{-1}v_i$ uvek izvedivo, prema $(b)$ izvedive su i reči $v_i^{-1}u_iv_i$, $i = 1, \ldots, n$, kao i njihov proizvod;

$(d)$ Pravac ($\Longleftarrow$) je jasan; $uv^{-1}$ se svodi na $vv^{-1}$, a ova opet na praznu reč.

Ako je pak $uv^{-1}$ određeno sa $P$, onda (koristeći se trivijalnim odrednicama) prvo od reči $u$ dobijemo $uv^{-1}v$, a potom izbrišemo $uv^{-1}$;

$(e)$ $uw^{-1}, \ldots, uv^{-1}vw^{-1}, \ldots, 1;$
$u^{-1}v, \ldots, u^{-1}uv^{-1}v, \ldots, 1;$

$(f)$ $u_1u_2v_2^{-1}v_1^{-1}$ se redukuje na reč $u_1v_1^{-1}$ (jer se $u_2v_2^{-1}$ svodi na praznu reč), a ova dalje na praznu reč.

Slično je i sa reči $w_1u_1w_2w_2^{-1}v_1^{-1}w_1^{-1}$.□

**Definicija 21.5** *Ako su sve odrednice izvedive iz (skupa odrednica) $P$, onda je $P$ kompletan skup odrednica, a uređen par $(A; P)$ prezentacija (predstavljanje, postavka) grupe $\mathbf{G}$ za preslikavanje $\varphi$ (uslov je, setimo se, da je $\overline{\varphi}$ surjektivno preslikavanje, tj. da je $(A)\varphi$ generatorni skup grupe $\mathbf{G}$).*

*Prezentacija je konačno generisana akko je $A$ (skup izvodnih simbola) konačan skup. Prezentacija je konačno određena akko je skup $P$ konačan. Prezentacija je konačna akko je i konačno generisana i konačno određena.*

Kod konačnih prezentacija obično samo navodimo elemente skupova $A$ i $P$. Tako, ako je $A = \{a, b\}$ i $P = \{a^3, b^2, aba^{-2}b^{-1}\}$, pisaćemo

$$(a, b;\ a^3,\ b^2,\ aba^{-2}b^{-1})$$

(elemente skupova $A$ i $P$ smo razdvojili sa ;). Takođe je uobičajeno da se umesto odrednica pišu relacije. U slučaju datog primera to izgleda ovako:

$$(a, b;\ a^3 \sim 1,\ b^2 \sim 1,\ aba^{-2}b^{-1} \sim 1)$$

ili npr. ovako

$$(a, b;\ a^3 \sim 1,\ b^2 \sim 1,\ ab \sim ba^2).$$

Neki put se kombinuju oba načina:

$$(a, b;\ a^3,\ b^2,\ aba^{-2}b^{-1} \sim 1),\ \ (a, b;\ a^3,\ b^2,\ ab \sim ba^2).$$

Ponovo napominjemo da se češće koristi notacija $u = v$ nego $u \sim v$, no iz razloga koje smo već naveli ostajemo pri "našoj".

**Primer 21.6** *(a) Neka je $\varphi$ bijektivno preslikavanje skupa $A$ na domen $G$ grupe $\mathbf{G}$ i neka je $O$ skup svih odrednica. Tada je $(A; O)$ prezentacija grupe $\mathbf{G}$;*

*(b) Neka je $\varphi$ bijektivno preslikavanje skupa $A = \{a, b, c, \ldots\}$ na domen $G$ grupe $\mathbf{G}$ (uzećemo da je $e_G$ slika elementa $e$; opet $1 \notin A$) i neka je $P = \{abc^{-1} \mid (ab)\overline{\varphi} = (c)\overline{\varphi}\}$. Tada je $(A; P)$ prezentacija grupe $\mathbf{G}$ (za preslikavanje $\varphi$), tzv. prezentacija multiplikativnom tablicom.*

**Dokaz.** Neka je $u$ odrednica. Na nama je da pokažemo da je izvediva iz $P$. Kao prvo eliminisaćemo (ukoliko ih uopšte ima) "negativne eksponente". Pretpostavimo da se $a^{-1}$ javlja u $u$ i da je $(a^{-1})\overline{\varphi} = g \in G$. Zbog surjektivnosti preslikavanja $\varphi$ postoji izvodni simbol (element skupa $A$), neka je to $b$, takav da je $(b)\varphi = g$. Onda je $(ab)\overline{\varphi} = e_G$, pa je $abe^{-1} \in P$, a niz

$$u \equiv va^{-1}w,\ va^{-1}abe^{-1}w,\ va^{-1}abe^{-1}eee^{-1}w,\ vbe^{-1}eee^{-1}w,\ vbee^{-1}w,\ vbw$$

objašnjava kako se $a^{-1}$ zamenjuje sa $b$ (koristili smo i očiglednu činjenicu da je $eee^{-1} \in P$). Dalje, pošto smo zamenili sve elemente iz $A^{-1}$ elementima iz $A$, recimo da je $u_1$ rezultat tog postupka i da je $l(u_1) > 1$, prelazimo na redukciju dužine reči. Neka je $u_1 \equiv cdv_1$ i $cdf^{-1} \in P$. Niz

$$u_1,\ cdf^{-1}fv_1,\ fv_1 \equiv u_2$$

pokazuje kako se reč $u_1$ svodi na reč manje dužine ($l(u_2) = l(u_1) - 1$). Nastavljajući postupak konačno bismo dobili reč dužine 1, preciznije slovo iz $A$. Kako je ona odrednica, s obzirom na injektivnost preslikavanja $\varphi$ to mora biti baš $e$. Nizom $e$, $eee^{-1}$, 1 završavamo svođenje reči $u$ na praznu reč (primenom, isključivo, operacija $(i)$ i $(ii)$ iz definicije 21.3).

Ovaj primer nam kazuje da svaka konačna grupa ima konačnu prezentaciju (što ne znači da nema i drugih).□

Prirodno, postavlja se pitanje kada je $(A; P)$ ($A \neq \emptyset$, $P$ podskup skupa svih reči nad azbukom $A \cup A^{-1}$) prezentacija neke grupe. Sledeća teorema pokazuje da s te strane, u izboru skupova $A$ i $P$, nema nikakvih ograničenja.



**Teorema 21.7** *Neka je dat (skoro) ma kakav neprazan skup $A$ (pretpostavićemo, naime, da $1 \notin A$; u suprotnom bismo morali za praznu reč da uzmemo simbol koji nije u $A$, no navikli smo već da 1 bude njena oznaka) i neka je $W$ skup svih reči nad azbukom $A \cup A^{-1}$ i $P \subseteq W$. Tada postoji jedinstvena (do na izomorfizam) grupa $\mathbf{G}_{(A;P)}$ sa prezentacijom $(A; P)$.*

**Dokaz.** Na skupu $W$ definišimo relaciju $\sim_P$ na sledeći način: $u \sim_P v$ akko postoji konačan niz $u \equiv u_0, u_1, \ldots, u_n \equiv v$ takav da je za svako $i$, $0 < i \leq n$, $u_i$ dobijeno od $u_{i-1}$ primenom jedne od operacija $(i)$ i $(ii)$ iz definicije 21.3.

$\sim_P$ je relacija kongruencije polugrupe $\mathbf{W} = \langle W, \cdot\rangle$; to je već pokazano tačkama $(d)$, $(e)$ i $(f)$ leme 21.4 - $u \sim_P v$ akko je $uv^{-1}$ izvedivo iz $P$ u smislu definicije 21.3. Neka je, za $u \in W$, $[u]$ klasa ekvivalencije (relacije $\sim_P$) određena sa $u$, dakle, $[u] \stackrel{\text{def}}{=} \{v \in W \mid u \sim_P v\}$. Na skupu $G_{(A;P)} = \{[u] \mid u \in W\}$ definišimo operaciju $\circ$ sa: $[u] \circ [v] = [u \cdot v]$ (definicija je korektna, tj. nezavisna od izbora predstavnika klasa ekvivalencija jer je $\sim_P$ relacija kongruencije; naravno, opet ćemo izostavljati znak operacije $\circ$ kada okolnosti to dozvoljavaju). $\mathbf{G}_{(A;P)} = \langle G_{(A;P)}, \circ\rangle$ je polugrupa sa jediničnim elementom $[1]$ (pošto je i $\mathbf{W} = \langle W, \cdot\rangle$ polugrupa sa jediničnim elementom 1) u kojoj su svi elementi inverzibilni: $[u]^{-1} = [u^{-1}]$, prema tome i grupa (u polugrupi $\mathbf{W}$ nijedan element, sem jediničnog, nije bio inverzibilan).

Tvrdimo da je $(A; P)$ prezentacija grupe $\mathbf{G}_{(A;P)}$ za preslikavanje $\varphi$ dato sa $(a)\varphi = [a]$ za $a \in A$ (jasno, $(u)\overline{\varphi} = [u]$ - primetimo samo da je, za $\alpha \in \{1, -1\}$ i $a \in A$, $(a^\alpha)\overline{\varphi} = ((a)\varphi)^\alpha = [a]^\alpha = [a^\alpha]$). Naravno, $(A)\varphi$ generiše grupu $\mathbf{G}$. Dalje, ako je $u \in P$, trivijalno $u \sim_P 1$, pa je $(u)\overline{\varphi} = [u] = [1]$ jedinični element grupe $\mathbf{G}_{(A;P)}$ i $u$ je odrednica. Ako je pak $v$ odrednica, tj. $(v)\overline{\varphi} = [1]$, onda je $[v] = [1]$, odnosno $v \sim_P 1$, i $v$ se može primenom operacija $(i)$ i $(ii)$ svesti na praznu reč.

Pretpostavimo dalje da je i $\mathbf{H} = \langle H, \star\rangle$ grupa sa prezentacijom $(A; P)$ za preslikavanje $\psi : A \longrightarrow H$. Tada je preslikavanje $\theta : G_{(A;P)} \longrightarrow H$ dato sa $([u])\theta = (u)\overline{\psi}$, $u \in W$, izomorfno preslikavanje grupe $\mathbf{G}_{(A;P)}$ na grupu $\mathbf{H}$. Pokažimo to.

$\theta$ je dobro definisano i injektivno preslikavanje:

$[u] = [v]$ akko je $u \sim_P v$ akko je $uv^{-1} \sim_P 1$ akko je $uv^{-1}$ izvedivo iz $P$ akko je $(uv^{-1})\overline{\psi} = e_H$ (jer je $(A; P)$ prezentacija grupe $\mathbf{H}$ za preslikavanje $\psi$) akko je $(u)\overline{\psi} = (v)\overline{\psi}$ akko je $([u])\theta = ([v])\theta$.

$\theta$ je homomorfno preslikavanje:

$$([u] \circ [v])\theta = ([u \cdot v])\theta = (u \cdot v)\overline{\psi} = (u)\overline{\psi} \star (v)\overline{\psi} = ([u])\theta \star ([v])\theta.$$

$\theta$ je surjektivno: $\langle(\{[a] \mid a \in A\})\theta\rangle = \langle(A)\psi\rangle = \mathbf{H}$.■

Napomenimo još ovde (ukoliko je to uopšte potrebno): ako je $(A; P)$ prezentacija grupe $\mathbf{G}$ i ako je $\mathbf{G} \cong \mathbf{H}$, tada je $(A; P)$ prezentacija i grupe $\mathbf{H}$. Jer, $\mathbf{H} \cong \mathbf{G}_{(A;P)}$ ($\cong \mathbf{G}$) i ako je $\theta \in Is(\mathbf{G}_{(A;P)}, \mathbf{H})$, onda je $(A; P)$ prezentacija

grupe $\mathbf{H}$ za preslikavanje $\varphi : A \longrightarrow H$, gde je $(a)\varphi = ([a])\theta$. Imamo, naime, za $u \equiv a_{i_1}^{\alpha_1} \dots a_{i_k}^{\alpha_k} \in W$:

$$(u)\overline{\varphi} = ((a_{i_1})\varphi)^{\alpha_1} \dots ((a_{i_k})\varphi)^{\alpha_k} = (([a_{i_1}])\theta)^{\alpha_1} \dots (([a_{i_k}])\theta)^{\alpha_k} =$$

$$([a_{i_1}^{\alpha_1} \dots a_{i_k}^{\alpha_k}])\theta = ([u])\theta$$

pa važi

$$(u)\overline{\varphi} = e_H \text{ akko } ([u])\theta = e_H \text{ akko } [u] = [1] \text{ akko } u \sim_P 1.$$

Obično ćemo za predstavnika klase grupa sa prezentacijom $(A; P)$ birati "karakterističnu" (kanoničku) grupu (klasa ekvivalencija):

$$\langle \{[u] \mid u \in W\}, \circ \rangle = \mathbf{G}_{(A;P)}.$$

**Definicija 21.8** *Grupa koja ima prezentaciju u kojoj je skup odrednica prazan skup zove se slobodna grupa (podsećamo na napomenu uz definiciju* 21.3*).*

**Korolar 21.9** *(a) Neka je dato $(A; P)$, $A = \{a_i \mid i \in I\} \neq \emptyset$, $P \subseteq W$ - skup reči nad azbukom $A \cup A^{-1}$, i grupa $\mathbf{H} = \langle H, \star \rangle$. Pretpostavimo da je za neko preslikavanje $\psi : A \longrightarrow H$, za svako $u \in P$, $(u)\overline{\psi} = e_H$ ($\overline{\psi} \in Hom(\mathbf{W}, \mathbf{H})$ je standardna ekstenzija preslikavanja $\psi$). Tada se grupa $\mathbf{G}_{(A;P)}$ homomorfno preslikava u grupu $\mathbf{H}$;*

*(b) Neka je $(A; P)$ prezentacija grupe $\mathbf{M}$ i $(A; P \cup Q)$ prezentacija grupe $\mathbf{N}$ (podrazumevamo, naravno, $Q \subseteq W$). Tada je $\mathbf{N}$ homomorfna slika grupe $\mathbf{M}$;*

*(c) Svaka grupa je homomorfna slika neke slobodne grupe;*

*(d) Elementi $u$ i $v$ skupa reči $W$ nisu u relaciji $\sim_P$ akko postoji homomorfno preslikavanje $\theta$ polugrupe $\mathbf{W}$ u neku grupu $\mathbf{G}$ takvo da je $(u)\theta \neq (v)\theta$ i $(w)\theta = e_G$ za svako $w \in P$.*

**Dokaz.** *(a)* Definišimo $\theta : G_{(A;P)} \longrightarrow H$ sa $([u])\theta = (u)\overline{\psi}$ (ako je $u \equiv a_{i_1}^{\alpha_1} \dots a_{i_k}^{\alpha_k}$ i $(a_i)\psi = h_i \in H$, često se $([u])\theta = (u)\overline{\psi} = h_{i_1}^{\alpha_1} \dots h_{i_k}^{\alpha_k}$ jednostavno obeležava sa $u(h_{i1}, \dots, h_{i_k})$ - izraz je "samoobjašnjiv"). Dokaz da je $\theta$ dobro definisano analogan je onom iz (prethodne) teoreme:

$[u] = [v]$ akko je $u \sim_P v$ akko je $uv^{-1} \sim_P 1$ (1 - prazna reč) akko se 1 može (konačnom) primenom operacija $(i)$ i $(ii)$ svesti na $uv^{-1}$. Neka je dat niz $1 \equiv w_0, w_1, \dots, w_n \equiv uv^{-1}$, gde se (za $0 < i \leq n$) $w_i$ dobija od $w_{i-1}$ jednom od operacija $(i)$, $(ii)$. Lako se pokazuje indukcijom po $i$ da je $(w_i)\overline{\psi} = e_H$ ($w_i$ nastaje umetanjem ili brisanjem, kao podreči, bilo trivijalne odrednice bilo reči iz $P$, u svakom slučaju je $(w_{i-1})\overline{\psi} = (w_i)\overline{\psi}$, jer je po pretpostavci $(w)\overline{\psi} = e_H$ za svako $w$ iz $P$).



Preslikavanje $\theta$ je, očigledno, i homomorfno:

$$([u] \circ [v])\theta = ([u \cdot v])\theta = (u \cdot v)\overline{\psi} = (u)\overline{\psi} \star (v)\overline{\psi} = ([u])\theta \star ([v])\theta.$$

*(b)* Obeležimo sa $[u]_P$ i $[u]_{P \cup Q}$ klase ekvivalencija određene elementom $u$ ($\in W$) relacija, respektivno, $\sim_P$ i $\sim_{P \cup Q}$. Kako je $\mathbf{M} \cong \mathbf{G}_{(A;P)}$ i $\mathbf{N} \cong \mathbf{G}_{(A;P \cup Q)}$, a $([u]_P)\theta = [u]_{P \cup Q}$ je (prema tački $(a)$) homomorfno preslikavanje grupe $\mathbf{G}_{(A;P)}$ na grupu $\mathbf{G}_{(A;P \cup Q)}$, to se i $\mathbf{M}$ homomorfno preslikava na grupu $\mathbf{N}$.

*(c)* Grupa $\mathbf{G}$ sa prezentacijom $(A; P)$ (takva jedna, videli smo, uvek postoji) homomorfna je slika slobodne grupe sa prezentacijom $(A; \emptyset)$.

*(d)* Ako $u$ i $v$ nisu u relaciji $\sim_P$, onda je $[u]_P \neq [v]_P$, pa je za kanoničko homomorfno preslikavanje $\overline{\varphi}$ polugrupe $\mathbf{W}$ u grupu $\mathbf{G}_{(A;P)}$ ($(u)\overline{\varphi} = [u]_P$) $(u)\overline{\varphi} \neq (v)\overline{\varphi}$ i, jasno, $(w)\overline{\varphi} = [1]_P$ za svako $w \in P$.

Ako je pak za homomorfno preslikavanje $\theta \in Hom(\mathbf{W}, \mathbf{G})$, $(u)\theta \neq (v)\theta$ i $(w)\theta = e_G$ za svako $w \in P$, onda, trivijalno, $u$ nije u relaciji $\sim_P$ sa $v$ ($u \sim_P v$ bi dalo $(u)\theta = (v)\theta$ - 21.4$(d)$).□

U narednim primerima uvek će $A$ biti skup izvodnih simbola, a $P$ skup odrednica. Shodno tome, kada je mogućnost zabune isključena, pisaćemo umesto $\sim_P$ jednostavno $\sim$.

**Primer 21.10** *(a)*

$$(1)\ (a; a); \quad (2)\ (a, b; ab^2a^{-1}b^{-3}, ba^3b^{-1}a^{-2});$$

*i*

$$(3)\ (a, b, c; a^3, b^3, c^4, acac^{-1}, aba^{-1}bc^{-1}b^{-1})$$

*su prezentacije jedinične grupa (tek tri od beskonačno mnogo - videti tačku $(i)$).*

**Dokaz.** Slučaj (1) je trivijalan. Dokažimo tvrđenje za (2) i (3).

(2) Jasno, $ab^2 \sim b^3a$, $ba^3 \sim a^2b$ (opet naglašavamo, često se koristi i $=$ umesto $\sim$). S obzirom na 21.4$(f)$ imamo:

$ab^2 \sim b^3a \Longrightarrow a^{-1}ab^2 \sim a^{-1}b^3a$, tj. $b^2 \sim a^{-1}b^3a$;

$ab^2 \sim b^3a \Longrightarrow ab^2a^{-1} \sim b^3aa^{-1}$, tj. $b^3 \sim ab^2a^{-1}$.

$b^2 \sim a^{-1}b^3a$ daje $b^4 \sim a^{-1}b^6a$ ($b^2b^2 \sim a^{-1}b^3aa^{-1}b^3a \sim a^{-1}b^6a$), dakle $ab^4a^{-1} \sim b^6$ $(I)$ i $a^2b^4a^{-2} \sim ab^6a^{-1}$. Zbog $b^9 \equiv b^3b^3b^3 \sim ab^2a^{-1}ab^2a^{-1}ab^2a^{-1} \sim ab^6a^{-1}$ i tranzitivnosti relacije $\sim$ tu je i $b^9 \sim a^2b^4a^{-2}$ $(II)$.

$ba^3 \sim a^2b$ implicira $a^3 \sim b^{-1}a^2b$, pa je $a^2b^4a^{-2} \sim b^9 \sim b^{-1}b^9b \sim b^{-1}a^2b^4a^{-2}b \sim b^{-1}a^2bb^4b^{-1}a^{-2}b \sim a^3b^4a^{-3}$ i stoga: $b^4 \sim ab^4a^{-1}$ $(III)$.

$(I)$ i $(III)$ daju $b^6 \sim b^4$, tj. $b^2 \sim 1$, a onda je, prema $(II)$, $b^9 \sim a^2b^4a^{-2} \sim 1$. Dalje, iz $b^2 \sim 1$ i $b^9 \sim 1$ sledi i $b \sim 1$, prema tome je i $a^3 \sim a^2$, odnosno $a \sim 1$. Znači, za svako $u \in W$, $[u] = [1]$ i $|G_{(A;P)}| = 1$.

(3) Iz $aba^{-1} \sim bcb^{-1}$ proizilazi $(aba^{-1})^3 \sim (bcb^{-1})^3$, tj. $ab^3a^{-1} \sim bc^3b^{-1}$, pa je zbog $b^3 \sim 1$ i $bc^3b^{-1} \sim 1$, dakle i $c^3 \sim 1$. Kako već imamo i $c^4 \sim 1$, sledi $c \sim 1$, a onda i $aba^{-1} \sim bcb^{-1} \sim 1$, te je i $b \sim 1$. Iz $acac^{-1} \sim 1$ i $c \sim 1$ dobijamo $a^2 \sim 1$, što zajedno sa $a^3 \sim 1$ daje $a \sim 1$.

$(b)$

$$(1)\ (a;\ a^4);\quad (2)\ (a;\ a^8, a^{12});\quad (3)\ (a,b;\ a^4, b^4, a^3b);\quad (4)\ (a,b;\ a^4, b^4, ab)$$

*su prezentacije cikične grupe reda* 4.

**Dokaz.** Osvrnimo se samo na treću prezentaciju: $A = \{a,b\}$, $P = \{a^4, b^4, a^3b\}$. Preslikavanje $\varphi : A \longrightarrow Z_4$, gde je $(a)\varphi = (b)\varphi = 1$ (da ne bude zabune – 1 je ovde (generatorni) element grupe $\mathbf{Z}_4$), inducira homomorfno preslikavanje grupe $\mathbf{G}_{(A;P)}$ na cikličnu grupu $\mathbf{Z}_4 = \langle 4, +_4\rangle$. No $\mathbf{G}_{(A;P)}$ i nema više od četiri elementa (svaka reč se svodi na $a^\alpha$, $\alpha \in \{0,1,2,3\} = 4$; setimo se: $a^0$ je oznaka prazne reči, a koristili smo $b \sim a^{-3} \sim a$).

$(c)$ $(a;\ a^n)$ *i* $(a;\ a^{n+k}, a^k)$ *gde* $n$ *deli* $k$, *prezentacije su ciklične grupe reda* $n$.

$(d)$ $(a,b;\ a^2, b^2, (ab)^2)$ *je prezentacija Kleinove grupe.*

**Dokaz.** Videti tačku $(i)$ i setiti se da je Kleinova grupa direktni prozvod dve ciklične grupe reda 2.

$(e)$ $(a,b;\ a^n, b^2, (ab)^2)$ *je prezentacija dijedarske grupe* $\mathbf{D}_n$ *stepena* $n$ *(videti* 3.4$(d)$*).*

**Dokaz.** Preslikajmo $a$ u $\rho_{\frac{2\pi}{n}}$ i $b$ u $\sigma_y$. Zbog $(\rho_{\frac{2\pi}{n}})^n = (\sigma_y)^2 = \imath$ (– identično preslikavanje) i $\rho_{\frac{2\pi}{n}}\sigma_y = \sigma_y(\rho_{\frac{2\pi}{n}})^{n-1}$, tj. $(\rho_{\frac{2\pi}{n}}\sigma_y)^2 = \imath$, dijedarska grupa je homomorfna slika grupe $\mathbf{G}_{(A;P)}$. Ali grupa $\mathbf{G}_{(A;P)}$ i nema više od $2n$ elementa. Naime, svaka reč (nad azbukom $A \cup A^{-1}$) je, očigledno, u relaciji $(\sim_P)$ sa reči oblika $b^\beta a^\alpha$, $\beta \in \{0,1\}$, $\alpha \in \{0,1,\ldots,n-1\}$ (jer je $ab \sim ba^{n-1}$).

$(f)$ $(a,b;\ a^3, b^2, (ab)^3)$ *je prezentacija alternativne grupe* $\mathbf{A}_4$.

**Dokaz.** Ako je $(a)\varphi = (1\ 2\ 3)$ i $(b)\varphi = (0\ 1)(2\ 3)$, s obzirom da je $(1\ 2\ 3)^3 = ((0\ 1)(2\ 3))^2 = ((1\ 2\ 3)(0\ 1)(2\ 3))^3 = \imath$ $((1\ 2\ 3)(0\ 1)(2\ 3) = (1\ 3\ 0)$ ), kao i da je grupa $\mathbf{A}_4$ generisana elementima $(1\ 2\ 3)$ i $(0\ 1)(2\ 3)$ (videti korolar 9.21), $\overline{\varphi}$ preslikava homomorfno grupu $\mathbf{G}_{(A;P)}$ na $\mathbf{A}_4$. S druge strane, reči $1$, $a$, $a^2$, $b$, $ab$, $ba$, $a^2b$, $ba^2$, $aba$, $a^2ba$, $aba^2$ i $a^2ba^2$ su predstavnici svih klasa ekvivalencija, te je $\overline{\varphi}$ zapravo izomorfizam. Zaista, nikoje dve od ovih dvanaest reči nisu u relaciji $\sim_P$, jer za $\overline{\varphi}$ imaju različite slike, a svaka druga reč je u relaciji sa nekom od njih. Dokaz je indukcijom po dužini reči. Sve reči dužine 0, 1, 2 su već "uključene" u spisak (npr. $a^{-1} \sim a^2$, $b^{-1} \sim b$, $a^{-2} \sim a$ i tako dalje). Pretpostavimo stoga da je tvrđenje tačno za reči dužine manje od $n+1$ $(n > 1)$ i neka je $l(u) = n+1$. Tada je $u \equiv av$ ili $u \equiv a^{-1}v$ ili



$u \equiv bv$ ili $u \equiv b^{-1}v$ $(l(v) = n)$. Razmotrimo delimično slučaj: $u \equiv bv$. $v$ je, po induktivnoj hipotezi, u relaciji $\sim_P$ sa nekom od ponuđenih reči, recimo sa $aba^2$, pa je

$$bv \sim_P baba^2 \sim_P a^2ababab^2a \equiv a^2(ab)^3ba \sim_P a^2ba;$$

ostali slučajevi se analogno proveravaju – ako je npr. $u \equiv a^{-1}v$, onda $u \sim_P a^2v$, te prvo nalazimo predstavnika klase ekvivalencije reči $av$.

$(g)$ $(x,y;\ x^3, y^4, (xy)^2)$ *je prezentacija simetrične grupe* $\mathbf{S}_4$.

**Dokaz.** Neka je $(x)\varphi = (2\ 1\ 3)$ i $(y)\varphi = (0\ 1\ 2\ 3)$. Lako se proverava da je $\overline{\varphi}$ homomorfno preslikavanje grupe $\mathbf{G}_{(A;P)}$ na grupu $\mathbf{S}_4$ (grupa $\mathbf{S}_4$ je generisana elementima $(2\ 1\ 3)$ i $(0\ 1\ 2\ 3)$ – videti 9.10$(b)$, a važi i $(2\ 1\ 3)^3 = (0\ 1\ 2\ 3)^4 = ((2\ 1\ 3)(0\ 1\ 2\ 3))^2 = (0\ 1)^2 = \imath$). Preostaje nam da pokažemo: $|G_{(A;P)}| \leq 24$ ($|G_{(A;P)}| \geq 24$ već imamo). Krenimo u tom cilju od podgrupe $\mathbf{H}$ grupe $\mathbf{G}_{(A;P)}$ generisane elementima $[x]$ i $[y]^2$. Pokazaćemo, a time i kompletirati dokaz, da je $\mathbf{H}$ normalna podgrupa indeksa 2 sa najviše 12 elemenata.

Zbog $y^{-1}xy \sim y^3xy \sim y^2x^{-1}xyxy \sim y^2x^{-1} \sim y^2x^2$ je $[y]^{-1}[x][y] = [y^{-1}xy] = [y^2][x]^2 \in H$, a onda i $[y][x][y^{-1}] = [y]^2[y]^{-1}[x][y][y]^{-2} \in H$ i, za svaki ceo broj $\alpha$, $[y]^{-1}[x]^\alpha[y]$, $[y][x]^\alpha[y]^{-1} \in H$. Prema tome, $\mathbf{H} \lhd \mathbf{G}_{(A;P)}$. $\mathbf{H}$ je i indeksa 2 – $[y]^\beta H$ je ili $H$ (za parno $\beta$) ili $[y]H$ (za neparno $\beta$). Da bismo pokazali $|H| \leq 12$ koristimo grupu iz prethodne tačke: preslikajmo $a$ u $[x]$ i $b$ u $[y^2]$. Pošto je $[x]^3 = [y^2]^2 = ([x][y^2])^3 = [1]$, $\mathbf{A}_4$ se homomorfno preslikava na $\mathbf{H}$; poslednja jednakost se dobija iz: $xy^2 \sim xyxx^{-1}y \sim xyxyy^{-1}x^{-1}y \sim y^{-1}x^{-1}y$, jer tada je $(xy^2)^3 \sim (y^{-1}x^{-1}y)^3 \sim y^{-1}x^{-3}y \sim 1$.

$(h)$

$$(a,b;\ a^4, a^2b^2, a^3ba^3b^3) = (A;\ P)$$

*i*

$$(c,d,e,f;\ c^2f^{-1}, d^2f^{-1}, e^2f^{-1}, f^2, cde^{-1}, dec^{-1}, ecd^{-1}) = (B;Q)$$

*su prezentacije grupe kvaterniona (primer* 5.6$(a)$*).*

**Dokaz.** Prvu prezentaciju ne treba objašnjavati ($[a] \longleftrightarrow \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ i $[b] \longleftrightarrow \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$). Ostavljamo za vežbu da se pokaže da su sve reči u relaciji $\sim_P$ sa nekom od reči $1$, $a$, $a^2$, $a^3$, $b$, $ab$, $a^2b$, $a^3b$.

Što se tiče druge prezentacije neka je $(c)\varphi = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $(d)\varphi = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, $(e)\varphi = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ i $(f)\varphi = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^2 = -I$. Lako se proverava da je $(u)\overline{\varphi} = I$ (jedinična matrica) za svako $u \in Q$. Moramo,

dakle, još da pokažemo da grupa $\mathbf{G}_{(B;Q)}$ ima najviše osam elemenata. Pokazaćemo da je svaka reč (azbuke $B \cup B^{-1}$) u relaciji $\sim_Q$ sa nekom od reči 1, $c$, $d$, $e$, $f$, $cf$, $df$, $ef$. Za reči dužine 0, 1 to je evidentno, npr. $c^{-1} \sim_Q c^{-1}c^2f^{-1} \sim_Q cf^{-1} \sim_Q cf^{-1}f^2 \sim_Q cf$. Pretpostavimo da je tvrđenje tačno za sve reči dužine manje od $n+1$ $(n \geq 1)$ i neka je $u$ reč dužine $n+1$. Onda je, za neku reč $v$ (dužine $n$), $u \equiv c^\alpha v$ ili $u \equiv d^\alpha v$ ili $u \equiv e^\alpha v$ ili $u \equiv f^\alpha v$, $\alpha \in \{1, -1\}$. Ako imamo npr. $u \equiv c^{-1}v$, prema već pokazanom je $c^{-1}v \sim_Q cfv$. Razmotrićemo samo jedan od mogućih slučajeva (ostali se analogno proveravaju): neka je $u \equiv c^{-1}v$ i $v \equiv ef$. Tada niz

$$u \equiv c^{-1}v, \ldots, cfv, \ldots, cfef, ce^2f^{-1}fef, cee^2f, cee^2f^{-1}f^2,$$

$$cef^2, ce, dec^{-1}ce, de^2, de^2f^{-1}f, df$$

daje $c^{-1}v \sim_Q df$.

*(i) Neka je $(A_i; P_i)$ prezentacija grupe $\mathbf{G}_i$ za $i \in I$ $(\neq \emptyset)$, $A_i = \{a_{i_m} \mid m \in J_i\}$ i za različite indekse $i, j$ iz $I$ neka je $A_i \cap A_j = \emptyset$. Tada je*

$$\left(\bigcup_{i\in I} A_i; \bigcup_{i\in I} P_i \cup \{ a_{i_m}^{-1}a_{j_n}^{-1}a_{i_m}a_{j_n} \mid i, j \in I, i \neq j, m \in J_i, n \in J_j\}\right)$$

*prezentacija grupe $\prod_{i\in I} \mathbf{G}_i$ (direktnog proizvoda familije grupa $\{\mathbf{G}_i \mid i \in I\}$).*

**Dokaz.** Možemo pretpostaviti da je $\mathbf{G}_i$ baš $\mathbf{G}_{(A_i;P_i)}$. Elemente te grupe obeležavaćemo sa $[u]_i$, relacije $\sim_{P_i}$ sa $\sim_i$, i stavićemo:

$$\bigcup_{i\in I} A_i = A, \quad \bigcup_{i\in I} A_i^{-1} = A^{-1}$$

i

$$\bigcup_{i\in I} P_i \cup \{ a_{i_m}^{-1}a_{j_n}^{-1}a_{i_m}a_{j_n} \mid i, j \in I, i \neq j, m \in J_i, n \in J_j\} = Q.$$

Neka je $\varphi$ preslikavanje skupa $A$ u $\prod_{i\in I}^d G_{(A_i;P_i)}$ dato sa $(a_{i_m})\varphi = f_{i_m}$, gde je $(i)f_{i_m} = [a_{i_m}]_i$ i, za $j \neq i$, $(j)f_{i_m} = [1]_j$ (jedinični element grupe $\mathbf{G}_{(A_j;P_j)}$). $\overline{\varphi}$ je, već znamo, standardna ekstenzija preslikavanja $\varphi$; $\overline{\varphi} : W \longrightarrow \prod_{i\in I}^d G_{(A_i;P_i)}$ ($W$ – skup svih reči nad azbukom $A \cup A^{-1}$). Lako se proverava da je, za svako $u \in Q$, $(u)\overline{\varphi} = e$ (jedinični element grupe $\prod_{i\in I} \mathbf{G}_{(A_i;P_i)}$ – za svako $i \in I$ je $(i)e = [1]_i$). Ako je $u \equiv a_{i_{m_1}}^{k_1} \ldots a_{i_{m_r}}^{k_r} \in P_i$ ($m_t \in J_i$, $k_t \in Z$), tada je $(u)\overline{\varphi} = f_{i_{m_1}}^{k_1} \ldots f_{i_{m_r}}^{k_r} \equiv f$ i $(i)f = [a_{i_{m_1}}]_i^{k_1} \ldots [a_{i_{m_r}}]_i^{k_r} = [a_{i_{m_1}}^{k_1} \ldots a_{i_{m_r}}^{k_r}]_i = [1]_i$, a za $j \neq i$, $(j)f = [1]_j^{k_1} \ldots [1]_j^{k_r} = [1]_j$. Ako je $u \equiv a_{i_m}^{-1}a_{j_n}^{-1}a_{i_m}a_{j_n}$, $i \neq j$, onda je $(u)\overline{\varphi} = f_{i_m}^{-1}f_{j_n}^{-1}f_{i_m}f_{j_n}$ i opet je, za svako $t \in I$, $(t)((u)\overline{\varphi}) = (t)(f_{i_m}^{-1}f_{j_n}^{-1}f_{i_m}f_{j_n}) = [1]_t$. Tako je npr. $(i)(f_{i_m}^{-1}f_{j_n}^{-1}f_{i_m}f_{j_n}) = [a_{i_m}]_i^{-1}[1]_i^{-1}[a_{i_m}]_i[1]_i = [1]_i$, a za $t \neq i, j$, $(t)(f_{i_m}^{-1}f_{j_n}^{-1}f_{i_m}f_{j_n}) = [1]_t^{-1}[1]_t^{-1}[1]_t[1]_t = [1]_t$. $\prod_{i\in I} \mathbf{G}_{(A_i;P_i)}$ je, znači, homomorfna slika grupe $\mathbf{G}_{(A;Q)}$ ($\overline{\varphi}$ je, jasno, surjektivno preslikavanje); homomorfizam $\theta$ je, naravno, dat sa $([u]_Q)\theta = (u)\overline{\varphi}$. Treba još pokazati da je $\theta$ injektivno preslikavanje.



Primetimo prvo da je svaka reč $u$ iz $W$ u relaciji $\sim_Q$ sa reči oblika $u_{i_1} \ldots u_{i_s}$, gde je $u_{i_t} \in W_{i_t}$, jer je (za $i \neq j$) $a_{i_k}^m a_{j_r}^n \sim_Q a_{j_r}^n a_{i_k}^m$ (iz $a_{i_k}a_{j_r} \sim_Q a_{j_r}a_{i_k}$, tj. $a_{j_r}^{-1}a_{i_k}a_{j_r} \sim_Q a_{i_k}$, sledi, za svaki ceo broj $m$, $a_{j_r}^{-1}a_{i_k}^m a_{j_r} \sim_Q a_{i_k}^m$, odnosno $a_{j_r} \sim_Q a_{i_k}^{-m}a_{j_r}a_{i_k}^m$, pa je, za svaki ceo broj $n$, $a_{j_r}^n \sim_Q (a_{i_k}^{-m}a_{j_r}a_{i_k}^m)^n \sim_Q a_{i_k}^{-m}a_{j_r}^n a_{i_k}^m$ i odatle $a_{i_k}^m a_{j_r}^n \sim_Q a_{j_r}^n a_{i_k}^m$).

Dalje, neka je $v \equiv v_{i_1} \ldots v_{i_k} \sim_Q w_{j_1} \ldots w_{j_m} \equiv w$, gde su indeksi $i_s$ $(1 \leq s \leq k)$ kao i $j_t$ $(1 \leq t \leq m)$ različiti, gde je (za svako $s$) $v_{i_s}$ reč polugrupe $\mathbf{W}_{i_s}$, (za svako $t$) $w_{j_t}$ reč polugrupe $\mathbf{W}_{j_t}$ i gde, konačno, za svako $s, t$, $v_{i_s} \not\sim_{i_s} 1$, $w_{j_t} \not\sim_{j_t} 1$. Tada je $k = m$, skupovi $\{i_1, \ldots, i_k\}$ i $\{j_1, \ldots, j_m\}$ su jednaki i ako je $i_s = j_t$, onda je $v_{i_s} \sim_{i_s} w_{i_s}$. Jer, pretpostavimo, recimo, $i_1 \notin \{j_1, \ldots, j_m\}$. Onda je $(i_1)((v)\overline{\varphi}) = [v_{i_1}]_{i_1}$, dok je $(i_1)((w)\overline{\varphi}) = [1]_{i_1}$, dakle, $([v]_Q)\theta = (v)\overline{\varphi} \neq (w)\overline{\varphi} = ([w]_Q)\theta$, kontradikcija. Odatle proizilazi prvi deo tvrđenja. Dokažimo i da je $v_{i_s} \sim_{i_s} w_{i_s}$. Neka je $\pi_{i_s}$ projekcija grupe $\prod_i \mathbf{G}_{(A_i;P_i)}$ na grupu $\mathbf{G}_{(A_{i_s};P_{i_s})}$. Tada je $[v_{i_s}]_{i_s} = (i_s)((v)\overline{\varphi}) = (i_s)(([v]_Q)\theta) = ([v]_Q)(\theta \circ \pi_{i_s}) = ([w]_Q)(\theta \circ \pi_{i_s}) = (i_s)(([w]_Q)\theta) = (i_s)((w)\overline{\varphi}) = [w_{i_s}]_{i_s}$.

Sada injektivnost preslikavanja $\theta$ direktno sledi: ako je $[v]_Q \neq [w]_Q$, $v \equiv v_{i_1} \ldots v_{i_k}$, $w \equiv w_{j_1} \ldots w_{j_m}$, $i_s, j_t \in I$, $v_{i_s} \not\sim_{i_s} 1$, $w_{j_t} \not\sim_{j_t} 1$, onda je ili $k \neq m$ ili $k = m$ i, za neko $s$, $i_s \notin \{j_1, \ldots, j_m\}$ ili $k = m$, $\{i_1, \ldots, i_k\} = \{j_1, \ldots, j_k\}$ ali, za neko $i_s$, $v_{i_s} \not\sim_{i_s} w_{i_s}$. U svakom slučaju:

$$([v]_Q)\theta = ([v_{i_1}]_Q \ldots [v_{i_k}]_Q)\theta = (v_{i_1})\overline{\varphi} \ldots (v_{i_k})\overline{\varphi} \neq$$

$$(w_{j_1})\overline{\varphi} \ldots (w_{j_m})\overline{\varphi} = ([w_{j_1}]_Q)\theta \ldots ([w_{j_m}]_Q)\theta = ([w_{j_1} \ldots w_{j_m}]_Q)\theta = ([w]_Q)\theta.$$

Imamo u vidu, ponavljamo, da je $(i_s)((v_{i_s})\overline{\varphi}) = [v_{i_s}]_{i_s}$, i da je, za $j \neq i_s$, $(j)((v_{i_s})\overline{\varphi}) = [1]_j$.

U vezi ove tačke recimo i sledeće: ako je za svako $i \in I$, $A_i$ jednoelementni skup $\{a_i\}$, a $P_i$ baš prazan skup, onda je, uz ostale pretpostavke, $(\{a_i \mid i \in I\}; \{a_i^{-1}a_j^{-1}a_ia_j \mid i, j \in I, i \neq j\})$ prezentacija direktnog proizvoda beskonačnih cikličnih grupa (imamo u vidu da je $(a; \emptyset)$ prezentacija beskonačne ciklične grupe; laki dokaz ostavljamo za vežbu). Ovakve grupe zovemo *slobodnim Abelovim grupama* (prema tome beskonačna ciklična grupa je poseban slučaj i slobodne i slobodne Abelove grupe). O njima će više biti reči u poglavlju o Abelovim grupama. Sada se samo podsetimo da je jedan primer takve grupe multiplikativna grupa pozitivnih racionalnih brojeva (koja je direktni proizvod beskonačnih cikličnih grupa generisanih prostim brojevima) i konstatujmo da je svaka Abelova grupa homomorfna slika neke slobodne Abelove grupe; Abelova grupa $\mathbf{H}$ (sa domenom $H$) homomorfna je slika slobodne Abelove grupe $\mathbf{G}_{(H;P)}$, gde je $P = \{a^{-1}b^{-1}ab \mid a, b \in H\}$.

Tačke $(c)$ i $(i)$ u kombinaciji sa 10.45$(a)$ daju: ako su $m_1, \ldots, m_k$ uzajamno prosti brojevi, tada je

$$(a_1, \ldots, a_k;\ a_1^{m_1}, \ldots, a_k^{m_k},\ a_1^{-1}a_2^{-1}a_1a_2,\ a_1^{-1}a_3^{-1}a_1a_3, \ldots, a_{k-1}^{-1}a_k^{-1}a_{k-1}a_k)$$

prezentacija ciklične grupe $\mathbf{C}_{m_1 \ldots m_k}$.

$(j)$ *Neka su* $(A;P)$ *i* $(A;Q)$ *takve prezentacije da je svako* $u$ *iz* $P$ *izvedivo iz* $Q$ *i svako* $v$ *iz* $Q$ *izvedivo iz* $P$. *Tada se grupe* $\mathbf{G}_{(A;P)}$ *i* $\mathbf{G}_{(A;Q)}$ *podudaraju.*

**Dokaz.** Neka je $W$ skup reči nad azbukom $A \cup A^{-1}$ i $u \in W$. Na nama je da pokažemo da je $[u]_P = [u]_Q$. Recimo, neka je $u \sim_P v$, tj. $uv^{-1} \sim_P 1$. Tada postoji niz $1 \equiv w_0, w_1, \ldots, w_n \equiv uv^{-1}$, gde se svako $w_i$ dobija od $w_{i-1}$ $(0 < i \leq n)$ primenom jedne od operacija $(i)$, $(ii)$ (definicije 21.3) s obzirom na skup $P$. Indukcijom po $i$ dokazujemo da se svako $w_i$ može dobiti od prazne reči primenom operacija $(i)$ i $(ii)$, s obzirom na skup $Q$. Slučaj $i = 0$ je trivijalan. $w_{i+1}$ je dobijeno ili umetanjem ili brisanjem neke reči iz $P$ ili neke trivijalne odrednice u $w_i$. Međutim, kako je svaka reč iz $P$ određena skupom $Q$ (dakle, može se svesti na praznu reč ili od nje dobiti primenom operacija umetanja i brisanja, s obzirom na skup $Q$), ako je tvrđenje tačno za $w_i$ tačno je i za $w_{i+1}$. Proizilazi: $uv^{-1} \sim_Q 1$, tj. $u \sim_Q v$.

Po simetriji stvari i $u \sim_Q v$ implicira $u \sim_P v$.

$(k)$ *Neka je* $u \equiv b_1 \ldots b_n$ *reč azbuke* $A \cup A^{-1}$ *(*$b_i$ *je ili* $a$ *ili* $a^{-1}$ *za neko* $a \in A$*). Ciklična permutacija* $u'$ *reči* $u$ *je reč oblika* $b_{i+1} \ldots b_n b_1 \ldots b_i$.

*Prezentacije* $(A;P)$ *i* $(A;P')$, *gde je* $P' = \{u' \mid u'$ *je (neka) ciklična permutacija reči* $u \in P\}$ *određuju istu grupu ekvivalencije:* $\mathbf{G}_{(A;P)} = \mathbf{G}_{(A;P')}$.

**Dokaz.** Prema prethodnoj tački dovoljno je pokazati da je, za $u \in P$, $u$ izvedivo iz $P'$, kao i da je $u'$ izvedivo iz $P$. Sledeći nizovi to potvrđuju:

$$u' \equiv b_{i+1} \ldots b_n b_1 \ldots b_i, \ldots, b_{i+1} \ldots b_n u^{-1} b_1 \ldots b_i \equiv$$

$$b_{i+1} \ldots b_n b_n^{-1} \ldots b_1^{-1} b_1 \ldots b_i, \ldots, 1;$$

$$u \equiv b_1 \ldots b_i b_{i+1} \ldots b_n, \ldots, b_1 \ldots b_i u'^{-1} b_{i+1} \ldots b_n \equiv$$

$$b_1 \ldots b_i b_i^{-1} \ldots b_1^{-1} b_n^{-1} \ldots b_{i+1}^{-1} b_{i+1} \ldots b_n, \ldots, 1.$$

$(l)$ *Neka je* $P = \{u_i \mid i \in I\}$ *(*$u_i$ *- reč nad azbukom* $A \cup A^{-1}$*),* $P^{-1} = \{u_i^{-1} \mid i \in I\}$ *i* $Q = \{v_i^{-1} u_i v_i \mid i \in I\}$, *gde su* $v_i$, $i \in I$, *proizvoljne reči (iste azbuke). Tada* $(A;P)$, $(A;P^{-1})$ *i* $(A;Q)$ *određuju istu grupu klasa ekvivalencija.*

**Dokaz.** Očigledno (koristiti 21.4).

$(m)$ $(a, b;\ a^r, b^s, ab \sim ba^t)$ *i* $(a, b;\ a^d, b^s, ab \sim ba^t)$, *gde je* $d = (r, t^s - 1)$, *određuju istu grupu klasa ekvivalencija.*



**Dokaz.** Neka je $P = \{a^r, b^s, ab \sim ba^t\}$. Naravno, dovoljno je da pokažemo da je $a^d \sim_P 1$. Iz $ab \sim_P ba^t$ sledi $a^t \sim_P b^{-1}ab$, a indukcijom se dokazuje: za svaki prirodan broj $k$ $(\geq 1)$ je $b^{-k}ab^k \sim_P a^{t^k}$; za $k = 1$ to nam je već dato, a iz pretpostavke da tvrđenje važi za $k$ izvodimo: $b^{-(k+1)}ab^{k+1} \sim_P b^{-1}(b^{-k}ab^k)b \sim_P b^{-1}a^{t^k}b \sim_P (b^{-1}ab)^{t^k} \sim_P (a^t)^{t^k} \sim_P a^{t^{k+1}}$. Stoga je $a \sim_P b^{-s}ab^s \sim_P a^{t^s}$, pa je $a^{t^s-1} \sim_P 1$. Preostaje još da se iskoristi teorema Euklida: neka su $u$ i $v$ celi brojevi takvi da je $ur + v(t^s - 1) = d$; tada je $a^d \sim_P a^{ur+v(t^s-1)} \sim_P 1$.

$(n)$ *Grupa klasa ekvivalencija prezentacije* $(a, b;\ a^r, b^s, ab \sim ba^t)$, *gde je* $r$ *prost faktor broja* $t^s - 1$, *konačna je grupa reda* $rs$ *sa elementima* $[b^m a^n]$, $0 \leq m < s$, $0 \leq n < r$, *i operacijom* $\circ$ *datom sa:*

$$[b^m a^n] \circ [b^p a^q] = [b^{m+sp} a^{nt^p+rq}].$$

**Dokaz.** Možemo odmah pretpostaviti da je $t < r$ (ako je $t \equiv t_1 \ (mod\ r)$; $t_1 \in r$ i $r|(t^s - 1)$, onda i $r|(t_1^s - 1)$, jer je takođe $t^s \equiv t_1^s \ (mod\ r)$, dakle i $t^s - 1 \equiv t_1^s - 1 \ (mod\ r)$). Jasno je da je svaka reč azbuke $\{a, b\}$ u relaciji (ekvivalentna) s rečju oblika $b^m a^n$. Dalje, prema prethodnoj tački imamo $b^m a^n \cdot b^p a^q \sim b^m b^p b^{-p} a^n b^p a^q \sim b^{m+p}(b^{-p}ab^p)^n a^q \sim b^{m+p}(a^{t^p})^n a^q \sim b^{m+sp} a^{nt^p+rq}$. Preostaje još da se pokaže da su elementi $[b^m a^n]$ i $[b^p a^q]$, gde je $(m, n) \neq (p, q)$, $0 \leq m,\ p < s$, $0 \leq n, q < r$, različiti. U tom cilju koristimo grupu regularnih matrica formata $2 \times 2$ sa elementima iz skupa $\{0, 1, \ldots, r-1\}$ s operacijom množenja, pri čemu se množenje i sabiranje elemenata matrica vrši po modulu $r$. Ukratko, radi se o multiplikativnoj grupi regularnih matrica, formata $2 \times 2$, nad poljem $\langle r, +_r, \cdot_r \rangle$ - $\mathbf{GL}_2(r)$. Neka $\varphi$ preslikava $a$ u $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = A$ i $b$ u $\begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix} = B$. Tada je $(a^r)\overline{\varphi} = A^r = I = (b^s)\overline{\varphi} = B^s$. Indukcijom se pokazuje da je $A^m = \begin{bmatrix} 1 & 0 \\ m - [\frac{m}{r}]r & 1 \end{bmatrix}$, a za množenje po *modulu* $r$ imamo:

$$\underbrace{t \cdot_r \ldots \cdot_r t}_{s-puta} = t^s - [\frac{t^s}{r}]r = t^s - [\frac{t^s - 1}{r} + \frac{1}{r}]r = t^s - (t^s - 1) + [\frac{1}{r}]r = 1.$$

Takođe je ispunjeno: $(ab)\overline{\varphi} = (ba^t)\overline{\varphi}$. Zaista,

$$(ab)\overline{\varphi} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} t & 0 \\ t & 1 \end{bmatrix} =$$

$$\begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ t & 1 \end{bmatrix} = \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^t = (ba^t)\overline{\varphi}$$

(u računu smo imali u vidu da je $t < r$). Prema tome, grupa $\mathbf{G}_{(A;P)}$ homomorfno se preslikava u grupu $\mathbf{GL}_2(r)$.

Pretpostavimo sada da je $[b^m a^n] = [b^p a^q]$, $0 \leq m,\ p < s,\ 0 \leq n,\ q < r$. Onda je i $(b^m a^n)\overline{\varphi} = (b^p a^q)\overline{\varphi}$, tj.

$$\begin{bmatrix} t^m - [\frac{t^m}{r}]r & 0 \\ n & 1 \end{bmatrix} = \begin{bmatrix} t^p - [\frac{t^p}{r}]r & 0 \\ q & 1 \end{bmatrix}.$$

Proizilazi da mora biti $n = q$. Na osnovu datih uslova nismo, međutim, u mogućnosti da zaključimo da mora biti i $m = p$ (dodatna pretpostavka – $s = min\{k \mid r$ je prost faktor broja $t^k - 1\}$ – bi nam to omogućila). Stoga u igru uvodimo i cikličnu grupu $\mathbf{Z}_s = \langle s, +_s \rangle$. Preslikavanje $\overline{\psi} : W \longrightarrow Z_s$ određeno sa $(a)\psi = 0$ i $(b)\psi = 1$ nam dokazuje da je $\mathbf{Z}_s$ homomorfna slika grupe $\mathbf{G}_{(A;P)}$. Pretpostavka $b^m \sim b^q$ implicira $(b^m)\overline{\psi} = (b^p)\overline{\psi}$, tj. $m = q$, doduše u $Z_s$, no već smo uzeli da je $m,\ p < s$.

Neko će se možda, na kraju, zapitati: čemu uslov da je $r$ baš prost faktor broja $t^s - 1$? ili, drugim rečima, gde smo taj uslov koristili? (deljivost smo "vidljivo" koristili). Zaboravne podsećamo da je za prirodan broj $k > 1$ polugrupa $\langle k \setminus \{0\}, \cdot_k \rangle$ grupa akko je $k$ prost broj; prema tome, s punim pravom smo koristili grupu $\mathbf{GL}_2(r)$; kad je $r$ složen broj skup regularnih matrica sa elementima iz $r$ nije uopšte zatvoren u odnosu na opisanu operaciju množenja.

($o$) *Prezentacija* $(a, b; a^2, (ab)^2)$ *određuje beskonačnu grupu, takozvanu beskonačnu dijedarsku grupu, u oznaci obično* $\mathbf{D}_\infty$.

**Dokaz.** Preslikajmo $a$ u matricu $M = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ i $b$ u matricu $N = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ (pišemo: $(a)\varphi = M$, $(b)\varphi = N$). Kako je $M^2 = I$ i $(MN)^2 = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}^2 = I$, grupa $\mathbf{G}_{(A;P)}$ se homomorfno preslikava na podgrupu multiplikativne grupe regularnih matrica, generisanu matricama $M$ i $N$ (primetimo: $\langle M, N \rangle = \{\begin{bmatrix} \alpha & k \\ 0 & 1 \end{bmatrix} \mid \alpha \in \{1, -1\}, k \in Z\}$). Matrica $N$ je beskonačnog reda (za $k \in Z$ je $N^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$), pa je i grupa $\mathbf{G}_{(A;P)}$ beskonačna.

Konstatujmo još da je svaka reč u relaciji $\sim_P$ sa jednom od reči $1$, $a$, $b^k$, $ab^m$ ($k, m \in Z \setminus \{0\}$). Jer, $a \sim_P a^{-1}$, a iz $abab \sim_P 1$ sledi $ba \sim_P ab^{-1}$ i $b^{-1}a \sim_P b^{-1}ab^{-1}b \sim_P b^{-1}bab \sim_P ab$ (odatle $b^k a \sim_P ab^{-k}$, $b^{-k}a \sim_P ab^k$). S druge strane, nikoje dve od ovih reči nisu u relaciji $\sim_P$, pošto za $\overline{\varphi}$ imaju različite slike. Prema tome: $G_{(A;P)} = \{[1], [a]\} \cup \{[b^k] \mid k \in Z\} \cup \{[ab^m] \mid m \in Z\}$, a preslikavanje $\theta : G_{(A;P)} \longrightarrow \langle M, N \rangle$ definisano sa $[u]\theta = (u)\overline{\varphi}$ izomorfno je preslikavanje grupe $\mathbf{G}_{(A;P)}$ na grupu $\langle M, N \rangle$.

Primetimo na kraju da smo samu beskonačnost grupe sa datom prezentacijom mogli i direktno izvesti iz činjenice da je svaka dijedarska grupa $\mathbf{D}_n$ ($n = 3, 4, \ldots$) njena homomorfna slika (videti tačku ($e$)); ako je dijedarska grupa $\mathbf{D}_n$ data prezentacijom $(x, y; x^2, y^n, (xy)^2)$, onda je preslikavanje $\psi$ domena grupe $\mathbf{D}_\infty$ u domen grupe $\mathbf{D}_n$ dato sa $([a^k b^r])\psi = [x^k y^{r-[\frac{r}{n}]n}]$, gde je $k \in \{0, 1\}$, $r \in Z$, surjektivni homomorfizam sa jezgrom $\langle [b^n] \rangle$. Pokažimo samo, primera radi, da važi (koristimo isti znak za operaciju u obe grupe):

$$([ab^k] \cdot [ab^r])\psi = ([ab^k ab^r])\psi = ([b^{-k+r}])\psi =$$

$$[y^{-k+r-[\frac{-k+r}{n}]n}] = [y^{(-k-[\frac{-k}{n}]n)+n(r-[\frac{r}{n}]n)}] = [y^{-k-[\frac{-k}{n}]n}] \cdot [y^{r-[\frac{r}{n}]n}] =$$

$$[x] \cdot [xy^{-k-[\frac{-k}{n}]n}x] \cdot [xy^{r-[\frac{r}{n}]n}] = [x] \cdot [y^{(-k-[\frac{-k}{n}]n)\cdot n(n-1)}] \cdot [xy^{r-[\frac{r}{n}]n}] =$$

$$[xy^{k-[\frac{k}{n}]n}] \cdot [xy^{r-[\frac{r}{n}]n}] = ([ab^k])\psi \cdot ([ab^r])\psi.$$



($p$) $(\{a_n \mid n = 1, 2, \ldots\};\ \{a_n \sim a_{n+1}^{n+1} \mid n = 1, 2, 3, \ldots\})$ *je prezentacija aditivne grupe racionalnih brojeva* $\mathbf{Ra}$.

**Dokaz.** Krenimo od preslikavanja $\varphi : A = \{a_n \mid n = 1, 2, \ldots\} \longrightarrow Ra$, gde je $(a_n)\varphi \stackrel{\text{def}}{=} \frac{1}{n!}$. Kako je $\frac{1}{n!} = (n+1)\frac{1}{(n+1)!}$ i kako je grupa $\mathbf{Ra}$ generisana skupom $\{\frac{1}{n!} \mid n = 1, 2, \ldots\}$, to je $\theta : G_{(A;P)} \longrightarrow Ra$ definisano sa $([u])\theta = (u)\overline{\varphi}$ surjektivni homomorfizam. Pokazaćemo i da je injektivan. Lako se izvodi da je $a_i \sim a_{i+k}^{(i+1)(i+2)\ldots(i+k)}$ za $k \geq 2$; posebno, za svako $n$ je $a_1 \sim a_n^{n!}$. Grupa $\mathbf{G}_{(A;P)}$ je, dakle, Abelova. S druge strane, iz $a_1 \sim a_2^2$ sledi $a_1 a_2^{-1} \sim a_2$, tj. $a_2^{-1} \sim a_1^{-1}a_2$. Analogno, $a_2 \sim a_3^3$ daje $a_3^{-1} \sim a_2^{-1}a_3^2$, pa je $a_3^{-1} \sim a_1^{-1}a_2a_3^2$. Indukcijom se lako proverava da je uopšte: $a_n^{-1} \sim a_1^{-1}a_2a_3^2 \ldots a_{n-1}^{n-2}a_n^{n-1}$. Prema dobijenom proizilazi da je svaka reč u relaciji sa reči oblika $a_1^{\alpha_1}a_2^{\alpha_2}\ldots a_n^{\alpha_n}$, gde je $\alpha_1$ ceo broj i $0 \leq \alpha_k < k$ za $1 < k \leq n$. Ako su svi "eksponenti" baš 0, imamo praznu reč; u suprotnom, dakle kad je bar jedan eksponent različit od nule, važi $(a_1^{\alpha_1} \ldots a_n^{\alpha_n})\overline{\varphi} \neq 0$ (jer $\frac{1}{2} + \frac{2}{3!} + \frac{3}{4!} + \cdots + \frac{n-2}{(n-1)!} + \frac{n-1}{n!} = \frac{1}{2} + (\frac{1}{2} - \frac{1}{3!}) + (\frac{1}{3!} - \frac{1}{4!}) + \cdots + (\frac{1}{(n-2)!} - \frac{1}{(n-1)!}) + (\frac{1}{(n-1)!} - \frac{1}{n!}) = 1 - \frac{1}{n!} < 1$). Znači, $\mathbf{Ker}(\theta) = \mathbf{E}$, tj. $\theta$ je injektivno.

($r$) *Za* $p$ *prost broj je*

$$(\{a_n \mid n = 1, 2, \ldots\};\ \{a_1^p\} \cup \{a_{n+1}^p \sim a_n \mid n = 1, 2, \ldots\})$$

*prezentacija Prüferove grupe* $\mathbf{p}^\infty$.

**Dokaz.** Neka je $(a_n)\varphi \stackrel{\text{def}}{=} e^{\frac{2\pi}{p^n}i}$. Kao i u prethodnom slučaju očigledno je da je preslikavanje $\theta$ dato sa $([u])\theta = (u)\overline{\varphi}$ surjektivno homomorfno preslikavanje grupe $\mathbf{G}_{(A;P)}$ na grupu $\mathbf{p}^\infty$. Kako je $a_n \sim a_{n+k}^{p^k}$ za $k \geq 1$, grupa $\mathbf{G}_{(A;P)}$ je Abelova, a zbog $a_n^{p^n} \sim 1$, tj. $a_n^{-1} \sim a_n^{p^n-1} \sim a_1^{p-1}a_2^{p-1}\ldots a_{n-1}^{p-1}a_n^{p-1} \sim a_{n-1}^{-1}a_n^{p-1}$ (koristili smo: $p^n - 1 = (p-1)(p^{n-1} + p^{n-2} + \cdots + p + 1)$ i $a_n^{p^k} \sim a_{n-k}$ za $k < n$), svaka reč je ekvivalentna sa reči oblika

$$a_1^{\alpha_1} \ldots a_n^{\alpha_n} \sim a_n^{\alpha_1 p^{n-1} + \alpha_2 p^{n-2} + \cdots + \alpha_{n-1} p + \alpha_n} \sim a_n^r,$$

gde je $0 \leq \alpha_k < p$, $k = 1, 2, \ldots, n$ i $r$ ostatak pri deljenju $\alpha_1 p^{n-1} + \alpha_2 p^{n-2} + \cdots + \alpha_{n-1} p + \alpha_n$ sa $p^n$. No ponovo je slika ovog elementa za $\overline{\varphi}$ jedinični element Prüferove grupe akko je $\alpha_k = 0$ za svako $k$, $1 \leq k \leq n$; dakle, $\mathbf{Ker}(\theta)$ je jedinična podgrupa grupe $\mathbf{G}_{(A;P)}$.

(*s*) *Neka su, za* $\alpha < c = 2^{\aleph_0}$, $(A_\alpha; P_\alpha)$ *prezentacije aditivne grupe racionalnih brojeva (jedna je data u tački* $(p)$*) i neka je* $A_\alpha \cap A_\beta = \emptyset$ *za* $\alpha < \beta < c$. *Tada je*

$$(\bigcup_{\alpha<c} A_\alpha;\ \bigcup_{\alpha<c} P_\alpha \cup \{a^{-1}b^{-1}ab \mid a \in A_\alpha, b \in A_\beta, \alpha < \beta < c\})$$

*prezentacija aditivne grupe realnih brojeva* – **Re**.

**Dokaz.** U odeljku o Abelovim grupama (33.19) pokazano je da je aditivna grupa realnih brojeva direktna suma kontinuum mnogo aditivnih grupa racionalnih brojeva (preciznije, izomorfna sa jednom takvom direktnom sumom) pa je preostalo samo da se pozovemo na tačku (*i*).□

**Lema 21.11** *Neka je* $(A; P)$, *gde je* $A = \{a_i \mid i \in I\}$ *i* $P = \{u_j \mid j \in J\}$, *prezentacija grupe* $\mathbf{G}$ *za preslikavanje* $\varphi$. *Ako je* $\mathbf{H}$ *normalna podgrupa grupe* $\mathbf{G}$ *generisana skupom (tj. normalno zatvorenje skupa)* $\{(v_k)\overline{\varphi} \mid k \in K\}$, *tada je* $(A;\ P \cup \{v_k \mid k \in K\})$ *prezentacija faktor grupe* $\mathbf{G/H}$ *za preslikavanje* $\overline{\Psi}$, *ekstenziju preslikavanja* $\Psi : A \longrightarrow G/H$ *datog sa* $(a_i)\Psi = (a_i)\varphi H$.

**Dokaz.** Očigledno, za svako $w \in Q = P \cup \{v_k \mid k \in K\}$ imamo: $(w)\overline{\Psi} = (w)\overline{\varphi}H = H$. Prema 21.9(*a*), grupa $\mathbf{G}_{(A;Q)}$ se homomorfno preslikava u (odnosno u ovom slučaju trivijalno *na*) grupu $\mathbf{G/H}$. Jedno surjektivno preslikavanje $\psi \in Hom(\mathbf{G}_{(A;Q)}, \mathbf{G/H})$ je, svakako: $([w])\psi \stackrel{\text{def}}{=} (w)\overline{\varphi}H$ $(= (w)\overline{\Psi})$. Pokažimo da je $\psi$ i injektivno preslikavanje. Neka je $([w])\psi = (w)\overline{\varphi}H = H$, tj. $(w)\overline{\varphi} \in H = \langle\{g^{-1}(v_k)\overline{\varphi}g \mid k \in K, g \in G\}\rangle$. Recimo da je $(w)\overline{\varphi} = ((z_1)\overline{\varphi})^{-1}((v_{k_1})\overline{\varphi})^{\alpha_1}(z_1)\overline{\varphi} \cdot \ldots \cdot ((z_m)\overline{\varphi})^{-1}((v_{k_m})\overline{\varphi})^{\alpha_m}(z_m)\overline{\varphi} = (z_1^{-1}v_{k_1}^{\alpha_1}z_1 \cdot \ldots \cdot z_m^{-1}v_{k_m}^{\alpha_m}z_m)\overline{\varphi}$ (gde su, naravno, $z_1, \ldots, z_m$ reči azbuke $A \cup A^{-1}$ i $\alpha_1, \ldots, \alpha_m \in \{1, -1\}$). Prema tome: $w \sim_P z_1^{-1}v_{k_1}^{\alpha_1}z_1 \cdot \ldots \cdot z_m^{-1}v_{k_m}^{\alpha_m}z_m \sim_Q 1$, stoga i $w \sim_Q 1$, tj. $[w] = [1]$.□

**Korolar 21.12** *Ako je* $\mathbf{H}$ *normalna podgrupa slobodne grupe* $\mathbf{G}_{(A;\emptyset)}$ *generisana skupom elemenata* $\{[u] \mid u \in P\}$, *tada je* $(A; P)$ *prezentacija grupe* $\mathbf{G}_{(A;\emptyset)}/\mathbf{H}$.

**Dokaz.** Direktna posledica prethodne leme. No možemo dati i direktan dokaz.

Za reč $v$ azbuke $A \cup A^{-1}$ važi: $v$ je u relaciji $\sim_P$ sa 1 akko je u relaciji $\sim_\emptyset$ sa proizvodom (u polugrupi $\langle W, \cdot\rangle$) konjugata nekih elemenata iz $P \cup P^{-1}$ ($P^{-1} \stackrel{\text{def}}{=} \{u^{-1} \mid u \in P\}$). Provera je indukcijom po broju koraka, $n$, potrebnih da se reč $v$ svede na praznu reč (korišćenjem trivijalnih odrednica i odrednica



iz $P$). Slučajevi $n = 0, 1$ su trivijalni (ako je $n = 0$, $v$ je prazna reč). Pretpostavimo da je tvrđenje tačno za sve reči koje se u $k$ ($\leq n$) koraka svode na praznu reč i neka je za $v$ potrebno $n + 1$ koraka: $v \equiv v_0, v_1, \ldots, v_{n+1} \equiv 1$. Po induktivnoj hipotezi je $v_1 \sim_\emptyset w_1^{-1}u_{i_1}^{\alpha_1}w_1 \cdot \ldots \cdot w_m^{-1}u_{i_m}^{\alpha_m}w_m$, gde su $w_j$, $j = 1, \ldots, m$, reči azbuke $A \cup A^{-1}$ (neke moguće prazne) i $\alpha_j \in \{1, -1\}$. Diskutujući sve moguće slučajeve kako je $v_1$ dobijeno od $v_0$, zaključujemo da je i $v_0$ u relaciji $\sim_\emptyset$ sa proizvodom konjugata nekih reči iz $P \cup P^{-1}$. Na primer, ako je $v_1$ dobijeno "brisanjem" neke (pod)reči $u$ iz $P$, tada je $v_0 \equiv v_0'uv_0''$, $v_1 = v_0'v_0''$, pa je $v_0 \sim_\emptyset v_0'v_0''(v_0'')^{-1}uv_0'' \sim_\emptyset w_1^{-1}u_{i_1}^{\alpha_1}w_1 \cdot \ldots \cdot w_m^{-1}u_{i_m}^{\alpha_m}w_m \cdot (v_0'')^{-1}uv_0''$. Ako smo pak umetali reč $u$ iz $P$, recimo: $v_0 \equiv v_0'v_0''$ i $v_1 \equiv v_0'uv_0''$, onda je $v_0 \sim_\emptyset v_0'uv_0'' \cdot (v_0'')^{-1}u^{-1}v_0'' \sim_\emptyset w_1^{-1}u_{i_1}^{\alpha_1}w_1 \cdot \ldots \cdot w_m^{-1}u_{i_m}^{\alpha_m}w_m \cdot (v_0'')^{-1}u^{-1}v_0''$. Ostali slučajevi su jednako trivijalni.□

**Korolar 21.13** *Ako je* $B \subseteq A$ *i* $\mathbf{H}$ *normalna podgrupa slobodne grupe* $\mathbf{G}_{(A;\emptyset)}$ *generisana skupom* $\{[b] \mid b \in B\}$, *onda je* $\mathbf{G}_{(A;\emptyset)}/\mathbf{H}$ *slobodna grupa.*

**Definicija 21.14** *Reči* $u$ *i* $v$ *azbuke* $A \cup A^{-1}$ *su slobodno jednake (eng. freely equal) akko je* $u \sim_\emptyset v$, *tj. akko one određuju isti element slobodne grupe* $\mathbf{G}_{(A;\emptyset)}$.

Očigledno, dužine slobodno jednakih reči su iste parnosti; formalni dokaz je indukcijom po broju koraka potrebnih da se reč $u$ svede na reč $v$.

**Primer 21.15** *Neka je* $A = \{a, b\}$. $(a, b;\ P = \{u \mid u$ *je reč parne dužine azbuke* $A \cup A^{-1}\}$*) je prezentacija ciklične grupe reda* 2.

**Dokaz.** Jasno, $H = \{[u] \mid u \in P\}$ je domen normalne podgrupe (slobodne) grupe $\mathbf{G}_{(A;\emptyset)}$ i to indeksa 2. Jedini koseti su $H$ i $[a]H$; jer $[a]H = [b]H = [a^{-1}]H = [b^{-1}]H$, zbog npr. $[b^{-1}a] \in H$.

Primetimo da je $\mathbf{H}$ normalno zatvorenje skupa $\{[a^2], [ab]\}$. Zaista, $ba \sim_\emptyset a^{-1} \cdot ab \cdot a$, $a^{-1}b \sim_\emptyset a^{-2} \cdot ab$, $ba^{-1} \sim_\emptyset a^{-2} \cdot (a(ab)a^{-1})$, $b^2 \sim_\emptyset (a^{-1} \cdot ab \cdot a) \cdot a^{-2} \cdot ab$ itd. S druge strane, $\mathbf{H}$ nije normalna podgrupa generisana jednoelementnim skupom. Jer, neka je $u$ bilo koja reč koja nije slobodno jednaka sa 1. Grupa s prezentacijom $(a, b;\ u, ab \sim ba)$ je beskonačna Abelova grupa. Za neke cele brojeve $m, n$ (od kojih bar jedan nije nula) je $[u] = [a^m b^n]$, te ako je $\psi$ preslikavanje grupe $\mathbf{G}_{(a,b;\, a^{-1}b^{-1}ab,\, a^m b^n)}$ u grupu $\mathbf{Z}$ dato sa $([a])\psi = n$, $([b])\psi = -m$, $(\mathbf{G}_{(a,b;\, a^{-1}b^{-1}ab,\, a^m b^n)})\psi$ je nenula podgrupa grupe $\mathbf{Z}$, dakle beskonačna grupa.□

Na kraju ovog paragrafa osvrnimo se u par reči na neke vrlo poznate i prilično stare probleme kombinatorne teorije grupa. Videli smo da svaka prezentacija određuje jedinstvenu (do na izomorfizam) grupu (21.7). No, na velike teškoće se može naići čim se želi ispitati grupa zadana nekom svojom prezentacijom. Čak i takva pitanja, naizgled laka: *da li je grupa jedinična?*,

*da li je grupa konačna?, da li je grupa Abelova?* itd., mogu predstavljati ozbiljan problem. Utoliko veći, ukoliko zahtevamo da se odgovor dobije nekim determinističkim postupkom u konačno mnogo koraka, drugim rečima, ako zahtevamo egzistenciju algoritma koji će nam ponuditi odgovor. Sam pojam algoritma nije matematički formulisan. Algoritam shvatamo kao uputstvo koje se sastoji od konačno mnogo instrukcija za izvršenje diskretnih, prostih operacija, čija primena kao i izvršenje operacija ne zahteva matematičku ingenioznost (nema komandi tipa: *rešiti problem četiri boje, pa onda ...*), niti bilo šta prepušta slučaju (nema komandi tipa: *baciti dinar, pa ako padne pismo, onda ...*); dakle celu proceduru bi mogao sprovesti i kakav student prava ili medicine. Dati algoritam je primenljiv na bilo koji element mogućeg skupa ulaznih informacija. Jednom unet ulazni podatak podleže obradi prema datim instrukcijama. Prva operacija ga obrađuje, a dobijeni rezultat se podvrgava sledećoj, instrukcijama određenoj operaciji i tako dalje. Sada, ili će se posle konačno mnogo koraka proces, diktiran instrukcijama, zaustaviti i izlazni podatak pročitati (na propisan način) ili jednostavno neće biti poslednjeg koraka, proces će teći u nedogled i nikada se neće dobiti izlazni podatak. Prvi slučaj imamo npr. u proveri, korišćenjem tablica istinitosti, da li je formula propozicionalnog računa tautologija, drugi se može javiti u proveri da li je neka rečenica predikatskog računa teorema. Problem sa neformalnim pristupom pojmu algoritma manifestuje se prevashodno kod "negativnih" rezultata, kada (odgovarajući) traženi algoritam ne postoji. Kod "pozitivnih" rezultata je već lakše. Navodi se adekvatna procedura i ona se "prepoznaje" kao algoritam. U matematici je inače generalno prihvaćena takozvana *Churchova teza* (Alonzo Church, 1903 - 1995):

*sve algoritamske funkcije su rekurzivne.*

O rekurzivnim funkcijama se može konsultovati bilo koji potpuniji udžbenik iz matematičke logike. Postoje inače brojni ekvivalenti rekurzivnih funkcija, a Churchova teza je posledica činjenice da su se u svim pokušajima da se okarakterišu algoritamske funkcije dobijale klase funkcija ekvivalentne bilo klasi bilo podklasi rekurzivnih funkcija. Prema tome, Churchova teza nije matematički dokaziva, jer ni sam pojam algoritma nije matematički precizno definisan; ona jednostavno "kaže" da klasa rekurzivnih funkcija tačno obuhvata pojam algoritamske izračunljivosti i stvar je našeg verovanja. U prilog joj ide da su sve, uslovno rečeno, proste algoritamske funkcije rekurzivne, pa bi algoritamska funkcija koja ne bi bila i rekurzivna, a čija egzistancija je uzgred vrlo malo verovatna, morala biti vrlo komplikovana.

Za datu $n$-arnu relaciju $P \subseteq \omega^n$ kažemo da je *odlučiva* (*rekurzivno odlučiva*) akko postoji totalna algoritamska (rekurzivna) $n$-arna funkcija $f$ takva da je, za svaku $n$-torku brojeva $\overline{a} = (a_0, \ldots, a_{n-1})$, $(\overline{a})f \leq 1$ (u pitanju je tzv. algoritamska, odnosno rekurzivna, $n$-arna relacija) i važi: $\overline{a} \in P$ akko $(\overline{a})f = 0$. $n$-arna relacija je rekurzivno-prebrojiva akko je ili prazan skup ili je prebrojiva nekom $n$-torkom totalnih rekurzivnih unarnih funkcija; posebno, rekurzivno-



prebrojiv skup je rang (kodomen) totalne rekurzivne unarne funkcije. Svaka rekurzivna relacija je i prebrojivo-rekurzivna, ali obrat ne mora da važi. Ali zato važi:

*Relacija je rekurzivna akko su i ona i njen komplement rekurzivno-prebrojive relacije.*

Dalje, o *aritmetičkoj hijerarhiji* nećemo govoriti, već zainteresovanog čitaoca upućujemo na, recimo, [152].

Takozvanim postupkom aritmetizacije rešavanje brojnih problema odlučivosti kod grupa se prevodi na rešavanje adekvatnih problema kod brojevnih funkcija (videti npr. [142] i [152].

Spomenućemo ovde probleme odlučivosti, koje je formulisao Max Dehn 1911. godine (postoje naravno i brojni drugi), a koji se već prema tome da li se tiču prirode elemenata ili grupe u celini dele u dve kategorije i navesti, bez dokaza, neke značajne rezultate. No pre toga još da kažemo da je prezentacija $(A; P)$ rekurzivna akko je $A$ konačan skup i $P$ rekurzivno-prebrojiv.

**Definicija 21.16** *Neka su date grupe* $\mathbf{G}$ *i* $\mathbf{H}$ *sa prezentacijama, respektivno,* $(A; P)$ *i* $(B; Q)$.

*Problem reči je rešiv za grupu* $\mathbf{G}$ *akko postoji algoritam kojim se za bilo koje dve reči azbuke* $A \cup A^{-1}$ *može utvrditi da li određuju isti element grupe, tj. da li su u relaciji* $\sim_P$*, ili, što je ekvivalentno, akko postoji algoritam kojim se za bilo koju reč azbuke* $A \cup A^{-1}$ *može utvrditi da li određuje jedinični element;*

*Problem konjugovanosti je rešiv za grupu* $\mathbf{G}$ *akko postoji algoritam kojim se za bilo koje dve reči azbuke* $A \cup A^{-1}$ *može utvrditi da li određuju konjugovane elemente grupe;*

*Problem izomorfizma je rešiv za grupe* $\mathbf{G}$ *i* $\mathbf{H}$ *akko postoji algoritam kojim se utvrđuje da li su te grupe izomorfne.*

**Napomena**. Svi navedeni problemi odlučivosti su vezani za specifičnu prezentaciju grupe (recimo, kada je o slobodnim grupama reč, po pravilu se podrazumeva da su prezentacije sa praznim skupom odrednica – u vezi sa ovim videti komentar uz lemu 23.2).

Jasno je da ako je problem konjugovanosti rešiv za grupu (sa datom prezentacijom), onda je rešiv i problem reči za tu grupu (obrat već ne važi). Problem izomorfizma je, međutim, najteži.

**Teorema 21.17** *([101], Teorema 4.14). Problem reči je rešiv za grupe sa konačnom prezentacijom koje imaju najviše jednu odrednicu (u slučaju slobodnih grupa imamo 23.4).*

**Teorema 21.18** *([119]). (a) Problem reči je rešiv za klasu rezidualno konačnih grupa; posebno, problem reči je rešiv za klase rešivih slobodnih i nilpotentnih grupa;*

(*b*) *Problem konjugovanosti je rešiv za klasu konjugovano separabilnih grupa (videti donju napomenu); posebno, problem konjugovanosti je rešiv za klasu svih nilpotentnih grupa;*

(*c*) *Problem da li je grupa izomorfna nekoj datoj konačnoj grupi je rešiv s obzirom na klasu konačno prezentovanih grupa sa rešivim problemom reči.*

**Napomena.** O nilpotentnim i rešivim grupama biće reči u četvrtoj glavi.

Grupa $\mathbf{G}$ je *konjugovano separabilna* akko za svaka dva njena elementa $a$ i $b$ koja nisu konjugovana postoji homomorfno preslikavanje, $\varphi$, grupe $\mathbf{G}$ na konačnu grupu, $\mathbf{H}$, takvo da $(a)\varphi$ i $(b)\varphi$ nisu konjugovani elementi u $\mathbf{H}$.

Drugi deo tačke (*b*) proizilazi iz činjenice da je svaka nilpotentna grupa ujedno i konjugovano separabilna (videti [18]).

**Teorema 21.19** *([125], [126]). Postoje grupe sa konačnim prezentacijama za koje su problemi reči i konjugovanosti nerešivi (neodlučivi).*

**Teorema 21.20** *([48]). Postoji grupa sa konačnom prezentacijom za koju je rešiv problem reči, ali ne i problem konjugovanosti.*

**Teorema 21.21** *([28]). Za svaki stepen aritmetičke hijerarhije postoji grupa sa konačnom prezentacijom za koje je problem reči tog stepena nerešivosti.*

**Teorema 21.22** *([2]). Problem izomorfizma je nerešiv za grupe s konačnim prezentacijama, štaviše nerešiv je problem izomorfizma grupa sa konačnim prezentacijama sa jediničnom grupom.*

**Napomena.** Iscrpan dokaz teoreme 21.19 može se naći u [142] (pogledati i [152]). Uopšte, o problemima odlučivosti videti u, recimo, [4], [15], [17], [96], [101] i [139]; [4] i [17] su zbornici radova o problemu reči (vezanom ne samo za teoriju grupa), a u ekspozitornim radovima [15] i [139] može se naći i iscrpan pregled literature na ovu temu (ali i neke druge).

## 22 Tietzeove transformacije

Prirodno se nameće pitanje kada dve prezentacije $(A;P)$ i $(B;Q)$ određuju istu grupu, tj. kada je $\mathbf{G}_{(A;P)} \cong \mathbf{G}_{(B;Q)}$ (u prethodnim primerima razmatrani su samo neki, gotovo očigledni slučajevi – tačke $(j)$ i $(k)$). Pokazaćemo prvo da su ova pitanja ekvivalentna.

Jasno, ako su $(A;P)$ i $(B;Q)$ prezentacije iste grupe – $\mathbf{G}$, onda je $\mathbf{G}_{(A;P)} \cong \mathbf{G} \cong \mathbf{G}_{(B;Q)}$. Opet, ako je $(A;P)$ prezentacija grupe $\mathbf{G}$ za preslikavanje $\varphi$, a $\psi$ je izomorfno preslikavanje grupe $\mathbf{G}_{(B;Q)}$ na grupu $\mathbf{G}_{(A;P)}$, gde je, za $b \in B$, $([b]_Q)\psi = [u_b]_P$ ($u_b$ je reč azbuke $A \cup A^{-1}$), onda je $(B;Q)$ prezentacija grupe $\mathbf{G}$ za preslikavanje $\rho$: $(b)\rho \stackrel{\text{def}}{=} (u_b)\overline{\varphi}$. Jer, ako je $u$ reč azbuke $A \cup A^{-1}$,



preslikavanje $([u]_P)\theta = (u)\overline{\varphi}$, već smo videli, izomorfno je preslikavanje grupe $\mathbf{G}_{(A;P)}$ na grupu $\mathbf{G}$. Kako je $\{[b]_Q \mid b \in B\}$ generatorni skup grupe $\mathbf{G}_{(B;Q)}$, to je i $\{[u_b]_P \mid b \in B\}$ generatorni skup grupe $\mathbf{G}_{(A;P)}$, a $\{([u_b]_P)\theta \mid b \in B\}$, tj. $\{(b)\rho \mid b \in B\}$ je generatorni skup grupe $\mathbf{G}$. Ako je, za $v \in Q$, $[v]_Q = [1]_Q$, onda je $(v)\overline{\rho} = (([v]_Q)\psi)\theta = e_G$; za $v \equiv b_1^{\beta_1} \dots b_k^{\beta_k}$ imali smo:

$$(v)\overline{\rho} = (b_1^{\beta_1} \dots b_k^{\beta_k})\overline{\rho} = ((b_1)\rho)^{\beta_1} \dots ((b_k)\rho)^{\beta_k} = (u_{b_1}^{\beta_1})\overline{\varphi} \dots (u_{b_k}^{\beta_k})\overline{\varphi} =$$

$$([u_{b_1}^{\beta_1}]_P)\theta \dots ([u_{b_k}^{\beta_k}]_P)\theta = ([u_{b_1}^{\beta_1}]_P \dots [u_{b_k}^{\beta_k}]_P)\theta =$$

$$(([b_1^{\beta_1}]_Q)\psi \dots ([b_k^{\beta_k}]_Q)\psi)\theta = (([b_1^{\beta_1}]_Q \dots [b_k^{\beta_k}]_Q)\psi)\theta = (([v]_Q)\psi)\theta.$$

Ako je pak $(v)\overline{\rho} = e_G$, $v \equiv b_1^{\beta_1} \dots b_k^{\beta_k}$, tada je

$$(v)\overline{\rho} = (u_{b_1}^{\beta_1} \dots u_{b_k}^{\beta_k})\overline{\varphi} = ([u_{b_1}^{\beta_1} \dots u_{b_k}^{\beta_k}]_P)\theta = e_G,$$

te je $[u_{b_1}^{\beta_1} \dots u_{b_k}^{\beta_k}]_P = [1]_P$; znači $[b_1^{\beta_1} \dots b_k^{\beta_k}]_Q = [1]_Q$ i $v \sim_Q 1$.

Za odgovor na gore postavljeno pitanje trebaju nam Tietzeove transformacije koje upravo definišemo.

**Definicija 22.1** *Neka je dato $(A;P)$. Sledeće transformacije, koje $(A;P)$ prevode u novu prezentaciju, su Tietzeove:*

*($T_1$) Ako su reči $u_i$, $i \in I$, izvedive iz $P$ proširujemo skup odrednica $P$ skupom $\{u_i \mid i \in I\}$ – tako dobijamo $(A;\ P \cup \{u_i \mid i \in I\})$;*

*($T_2$) Ako su odrednice $u_i \in P$, $i \in I$, izvedive iz $P \setminus \{u_i \mid i \in I\}$ eliminišemo ih – sada imamo $(A;\ P \setminus \{u_i \mid i \in I\})$;*

*($T_3$) Neka su $u_i$, $i \in I$, ma kakve reči iz $W$ i $b_i$, $i \in I$, skup novih simbola ($b_i \notin A$). Proširujemo skup izvodnih simbola $A$ skupom $\{b_i \mid i \in I\}$ i skup odrednica $P$ skupom $\{b_i \sim u_i \mid i \in I\}$. Rezultat je $(A \cup \{b_i \mid i \in I\};\ P \cup \{b_i \sim u_i \mid i \in I\})$;*

*($T_4$) Ako je $a_k \sim u_k \in P$, $k \in I$, i ako se u rečima $u_k$ ne javljaju, kao podreči, reči $a_i$, $a_i^{-1}$, $i \in I$, eliminišemo izvodne simbole $a_i$, odrednice $a_i \sim u_i$, $i \in I$, i u preostalim odrednicama iz $P$ zamenjujemo $a_i^{\alpha}$ sa $u_i^{\alpha}$.*

*Tietzeova transformacija je elementarna akko uvodi (briše) samo jednu odrednicu ili uvodi (briše) samo jedan izvodni simbol i odgovarajuću odrednicu.*

**Lema 22.2** *($T_1$) i ($T_2$) su inverzne transformacije, tj. ako se prezentacija $(B;Q)$ dobija od $(A;P)$ primenom transformacije ($T_1$) (($T_2$)), onda se i $(A;P)$ dobija od $(B;Q)$ primenom transformacije ($T_2$) (($T_1$)).*

*($T_4$) je transformacija inverzna transformaciji ($T_3$). Transformacija inverzna transformaciji ($T_4$) je "kompozicija" transformacija ($T_3$), ($T_1$) i ($T_2$).*

**Dokaz**. Osvrnimo se samo na poslednji deo tvrđenja. Neka je $A = A_1 \cup \{a_i \mid i \in I\}$, $A_1 \cap \{a_i \mid i \in I\} = \emptyset$, $P = Q \cup \{a_i \sim u_i \mid i \in I\}$, gde su $u_i$ reči koje ne sadrže kao podreči reči $a_j$, $a_j^{-1}$, $j \in I$, i neka je $P_1$ skup reči dobijenih od reči iz $Q$ zamenom $a_i^{\alpha}$ sa $u_i^{\alpha}$, $i \in I$. Tada je $(A_1; P_1)$ dobijeno od $(A; P)$ primenom transformacije $(T_4)$. Koristeći $(T_3)$ transformišemo $(A_1; P_1)$ u $(A; P_1 \cup \{a_i \sim u_i \mid i \in I\})$. Dalje, svaka reč iz $Q$ je izvediva iz $P_1 \cup \{a_i \sim u_i \mid i \in I\}$, pa nam $(T_1)$ daje $(A; P_1 \cup \{a_i \sim u_i \mid i \in I\} \cup Q)$. Analogno, svaka reč iz $P_1$ je izvediva iz $Q \cup \{a_i \sim u_i \mid i \in I\}$, te sa $(T_2)$ konačno dobijamo (od poslednje prezentacije) $(A; P)$.□

**Lema 22.3** *Ako je $(A; P)$ prezentacija grupe $\mathbf{G}$ i ako je $(A_1; P_1)$ dobijeno od $(A; P)$ primenom Tietzeovih transformacija onda je i $(A_1; P_1)$ prezentacija grupe $\mathbf{G}$.*

**Dokaz**. Naravno, dovoljno je tvrđenje proveriti za svaku transformaciju ponaosob.

Ako je $(A; P)$ prezentacija grupe $\mathbf{G}$ za preslikavanje $\varphi$ i ako je $(A_1; P_1)$ dobijeno od $(A; P)$ primenom bilo $(T_1)$ bilo $(T_2)$, onda je i $(A_1; P_1)$ $(A = A_1)$ očigledno prezentacija grupe za isto preslikavanje.

Ako je $(A_1; P_1)$ dobijeno pomoću $(T_3)$, $A_1 = A \cup \{b_i \mid i \in I\}$, $P_1 = P \cup \{b_i \sim u_i \mid i \in I\}$, tada je $(A_1; P_1)$ prezentacija grupe $\mathbf{G}$ za preslikavanje $\psi$, gde je $\psi|_A = \varphi$ i $(b_i)\psi = (u_i)\overline{\varphi}$. Zaista, ako je $v$ odrednica $((v)\overline{\psi} = e_G)$, koristeći relacije $b_i \sim u_i$ možemo prvo reč $v$ transformisati u reč $w$ zamenom $b_i^{\alpha}$ sa $u_i^{\alpha}$. Kako je $(v)\overline{\psi} = (w)\overline{\psi} = (w)\overline{\varphi}$ (jer je $(b_i)\overline{\psi} = (u_i)\overline{\psi} = (u_i)\overline{\varphi}$), $w$ je odrednica za prezentaciju $(A; P)$, pa je izvedivo iz $P$, dakle, $v$ je izvedivo iz $P \cup \{b_i \sim u_i \mid i \in I\}$.

Pretpostavimo konačno da je $(A_1; P_1)$ nastalo od $(A; P)$ transformacijom $(T_4)$ (koristimo oznake i pretpostavke iz dokaza prethodne leme: $A = A_1 \cup \{a_i \mid i \in I\}$, $P = Q \cup \{a_i \sim u_i \mid i \in I\}$). $(A_1; P_1)$ je prezentacija grupe $\mathbf{G}$ za preslikavanje $\psi = \varphi|_{A_1}$. $\{(a)\psi \mid a \in A_1\}$ je generatorni skup grupe $\mathbf{G}$, jer je za $a_i$, $i \in I$, $(a_i)\varphi = (u_i)\overline{\psi}$. Ako je $w \in P_1$ dobijeno od $v \in Q$ zamenom $a_i^{\alpha}$ sa $u_i^{\alpha}$, onda je $(w)\overline{\psi} = (v)\overline{\varphi} = e_G$. S druge strane, ako je za reč $v$, azbuke $A_1 \cup A_1^{-1}$, $(v)\overline{\psi} = e_G$, sledi da je $v$ izvedivo iz $P$. Neka je dat niz $v \equiv v_0, v_1, \ldots, v_k \equiv 1$, gde je, za $0 < j \leq k$, $v_j$ nastalo od $v_{j-1}$ umetanjem ili brisanjem bilo trivijalne odrednice bilo reči iz $P$. Zamenjujući u svakoj reči $v_j$ reč $a_i^{\alpha}$ sa $u_i^{\alpha}$, dobijamo niz $v \equiv v_0 \equiv w_0, w_1, \ldots, w_k \equiv 1$. Lako se proverava da ako je $v_j$ nastalo od $v_{j-1}$ umetanjem (brisanjem) trivijalne odrednice ili reči $a_i u_i^{-1}$ $(u_i^{-1} a_i$, $u_i a_i^{-1}$, $a_i^{-1} u_i)$, $w_j$ nastaje od reči $w_{j-1}$ umetanjem (brisanjem) trivijalne odrednice ili reči $u_i u_i^{-1}$ $(u_i^{-1} u_i)$; primetimo: umetanju (brisanju) i trivijalne odrednice $a_i a_i^{-1}$ $(a_i^{-1} a_i)$ i reči $a_i u_i^{-1}$ $(u_i a_i^{-1})$ u reči $v_{j-1}$ odgovara umetanje (brisanje) reči $u_i u_i^{-1}$ $(u_i^{-1} u_i)$ u reči $w_{j-1}$. Ako je $v_j$ nastalo umetanjem (brisanjem) reči $u$ iz $Q$ u $v_{j-1}$, $w_j$ se dobija iz $w_{j-1}$ umetanjem (brisanjem) odgovarajuće reči $u'$ (dobijene od $u$ zamenom $a_i^{\alpha}$ sa $u_i^{\alpha}$) iz $P_1$. Prema tome, $v$ je izvedivo iz $P_1$.□



**Teorema 22.4** *Ako su $(A; P)$ i $(B; Q)$ prezentacije grupe $\mathbf{G}$, tada se $(B; Q)$ može dobiti od $(A; P)$ primenom Tietzeovih transformacija.*

**Dokaz**. Neka je $(A; P)$ prezentacija grupe $\mathbf{G}$ za preslikavanje $\varphi$, $(B; Q)$ za preslikavanje $\psi$ i neka je, za $a \in A$, $(a)\varphi = (v_a)\overline{\psi}$, gde je, treba li to reći, $v_a$ reč azbuke $B \cup B^{-1}$, za $b \in B$, $(b)\psi = (u_b)\overline{\varphi}$, gde je, treba li i to reći, $u_b$ reč azbuke $A \cup A^{-1}$. Primenom $(T_3)$ transformišemo $(A; P)$ u $(A \cup B; P \cup \{b \sim u_b \mid b \in B\})$. Ovo je prezentacija grupe $\mathbf{G}$ za preslikavanje $\rho$: $\rho|_A = \varphi$, $\rho|_B = \psi$ (primetimo samo: $(b)\rho = (b)\psi = (u_b)\overline{\varphi} = (u_b)\overline{\rho}$). Ako je $v \in Q$, onda je $(v)\overline{\rho} = (v)\overline{\psi} = e_G$ i $v$ je izvedivo iz skupa odrednica $P \cup \{b \sim u_b \mid b \in B\}$. Isto tako izvedivo je i $a \sim v_a$ jer je $(a)\rho = (a)\varphi = (v_a)\overline{\psi} = (v_a)\overline{\rho}$. $(T_1)$ nam stoga daje novu prezentaciju (za isto preslikavanje $\rho$) $(A \cup B; P \cup Q \cup \{b \sim u_b \mid b \in B\} \cup \{a \sim v_a \mid a \in A\})$. Po simetriji stvari do ove prezentacije se može stići Tietzeovim transformacijama i ako se pođe od $(B; Q)$. Odatle sledi, prema 22.2, da se $(A; P)$ može Tietzeovim transformacijama prevesti u $(B; Q)$.■

**Korolar 22.5** *Ako su prezentacije $(A; P)$ i $(B; Q)$ grupe $\mathbf{G}$ konačne, $(A; P)$ se transformiše u $(B; Q)$ pomoću konačno mnogo elementarnih Tietzeovih transformacija.*

**Primer 22.6** $(a)$ $(b, c; b^m, c^n, bc \sim cb)$, *gde je $(m, n) = 1$, prezentacija je ciklične grupe reda $mn$.*

**Dokaz**. Ovo nam je već poznato (videti 21.10($i$)). Dokaz ovog puta dajemo prevodeći (Tietzeovim transformacijama) poznatu (očiglednu) prezentaciju ciklične grupe reda $mn$, $(a; a^{mn})$, u datu. Tako redom imamo niz prezentacija (svaka je dobijena od prethodne primenom Tietzeove transformacije date sa strane – dokaze detalja ili detalje dokaza, po volji, ostavljamo kao laku vežbu):

$(a; a^{mn})$

$(T_3)$ $(a, b, c; a^{mn}, b \sim a^n, c \sim a^m)$

$(T_1)$ $(a, b, c; a^{mn}, b \sim a^n, c \sim a^m, b^m, c^n, bc \sim cb, a \sim b^v c^u)$ ($u$ i $v$ su celi brojevi takvi da je $um + vn = 1$)

$(T_2)$ $(a, b, c; b \sim a^n, c \sim a^m, b^m, c^n, bc \sim cb, a \sim b^v c^u)$

$(T_4)$ $(b, c; b \sim (b^v c^u)^n, c \sim (b^v c^u)^m, b^m, c^n, bc \sim cb)$

$(T_2)$ $(b, c; b^m, c^n, bc \sim cb)$.

$(b)$ *Prezentacije $(a, b; a^3, b^2, ab \sim ba^2)$ i $(c, d; c^2, d^2, (cd)^3)$ određuju istu grupu.*

**Dokaz**. Imamo redom:

$(a, b; a^3, b^2, ab \sim ba^2)$

$(T_3)$ $(a, b, c, d; a^3, b^2, ab \sim ba^2, c \sim b, d \sim ab)$

$(T_1)$ $(a, b, c, d; a^3, b^2, ab \sim ba^2, c \sim b, d \sim ab, c^2, d^2, (cd)^3, a \sim dc)$

(koristimo: $d^2 \sim (ab)^2 \equiv abab \sim 1$, zbog $ab \sim ba^2 \implies aba \sim ba^3 \sim b \implies abab \sim b^2 \sim 1$; $(cd)^3 \sim (bab)^3 \equiv babbabbab \sim ba^3b \sim b^2 \sim 1$; $d \sim ab \implies db \sim ab^2 \sim a \implies dc \sim a$)

$(T_2)$ $(a, b, c, d;\ c \sim b,\ d \sim ab,\ c^2,\ d^2,\ (cd)^3, a \sim dc)$

(imamo: $a^3 \sim (dc)^3 \equiv dcdcdc \sim dcdcdcdd \equiv d(cd)^3d \sim d^2 \sim 1$; $ab \sim d \sim (cd)^3d \equiv cdcdcdd \equiv c(dc)^2d^2 \sim ba^2d^2 \sim ba^2$)

$(T_4)$ $(c, d;\ c^2,\ d^2,\ (cd)^3,\ d \sim dc^2)$

$(T_2)$ $(c, d;\ c^2,\ d^2,\ (cd)^3)$.□

**Lema 22.7** *Ako je $|A| > |P|$, grupa $\mathbf{G}_{(A;P)}$ je beskonačna; posebno, ima element beskonačnog reda.*

**Dokaz**. Ako su $A$ i $P$ beskonačni skupovi ili ako je $A$ beskonačan i $P$ konačan skup, imamo element u $A$, recimo $a$, koji se ne javlja ni u jednoj reči iz $P$. Za preslikavanje $\varphi : A \longrightarrow Z$, gde je $(a)\varphi = 1$ i $(b)\varphi = 0$ za $b \in A \setminus \{a\}$, postoji homomorfno preslikavanje $\theta$ grupe $\mathbf{G}_{(A;P)}$ u grupu $\mathbf{Z}$ ($[u])\theta = (u)\overline{\varphi}$). $\theta$ je, jasno, surjektivno preslikavanje pa je grupa $\mathbf{G}_{(A;P)}$ beskonačna. Zapravo s malo volje lako se pokazuje da je u svim ovim slučajevima $|G_{(A;P)}| = |A|$.

Situacija je nešto složenija ako su $A$ i $P$ konačni skupovi. Uzmimo da je $A = \{a_1, \ldots, a_n\}$, $P = \{u_1, \ldots, u_m\}$, $n > m$, i neka je $\alpha_{ij}$ suma eksponenata elementa $a_i$ u reči $u_j$ (npr. ako je $u_j \equiv a_i a_k a_i^{-2} a_l$, onda je $\alpha_{ij} = -1$). Posmatrajmo sada homogeni sistem linearnih jednačina:

$$\alpha_{11}x_1 + \alpha_{21}x_2 + \cdots + \alpha_{n1}x_n = 0$$

$$\vdots$$

$$\alpha_{1m}x_1 + \alpha_{2m}x_2 + \cdots + \alpha_{nm}x_n = 0.$$

Kako je broj nepoznatih veći od broja jednačina i kako su svi koeficijenti $\alpha_{ij}$, $1 \le i \le n$, $1 \le j \le m$, celi brojevi, sistem ima netrivijalno rešenje $(k_1, \ldots, k_n)$, gde su $k_i$, $1 \le i \le n$, celi brojevi i bar jedan od njih je različit od 0 (ustvari znamo da takvih rešenja ima beskonačno mnogo). Sada za preslikavanje $\varphi : A \longrightarrow Z$, gde je $(a_i)\varphi = k_i$, $i = 1, \ldots, n$, imamo, s obzirom da je $\mathbf{Z}$ Abelova grupa, $(u_j)\overline{\varphi} = \alpha_{1j}k_1 + \alpha_{2j}k_2 + \cdots + \alpha_{nj}k_n = 0$. Znači, opet se $\mathbf{G}_{(A;P)}$ homomorfno preslikava u grupu $\mathbf{Z}$, a kako je bar jedno $k_i \neq 0$, ta slika je nenula podgrupa.

Iz gore datih primera se vidi da se samo iz činjenice $|A| \le |P|$ ne može ništa zaključiti o tome da li je grupa $\mathbf{G}_{(A;P)}$ konačna ili beskonačna.□

## 23 Slobodne grupe

Već smo definisali slobodne grupe i konstatovali da je svaka grupa homomorfna slika neke slobodne grupe. Pre nego što pređemo na ispitivanje nekih



elementarnih svojstava slobodnih grupa, ukazaćemo na još jednog tipičnog predstavnika grupa s prezentacijom $(A; \emptyset)$ (pored grupe $\mathbf{G}_{(A;\emptyset)}$ klase ekivalencija). No prvo uvedimo neke nove pojmove.

**Definicija 23.1** *Reč azbuke $A \cup A^{-1}$ je slobodno reducirana akko se nijedna trivijalna odrednica $(aa^{-1},\ a^{-1}a)$ ne javlja kao njena podreč.*

*Reč $u \equiv a_{i_1}^{\alpha_1} \ldots a_{i_k}^{\alpha_k}$, $\alpha_i \in \{1, -1\}$, ciklično je reducirana akko je slobodno reducirana i ako je ili $i_1 \neq i_k$ ili $i_1 = i_k$ i $\alpha_1 = \alpha_k$.*

Prazna reč, $a_{i_1}^2 a_{i_2}^{-1} a_{i_1}^{-1}$, $a_{i_1} a_{i_2}^{-2} a_{i_1} a_{i_3}$ $(i_1 \neq i_2)$ su primeri slobodno reduciranih reči. Prva i treća reč su ujedno i ciklično reducirane.

Uočimo: reč je ciklično reducirana akko je svaka njena ciklična permutacija (21.10($k$)) slobodno reducirana.

**Lema 23.2** *Svaki element grupe $\mathbf{G}_{(A;\emptyset)}$ određen je jedinstvenom slobodno reduciranom reči (azbuke $A \cup A^{-1}$).*

**Dokaz**. Definišimo, po dužini reči, preslikavanje $\rho$ skupa reči $W$ (nad azbukom $A \cup A^{-1}$) u sebe na sledeći način:

$$(1)\rho = 1,$$

$$(a^\alpha)\rho = a^\alpha$$

i ako je $(u)\rho = a_{i_1}^{\alpha_1} \ldots a_{i_k}^{\alpha_k}$, tada je

$$(ua_{i_{k+1}}^{\alpha_{k+1}})\rho = \begin{cases} a_{i_1}^{\alpha_1} \ldots a_{i_{k-1}}^{\alpha_{k-1}} & \text{ako je } i_k = i_{k+1} \text{ i } \alpha_k + \alpha_{k+1} = 0 \\ a_{i_1}^{\alpha_1} \ldots a_{i_k}^{\alpha_k} a_{i_{k+1}}^{\alpha_{k+1}} & \text{inače} \end{cases};$$

naravno, pretpostavljamo $a_{i_1}^{\alpha_1} \ldots a_{i_{k-1}}^{\alpha_{k-1}} \equiv 1$ ako je $k = 1$.

Preslikavanje $\rho$ karakterišu (između ostalih) sledeća svojstva:

$(a)$ $(u)\rho$ je slobodno reducirana reč;

$(b)$ $(u)\rho \sim_\emptyset u$;

$(c)$ ako je $u$ slobodno reducirana reč, tada je $(u)\rho = u$;

$(d)$ $(ua_i^\alpha a_i^{-\alpha})\rho = (u)\rho$, $\alpha \in \{1, -1\}$;

$(e)$ (I) $(u \cdot v)\rho = ((u)\rho \cdot v)\rho$; (II) $(u \cdot v)\rho = (u \cdot (v)\rho)\rho$; (III) $(u \cdot v)\rho = ((u)\rho \cdot (v)\rho)\rho$;

$(f)$ $(ua_i^\alpha a_i^{-\alpha} v)\rho = (uv)\rho$, $\alpha \in \{1, -1\}$;

$(g)$ $u \sim_\emptyset v$ akko je $(u)\rho = (v)\rho$; posebno, ako su $u$ i $v$ reducirane reči i $u \sim_\emptyset v$, onda je $u \equiv v$.

Prve četiri tačke se dokazuju indukcijom po dužini reči $u$, $(e)$ indukcijom po dužini reči $v$ (ili $u$), a $(f)$ je neposredna posledica tačaka $(d)$ i $(e)$. Pretpostavimo da su tačke $(a)$, $(b)$ i $(c)$ već proverene, pa se, vežbe radi, osvrnimo na tačke $(d)$, $(e)$ i $(g)$.

($d$) Trivijalno, $(1a_i^{\alpha}a_i^{-\alpha})\rho = (1)\rho = 1$. Neka je tvrđenje tačno za reči dužine manje od ili jednake $n$ i neka je $u \equiv va_j^{\alpha_j}$, gde je $l(v) = n$ i $(v)\rho = a_{i_1}^{\alpha_1} \dots a_{i_k}^{\alpha_k}$. Ako je $j = i$ i $\alpha_j + \alpha = 0$, po induktivnoj pretpostavci je $(ua_i^{\alpha})\rho = (va_j^{\alpha_j}a_i^{\alpha})\rho = (va_i^{-\alpha}a_i^{\alpha})\rho = (v)\rho$, pa je

$$(ua_i^{\alpha}a_i^{-\alpha})\rho = \begin{cases} a_{i_1}^{\alpha_1} \dots a_{i_{k-1}}^{\alpha_{k-1}} & \text{ako je } i_k = i,\ \alpha_k = \alpha \\ a_{i_1}^{\alpha_1} \dots a_{i_k}^{\alpha_k}a_i^{-\alpha} & \text{inače} \end{cases} = (va_i^{-\alpha})\rho = (u)\rho.$$

Uzmimo sada da je bilo $j \neq i$ bilo $\alpha_j + \alpha \neq 0$. Ako je $i_k = j$ i $\alpha_k + \alpha_j = 0$, tada je $(u)\rho = a_{i_1}^{\alpha_1} \dots a_{i_{k-1}}^{\alpha_{k-1}}$ i

$$(ua_i^{\alpha})\rho = \begin{cases} a_{i_1}^{\alpha_1} \dots a_{i_{k-2}}^{\alpha_{k-2}} & \text{ako je } i_{k-1} = i \text{ i } \alpha_{k-1} = -\alpha \\ a_{i_1}^{\alpha_1} \dots a_{i_{k-1}}^{\alpha_{k-1}}a_i^{\alpha} & \text{inače} \end{cases},$$

te je, u svakom slučaju, $(ua_i^{\alpha}a_i^{-\alpha})\rho = (u)\rho$ (koristili smo da je $(v)\rho$ slobodno reducirana reč).

Ako je $i_k \neq j$ ili $\alpha_k + \alpha_j \neq 0$, onda je $(u)\rho = a_{i_1}^{\alpha_1} \dots a_{i_k}^{\alpha_k}a_j^{\alpha_j}$, $(ua_i^{\alpha})\rho = a_{i_1}^{\alpha_1} \dots a_{i_k}^{\alpha_k}a_j^{\alpha_j}a_i^{\alpha}$ i $(ua_i^{\alpha}a_i^{-\alpha})\rho = a_{i_1}^{\alpha_1} \dots a_{i_k}^{\alpha_k}a_j^{\alpha_j} = (u)\rho$.

($e$) (I) Indukcijom po dužini reči $v$. Ako je $v$ prazna reč, prema ($a$) i ($c$) je $(u \cdot 1)\rho = (u)\rho = ((u)\rho)\rho = ((u)\rho \cdot 1)\rho$. Opet, ako je $u$ reč proizvoljne dužine, prema definiciji preslikavanja $\rho$ i činjenici da je $((u)\rho)\rho = (u)\rho$ neposredno sledi (za $\alpha \in \{1, -1\}$): $(ua^{\alpha})\rho = ((u)\rho a^{\alpha})\rho$, a uz pretpostavku da je tvrđenje tačno za sve reči $v$ dužine manje od ili jednake $n$ ($n \geq 1$), za $v \equiv wa^{\alpha}$, $l(w) = n$, imamo: $(u \cdot v)\rho = ((u \cdot w) \cdot a^{\alpha})\rho = ((u \cdot w)\rho \cdot a^{\alpha})\rho = (((u)\rho \cdot w) \cdot a^{\alpha})\rho = ((u)\rho \cdot wa^{\alpha})\rho = ((u)\rho \cdot v)\rho$.

(II) Sada koristimo indukciju po dužini reči $u$.

Opet trivijalno $(1 \cdot v)\rho = (v)\rho = ((v)\rho)\rho = (1 \cdot (v)\rho)\rho$. Indukcijom po dužini reči $v$ dokazujemo da je $(a_i^{\alpha_i}v)\rho = (a_i^{\alpha_i}(v)\rho)\rho$. Slučaj $v \equiv 1$ (tj. $l(v) = 0$) je jasan, a uz induktivnu pretpostavku da je jednakost tačna za reči dužine manje od ili jednake $n$ i na osnovu prethodno dokazanog proizilazi za $v \equiv wa_j^{\alpha_j}$, $l(w) = n$, $\alpha_j \in \{1, -1\}$:

$$(a_i^{\alpha_i} \cdot wa_j^{\alpha_j})\rho = ((a_i^{\alpha_i}w)\rho\, a_j^{\alpha_j})\rho = ((a_i^{\alpha_i}(w)\rho)a_j^{\alpha_j})\rho =$$

$$(a_i^{\alpha_i}(wa_j^{\alpha_j})\rho)\rho = (a_i^{\alpha_i}(v)\rho)\rho.$$

Konačno, uz hipotezu da je (II) tačno za reči $u$ dužine manje od ili jednake $n$, ako je $l(w) = n$ i $u \equiv a^{\alpha}w$, dobijamo:

$$(u \cdot v)\rho = (a^{\alpha}wv)\rho = (a^{\alpha}(wv)\rho)\rho = (a^{\alpha}(w(v)\rho))\rho =$$

$$((a^{\alpha}w)(v)\rho)\rho = (u \cdot (v)\rho)\rho.$$

($g$) Ako je $u \sim_{\emptyset} v$, postoji niz $u \equiv u_0, \dots, u_n \equiv v$ takav da se $u_i$ dobija od $u_{i-1}$ bilo umetanjem bilo brisanjem trivijalne odrednice. U svakom slučaju je, prema ($f$), $(u_{i-1})\rho = (u_i)\rho$.



S druge strane, ako je $(u)\rho = (v)\rho$, prema ($b$) je $u \sim_{\emptyset} (u)\rho = (v)\rho \sim_{\emptyset} v$.

Zaključujemo, prema tome, da svaka klasa ekvivalencije $[u]_{\emptyset}$ relacije $\sim_{\emptyset}$ (tj. svaki element grupe $\mathbf{G}_{(A;\emptyset)}$) sadrži tačno jednu reduciranu reč – $(u)\rho$. Ovo nam omogućava da kao tipičnog predstavnika slobodne grupe sa prezentacijom $(A;\emptyset)$ uzmemo i grupu slobodno reduciranih reči čiji je domen skup slobodno reduciranih reči (azbuke $A \cup A^{-1}$) $\{(u)\rho \mid u \in W\}$, a množenje, u oznaci $\bullet$, definisano je na sledeći način: $(u)\rho \bullet (v)\rho = (u \cdot v)\rho$.

Tačka ($g$) i svojstvo kongruentnosti relacije $\sim_{\emptyset}$ garantuju dobru definisanost operacije $\bullet$ (tj. njenu nezavisnost od izbora predstavnika):

ako je $(u)\rho = (u_1)\rho$ i $(v)\rho = (v_1)\rho$, onda je $u \sim_{\emptyset} u_1$, $v \sim_{\emptyset} v_1$, pa je i $u \cdot v \sim_{\emptyset} u_1 \cdot v_1$, stoga i $(u \cdot v)\rho = (u_1 \cdot v_1)\rho$.

Asocijativnost važi očigledno:

$$(u)\rho \bullet ((v)\rho \bullet (w)\rho) = (u)\rho \bullet (v \cdot w)\rho = (u \cdot (v \cdot w))\rho =$$

$$((u \cdot v) \cdot w)\rho = (u \cdot v)\rho \bullet (w)\rho = ((u)\rho \bullet (v)\rho) \bullet (w)\rho,$$

$1 = (1)\rho$ je neutralni element, a $((u)\rho)^{-1} = (u^{-1})\rho$.

Mogli smo i odmah konstatovati da je preslikavanje $\overline{\rho} : [u] \longrightarrow (u)\rho$ izomorfno preslikavanje grupe $\mathbf{G}_{(A;\emptyset)}$ na grupoid $\langle \{(u)\rho \mid u \in W\}, \bullet \rangle$ (to čini izlišnim proveru asocijativnosti i egzistencije neutralnog i inverznih elemenata). Dobra definisanost i injektivnost su posledica tačke ($g$), surjektivnost je očigledna (možemo se pozvati i na tačke ($a$) i ($c$): $([(u)\rho]\overline{\rho} = ((u)\rho)\rho = (u)\rho$), a i svojstvo homomorfnosti direktno sledi:

$$([u] \circ [v])\overline{\rho} = ([u \cdot v])\overline{\rho} = (u \cdot v)\rho = (u)\rho \bullet (v)\rho = ([u])\overline{\rho} \bullet ([v])\overline{\rho}.\square$$

Navedene slobodne grupe ćemo u narednim tvrđenjima ravnopravno koristiti, i kad nije neophodno da se naglasi o kojoj od njih je reč, obeležavaćemo ih jednostavno sa $\mathbf{F}_A$ ($\mathbf{F}$ od engleske reči *free* = slobodan). Indeks $A$ nam kaže da se radi o grupama sa prezentacijom $(A;\emptyset)$ – ovde, napomenimo, podrazumevamo da je skup (netrivijalnih) odrednica prazan. Jer, u prezentaciji slobodne grupe skup odrednica ne mora biti prazan. Tako je npr. i

$$\langle a, b, c;\ a^2b(ac)^2ab \rangle$$

prezentacija slobodne grupe. Pokazaćemo to koristeći se Tietzeovim transformacijama:

$(a, b, c;\ a^2b(ac)^2ab)$

($T_3$) $(a, b, c, x, y;\ x \sim ab, y \sim ac, a^2b(ac)^2ab)$

($T_1$) $(a, b, c, x, y;\ x \sim ab, y \sim ac, a \sim (ab)^{-1}(ac)^{-2}(ab)^{-1}, a^2b(ac)^2ab,$
$a \sim x^{-1}y^{-2}x^{-1}, b \sim xy^2x^2, c \sim xy^2xy)$

($T_2$) $(a, b, c, x, y;\ a \sim x^{-1}y^{-2}x^{-1}, b \sim xy^2x^2, c \sim xy^2xy)$

($T_4$) $(x, y;\ \emptyset)$.

Važi, zapravo, da svaka slobodna grupa ima i prezentaciju sa nepraznim skupom odrednica. Tako je na primer, da uzmemo najtrivijalni slučaj, $(A \cup B;\ B)$, gde je $A \cap B = \emptyset$, prezentacija slobodne grupe $\mathbf{F}_A$.

U opštem ne postoji algoritam koji bi nam omogućio da za svaku zadanu prezentaciju, čak ni konačnu, odredimo da li se radi o slobodnoj grupi ili ne.

**Lema 23.3** *Neka je $\mathbf{F}_A$ slobodna grupa slobodno reduciranih reči (nad azbukom $A \cup A^{-1}$). Tada važi:*

*(a) $\mathbf{F}_A$ je torziono slobodna;*

*(b) Ako je $|A| > 1$, grupa $\mathbf{F}_A$ je bez centra; ako je $|A| = 1$, onda je $\mathbf{F}_A$ beskonačna ciklična grupa;*

*(c) Neka je $u \equiv a_i^{\alpha} u_1$, $v \equiv v_1 a_j^{\beta}$, $\alpha, \beta \in \{1, -1\}$. Ako je $u \neq w_1 v^{-1}$ i $v \neq u^{-1} w_2$ ($w_1 v^{-1}$, $u^{-1} w_2$ su slobodno reducirane reči), onda $u \bullet v$ počinje sa $a_1^{\alpha}$ i završava sa $a_j^{\beta}$.*

*(d) Neka su $u$ i $v$ elementi grupe $\mathbf{F}_A$. Tada $u^n = v^n$, $n \in Z \setminus \{0\}$, implicira $u = v$; $u^m \bullet v^n = v^n \bullet u^m$ implicira $u \bullet v = v \bullet u$, a ako je $u \bullet v = v \bullet u$, onda su $u$ i $v$ stepeni (za neke cele brojeve) iste reči;*

*(e) Svaki nejedinični element iz $F_A$ ima najviše konačno mnogo korena; (Definicija: neka je $n$ ceo broj; u grupi $\mathbf{G}$ element $b$ je $n$-ti koren elementa $a$ akko je $a = b^n$.)*

*(f) Ako jednačina $u = x^n$ ima rešenje za svaki pozitivan prirodan broj $n$, onda je $u$ jedinični element;*

*(g) Centralizator svakog nejediničnog elementa je ciklična grupa;*

*(h) $\mathbf{F}_A$ ima svojstvo konačnosti rezidualno – kažemo i da je rezidualno konačna;*

*(i) Presek svih podgrupa konačnog indeksa grupe $\mathbf{F}_A$ je jedinična grupa;*

*(j) $\mathbf{F}_A$ je podgrupa kartezijanskog proizvoda odgovarajućeg skupa konačnih grupa.*

*(k) Elementi (slobodno reducirane reči) $u^{-1} v u$ i $x^{-1} y x$, gde su $v$ i $y$ ciklično reducirane reči, konjugovani su akko je $y$ ciklična permutacija reči $v$.*

**Dokaz.** $(a)$ Svaki nejedinični element, $u$, iz $F_A$, tj. svaka neprazna slobodno reducirana reč azbuke $A \cup A^{-1}$, oblika je $v^{-1} w v$, gde je $w$ nejedinična ciklično reducirana reč (dok $v$ eventualno može biti i 1). Prema tački $(f)$ prethodne leme i definiciji operacije $\bullet$ imamo:

$$u \bullet u = v^{-1} w v \bullet v^{-1} w v = (v^{-1} w v \cdot v^{-1} w v)\rho = (v^{-1} w^2 v)\rho = v^{-1} w^2 v$$

(za samu ciklično reduciranu reč $w$ važi: $w \bullet w = (w \cdot w)\rho = ww = w^2$, jer ako je $w \equiv a_{i_1}^{\alpha_1} \ldots a_{i_k}^{\alpha_k}$, $\alpha_j \in \{1, -1\}$ i $k > 1$, onda je ili $i_1 \neq i_k$ ili $\alpha_1 = \alpha_k$) i



uopšte:

$$u^n = \underbrace{u \bullet \cdots \bullet u}_{n-puta} = v^{-1} w v \bullet \cdots \bullet v^{-1} w v = v^{-1} w^n v \neq 1.$$

Uočimo još da je $l(u^n) = 2l(v) + nl(w)$, gde, kao i u polugrupi reči $\mathbf{W}$, $l(u)$ označava dužinu reči $u$. Naravno, u grupi slobodno reduciranih reči $\mathbf{F}_A$ dužina proizvoda reči nije nužno zbir dužina tih reči. Napominjemo još, za svaki slučaj, da kada govorimo o stepenu neke reči mora se znati, a to će biti jasno iz konteksta, da li se radi o stepenu u polugrupi $\mathbf{W}$ (gde smo jednostavno dopisivali reči) ili u grupi $\mathbf{F}_A$.

$(b)$ Neka je $|A| > 1$ i neka je $u \equiv a_{i_1}^{\alpha_1} \ldots a_{i_k}^{\alpha_k}$, $\alpha_j \in \{1, -1\}$, $j = 1, \ldots, k$. Ako je $a \in A \setminus \{a_{i_1}\}$, tada je $a \bullet u = a a_{i_1}^{\alpha_1} \ldots a_{i_k}^{\alpha_k}$, dok je $u \bullet a = (ua)\rho$ ili $a_{i_1}^{\alpha_1} \ldots a_{i_k}^{\alpha_k} a$ ili $a_{i_1}^{\alpha_1} \ldots a_{i_{k-1}}^{\alpha_{k-1}}$, ukoliko je $\alpha_k = -1$ i $a_{i_k} = a$ ( u tom slučaju je, jasno, $k > 1$ jer $a \neq a_{i_1}$ ), no svakako je $a \bullet u \neq u \bullet a$, jer "proizvodi" počinju različitim slovima – u drugom slučaju su i različite dužine.

$(c)$ Dokaz je indukcijom po zbiru dužina reči $u$ i $v$. Slučaj $l(u) + l(v) = 2$ je jasan, kao i uopšte slučaj kad je $u \bullet v = uv$. Uzmimo stoga da je $u = u_2 a^{\gamma}$, $v = a^{-\gamma} v_2$, $\gamma \in \{1, -1\}$. S obzirom na pretpostavke isključeno je da je bilo koja od reči $u_2$, $v_2$ prazna reč (dakle, $u_2$ počinje sa $a_i^{\alpha}$, $v_2$ se završava sa $a_j^{\beta}$) kao i da je $u_2$ oblika $w v_2^{-1}$ ili da je $v_2$ oblika $u_2^{-1} w$, pa tvrđenje sledi iz induktivne pretpostavke i činjenice da je $u \bullet v = u_2 \bullet v_2$.

$(d)$ Neka je $u^n = v^n$. Pretpostavićemo $n > 0$ (ovo, naravno, ne utiče na opštost razmatranja; u slučaju $n < 0$ posmatrali bismo jednostavno stepene elemenata $u^{-1}$ i $v^{-1}$). Prema $(a)$ ili su i $u$ i $v$ jedinični elementi ili su oba nejedinična. Takođe, videli smo u dokazu iste tačke, ili su oba elementa ciklično reducirana ili to nije nijedan od njih. Ako su i $u$ i $v$ ciklično reducirane reči, onda očigledno iz $u^n = v^n$ sledi $u = v$. Pretpostavimo zato da je $u = u_1^{-1} u_2 u_1$, $v = v_1^{-1} v_2 v_1$, gde je $u_1, v_1 \neq 1$. No kako je $u^n = u_1^{-1} u_2^n u_1 = v_1^{-1} v_2^n v_1 = v^n$, mora biti $u_1 = v_1$, a onda i $u_2 = v_2$, u suprotnom bismo nakon "skraćivanja" dobili jednakost ciklično reducirane reči i reči koja to nije; npr. ako bi bilo $u_1 \equiv a_{i_1}^{\alpha_1} \ldots a_{i_k}^{\alpha_k}$, $v_1 \equiv a_{j_1}^{\beta_1} \ldots a_{j_m}^{\beta_m}$ i $k > m$, $a_{i_k}^{\alpha_k} = a_{j_m}^{\beta_m}, \ldots, a_{i_{k-m+1}}^{\alpha_{k-m+1}} = a_{j_1}^{\beta_1}$, sledilo bi $a_{i_{k-m}}^{-\alpha_{k-m}} \ldots a_{i_1}^{-\alpha_1} u_2^n a_{i_1}^{\alpha_1} \ldots a_{i_{k-m}}^{\alpha_{k-m}} = v_2^n$.

Neka je sada $u^m \bullet v^n = v^n \bullet u^m$. Onda, zbog $v^n = u^{-m} \bullet v^n \bullet u^m = (u^{-m} \bullet v \bullet u^m)^n$, imamo $v = u^{-m} \bullet v \bullet u^m$, i odatle $v^{-1} \bullet u^m \bullet v = (v^{-1} \bullet u \bullet v)^m = u^m$, te je $v^{-1} \bullet u \bullet v = u$, odnosno $u \bullet v = v \bullet u$.

Pokažimo na kraju da iz $u \bullet v = v \bullet u$ sledi da su $u$ i $v$ stepeni iste reči. Dokaz je indukcijom po zbiru dužina reči $u$ i $v$. Trivijalno, za $l(u) + l(v) = 0$ imamo $u = v = 1$. Pretpostavimo stoga da su $u$ i $v$ neprazne reči i neka je $l(u) \leq l(v)$. Ako je $u \equiv u_1 a_i^{\alpha}$, $v \equiv a_j^{\beta} v_1$, $\alpha, \beta \in \{1, -1\}$ (gde su $u_1$ i $v_1$ ili samo $u_1$ eventualno prazna reč) i ili $i \neq j$ ili $\alpha = \beta$, onda je $u \bullet v = uv$, pa mora biti i $v \bullet u = vu$ (u suprotnom bismo imali $l(v \bullet u) < l(u \bullet v)$). Zbog $l(u) \leq l(v)$ proizilazi da je $u$ početni segment reči $v$, dakle, za neko $v_2$ (koje

može biti i 1) $v \equiv uv_2$. Prema tome je $uv = uuv_2 = vu = uv_2u$, tj. $uv_2 = v_2u$, odnosno $u \bullet v_2 = v_2 \bullet u$. Po induktivnoj pretpostavci je, za neko $w \in F_A$ i neke cele brojeve $m, n$, $u = w^m$, $v_2 = w^n$, te je i $v \equiv uv_2$ stepen reči $w$.

Uzmimo dalje da je $u$ ciklično reducirana reč i da je $i = j$, $\alpha + \beta = 0$. Onda $u \bullet v = (u_1 a_i^\alpha \cdot a_i^{-\alpha} v_1)\rho = (u_1 \cdot v_1)\rho = u_1 \bullet v_1$. Ako je $u_1 = v_1 = 1$, direktno dobijamo $v = u^{-1}$. Ako je samo $u_1 = 1$ (imamo u vidu pretpostavku $l(u) \leq l(v)$), tada je $u \bullet v = a_i^\alpha \bullet a_i^{-\alpha} v_1 = v_1 = a_i^{-\alpha} v_1 \bullet a_i^\alpha$, znači $v_1 \bullet a_i^{-\alpha} = a_i^{-\alpha} v_1 = a_i^{-\alpha} \bullet v_1$, te je po induktivnoj pretpostavci $v_1$, a onda i $v$, stepen od $a_i$ (prema prethodnim razmatranjima, a i inače, lako se izvodi da iz $a^\alpha = w^n$, $\alpha \in \{1, -1\}$, $n$ prirodan broj, sledi $n = 1$ i $w = a^\alpha$). Pretpostavimo, dakle, da su $u_1$ i $v_1$ elementi različiti od 1. Prema prethodnoj tački ili je $u_1 = v_1^{-1}$ ili je $v_1 = u_1^{-1} v_2$ (za neko $v_2$) ili $u_1 \bullet v_1$ počinje prvim simbolom iz reči $u_1$ i završava se poslednjim simbolom iz reči $v_1$. Iz, recimo, $v_1 = u_1^{-1} v_2$ sledi $u \bullet v = u_1 \bullet v_1 = v_2 = v \bullet u = a_i^{-\alpha} u_1^{-1} v_2 \bullet u_1 a_i^\alpha$; reči $u_1 a_i^\alpha = u$ i $v_2$ su, znači, permutabilne i prema induktivnoj hipotezi obe su stepeni neke reči, a onda su i $u$ i $v$ stepeni iste reči.

U slučaju $u_1 \neq v_1^{-1}$ i $v_1 \neq u_1^{-1} v_2$, kako je $u$ ciklično reducirana reč, pa prema tome $u_1$ ne počinje sa $a_i^{-\alpha}$, već, recimo, sa $a_l^\delta$, $\delta \in \{1, -1\}$ (gde je ili $i \neq l$ ili $\alpha + \delta \neq 0$ ili i jedno i drugo), proizvod $u \bullet v$ bi počinjao sa $a_l^\delta$, a $v \bullet u$ sa $a_i^{-\alpha}$, kontradikcija.

Konačno, ako $u$ nije ciklično reducirana reč već je oblika $u_1^{-1} u_2 u_1$ (gde je $u_2$ ciklično reducirana reč različita od 1), onda je $u_2$ permutabilno sa $u_1 \bullet v \bullet u_1^{-1}$, i pošto je $l(u_2) + l(u_1 \bullet v \bullet u_1^{-1}) \leq l(u) + l(v)$, na osnovu prethodnog razmatranja $u_2$ i $u_1 \bullet v \bullet u_1^{-1}$ su stepeni iste reči $w$. Ali ako je $u_2 = w^m$ i $u_1 \bullet v \bullet u_1^{-1} = w^n$, $m, n \in Z$, tada je $u \equiv u_1^{-1} u_2 u_1 = u_1^{-1} w^m u_1 = (u_1^{-1} w u_1)^m$ i $v = u_1^{-1} w^n u_1 = (u_1^{-1} w u_1)^n$ (koristili smo da su prvi i zadnji element reči $u_2$ i $w$ isti – opet prema prethodnoj tački).

($e$) U dokazu tačke ($a$) pokazali smo: ako je $u = v^k$ i $v = v_1^{-1} v_2 v_1$, gde je $v_2$ ciklično reducirana reč, onda je $l(u) = 2l(v_1) + kl(v_2)$. Dakle neprazna reč dužine $n$ može imati, i to ne nužno, samo $k$-te korene, gde je $k \leq n$ (ustvari $-n \leq k \leq n$ ako uzimamo u obzir i "negativne" korene), a ako za dato $k$ postoji $k$-ti koren, on je, prema prethodnoj tački, jedinstven.

($g$) Neka je $u \neq 1$, $n$ najveći (pozitivan) koren elementa $u$ i neka je $u = w^n$. Jasno, $\langle w \rangle \subseteq C(u)$ (centralizator elementa $u$). S druge strane, prema ($d$), ako je $v \in C(u)$, $u$ i $v$ su stepeni istog elementa. No ako je $u = z^m$, tada su (prema ($d$)) i $w$ i $z$ permutabilni, dakle i stepeni istog elementa. Ali $w$ ne može imati korene veće od 1, te je $v$ stepen od $w$. Zaključujemo: $C(u) = \langle w \rangle$.

($h$) Neka je $(1 \neq) u \equiv a_{i_0}^{\alpha_0} \dots a_{i_{n-1}}^{\alpha_{n-1}}$ ($\alpha_j \in \{1, -1\}$) proizvoljan element grupe $\mathbf{F}_A$. Definišimo preslikavanje $\varphi$ skupa $A = \{a_i \mid i \in I\}$ u skup permutacija $S_{n+1}$ skupa $n+1 = \{0, \dots, n\}$ na sledeći način: ako $i \notin \{i_0, \dots, i_{n-1}\}$, onda je $(a_i)\varphi = \imath$ (– identična permutacija skupa $n+1$). Za $i_k$, $k = 0, \dots, n-1$, $(a_{i_k})\varphi$ je permutacija koja preslikava $k$ u $k+1$ ako je $\alpha_k = 1$, u suprotnom ($\alpha_k = -1$) preslikava $k+1$ u $k$. Naravno, moguće je da je nekoliko izvodnih simbola u reči $u$ isto, no neprilika ne može biti: $u$ je slobodno reducirana reč pa ako je $i_k = i_{k+1}$, $0 \leq k < n-1$, onda mora biti i $\alpha_k = \alpha_{k+1}$; prema tome ne može se dogoditi da se za sliku elementa $a_{i_k} = a_{i_{k+1}}$ zahteva da preslikava $k+1$ i u $k$ i u $k+2$. Drugih uslova nema, pa u opštem preslikavanje $\varphi$ nije na jedinstven način određeno. Ako je $\overline{\varphi}$ odgovarajuće homomorfno preslikavanje grupe $\mathbf{F}_A$ u grupu $\mathbf{S}_{n+1}$ (ekstenzija preslikavanja $\varphi$), onda je $(u)\overline{\varphi}$ permutacija koja preslikava 0 u $n$, jer $(a_{i_k}^{\alpha_k})\overline{\varphi} = ((a_{i_k})\varphi)^{\alpha_k}$ preslikava $k$ u $k+1$. Dakle, $u \notin Ker(\overline{\varphi})$ i $\mathbf{F}_A/\mathbf{Ker}(\overline{\varphi}) \cong (\mathbf{F}_A)\overline{\varphi} \leq \mathbf{S}_{n+1}$.



($i$) Prema prethodnoj tački je presek svih normalnih podgrupa konačnog indeksa jedinična grupa.

($j$) Videti 10.21.

($k$) Ako je $y$ ciklična permutacija reči $v$, npr. $v \equiv a_{i_1}^{\alpha_1} \dots a_{i_k}^{\alpha_k} a_{i_{k+1}}^{\alpha_{k+1}} \dots a_{i_n}^{\alpha_n}$ i $y \equiv a_{i_{k+1}}^{\alpha_{k+1}} \dots a_{i_n}^{\alpha_n} a_{i_1}^{\alpha_1} \dots a_{i_k}^{\alpha_k}$, onda je $y = (a_{i_1}^{\alpha_1} \dots a_{i_k}^{\alpha_k})^{-1} \bullet v \bullet a_{i_1}^{\alpha_1} \dots a_{i_k}^{\alpha_k}$ i reči $u^{-1}vu$ i $x^{-1}yx$ su konjugovane.

Očigledno, $u^{-1}vu$ i $x^{-1}yx$ su konjugovane elementi akko su $v$ i $y$ konjugovani elementi. Indukcijom po dužini slobodno reducirane reči kojom se, da se malo igramo rečima, "konjugira", pokazaćemo da ako su ciklično reducirane reči $v$ i $y$ konjugovane reči, tada je $y$ ciklična permutacija reči $v$. Neka je $y = w^{-1} \bullet v \bullet w$. Slučaj kada je $w$ prazna reč je trivijalan. Pretpostavimo da je tvrđenje tačno za sve reči dužine manje od $m$ i neka je $v \equiv a_{i_1}^{\alpha_1} a_{i_2}^{\alpha_2} \dots a_{i_n}^{\alpha_n}$ i $w \equiv a_{j_1}^{\beta_1} \dots a_{j_m}^{\beta_m}$; dakle, $y = a_{j_m}^{-\beta_m} \dots a_{j_1}^{-\beta_1} \bullet a_{i_1}^{\alpha_1} a_{i_2}^{\alpha_2} \dots a_{i_n}^{\alpha_n} \bullet a_{j_1}^{\beta_1} \dots a_{j_m}^{\beta_m}$. Naravno, ne može biti istovremeno i $a_{j_1}^{-\beta_1} \bullet a_{i_1}^{\alpha_1} = a_{j_1}^{-\beta_1} a_{i_1}^{\alpha_1}$ i $a_{i_n}^{\alpha_n} \bullet a_{j_1}^{\beta_1} = a_{i_n}^{\alpha_n} a_{j_1}^{\beta_1}$ (na desnoj strani imali bismo reč koja nije ciklično reducirana). Recimo da je $a_{j_1}^{-\beta_1} \bullet a_{i_1}^{\alpha_1} = 1$ (prema tome, $i_1 = j_1$ i $\alpha_1 = \beta_1$). Pošto je $v$ ciklično reducirana reč, ne može biti i $a_{i_n}^{\alpha_n} \bullet a_{j_1}^{\beta_1} = a_{i_n}^{\alpha_n} \bullet a_{i_1}^{\alpha_1} = 1$, pa je $y = (a_{j_2}^{\beta_2} \dots a_{j_m}^{\beta_m})^{-1} \bullet a_{i_2}^{\alpha_2} \dots a_{i_n}^{\alpha_n} a_{i_1}^{\alpha_1} \bullet a_{j_2}^{\beta_2} \dots a_{j_m}^{\beta_m}$. Prema induktivnoj pretpostavci $y$ je ciklična permutacija reči $a_{i_2}^{\alpha_2} \dots a_{i_n}^{\alpha_n} a_{i_1}^{\alpha_1}$, stoga i ciklična permutacija reči $v$.□

**Korolar 23.4** *Problem konjugovanosti i problem reči rešivi su za slobodnu grupu sa prezentacijom* $(A; \emptyset)$.

**Napomena**. Uz prethodni korolar dodajmo: za grupu sa konačnom prezentacijom i za koju znamo da je slobodna problem reči je rešiv, no to već ne važi za slobodne grupe sa, recimo, beskonačnim skupom generatora i rekurzivnim skupom odrednica – kontraprimer je dat u [18].

U mnogim knjigama kad je reč o slobodnim grupama daje se prednost jednoj drugoj njihovoj karakterizaciji već i iz razloga što je taj pristup generalan u razmatranju adekvatnih podklasa (slobodnih algebri – videti npr. [57]) raznih klasa algebri. No prvo definicija.

**Definicija 23.5** *Podskup $A$ domena $G$ grupe $\mathbf{G}$ je slobodna baza ili slobodni generatorni skup (kaže se i samo baza) grupe $\mathbf{G}$ akko za svako preslikavanje $\varphi$ skupa $A$ u domen $H$ (ma koje) grupe $\mathbf{H}$ postoji njegova jedinstvena ekstenzija $\overline{\varphi} \in Hom(\mathbf{G},\mathbf{H})$ $(\overline{\varphi}|_A = \varphi)$.*

**Lema 23.6** *Neka su $\mathbf{G}$ i $\mathbf{H}$ izomorfne grupe i neka je $\varphi \in Is(\mathbf{G},\mathbf{H})$. Ako je $A$ slobodna baza grupe $\mathbf{G}$, onda je $(A)\varphi$ slobodna baza grupe $\mathbf{H}$.*

**Dokaz.** Neka je $\psi$ preslikavanje skupa $(A)\varphi$ u domen $K$ grupe $\mathbf{K}$. Kako je $A$ slobodna baza grupe $\mathbf{G}$ postoji jedinstvena ekstenzija $\overline{\theta} \in Hom(\mathbf{G},\mathbf{K})$ preslikavanja $\theta : A \longrightarrow K$ datog sa $(a)\theta = ((a)\varphi)\psi$. No onda je $\overline{\psi} = \varphi^{-1} \circ \overline{\theta}$ jedinstveno homomorfno preslikavanje grupe $\mathbf{H}$ u $\mathbf{K}$ koje je ekstenzija preslikavanja $\psi$. Homomorfno je kao kompozicija homomorfnih preslikavanja, za $(a)\varphi \in (A)\varphi$ je $((a)\varphi)\overline{\psi} = ((a)\varphi)\varphi^{-1})\overline{\theta} = (a)\overline{\theta} = ((a)\varphi)\psi$, a ako je i $\overline{\psi_1} \in Hom(\mathbf{H},\mathbf{K})$ i $\overline{\psi_1}|_{(A)\varphi} = \psi$, tada je $\overline{\theta_1} = \varphi \circ \overline{\psi_1} \in Hom(\mathbf{G},\mathbf{K})$, $\overline{\theta_1}|_A = \theta$, pa je $\overline{\theta_1} = \overline{\theta}$, tj. $\overline{\psi_1} = \varphi^{-1} \circ \overline{\theta} = \overline{\psi}$.□

**Lema 23.7** *Grupa $\mathbf{G}$ je slobodna (ima prezentaciju sa praznim skupom netrivijalnih odrednica) akko ima slobodnu bazu.*

**Dokaz.** Neka je $(A;\emptyset)$ prezentacija grupe $\mathbf{G}$. Onda je $\mathbf{G}$ izomorfna sa slobodnom grupom slobodno reduciranih reči $\mathbf{F}_A$, za koju je, to smo već pokazali, $A$ slobodna baza – videti npr. 21.9$(a)$ i kraj dokaza leme 23.2. Ali tada, prema prethodnoj lemi, ako je $\varphi \in Is(\mathbf{F}_A,\mathbf{G})$, $(A)\varphi$ je slobodna baza grupe $\mathbf{G}$.

Pretpostavimo sada da je $A$ slobodna baza grupe $\mathbf{G}$. Za identično preslikavanje $\imath_A : A \longrightarrow A$ postoje jedinstvene ekstenzije $\psi \in Hom(\mathbf{G},\mathbf{F}_A)$ i $\theta \in Hom(\mathbf{F}_A,\mathbf{G})$ (opet je $\mathbf{F}_A$ slobodna grupa slobodno reduciranih reči). Ali tada je $\psi\circ\theta \in End(\mathbf{G})$, $\theta\circ\psi \in End(\mathbf{F}_A)$, pa zbog činjenice da je $A$ slobodna baza grupa $\mathbf{G}$ i $\mathbf{F}_A$, te ekstenzije su jedinstvene (imamo u vidu $(\psi\circ\theta)|_A = \imath_A$, $(\theta\circ\psi)|_A = \imath_A$). Prema tome je $\theta\circ\psi = \imath_G$, $\psi\circ\theta = \imath_{F_A}$. Odatle proizilazi da su $\psi$ i $\theta$ bijektivna preslikavanja, te je $\mathbf{G} \cong \mathbf{F}_A$, a $(A;\emptyset)$ je prezentacija i grupe $\mathbf{G}$ (videti napomenu posle 21.7).□

**Korolar 23.8** $(a)$ *Neka je $A$ neprazni podskup domena $G$ grupe $\mathbf{G} = \langle G, *\rangle$ takav da je $A \cap A^{-1} = \emptyset$. Tada, $A$ je slobodna baza podgrupe $\langle A\rangle$ akko je svaki proizvod oblika $a_{i_1}^{\alpha_1} * \cdots * a_{i_k}^{\alpha_k}$, gde je $k \geq 1$, $\alpha_j \in \{1,-1\}$ i $i_j \neq i_{j+1}$ ili $\alpha_j = \alpha_{j+1}$, različit od jediničnog elementa.*

$(b)$ *Neka je $A$ (neprazni) podskup grupe $\mathbf{G} = \langle G, *\rangle$. Tada je $A$ slobodna baza akko se svaki element $u$ iz $G$ može na jedinstven način predstaviti kao proizvod elemenata iz $A \cup A^{-1}$ oblika kao u tački $(a)$.*

$(c)$ *Svaki neprazni podskup slobodne baze i sam je slobodna baza za podgrupu koju generiše.*

*Nijedan pravi podskup slobodne baze ne generiše celu grupu.*



**Dokaz.** $(a)$ Pravac $(\Longrightarrow)$ je već dokazan. Videli smo da je grupa sa slobodnim generatornim skupom $A$ izomorfna grupi $\mathbf{F}_A$ slobodno reduciranih reči, pri čemu imamo izomorfizam koji ostavlja fiksnim elemente iz $A$.

$(\Longleftarrow)$ Ako je $\varphi$ jedinstveno homomorfno preslikavanje grupe $\mathbf{F}_A$ na podgrupu $\langle A\rangle$ grupe $\mathbf{G}$, gde je $\varphi|_A = \imath_A$, vidimo da je $\varphi$ i injektivno. Jer, $(a_{i_1}^{\alpha_1} \cdot \ldots \cdot a_{i_k}^{\alpha_k})\varphi = a_{i_1}^{\alpha_1} * \cdots * a_{i_k}^{\alpha_k}$, te se nijedna neprazna slobodno reducirana reč ne preslikava u jedinični element.□

**Korolar 23.9** *Uslov o jedinstvenosti ekstenzije $\overline{\varphi}$ u definiciji 23.5 ekvivalentan je sa uslovom da je $A$ i generatorni skup grupe $\mathbf{G}$ (podrazumevamo, naravno, da su ostali uslovi definicije ostali nepromenjeni).*

**Dokaz.** Ako je $A$ generatorni skup grupe $\mathbf{G}$, a $\overline{\varphi} \in Hom(\mathbf{G},\mathbf{H})$ ekstenzija preslikavanja $\varphi : A \longrightarrow H$, onda je, to znamo odavno – 5.5, $\overline{\varphi}$ jedinstveno. S druge strane, prema dokazu leme 23.7, s obzirom da je $A$ generatorni skup grupe $\mathbf{F}_A$ i $\theta \in Is(\mathbf{F}_A,\mathbf{G})$, $(A)\theta = A$ je generatorni skup grupe $\mathbf{G}$.□

**Lema 23.10** *Neka su $\mathbf{G}$ i $\mathbf{H}$ slobodne grupe sa slobodnim bazama, respektivno, $A$ i $B$. Tad je $\mathbf{G} \cong \mathbf{H}$ akko je $|A| = |B|$.*

**Dokaz.** Neka su grupe $\mathbf{G}$ i $\mathbf{H}$ izomorfne i neka je $\lambda = |G| = |H|$. Ako je $\lambda > \aleph_0$, onda mora biti i $|A| = |B| = \lambda$ jer su $A$ i $B$ generatorni skupovi tih grupa. Ako je $\lambda = \aleph_0$, 23.8$(b)$ isključuje mogućnost da je jedan od skupova $A$, $B$ beskonačan, a drugi konačan. Preostaje nam, dakle, da ispitamo slučaj kad su $A$ i $B$ konačni skupovi.

Neka je $|A| = m$ i $|B| = n$, $m, n$ – prirodni brojevi. Kako ima $2^m$ različitih preslikavanja skupa $A$ u $\{0,1\}$ to postoji tačno $2^m$ homomorfnih preslikavanja grupe $\mathbf{G}$ u cikličnu grupu $\mathbf{Z}_2$ (svaki homomorfizam je potpuno određen preslikavanjem skupa $A$ u $\{0,1\}$). Za svaki surjektivni homomorfizam $\psi$ (a takvih je $2^m - 1$) $\mathbf{Ker}(\psi)$ je normalna podgrupa grupe $\mathbf{G}$ indeksa 2. Opet, ako je $\mathbf{N}$ normalna podgrupa grupe $\mathbf{G}$ indeksa 2 i $\varphi$ kanoničko homomorfno preslikavanje grupe $\mathbf{G}$ u grupu $\mathbf{G/N}$, a $\theta$ izomorfno preslikavanje grupe $\mathbf{G/N}$ u $\mathbf{Z}_2$, onda je $\varphi\circ\theta \in Hom(\mathbf{G},\mathbf{Z}_2)$ i $\mathbf{N} = \mathbf{Ker}(\varphi\circ\theta)$. Prema tome $\mathbf{G}$ ima (tačno) $2^m - 1$ normalnih podgrupa indeksa 2. Po simetriji stvari $\mathbf{H}$ ima $2^n - 1$ takvih podgrupa, pa je zbog izomorfnosti grupa $\mathbf{G}$ i $\mathbf{H}$ $2^m - 1 = 2^n - 1$, tj. $m = n$.

Neka je sada $|A| = |B|$ i $\phi$ bijektivno preslikavanje skupa $A$ na skup $B$. Dokaz o izomorfizmu grupa $\mathbf{G}$ i $\mathbf{H}$ analogan je dokazu leme 23.7 i dajemo ga (ponavljamo) više vežbe radi. Postoje (jedinstveni) homomorfizmi (ekstenzije preslikavanja $\phi$ i $\phi^{-1}$), koji su jasno i surjektivni, $\overline{\phi} \in Hom(\mathbf{G},\mathbf{H})$, $\overline{\phi^{-1}} \in Hom(\mathbf{H},\mathbf{G})$. Kako je $\overline{\phi}\circ\overline{\phi^{-1}} \in End(\mathbf{G})$ i $(\overline{\phi}\circ\overline{\phi^{-1}})|_A = \imath_A$, mora biti $\overline{\phi}\circ\overline{\phi^{-1}} = \imath_G$, pa je $\overline{\phi}$ i injektivno, znači i izomorfno preslikavanje.□

**Korolar 23.11** *Ako su $A$ i $B$ slobodne baze grupe $\mathbf{G}$, onda je $|A| = |B|$.*

**Definicija 23.12** *Kardinalnost slobodne baze (slobodne grupe)* $\mathbf{G}$ *zovemo rangom grupe* $\mathbf{G}$.

Primetimo da se u nekim knjigama i jedinična grupa tretira kao slobodna grupa ranga 0, drugim rečima to je slobodna grupa čija je slobodna baza prazni skup. Ovo se obično usvaja zbog koherentnosti teksta, no naravno, ova grupa nam je od malog interesa, pa ćemo, kada govorimo o nekoj slobodnoj grupi, gotovo po pravilu podrazumevati da je njen rang veći od 0.

**Definicija 23.13** *Grupa je Hopfova (Heinz Hopf,* 1894 - 1971*) akko nije izomorfna ni jednoj svojoj pravoj faktor grupi (faktor grupi po nejediničnoj normalnoj podgrupi), tj. akko je svaki njen surjektivni endomorfizam ujedno i automorfizam.*

*Grupa je kohopfova akko je svaki njen injektivni endomorfizam ujedno i automorfizam.*

Trivijalno, svaka konačna i svaka prosta grupa je Hopfova.

**Lema 23.14** *Konačno generisana konačno rezidualna grupa je Hopfova, a njena grupa automorfizama je rezidualno konačna.*

**Dokaz.** Neka je $\mathbf{G}$ konačno generisana konačno rezidualna grupa i $\varphi$ jedan njen surjektivni endomorfizam. Pretpostavimo da je $\mathbf{Ker}(\varphi) \neq \mathbf{E}$ i neka $e \neq g \in Ker(\varphi)$. Tada, za neku normalnu podgrupu $\mathbf{N}$, $g \notin N$ i $\overline{\mathbf{G}} = \mathbf{G/N}$ je konačna grupa. Pošto je $\mathbf{G}$ konačno generisana grupa i $\overline{\mathbf{G}}$ konačna grupa, postoji samo konačno mnogo homomorfnih preslikavanja grupe $\mathbf{G}$ u grupu $\overline{\mathbf{G}}$; neka je $\theta_1, \ldots, \theta_n$ spisak svih tih homomorfizama. Ako je $\overline{\varphi}$ izomorfno preslikavanje grupe $\mathbf{G/Ker}(\varphi)$ na $\mathbf{G}$, dato sa $(aKer(\varphi))\overline{\varphi} = (a)\varphi$, i $\nu : G \longrightarrow G/Ker(\varphi)$ prirodni (kanonički) homomorfizam, tada su $\nu \circ \overline{\varphi} \circ \theta_i : G \longrightarrow \overline{G}$, $i = 1, \ldots, n$, različiti homomorfizmi (jer je $\nu \circ \overline{\varphi}$ surjektivno preslikavanje), dakle to su sva homomorfna preslikavanja grupe $\mathbf{G}$ u grupu $\overline{\mathbf{G}}$. No, za svako $i$ ($\in \{1, \ldots, n\}$), $(g)(\nu \circ \overline{\varphi} \circ \theta_i) = (Ker(\varphi))(\overline{\varphi} \circ \theta_i) = (e)\theta_i = N$, dok je za kanoničko homomorfno preslikavanje $\psi : G \longrightarrow \overline{G} = G/N$, $(g)\psi = gN \neq N$, kontradikcija.

Pokažimo sada da je i grupa $\mathbf{Aut(G)}$ rezidualno konačna. Neka je $\phi$ nejedinični automorfizam grupe $\mathbf{G}$. Onda, za neko $a \in G$, $(a)\phi \neq a$, pa postoji normalna podgrupa $\mathbf{H}$ grupe $\mathbf{G}$ koja je konačnog indeksa i koja ne sadrži element $a^{-1} \cdot (a)\varphi$. S obzirom da je $\mathbf{G}$ konačno generisana grupa, karakteristično jezgro podgrupe $\mathbf{H}$, $\mathbf{K} = \bigcap_{\chi \in Aut(\mathbf{G})} (\mathbf{H})\chi$, je takođe konačnog indeksa (za svako $\chi \in Aut(\mathbf{G})$ je $[\mathbf{G} : \mathbf{H}] = [\mathbf{G} : (\mathbf{H})\chi]$, a $\mathbf{G}$ sadrži samo konačno mnogo podgrupa indeksa $[\mathbf{G} : \mathbf{H}]$ - videti 3.18 i 9.40). Za $\chi \in Aut(\mathbf{G})$ definišimo preslikavanje $\overline{\chi} : G/K \longrightarrow G/K$ sa $(bK)\overline{\chi} = (b)\chi K$. $\overline{\chi}$ je, ispostavlja se, automorfizam grupe $\mathbf{G/K}$; imamo u vidu da je za svako $b \in G$, $b \in K$ akko je, za svako (neko) $\theta \in Aut(\mathbf{G})$, $(b)\theta \in K$. Prema tome je preslikavanje $\Phi : Aut(\mathbf{G}) \longrightarrow Aut(\mathbf{G/K})$ dato sa $(\chi)\Phi = \overline{\chi}$ homomorfno



preslikavanje. Sledi: $\mathbf{Aut(G)/Ker}(\Phi)$ je konačna grupa i $\phi \notin Ker(\Phi)$; jer $(aK)\overline{\phi} = (a)\phi K \neq aK$, tj. $(\phi)\Phi = \overline{\phi} \neq \imath_{G/K}$.□

**Korolar 23.15** *Slobodna grupa konačnog ranga je Hopfova, a njena grupa automorfizama je rezidualno konačna.*

**Dokaz.** Podsetimo se samo: slobodne grupe su rezidualno konačne – 23.3($h$).□

**Korolar 23.16** *Ako je slobodna grupa* $\mathbf{F}$ *generisana skupom konačne kardinalnosti* $m$*, tada je njen rang manji od ili jednak* $m$.

**Dokaz.** Neka je $\{a_1, \ldots, a_r\}$ slobodna baza grupe $\mathbf{F}$, $\{b_1, \ldots, b_m\}$ jedan njen generatorni skup i pretpostavimo da je $r > m$. Tada je endomorfizam $\varphi$ grupe $\mathbf{F}$ određen sa $(a_i)\varphi = b_i$, za $i = 1, \ldots, m$, i $(a_j)\varphi = 1$, za $m < j \leq r$, surjektivan, dok je njegovo jezgro nejedinična grupa, kontradikcija.□

**Korolar 23.17** *Neka je* $\mathbf{F}$ *slobodna grupa konačnog ranga* $n$*. Tada je svaki njen generatorni skup kardinalnosti* $n$ *ujedno i njena slobodna baza.*

**Dokaz.** Neka je $\{a_1, \ldots, a_n\}$ slobodna baza grupe $\mathbf{F}$ i $\{b_1, \ldots, b_n\}$ jedan njen generatorni skup. Tada je endomorfizam $\varphi$ grupe $\mathbf{F}$ dat sa $(a_i)\varphi = b_i$, $i = 1, \ldots, n$, surjektivan, pa dakle, i automorfizam. Prema 23.6, $\{b_1, \ldots, b_n\}$ je takođe slobodna baza grupe $\mathbf{F}$.□

**Napomena.** Primetimo samo da su poslednji korolari neposredne posledice i Gruško-Neumannove teoreme.

**Lema 23.18** *Neka je* $\mathbf{H}$ *normalna podgrupa grupe* $\mathbf{G}$ *i neka je* $\mathbf{G/H}$ *slobodna grupa. Tada je* $\mathbf{G}$ *poludirektni proizvod sa normalnim faktorom* $\mathbf{H}$.

**Dokaz.** Neka je $\{g_i H \mid i \in I\}$ slobodna baza grupe $\mathbf{G/H}$. Tada je, za $\mathbf{K} = \langle\{g_i \mid i \in I\}\rangle$, $\mathbf{G} = \mathbf{H} \rtimes \mathbf{K}$. Očigledno, $\mathbf{K}$ je slobodna grupa, sa slobodnom bazom $\{g_i \mid i \in I\}$, a pretpostavka da je slobodno reducirana reč $g_{i_1}^{\alpha_1} \ldots g_{i_k}^{\alpha_k}$ nejedinični element i podgrupe $\mathbf{H}$ dala bi $(g_{i_1}H)^{\alpha_1} \ldots (g_{i_k}H)^{\alpha_k} = H$, kontradikcija.

Obrat ovog tvrđenja je dat u 23.25.□

**Teorema 23.19** *(Teorema Nielsen-Schreiera). Podgrupa slobodne grupe je slobodna grupa.*

**Dokaz.** (A. J. Weir). Neka je $\mathbf{H}$ podgrupa slobodne grupe slobodno reduciranih reči $\mathbf{F}_A$ i neka je $\mathcal{T} = \{\overline{u} \mid Hu = H\overline{u}\}$ njena desna transverzala, uz uslov da je predstavnik koseta $H$ baš 1 (dakle, za svako $h \in H$, $\overline{h} = 1 = \overline{1}$). Za svako $a \in A$, $\overline{u} \bullet a$ i $\overline{u \bullet a}$ su elementi istog koseta, pa je $\overline{u} \bullet a \bullet (\overline{u \bullet a})^{-1} = z_{\overline{u},a} \in H$. Svakom elementu $z_{\overline{u},a}$ pridružimo element $b_{\overline{u},a}$ i neka je $\mathbf{F}_B$ slobodna grupa slobodno reduciranih reči (nad azbukom $B \cup B^{-1}$), gde je $B = \{b_{\overline{u},a} \mid \overline{u} \in \mathcal{T}, a \in A\}$. Tada imamo

**Lema 23.20** *Ako je $\varphi$ homomorfno preslikavanje grupe $\mathbf{F}_B$ u grupu $\mathbf{H}$ za koje je $(b_{\overline{u},a})\varphi = z_{\overline{u},a}$, tada postoji homomorfno preslikavanje $\psi$ grupe $\mathbf{H}$ u $\mathbf{F}_B$ takvo da je $\psi \circ \varphi = \imath_H$.*

**Dokaz.** Konstruisaćemo simultano preslikavanja $\psi_{\overline{u}} : F_A \longrightarrow F_B$ za svako $\overline{u} \in \mathcal{T}$, tako da bude ispunjeno:

$$(v \bullet w)\psi_{\overline{u}} = (v)\psi_{\overline{u}} \bullet (w)\psi_{\overline{u \bullet v}} \qquad (*);$$

(već smo rekli: $\overline{u \bullet v} = \overline{\overline{u} \bullet v}$). Za svako $a \in A$ i svako $\overline{u} \in \mathcal{T}$ stavljamo: $(a)\psi_{\overline{u}} = b_{\overline{u},a}$ i $(1)\psi_{\overline{u}} = 1$. Uslov $(*)$ determiniše:

$$1 = (1)\psi_{\overline{u}} = (a^{-1} \bullet a)\psi_{\overline{u}} = (a^{-1})\psi_{\overline{u}} \bullet (a)\psi_{\overline{u \bullet a^{-1}}} = (a^{-1})\psi_{\overline{u}} \bullet b_{\overline{u \bullet a^{-1}},a},$$

tj. $(a^{-1})\psi_{\overline{u}} = b^{-1}_{\overline{u \bullet a^{-1}},a}$. Pretpostavimo da smo definisali sva preslikavanja $\psi_{\overline{u}}$ za sve reči dužine manje od ili jednake $n$ i neka je $v \equiv a^{\alpha}w$ $(\alpha \in \{1,-1\})$ reč dužine $n+1$. Definišimo:

$$(v)\psi_{\overline{u}} = (a^{\alpha} \bullet w)\psi_{\overline{u}} \stackrel{\text{def}}{=} (a^{\alpha})\psi_{\overline{u}} \bullet (w)\psi_{\overline{u \bullet a^{\alpha}}}.$$

Indukcijom po dužini reči $v$ pokazujemo da važi $(*)$. Slučaj $l(v) = 0$ je trivijalan. Ako je $l(v) = 1$ i npr. $v \equiv a^{-1}$, prelazimo na indukciju po dužini reči $w$. Opet je $l(w) = 0$ trivijalno. Pretpostavimo da $(*)$ važi za sve reči dužine manje od ili jednake $m$ i neka je $l(w) = m+1$, recimo: $w \equiv a_i^{\alpha_i}z$. Ako je $a_i \not\equiv a$ ili $\alpha_i \neq 1$, imamo:

$$(a^{-1} \bullet w)\psi_{\overline{u}} = (a^{-1}w)\psi_{\overline{u}} \stackrel{\text{def}}{=} (a^{-1})\psi_{\overline{u}} \bullet (w)\psi_{\overline{u \bullet a^{-1}}}.$$

Ako je $a \equiv a_i$ i $\alpha_i = 1$, tada je: $(a^{-1} \bullet az)\psi_{\overline{u}} = (z)\psi_{\overline{u}}$, ali i

$$(a^{-1})\psi_{\overline{u}} \bullet (az)\psi_{\overline{u \bullet a^{-1}}} = (a^{-1})\psi_{\overline{u}} \bullet (a)\psi_{\overline{u \bullet a^{-1}}} \bullet (z)\psi_{\overline{u \bullet a^{-1} \bullet a}} =$$

$$b^{-1}_{\overline{u \bullet a^{-1}},a} \bullet b_{\overline{u \bullet a^{-1}},a} \bullet (z)\psi_{\overline{u}} = (z)\psi_{\overline{u}}.$$

Ako je pak po induktivnoj hipotezi uslov $(*)$ ispunjen za sve reči $v$ dužine manje od ili jednake $n$ (i sve reči $w$) i ako je $v = a^{\alpha}z$ reč dužine $n+1$, izvodimo:

$$(v \bullet w)\psi_{\overline{u}} = (a^{\alpha} \bullet (z \bullet w))\psi_{\overline{u}} = (a^{\alpha})\psi_{\overline{u}} \bullet (z \bullet w)\psi_{\overline{u \bullet a^{\alpha}}} =$$

$$(a^{\alpha})\psi_{\overline{u}} \bullet (z)\psi_{\overline{u \bullet a^{\alpha}}} \bullet (w)\psi_{\overline{u \bullet a^{\alpha} \bullet z}} = (a^{\alpha}z)\psi_{\overline{u}} \bullet (w)\psi_{\overline{u \bullet (a^{\alpha}z)}} = (v)\psi_{\overline{u}} \bullet (w)\psi_{\overline{u \bullet v}}.$$

Lako se pokazuje i nezavisnost od "rastavljanja"; naime, ako je $v_1 \bullet v_2 = w_1 \bullet w_2$, tada je i $(v_1 \bullet v_2)\psi_{\overline{u}} = (w_1 \bullet w_2)\psi_{\overline{u}}$. U osnovi provere je činjenica da je obezbeđeno: $1 = (a \bullet a^{-1})\psi_{\overline{u}} = (a^{-1} \bullet a)\psi_{\overline{u}}$.



Indukcijom po dužini reči $v$ dokazujemo da za svako $\overline{u} \in \mathcal{T}$ važi i:

$$(v)(\psi_{\overline{u}} \circ \varphi) = \overline{u} \bullet v \bullet (\overline{u \bullet v})^{-1} \qquad (**).$$

Za jedinični element to je očigledno, za $a \in A$ je:

$$(a)(\psi_{\overline{u}} \circ \varphi) = (b_{\overline{u},a})\varphi = z_{\overline{u},a} = \overline{u} \bullet a \bullet (\overline{u \bullet a})^{-1},$$

$$(a^{-1})(\psi_{\overline{u}} \circ \varphi) = (b^{-1}_{\overline{u \bullet a^{-1}},a})\varphi = z^{-1}_{\overline{u \bullet a^{-1}},a} = ((\overline{u \bullet a^{-1}}) \bullet a \bullet (\overline{u \bullet a^{-1} \bullet a})^{-1})^{-1} =$$

$$\overline{u} \bullet a^{-1} \bullet (\overline{u \bullet a^{-1}})^{-1}.$$

Ako tvrđenje važi za sve reči $v$ dužine manje od ili jednake $n$ i ako je $v \equiv a^{\alpha}w$ reč dužine $n+1$, tada je:

$$(v)(\psi_{\overline{u}} \circ \varphi) = ((a^{\alpha} \bullet w)\psi_{\overline{u}})\varphi = ((a^{\alpha})\psi_{\overline{u}})\varphi \bullet ((w)\psi_{\overline{u \bullet a^{\alpha}}})\varphi =$$

$$(\overline{u} \bullet a^{\alpha} \bullet (\overline{u \bullet a^{\alpha}})^{-1}) \bullet (\overline{u \bullet a^{\alpha}} \bullet w \bullet (\overline{u \bullet a^{\alpha} \bullet w})^{-1}) = \overline{u} \bullet v \bullet (\overline{u \bullet v})^{-1}.$$

Neka je $\psi = \psi_1|_H$. Prema $(*)$, $\psi$ je homomorfno preslikavanje; za $v, w \in H$ je: $(v \bullet w)\psi = (v \bullet w)\psi_1 = (v)\psi_1 \bullet (w)\psi_{\overline{v}} = (v)\psi_1 \bullet (w)\psi_1 = (v)\psi \bullet (w)\psi$. Prema $(**)$, $\psi \circ \varphi$ je identično preslikavanje (skupa $H$).□

**Lema 23.21** *$(\{b_{\overline{u},a} \mid \overline{u} \in \mathcal{T}, a \in A\}; \{(\overline{u})\psi \sim 1 \mid \overline{u} \in \mathcal{T}\})$ je prezentacija podgrupe $\mathbf{H}$ (koristimo notaciju i znanje prethodne leme).*

**Dokaz.** Neka je $\theta = \varphi \circ \psi$. Zbog $\psi \circ \varphi = \imath_H$, $\theta$ je retrakcija grupe $\mathbf{F}_B$ (videti 12.4): $\theta^2 = \varphi \circ (\psi \circ \varphi) \circ \psi = \varphi \circ \psi = \theta$, $\varphi$ je surjektivno i $\psi$ injektivno preslikavanje. Odatle i prema 12.4 sledi: $\mathbf{Ker}(\varphi) = \mathbf{Ker}(\theta) = \langle\{v^{-1} \bullet (v)\theta \mid v$ je reč azbuke $B \cup B^{-1}\}\rangle$. Stoga je $(B; \{v \sim (v)\theta \mid v$ je reč azbuke $B \cup B^{-1}\})$ prezentacija podgrupe $\mathbf{H}$, a onda, prema 22.3, i $(B; \{b_{\overline{u},a} \sim (b_{\overline{u},a})\theta \mid b_{\overline{u},a} \in B\})$. Dalje je, prema prethodnoj lemi (ponavljamo: $\psi = \psi_1$):

$$(b_{\overline{u},a})\theta = ((b_{\overline{u},a})\varphi)\psi = (z_{\overline{u},a})\psi = (\overline{u} \bullet a \bullet (\overline{u \bullet a})^{-1})\psi =$$

$$(\overline{u})\psi \bullet (a \bullet (\overline{u \bullet a})^{-1})\psi_{\overline{u}} = (\overline{u})\psi \bullet (a)\psi_{\overline{u}} \bullet ((\overline{u \bullet a})^{-1})\psi_{\overline{u \bullet a}} =$$

$$(\overline{u})\psi \bullet b_{\overline{u},a} \bullet ((\overline{u \bullet a})\psi)^{-1};$$

u poslednjem koraku smo koristili:

$$1 = ((\overline{u \bullet a})^{-1} \bullet \overline{u \bullet a})\psi_{\overline{u \bullet a}} =$$

$$((\overline{u \bullet a})^{-1})\psi_{\overline{u \bullet a}} \bullet (\overline{u \bullet a})\psi_{\overline{u \bullet a \bullet (\overline{u \bullet a})^{-1}}} = ((\overline{u \bullet a})^{-1})\psi_{\overline{u \bullet a}} \bullet (\overline{u \bullet a})\psi.$$

Pokazaćemo, a time i dokazati lemu, da su normalne podgrupe $\mathbf{Ker}(\theta)$ i $\mathbf{M}$, generisana skupom $\{(\overline{u})\psi \mid \overline{u} \in \mathcal{T}\}$, jednake. Jasno, $b^{-1}_{\overline{u},a} \bullet (b_{\overline{u},a})\theta = (b^{-1}_{\overline{u},a} \bullet (\overline{u})\psi \bullet b_{\overline{u},a}) \bullet ((\overline{u \bullet a})\psi)^{-1} \in M$. No i $(\overline{u})\psi \in Ker(\theta)$. Pošto je, videli smo, $((\overline{u})\psi)^{-1} = (\overline{u}^{-1})\psi_{\overline{u}}$, prema $(**)$ sledi:

$$((\overline{u})\psi)\theta = ((((\overline{u}^{-1})\psi_{\overline{u}})^{-1})\varphi)\psi =$$

$$((((\overline{u}^{-1})\psi_{\overline{u}})\varphi)^{-1})\psi = ((\overline{u} \bullet \overline{u}^{-1} \bullet (\overline{u \bullet u^{-1}})^{-1})\psi = (1)\psi = 1.\square$$

**Lema 23.22** *Postoji desna transverzala podgrupe* $\mathbf{H}$ *grupe* $\mathbf{F}_A$ *takva da je svaki početni segment svakog njenog elementa opet njen element.*

**Dokaz.** Desna transverzala o kojoj je reč je tzv. *desna Schreierova transverzala.* Obeležićemo je za ovu priliku sa $\mathcal{T}_S$.

Definišimo *dužinu koseta* $Hu$, u oznaci $l(Hu)$, sa: $l(Hu) = min\{l(v) \mid v \in Hu\}$. Indukcijom po dužini koseta biramo elemente Schreierove transverzale. Samo je koset $H$ dužine 0 i za njegovog predstavnika uzimamo praznu reč (1). Predpostavimo da smo već izabrali predstavnike koji ispunjavaju postavljeni uslov za sve kosete dužine manje od ili jednake $n$ i neka je $Hu$ koset dužine $n+1$, a $v = wa^\alpha$ reč ovog koseta dužine $n+1$. Koset $Hw$ je dužine najviše $n$, dakle njegovog predstavnika znamo – neka je to $z$. Tada $z \bullet a^\alpha$ biramo za predstavnika koseta $Hu$ $(Hu = (Hw)a^\alpha = (Hz)a^\alpha = H(z \bullet a^\alpha))$.□.

S poslednjom lemom dajemo i dokaz teoreme.

**Lema 23.23** *Neka je* $\mathcal{T}_S$ *Schreierova transverzala podgrupe* $\mathbf{H}$. *Tada je* $(\{b_{\overline{u},a} \mid z_{\overline{u},a} \neq 1\}; \emptyset)$ *prezentacija podgrupe* $\mathbf{H}$.

*Posebno,* $\{z_{\overline{u},a} \mid \overline{u} \in \mathcal{T}_S, a \in A, z_{\overline{u},a} \neq 1\}$ *je slobodna baza podgrupe* $\mathbf{H}$.

**Dokaz.** Prema prethodnoj lemi već imamo prezentaciju $(B; \{(\overline{u})\psi \mid \overline{u} \in \mathcal{T}_S\})$. Pokazujemo da su normalne podgrupe $\mathbf{M}$ $(= \mathbf{Ker}(\theta))$ (normalno zatvorenje skupa $\{(\overline{u})\psi \mid \overline{u} \in \mathcal{T}_S\}$) i $\mathbf{N}$, normalno zatvorenje skupa $\{b_{\overline{u},a} \mid \overline{u} \in \mathcal{T}_S, a \in A, z_{\overline{u},a} = 1\}$ jednake, a tada prema 21.13 proizilazi da je $\mathbf{H}$ $(\cong \mathbf{F}_B/\mathbf{N})$ slobodna grupa (videti i komentar uz lemu 23.2). Kao i malopre, za $b_{\overline{u},a}$, gde je $z_{\overline{u},a} = 1$, imamo:

$$(b_{\overline{u},a})\theta = (((a)\psi_{\overline{u}})\varphi)\psi = (\overline{u} \bullet a \bullet (\overline{u \bullet a})^{-1})\psi = (z_{\overline{u},a})\psi = (1)\psi = 1.$$

S druge strane, indukcijom po dužini elemenata transverzale $\mathcal{T}_S$ dokazujemo da je $(\overline{u})\psi \in N$. To je jasno za praznu reč (element dužine 0). Pretpostavimo da tvrđenje važi za sve elemente transverzale dužine manje od ili jednake $n$ i neka je $l(\overline{u}) = n+1$, $\overline{u} \equiv \overline{v}a^\alpha$, $\alpha \in \{1, -1\}$. Po induktivnoj hipotezi je $(\overline{v})\psi \in N$, a prema $(*)$ je: $(\overline{u})\psi = (\overline{v} \bullet a^\alpha)\psi = (\overline{v})\psi \bullet (a^\alpha)\psi_{\overline{v}}$. Za $\alpha = 1$ je $(a)\psi_{\overline{v}} = b_{\overline{v},a}$, pa je, zbog $z_{\overline{v},a} = \overline{v} \bullet a \bullet (\overline{v \bullet a})^{-1} = \overline{u} \bullet \overline{u}^{-1} = 1$, $(\overline{u})\psi \in N$. Ako je $\alpha = -1$, tada je $\overline{v} = \overline{\overline{u} \bullet a}$ i $(a^{-1})\psi_{\overline{v}} = (a^{-1})\psi_{\overline{\overline{u} \bullet a}} = ((a)\psi_{\overline{u}})^{-1}$ (jer $1 = (a \bullet a^{-1})\psi_{\overline{u}} = (a)\psi_{\overline{u}} \bullet (a^{-1})\psi_{\overline{\overline{u} \bullet a}}) = b_{\overline{u},a}^{-1}$, a $(b_{\overline{u},a}^{-1})\varphi = ((b_{\overline{u},a})\varphi)^{-1} = z_{\overline{u},a}^{-1} = (\overline{u} \bullet a \bullet (\overline{u \bullet a})^{-1})^{-1} = (\overline{v} \bullet \overline{v}^{-1})^{-1} = 1$, i opet $(\overline{u})\psi \in N$.

Dodajmo. Neka je $u \equiv a_1^{\alpha_1} \dots a_n^{\alpha_n} \in H$, $\alpha_i \in \{1, -1\}$ (zbog bolje preglednosti ne koristimo dvojne indekse; dakle, umesto pravilnog $a_{i_1}$ stavljamo jednostavno $a_1$). Tada je, prema $(*)$ i ostalom već dokazanom:

$$u = ((u)\psi)\varphi = ((a_1^{\alpha_1})\psi \bullet (a_2^{\alpha_2})\psi_{\overline{a_1^{\alpha_1}}} \bullet (a_3^{\alpha_3})\psi_{\overline{a_1^{\alpha_1} a_2^{\alpha_2}}} \bullet \dots \bullet (a_n^{\alpha_n})\psi_{\overline{a_1^{\alpha_1} a_2^{\alpha_2} \dots a_{n-1}^{\alpha_{n-1}}}})\varphi =$$

$$((a_1^{\alpha_1})\psi)\varphi \bullet ((a_2^{\alpha_2})\psi_{\overline{a_1^{\alpha_1}}})\varphi \bullet \dots \bullet ((a_n^{\alpha_n})\psi_{\overline{a_1^{\alpha_1} a_2^{\alpha_2} \dots a_{n-1}^{\alpha_{n-1}}}})\varphi.$$



Ako je, za dato $i$, $1 \leq i \leq n$ (gde ćemo za $i = 1$, jasno, podrazumevati: $a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}} \equiv 1$), $\alpha_i = 1$, imamo:

$$((a_i)\psi_{\overline{a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}}}})\varphi = (b_{\overline{a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}}}, a_i})\varphi = z_{\overline{a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}}}, a_i} =$$

$$\overline{a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}}} \bullet a_i \bullet (\overline{a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}} a_i})^{-1}.$$

Ako je pak $\alpha_i = -1$, onda je:

$$((a_i^{-1})\psi_{\overline{a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}}}})\varphi = (b_{\overline{a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}} a_i^{-1}}, a_i})\varphi = z_{\overline{a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}} a_i^{-1}}, a_i}^{-1} =$$

$$(\overline{a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}} a_i^{-1}} \bullet a_i \bullet (\overline{a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}} a_i^{-1} \bullet a_i})^{-1})^{-1} =$$

$$\overline{a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}}} \bullet a_i^{-1} \bullet (\overline{a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}} a_i^{-1}})^{-1}.$$

Prema tome, ako je $u_0 = 1$ i $u_i \equiv a_1^{\alpha_1} \dots a_i^{\alpha_i}$ za $1 \leq i \leq n$, tada je:

$$u = a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n} = \prod_{i=1}^{n} (\overline{u_{i-1}} \bullet a_i^{\alpha_i} \bullet \overline{u_i}^{-1}) \qquad (***).$$

Posebno, primetimo, pokazali smo da je dužina svakog elementa $u$ iz $\mathbf{H}$ s obzirom na izabranu slobodnu bazu za $\mathbf{H}$ jednaka ili manja od dužine tog elementa s obzirom na slobodnu bazu grupe $\mathbf{F}_A$.□

Recimo na kraju da je ova teorema direktna posledica teoreme 26.1 (korolar 26.5). Svejedno, ponudili smo i ovaj interesantan dokaz jer će nam još biti od koristi.■

Sada smo u mogućnosti da ponudimo i pojačanu verziju tvrđenja 23.15.

**Lema 23.24** *Unija rastućeg lanca slobodnih grupa ograničenog konačnog ranga je Hopfova.*

**Dokaz.** Primetimo prvo da je, prema prethodnoj teoremi, unija rastućeg lanca slobodnih grupa *lokalno slobodna* grupa, tj. svaki konačan podskup generiše slobodnu grupu. Generalno, unija lanca ne mora biti slobodna grupa. Tako je npr. aditivna grupa racionalnih brojeva unija rastućeg lanca slobodnih grupa ranga 1, sve njene konačno generisane podgrupe su slobodne grupe ranga 1 (tj. beskonačne ciklične grupe), ali sama nije slobodna.

Neka je dat lanac slobodnih grupa $\mathbf{F}_0 \leq \mathbf{F}_1 \leq \dots \leq \mathbf{F}_\alpha \leq \dots$, $\alpha < \lambda$, takav da je rang svake grupe $\mathbf{F}_\alpha$ manji od ili jednak $r$ $(\in \omega)$. Indukcijom po $r$ pokazujemo da je $\mathbf{G} = \bigcup_{\alpha<\lambda} \mathbf{F}_\alpha$ Hopfova grupa. Slučaj $r = 0$ je trivijalan. Pretpostavimo da je tvrđenje tačno za sve lance slobodnih grupa ranga manjeg od pozitivnog prirodnog broja $r$ kao i da je, za "naš" dati lanac, $\mathbf{G} \cong \mathbf{G}/\mathbf{N}$ za neku nejediničnu normalnu podgrupu $\mathbf{N}$ (tj. da grupa $\mathbf{G}$ nije Hopfova). Ako je $\mathbf{F}_\beta \cap \mathbf{N} \neq \mathbf{E}$, onda je, za svako $\gamma \geq \beta$, $\mathbf{F}_\gamma \cap \mathbf{N} \neq \mathbf{E}$, i $(\mathbf{F}_\gamma \mathbf{N})/\mathbf{N}$ $(\cong \mathbf{F}_\gamma/(\mathbf{F}_\gamma \cap \mathbf{N})$ je konačno generisana podgrupa lokalno slobodne grupe $\mathbf{G}/\mathbf{N}$ $(\cong \mathbf{G})$, znači

slobodna grupa i to ranga manjeg od $r$; ako je $\{a_1, \ldots, a_n\}$ slobodna baza grupe $\mathbf{F}_\gamma$, $n \leq r$, i $e \neq a_{j_1}^{m_1} \ldots a_{j_k}^{m_k} \in F_\gamma \cap N$, tada je $(a_{j_1}N)^{m_1} \ldots (a_{j_k}N)^{m_k} = N$, pa je $\{a_1N, \ldots, a_nN\}$ generatorni skup ali ne i slobodna baza grupe $(\mathbf{F}_\gamma\mathbf{N})/\mathbf{N}$ (videti 23.16 i 23.17). No $\mathbf{G}/\mathbf{N} = \bigcup_{\gamma \geq \beta}(\mathbf{F}_\gamma\mathbf{N})/\mathbf{N}$ i prema induktivnoj hipotezi je $\mathbf{G}/\mathbf{N}$ (a onda i $\mathbf{G}$) Hopfova grupa, kontradikcija.□

**Korolar 23.25** *Neka je* $\mathbf{G}$ *takva grupa da je za svaku grupu* $\mathbf{H}$ *ekstenzija grupe* $\mathbf{H}$ *grupom* $\mathbf{G}$ *poludirektni proizvod sa normalnim faktorom* $\mathbf{H}$. *Tada je* $\mathbf{G}$ *slobodna grupa.*

**Dokaz.** Neka je $\mathbf{G} \cong \mathbf{F}_A/\mathbf{H}$. Prema uslovu korolara je, za neku podgrupu $\mathbf{K}$ grupe $\mathbf{F}_A$, $\mathbf{F}_A = \mathbf{H} \leftthreetimes \mathbf{K}$. Odatle, $\mathbf{G} \cong \mathbf{K}$ i $\mathbf{G}$ je slobodna grupa.□

**Korolar 23.26** (*a*) *Neka je* $\mathbf{H}$ *podgrupa konačnog indeksa* $m$ *slobodne grupe konačnog ranga* $n$ *(slobodno reduciranih) reči* $\mathbf{F}_A$ $(A = \{a_1, \ldots, a_n\})$. *Tada je* $\mathbf{H}$ *slobodna grupa ranga* $m(n-1)+1$;

(*b*) *Ako je* $\mathbf{F}_A$ *konačnog ranga i* $\mathbf{F}_A/\mathbf{K}$ *konačna neciklična grupa, tada je rang podgrupe* $\mathbf{K}$ *veći od ranga grupe* $\mathbf{F}_A$.

(*c*) *Ako su* $\mathbf{H}$ *i* $\mathbf{K}$ *podgrupe istog konačnog indeksa slobodne grupe konačnog ranga, tada su te podgrupe i izomorfne.*

**Dokaz.** (*a*) Koristimo notaciju iz dokaza prethodne teoreme. Neka je $\mathcal{T}_S$ desna Schreierova transverzala podgrupe $\mathbf{H}$ kakvu smo konstruisali u 23.22. Elemenata $z_{\overline{u},a_i}$ ima $mn$ pa je, prema poslednjoj lemi, rang podgrupe $\mathbf{H}$ $mn-k$, gde je $k = |\{z_{\overline{u},a_i} \mid z_{\overline{u},a_i} = 1\}|$. Definišimo preslikavanje $\Psi$ skupa $K = \{H\overline{u} \mid \overline{u} \in \mathcal{T}_S \setminus \{1\}\}$ u skup $\mathcal{T}_S \times A$ na sledeći način: ako je $\overline{u} = \overline{w}a_i^\alpha$, $\alpha \in \{1, -1\}$, tada je:

$$(H\overline{u})\Psi = \begin{cases} (\overline{u}, a_i) & \alpha = -1 \\ (\overline{w}, a_i) & \alpha = 1 \end{cases}.$$

Preslikavanje $\Psi$ je jedan-jedan. Zaista, neka je za $\overline{u} = \overline{w}a_i^\alpha$, $\overline{v} = \overline{z}a_j^\beta \in \mathcal{T}_S$, $(H\overline{u})\Psi = (H\overline{v})\Psi$. Jasno, $a_i \equiv a_j$, tj. $i = j$. Ako je $\alpha = \beta = 1$ ili $\alpha = \beta = -1$, odmah sledi i $\overline{u} = \overline{v}$. Pretpostavima stoga da je npr. $\alpha = -1$, $\beta = 1$; dakle, $(H\overline{u})\Psi = (\overline{u}, a_i) = (\overline{z}, a_i) = (H\overline{v})\Psi$. Odatle, $\overline{u} = \overline{z}$, no $\overline{u}$ se završava sa $a_i^{-1}$ dok se $\overline{z}$, kao početni segment reducirane reči $\overline{v}$, ne može završavati sa $a_i^{-1}$, kontradikcija. Za svako $(\overline{w}, a_i) \in (K)\Psi$ je $z_{\overline{u},a_i} = 1$. Jer, ako je $(\overline{w}, a_i) = (H\overline{u})\Psi$, onda je ili $\overline{w} = \overline{u}$ i $\overline{u} = \overline{w}a_i^{-1}$ ili $\overline{u} = \overline{w}a_i$; u prvom slučaju imamo: $z_{\overline{u},a_i} = \overline{u} \bullet a_i \bullet (\overline{\overline{u} \bullet a_i})^{-1} = \overline{w}a_i^{-1} \bullet a_i \bullet (\overline{\overline{w}a_i^{-1} \bullet a_i})^{-1} = \overline{w} \bullet \overline{w}^{-1} = 1$, u drugom: $\overline{\overline{w}a_i} = \overline{w} \bullet a_i \bullet (\overline{w} \bullet a_i)^{-1} = \overline{u} \bullet \overline{u}^{-1} = 1$ (trivijalno, $\overline{w} = \overline{w}$). Prema tome, za $m-1$ elemenata $z_{\overline{u},a_i}$ već znamo da su jedinični element. No u tom spisku su zapravo i svi elementi $z_{\overline{u},a_i}$ jednaki jediničnom. Neka je $z_{\overline{u},a_i} = \overline{u} \bullet a_i \bullet (\overline{u \bullet a_i})^{-1} = 1$, tj. $\overline{u} \bullet a_i = \overline{u \bullet a_i}$. Ako je $\overline{u} = \overline{w}a_j^\alpha$, gde je $j \neq i$ ili $\alpha \neq -1$, onda je $\overline{w}a_j^\alpha a_i = \overline{\overline{w}a_j^\alpha a_i}$ i $(\overline{u}, a_i) = (H(\overline{w}a_j^\alpha a_i))\Psi$. Ako je pak $\overline{u} = \overline{w}a_i^{-1}$, tada je $(\overline{u}, a_i) = (H\overline{u})\Psi$. Zaključujemo: $|\{(\overline{u}, a_i) \mid z_{\overline{u},a_i} = 1\}| = m-1$, pa je grupa $\mathbf{H}$ ranga $nm-(m-1) = m(n-1)+1$.

(*b*) i (*c*) su direktna posledica tačke (*a*); za (*c*) nam treba i 23.10.□



**Korolar 23.27** *(O. Schreier). Podgrupa konačnog indeksa konačno generisane grupe je i sama konačno generisana.*

**Dokaz.** Ovo tvrđenje smo već dokazali – 9.39. Sada ćemo, u ovom drugom dokazu, iskoristiti 23.26(*a*). Neka je $\mathbf{H}$ podgrupa konačnog indeksa grupe $\mathbf{G}$, koja je pak konačno generisana, i neka je $\mathbf{G} \cong \mathbf{F}_A/\mathbf{K}$, gde je rang grupe $\mathbf{F}_A$ jednak (konačnom) broju generatornih elemenata grupe $\mathbf{G}$. Ako je, za podgrupu $\mathbf{L}$ grupe $\mathbf{F}_A$, $\mathbf{H} \cong \mathbf{L}/\mathbf{K}$, sledi (pošto je $[\mathbf{F}_A : \mathbf{L}] = [\mathbf{G} : \mathbf{H}]$) da je $\mathbf{L}$ slobodna grupa konačnog ranga, te je i $\mathbf{H}$ konačno generisana.□

**Lema 23.28** (*a*) *Neka je* $\mathbf{F}_A$ *slobodna grupa (slobodno reduciranih reči) konačnog ranga* $n$ *većeg od* 1. *Tada je* $\mathbf{F}'_A$ *slobodna grupa prebrojivog ranga;*

(*b*) *Izvodna podgrupa slobodne necikличne grupe je beskonačnog ranga.*

(*c*) *Ako je slobodna grupa* $\mathbf{F}_A$ *ranga većeg od* 1 *(tj. ako nije ciklična), onda je* $\mathbf{F}_A^{(n)} \neq \mathbf{E}$ *za svaki prirodan broj* $n$.

**Dokaz.** (*a*) $\mathbf{F}_A/\mathbf{F}'_A$ je slobodna Abelova grupa ranga $n$ (videti 21.10(*i*) i 21.12), pa svaki desni koset podgrupe $\mathbf{F}'_A$ sadrži jedinstven element oblika $a_1^{\alpha_1} \ldots a_n^{\alpha_n}$, gde su $\alpha_i$, $i = 1, \ldots, n$, celi brojevi. Skup svih tih elemenata je evidentno Schreierova transverzala podgrupe $\mathbf{F}'_A$ – $\mathcal{T}_S$. Ali za svako $\overline{u} \equiv a_1^{\alpha_1} \ldots a_k^{\alpha_k}$, $k \leq n$, gde je $\alpha_k \neq 0$, i svako $a_i$, gde je $i < k$, važi:

$$z_{\overline{u},a_i} = \overline{u} \bullet a_i \bullet (\overline{\overline{u} \bullet a_i})^{-1} = a_1^{\alpha_1} \ldots a_i^{\alpha_i} \ldots a_k^{\alpha_k} \bullet a_i \bullet a_1^{\alpha_1} \ldots a_i^{\alpha_i+1} \ldots a_k^{\alpha_k} =$$

$$a_1^{\alpha_1} \ldots a_i^{\alpha_i} \ldots a_k^{\alpha_k} a_i a_k^{-\alpha_k} \ldots a_i^{-(\alpha_i+1)} \ldots a_1^{-\alpha_1} \neq 1,$$

jer je

$$F'_A(a_1^{\alpha_1} \ldots a_i^{\alpha_i} \ldots a_k^{\alpha_k} \bullet a_i) = (F'_A a_1)^{\alpha_1} \cdot \ldots \cdot (F'_A a_i)^{\alpha_i} \cdot \ldots \cdot (F'_A a_k)^{\alpha_k} \cdot F'_A a_i =$$

$$(F'_A a_1)^{\alpha_1} \cdot \ldots \cdot (F'_A a_i)^{\alpha_i+1} \cdot \ldots \cdot (F'_A a_k)^{\alpha_k} = F'_A(a_1^{\alpha_1} \ldots a_i^{\alpha_i+1} \ldots a_k^{\alpha_k}).$$

Prema tome, beskonačno mnogo elemenata $z_{\overline{u},a_i}$ je različito od 1 i $\mathbf{F}'_A$ je beskonačno prebrojivog ranga.

U vezi tačke (*c*) videti i korolar 23.31.□

**Korolar 23.29** *Nijedna slobodna nejedinična grupa nije kohopfova.*

**Dokaz.** Direktno prema tački (*b*) prethodne leme i trivijalnoj činjenici da grupa $\mathbf{Z}$ ima injektivne endomorfizme koji nisu automorfizmi.□

**Teorema 23.30** *(M. Hall). Neka je* $\mathbf{F}_A$ *slobodna grupa (slobodno reduciranih reči) i neka je* $\mathbf{F}_A = \mathbf{H}_0 > \mathbf{H}_1 > \cdots > \mathbf{H}_k > \cdots$ *opadajući niz podgrupa sa svojstvom: za svaki izbor slobodnih baza podgrupa* $\mathbf{H}_k$, $k \geq 1$, *svaki nejedinični element podrupe* $\mathbf{H}_k$ *ima, s obzirom na bazu u* $\mathbf{H}_{k-1}$, *dužinu veću od* 2. *Tada je* $\bigcap_{k\in\omega} \mathbf{H}_k = \mathbf{E}$.

**Dokaz**. U svakoj podgrupi $\mathbf{H}_k$, $k \geq 1$, posmatranoj kao podgrupu grupe $\mathbf{H}_{k-1}$, za slobodnu bazu biramo onu koju nam daje dokaz Nielsen-Schreierove teoreme (dakle, posebno, slobodna baza podgrupe $\mathbf{H}_1$ biće $\{z_{\overline{u},a} \mid \overline{u}$ je element transverzale podgrupe $\mathbf{H}_1$, $a \in A$, $z_{\overline{u},a} \neq 1\}$). Pokazaćemo, što je i dovoljno, da ako je $v$ nejedinični element podgrupe $\mathbf{H}_k$, $k > 1$, onda je njegova dužina, s obzirom na slobodnu bazu podgrupe $\mathbf{H}_{k-1}$, $l_{k-1}(v)$, strogo veća od njegove dužine, s obzirom na slobodnu bazu podgrupe $\mathbf{H}_k$, $l_k(v)$. Posmatrajmo samo, a više nam i ne treba, podgrupe $\mathbf{F}_A = \mathbf{H}_0$ i $\mathbf{H}_1$. Već znamo (23.23) da je $l_1(v) \leq l_0(v)$ ($\geq 3$ – po uslovu teoreme). Neka je $v \equiv a_1^{\alpha_1} \ldots a_n^{\alpha_n}$. Pretpostavimo da je $a_1^{\alpha_1} \neq \overline{a_1^{\alpha_1}}$. Tada je, za neko $w \in H_1$, $w = a_1^{\alpha_1}\overline{a_1^{\alpha_1}}^{-1}$. No prema konstrukciji Schreierove transverzale je $l_0(\overline{a_1^{\alpha_1}}) = 1$, pa je dužina elementa $w$ iz $\mathbf{H}_1$ manja (u $\mathbf{H}_0$) od 3, protivno uslovu teoreme. Odatle sledi da je prvi faktor u prouzvodu

$$v = a_1^{\alpha_1}a_2^{\alpha_2}\ldots a_n^{\alpha_n} = \prod_{i=1}^{n}(\overline{v_{i-1}} \bullet a_i^{\alpha_i} \bullet \overline{v_i}^{-1}) \qquad (***)$$

(videti formulu $(***)$ u 23.23), a svi ti faktori su oblika $z_{\overline{u},a}^{\alpha}$, $\alpha \in \{1,-1\}$, jedinični element. Jasno, pretpostavka da postoji nejedinični element $v$ u preseku svih podgrupa $\mathbf{H}_k$, $k \in \omega$, implicirala bi egzistenciju beskonačnog strogo opadajućeg niza prirodnih brojeva: $l_0(v) > l_1(v) > \cdots > l_k(v) > \cdots$, kontradikcija.■

**Korolar 23.31** *Za svaku slobodnu grupu* $\mathbf{F}_A$ *(slobodno reduciranih reči) važi:*

$$\mathbf{F}_A^{(\omega)} \stackrel{\text{def}}{=} \bigcap_{k\in\omega} \mathbf{F}_A^{(k)} = \mathbf{E}.$$

**Dokaz**. Neka je $1 \neq w = [u_1, v_1]^{\alpha_1}\ldots[u_m, v_m]^{\alpha_m} = a_1^{\beta_1}\ldots a_n^{\beta_n} \in F_A'$ $(= F_A^{(1)})$, $\alpha_i, \beta_j \in \{1,-1\}$. Pošto je zbir eksponenata svakog slova $a_j$ u redukovanoj reči $a_1^{\beta_1}\ldots a_n^{\beta_n}$ nula, što će reći da se svako slovo javlja paran broj puta, $n$ mora biti veće od ili jednako 4. Preostalo je samo da se pozovemo na prethodnu teoremu.

Ovaj rezultat je, inače, i direktna posledica Magnusove teoreme – 48.52.□

Daćemo na kraju ovog paragrafa još jedno svojstvo slobodnih grupa. No prvo

**Definicija 23.32** *Grupa* $\mathbf{G}$ *je projektivna akko za svake dve grupe* $\mathbf{H}$ *i* $\mathbf{K}$ *i svako homomorfno preslikavanje* $\varphi$ *grupe* $\mathbf{H}$ *na* $\mathbf{K}$ *(ako takvo postoji) i svako homomorfno preslikavanje* $\psi$ *grupe* $\mathbf{G}$ *u* $\mathbf{K}$, *postoji homomorfno preslikavanje* $\theta$ *grupe* $\mathbf{G}$ *u* $\mathbf{H}$ *takvo da je* $\theta \circ \varphi = \psi$.



**Lema 23.33** *Grupa je projektivna akko je slobodna.*

**Dokaz**. ($\Longrightarrow$) Neka je $\mathbf{G}$ projektivna grupa i neka je $\varphi$ surjektivno homomorfno preslikavanje slobodne grupe $\mathbf{F}$ na $\mathbf{G}$ (21.9($c$)). Tada, za identično preslikavanje grupe $\mathbf{G}$ na sebe, postoji homomorfno preslikavanje $\theta$ grupe $\mathbf{G}$ u $\mathbf{F}$ takvo da je $\theta \circ \varphi = \imath_G$. Odatle sledi da je $\theta$ injektivno preslikavanje, $\varphi \circ \theta$ je retrakcija grupe $\mathbf{F}$ ($(\varphi \circ \theta)^2 = \varphi \circ \theta \circ \varphi \circ \theta = \varphi \circ \imath_G \circ \theta = \varphi \circ \theta$) i $(\mathbf{F})(\varphi \circ \theta) = (\mathbf{G})\theta \cong \mathbf{G}$. Kao podgrupa slobodne grupe $(\mathbf{G})\theta$ je slobodna grupa pa je i $\mathbf{G}$ slobodna grupa.

Ovaj pravac se neki put definiše ovako:

*Projektivne grupe su retrakti slobodnih grupa*

($\Longleftarrow$) Neka je $\mathbf{F}$ slobodna grupa sa slobodnom bazom $\{a_i \mid i \in I\}$, $\psi \in Hom(\mathbf{F}, \mathbf{K})$ i neka je $\varphi$ surjektivno homomorfno preslikavanje grupe $\mathbf{H}$ na grupu $\mathbf{K}$. Za svaki element $(a)\psi$ $(\in K)$ postoji (bar jedan) element $h_i$ u $\mathbf{H}$ za koji je $(h_i)\varphi = (a_i)\psi$ (aksioma izbora nam dozvoljava da u opštem slučaju fiksiramo po jedno $h_i$ za svako $i \in I$). Ako je homomorfizam $\theta \in Hom(\mathbf{F}, \mathbf{H})$ određen sa $(a_i)\theta = h_i$ za svako $i \in I$, imaćemo: $(a_i)(\theta \circ \varphi) = (a_i)\psi$, te je $\theta \circ \varphi = \psi$.□

# 24 Varijeteti grupa

Neka su dati skup simbola $\{a_i \mid i \in I\}$ i (neprazna) reč $v = v(a_{i_1}, \ldots, a_{i_m}) \equiv a_{i_1}^{\alpha_1}\ldots a_{i_m}^{\alpha_m}$ (gde je $\alpha_j \in \{1,-1\}$ za $1 \leq j \leq m$) azbuke $A \cup A^{-1}$ (videti uvodni deo paragrafa 21). Za datu grupu $\mathbf{G}$ i njene elemente $g_1, \ldots, g_m$, gde podrazumevamo da su elementi $g_j$ i $g_k$ jednaki ukoliko su i simboli $a_{i_j}$ i $a_{i_k}$ jednaki (isti), izraz $v(g_1, \ldots, g_m) \equiv g_1^{\alpha_1}\ldots g_m^{\alpha_m}$ (videti dokaz tačke ($a$) korolara 21.9) zove se *vrednost reči* $v$ za (uređenu) $m$-torku $(g_1, \ldots, g_m)$. Reč $v$ je *relacija identiteta* ili *zakon* grupe $\mathbf{G}$ akko je njena vrednost za svaku $m$-torku (ne nužno različitih) elemenata grupe $\mathbf{G}$ baš jedinični element ili, drugim rečima, akko svako homomorfno preslikavanje polugrupe reči nad azbukom $A \cup A^{-1}$ u grupu $\mathbf{G}$ preslikava $v$ u jedinični element (videti 21.1, 21.2).

Neka je, uopšte, $R$ skup reči azbuke $A \cup A^{-1}$. Podgrupa grupe $\mathbf{G}$ generisana skupom $\{v(g_1, \ldots, g_m) \mid v = v(a_{i_1}, \ldots, a_{i_m}) \in R, g_i \in G\}$, obeležimo je, za potrebe ovog paragrafa (notacija nije standardna), sa $\mathbf{G}(R)$ (i njen domen sa $G(R)$), je takozvana *verbalna* ili *rečenična podgrupa* grupe $\mathbf{G}$ s obzirom na $R$. Imamo

**Lema 24.1** ($a$) *Verbalna podgrupa grupe* $\mathbf{G}$ *je potpuno invarijantna podgrupa;*

($b$) *Verbalna podgrupa,* $(\mathbf{G}(R))(S)$, *verbalne podgrupe* $\mathbf{G}(R)$ *grupe* $\mathbf{G}$ *je verbalna podgrupa grupe* $\mathbf{G}$.

**Dokaz**. $(a)$ Jasno. Neka je $R$ skup reči (azbuke $A \cup A^{-1}$), $\mathbf{G}(R)$ njemu odgovarajuća verbalna podgrupa grupe $\mathbf{G}$ i $\varphi$ endomorfizam grupe $\mathbf{G}$. No kako je svaki element iz $\mathbf{G}(R)$ proizvod vrednosti reči iz $R$ ili njima inverznog elementa, a slika vrednosti reči $v = v(a_{i_1}, \ldots, a_{i_m})$ $(\in R)$ za $m$-torku $(g_1, \ldots, g_m)$, za endomorfizam $\varphi$, je baš vrednost reči $v$ za $m$-torku $((g_1)\varphi, \ldots, (g_m)\varphi)$, to direktno sledi da je $\mathbf{G}(R)$ potpuno invarijantna podgrupa.

$(b)$ Neka je $u(h_1, \ldots, h_m) = h_1^{\alpha_1} \ldots h_m^{\alpha_m}$, gde je $u = u(a_{i_1}, \ldots, a_{i_m}) \equiv a_{i_1}^{\alpha_1} \ldots a_{i_m}^{\alpha_m} \in S$ $(\alpha_k \in \{1, -1\}$ za $1 \leq k \leq m)$ i $h_1, \ldots, h_m \in G(R)$, jedan element generatornog skupa grupe $(\mathbf{G}(R))(S)$. Da bismo pojednostavili "priču" pretpostavimo da su elementi $h_1, \ldots, h_m$ različiti (dakle, posebno, simboli $a_{i_1}, \ldots, a_{i_m}$ su različiti). Neka je $h_j = (v_1^j(\overline{g}_1^j))^{\beta_1^j} \ldots (v_{n_j}(\overline{g}_{n_j}^j))^{\beta_{n_j}^j}$ za $1 \leq j \leq m$, gde su $v_1^j, \ldots, v_{n_j}^j$ reči skupa $R$, $\overline{g}_1^j, \ldots, \overline{g}_{n_j}^j$ nizovi (adekvatne dužine) elemenata grupe $\mathbf{G}$ i, za $1 \leq k \leq n_j$, $\beta_k^j \in \{1, -1\}$. Preindeksacijom simbola formirajmo reči koje su "slike" reči $v_1^1, \ldots, v_{n_1}^1, \ldots, v_1^m, \ldots, v_{n_m}^m$, obeležimo ih sa $w_1^1, \ldots, w_{n_1}^1, \ldots, w_1^m, \ldots, w_{n_m}^m$, a koje imaju svojstvo da nemaju zajedničkih simbola. Onda je, jasno, $u(h_1, \ldots, h_m)$ vrednost reči $u((w_1^1)^{\beta_1^1} \ldots (w_{n_1}^1)^{\beta_{n_1}^1}, \ldots, (w_1^m)^{\beta_1^m} \ldots (w_{n_m}^m)^{\beta_{n_m}^m}) \equiv ((w_1^1)^{\beta_1^1} \ldots (w_{n_1}^1)^{\beta_{n_1}^1})^{\alpha_1} \ldots ((w_1^m)^{\beta_1^m} \ldots (w_{n_m}^m)^{\beta_{n_m}^m})^{\alpha_m}$ za adekvatno formiran niz elemenata grupe $\mathbf{G}$. Isto tako je očigledno da je svaka druga vrednost date reči takođe jedan element podgrupe $(\mathbf{G}(R))(S)$; jer, svaka vrednost reči $w_k^j$ je ujedno i vrednost reči $v_k^j$, dakle element podgrupe $\mathbf{G}(R)$. Konstatujmo još na kraju: ako među elementima $h_1, \ldots, h_m$ ima jednakih, recimo da su samo $h_j$ i $h_k$ jednaki, ali simboli $a_{i_j}$ i $a_{i_k}$ nisu, ništa se ne mora menjati u dokazu. No ako su neki od simbola $a_{i_1}, \ldots, a_{i_m}$ jednaki, onda, naravno, moramo voditi računa da u reči koju formiramo po opisanom postupku, na pozicije jednakih simbola dođu identične reči.□

Obrat tačke $(a)$ prethodne leme već ne mora da važi, tj. nije u svakoj grupi svaka potpuno invarijantna podgrupa nužno i verbalna podgrupa. Sledeći primer nam to pokazuje.

**Primer 24.2** *U Prüferovoj grupi* $\mathbf{p}^\infty$ *jedine verbalne podgrupe su cela grupa i jedinična podgrupa.*

**Dokaz**. Očigledno su trivijalne podgrupe ma koje grupe $\mathbf{G}$ i verbalne podgrupe; jer, ako je $a$ ma koji simbol azbuke $A$, onda je jedinična podgrupa generisana vrednostima reči $aa^{-1}$, dok je cela grupa generisana vrednostima reči $a$.

Neka je sada $\mathbf{H}$ bilo koja prava nejedinična podgrupa grupe $\mathbf{p}^\infty$. Znamo da je to ciklična grupa čiji je red (nenula) stepen broja $p$, npr. $p^k$; znači $\mathbf{H} = \langle e^{\frac{2\pi}{p^k}i} \rangle$ (videti napomenu uz 7.10). $\mathbf{H}$ je potpuno invarijantna podgrupa s obzirom da su njeni elementi upravo svi elementi grupe $\mathbf{p}^\infty$ reda manjeg od ili jednakog $p^k$. Pretpostavimo da je $\mathbf{H}$ i verbalna podgrupa, recimo, $\mathbf{H} = \mathbf{p}^\infty(R)$. Kako je $\mathbf{p}^\infty$ Abelova grupa, postoji (bar jedna) reč $v \equiv a_{i_1}^{\alpha_1} \ldots a_{i_m}^{\alpha_m}$ u



$R$ kod koje je bar jedan zbir "stepena" uz iste simbole različit od nule. Neka je npr. $a_{i_{j_1}} = a_{i_{j_2}} = \cdots = a_{i_{j_r}}$ (tj. $i_{j_1} = i_{j_2} = \cdots = i_{j_r}$) i $\alpha_{j_1} + \alpha_{j_2} + \cdots + \alpha_{j_r} = n > 0$. Tada je vrednost reči $v$ za niz elemenata grupe $\mathbf{p}^\infty$ koji simbolu $a_{i_{j_1}}$ "dodeljuje" $e^{\frac{2\pi}{p^t}i}$, gde je $p^t > np^k$, a ostalim (od njega različitim) simbolima jedinicu, $e^{\frac{2n\pi}{p^t}i}$, a red ovog elementa je veći od $p^k$, kontradikcija.□

**Napomena**. Pošto su, trivijalno, reči oblika $aa^{-1}$, $a^{-1}a$ zakoni za svaku grupu, u daljim razmatranjima će reči, ukoliko ne naglasimo drugačije, biti slobodno reducirane, dakle elementi slobodne grupe (slobodno reduciranih reči), sa slobodnom bazom $A$ – $\mathbf{F}_A$; generalno, skup simbola $A$ je proizvoljne kardinalnosti. Jediničnu (pod)grupu možemo onda tretirati kao verbalnu (pod)grupu koja odgovara bilo praznom skupu reči bilo skupu koji sadrži samo praznu reč, čija je vrednost, dogovorno definišemo, jedinični element.

**Definicija 24.3** *Neka je $R$ skup slobodno reduciranih reči azbuke $A \cup A^{-1}$ (podskup domena slobodne grupe $\mathbf{F}_A$). Klasa svih grupa za koje su svi elementi iz $R$ zakoni (relacije identiteta) zove se varijetet ili jednakosna klasa grupa određena skupom $R$; eng. variety ili equational class, takođe i primitive class ([57]) – termin varijetet je preuzet iz algebarske geometrije. Taj varijetet ćemo obeležiti sa $\mathcal{V}(R)$.*

Mogli smo, naravno, varijetet $\mathcal{V}(R)$ definisati i kao klasu svih grupa $\mathbf{G}$ takvih da je $(v)\varphi = e_G$ za svako $\varphi \in Hom(\mathbf{F}_A, \mathbf{G})$ i svako $v \in R$ (tj. $R \subseteq Ker(\varphi)$), odnosno takvih da je $\mathbf{G}(R) = \mathbf{E}$.

Za $R = \{a^{-1}b^{-1}ab\}$, $\mathcal{V}(R)$ je klasa Abelovih grupa; za $S = \{a^{-1}b^{-1}ab, a^p\}$, gde je $p$ prost broj, $\mathcal{V}(S)$ je klasa direktnih proizvoda cikličnih grupa reda $p$ (10.30); posebno, ako je $p$ baš 2, skupovi $\{a^{-1}b^{-1}ab, a^2\}$ i $\{a^2\}$ određuju isti varijetet $(2.7(f))$.

**Lema 24.4** *Svaka potpuno invarijantna podgrupa slobodne grupe je verbalna podgrupa.*

**Dokaz**. Neka je $\mathbf{H}$ potpuno invarijantna podgrupa slobodne grupe $\mathbf{F}_A$. Tvrdimo: $\mathbf{H} = \mathbf{F}_A(H)$. Jer, neka je $v \equiv a_{i_1}^{\alpha_1} \ldots a_{i_m}^{\alpha_m} \in H$ i $u_1, \ldots, u_m$ niz elemenata grupe $\mathbf{F}_A$, gde su elementi $u_j$ i $u_k$ jednaki ako su simboli $a_{i_j}$ i $a_{i_k}$ jednaki (tj. ako je $i_j = i_k$). No tada postoji endomorfizam $\varphi$ grupe $\mathbf{F}_A$ za koji je $(a_{i_j})\varphi = u_j$, $j = 1, \ldots, m$, pa je $v(u_1, \ldots, u_m) = (v)\varphi \in H$; dakle, svaka vrednost reči $v$ je u $\mathbf{H}$.□

Ako je $\mathcal{C}$ klasa grupa i $\mathbf{F}_A$ slobodna grupa slobodno reduciranih reči, što ćemo do kraja ovog paragrafa podrazumevati, onda klasi $\mathcal{C}$ dodeljujemo podskup domena grupe $\mathbf{F}_A$ čiji su elementi relacije identiteta svake grupe klase $\mathcal{C}$. Lako se proverava da je dati skup domen potpuno invarijantne podgrupe grupe $\mathbf{F}_A$; jer, očigledno (a i na osnovu dokaza prethodne leme), ako je $\mathbf{G} \in \mathcal{V}(\{v\})$

i $\theta \in End(\mathbf{F}_A)$, onda je $\mathbf{G} \in \mathcal{V}(\{(v)\theta\})$. Saglasno sa uvedenom notacijom, označićemo dobijenu potpuno invarijantnu podgrupu sa $\mathbf{F}_A(C)$. Njen domen, $F_A(C) \stackrel{\text{def}}{=} \{v \in F_A \mid \mathbf{G} \in \mathcal{V}(\{v\}) \text{ za svako } \mathbf{G} \text{ iz } C\}$, zove se *relacioni skup* grupe $\mathbf{F}_A$ određen klasom grupa $C$.

**Lema 24.5** *Neka je $R$ podskup domena grupe $\mathbf{F}_A$. Tada je $\mathcal{V}(R) = \mathcal{V}(F_A(R))$.*

**Dokaz.** Inkluzija ($\supseteq$) je (više nego) jasna. Opet, neka je $\mathbf{G} \in \mathcal{V}(R)$. Kako je podgrupa $\mathbf{F}_A(R)$ generisana skupom $\bigcup\{(R)\theta \mid \theta \in End(\mathbf{F}_A)\}$, dovoljno je da pokažemo da je, za svako $\varphi \in Hom(\mathbf{F}_A, \mathbf{G})$ i svako $\theta \in End(\mathbf{F}_A)$, $(R)\theta \in Ker(\varphi)$. No $\theta \circ \varphi$ je homomorfno preslikavanje grupe $\mathbf{F}_A$ u grupu $\mathbf{G}$, te je, zbog $\mathbf{G} \in \mathcal{V}(R)$, $R \subseteq Ker(\theta\circ\varphi)$, a odatle sledi traženo $(R)\theta \subseteq Ker(\varphi)$.□

**Lema 24.6** *Neka su dati slobodna grupa $\mathbf{F}_A$, podskupovi njenog domena $R$, $S$, $R_i$, $i \in I$, i klase grupa $C$, $\mathcal{D}$, $C_j$, $j \in J$. Tada važi:*

*(a) Ako je $R \subseteq S$, onda je $\mathcal{V}(S) \subseteq \mathcal{V}(R)$;*

*(b) Ako je $C \subseteq \mathcal{D}$, onda je $\mathbf{F}_A(\mathcal{D}) \leq \mathbf{F}_A(C)$;*

*(c) $\mathcal{V}(\bigcup_{i\in I} R_i) = \bigcap_{i\in I} \mathcal{V}(R_i)$;*

*(d) $\mathbf{F}_A(\bigcup_{i\in I} C_i) = \bigcap_{i\in I} \mathbf{F}_A(C_i)$;*

*(e) $R \subseteq F_A(\mathcal{V}(R))$;*

*(f) $C \subseteq \mathcal{V}(F_A(C))$;*

*(g) $\mathcal{V}(R) = \mathcal{V}(F_A(\mathcal{V}(R)))$;*

*(h) $\mathbf{F}_A(C) = \mathbf{F}_A(\mathcal{V}(F_A(C)))$.*

**Dokaz.** Sve je manje-više očigledno.

*(d)* Jasno, za svako $j \in I$ je, zbog $C_j \subseteq \bigcup_{i\in I} C_i$, $\mathbf{F}_A(\bigcup_{i\in I} C_i) \leq \mathbf{F}_A(C_j)$, pa je $\mathbf{F}_A(\bigcup_{i\in I} C_i) \leq \bigcap_{i\in I} \mathbf{F}_A(C_i)$. Ako pak $v \notin F_A(\bigcup_{i\in I} C_i)$, onda je, za neku grupu $\mathbf{G}$ i neki indeks $j$, $\mathbf{G} \in C_j$ i $\mathbf{G} \notin \mathcal{V}(\{v\})$, pa $v \notin F_A(C_j)$.

*(e)* Neka je $v \in R$. Onda je, za svaku grupu $\mathbf{G}$ iz $\mathcal{V}(R)$, $\mathbf{G} \in \mathcal{V}(\{v\})$, te je $v \in F_A(\mathcal{V}(R))$.

*(f)* Neka je grupa $\mathbf{G}$ iz $C$. Tada je, za svaku reč $v$ iz $F_A(C)$, $\mathbf{G} \in \mathcal{V}(\{v\})$, dakle $\mathbf{G} \in \mathcal{V}(F_A(C))$.

*(g)* Inkluzija ($\supseteq$) je direktna posledica tačaka *(a)* i *(e)*. Pretpostavimo sada da grupa $\mathbf{G}$ nije u varijetetu $\mathcal{V}(F_A(\mathcal{V}(R)))$. Onda, za neku reč $v$ iz $F_A(\mathcal{V}(R))$, $\mathbf{G} \notin \mathcal{V}(\{v\})$ i stoga $\mathbf{G} \notin \mathcal{V}(R)$.

*(h)* Inkluzija $\geq$ je direktna posledica tačaka *(b)* i *(f)*. Ako pak $v$ nije element podgrupe $\mathbf{F}_A(\mathcal{V}(F_A(C)))$, tada $\mathbf{G} \notin \mathcal{V}(\{v\})$ za neku grupu $\mathbf{G}$ iz $\mathcal{V}(F_A(C))$, znači $v \notin F_A(C)$.□

**Korolar 24.7** *Presek familije varijeteta grupa je varijetet grupa.*



**Definicija 24.8** *Grupa $\mathbf{G}$ je slobodna grupa klase grupa $C$ (kaže se i: slobodna grupa za klasu ili nad klasom $C$) sa slobodno generatornim skupom (slobodnom bazom) $B = \{g_i \mid i \in I\}$ $(\subseteq G)$ akko pripada klasi $C$, $B$ je njen generatorni skup i za svaku grupu $\mathbf{H}$ iz $C$ i svako preslikavanje $\varphi : B \longrightarrow H$ postoji homomorfno preslikavanje $\overline{\varphi}$ grupe $\mathbf{G}$ u $\mathbf{H}$ koje je ekstenzija preslikavanja $\varphi$. Dozvoljavamo mogućnost da je $I$ prazan skup, tj. da je jedinična grupa slobodna grupa.*

**Napomena.** Jasno, ako klasa $C$ sadrži samo jedinične grupe, imamo trivijalan slučaj (svaki njen element je ujedno i njena slobodna grupa), pa ga, kao takvog, i ne uzimamo u razmatranje.

Primetimo, dokaz sledi kao i u ranijim razmatranjima (videti 23.5 i 23.9), da je homomorfizam $\overline{\varphi}$ jedinstven; konačno, slobodne grupe o kojima je dosad bilo reč su slobodne grupe nad klasom svih grupa.

**Lema 24.9** *Neka je dat skup reči $R$ azbuke $X \cup X^{-1}$. Tada je, za svaki skup $A$, $\mathbf{F}_A/\mathbf{F}_A(R)$ slobodna grupa varijeteta $\mathcal{V}(R)$ sa slobodnom bazom (ukoliko nije jedinična grupa): $B = \{aF_A(R) \mid a \in A\}$. Takođe važi: svaka slobodna grupa varijeteta $\mathcal{V}(R)$ izomorfna je nekoj od grupa datog oblika.*

**Dokaz.** Trivijalno sledi: $\mathbf{F}_A/\mathbf{F}_A(R) \in \mathcal{V}(R)$. Jer, neka je $x_{i_1}^{\alpha_1} \dots x_{i_m}^{\alpha_m} \in R$ i neka je $u_1F_A(R), \dots, u_mF_A(R)$ niz elemenata date faktor grupe, gde su elementi $u_jF_A(R)$ i $u_kF_A(R)$ jednaki ako su simboli $x_{i_j}$ i $x_{i_k}$ isti. No ako su elementi $u_jF_A(R)$ i $u_kF_A(R)$ jednaki, uzećemo da su i reči $u_j$ i $u_k$ jednake (kako je svaki element koseta ravnopravno njegov predstavnik imamo na to pravo) i tako dobijamo (s obzirom na učinjenu pretpostavku i definiciju podgrupe $\mathbf{F}_A(R)$): $(u_1F_A(R))^{\alpha_1} \dots (u_mF_A(R))^{\alpha_m} = (u_1^{\alpha_1} \dots u_m^{\alpha_m})F_A(R) = F_A(R)$. Dalje, neka je $\mathbf{H} \in \mathcal{V}(R)$ i neka je preslikavanje $\varphi : B \longrightarrow H$ dato sa $(a_iF_A(R))\varphi = h_i$. Ako je $\overline{\psi}$ homomorfno preslikavanje grupe $\mathbf{F}_A$ u grupu $\mathbf{H}$ koje je ekstenzija preslikavanja $\psi : A \longrightarrow H$, gde je $(a_i)\psi = h_i$, tada $\mathbf{F}_A(R) \leq \mathbf{Ker}(\overline{\psi})$, jer se svi generatorni elementi grupe $\mathbf{F}_A(R)$, a to su vrednosti reči iz $R$ u $\mathbf{F}_A$, preslikavaju u jedinični element grupe $\mathbf{H}$. No ako je $\theta$ kanoničko homomorfno preslikavanje grupe $\mathbf{F}_A/\mathbf{F}_A(R)$ u grupu $\mathbf{F}_A/\mathbf{Ker}(\overline{\psi})$, i $\Psi$ kanoničko izomorfno preslikavanje grupe $\mathbf{F}_A/\mathbf{Ker}(\overline{\psi})$ na grupu $(\mathbf{H})\overline{\psi}$, tada je kompozicija $\overline{\varphi} = \theta \circ \Psi$ traženo homomorfno preslikavanje; zaista, $(a_iF_A(R))\overline{\varphi} = ((a_iF_A(R))\theta)\Psi = (a_iKer(\overline{\psi}))\Psi = (a_i)\overline{\psi} = h_i$.

Drugi deo tvrđenja se dokazuje kao i lema 23.10. Ako je $\mathbf{G}$ slobodna grupa varijeteta $\mathcal{V}(R)$ sa slobodnom bazom $C = \{g_j \mid j \in J\}$, onda će ona biti izomorfna grupi $\mathbf{F}_B/\mathbf{F}_B(R)$, gde je $B$ ma kakav skup kardinalnosti $|J|$.□

**Korolar 24.10** *Slobodne grupe varijeteta Abelovih grupa su slobodne Abelove grupe.*

**Dokaz.** Varijetet Abelovih grupa je određen jednoelementnim skupom $R = \{a^{-1}b^{-1}ab\}$ (gde, jasno, $a \neq b$). No, $\mathbf{F}_A(R) = \mathbf{F}'_A$ i $\mathbf{F}_A/\mathbf{F}'_A$ je slobodna

Abelova grupa (21.10($i$)). Dodajmo da ćemo ovo tvrđenje još jednom dokazati (videti 31.17 i 31.18).□

**Definicija 24.11** *Faktor grupa slobodne grupe po invarijantnoj podgrupi se zove reducirana slobodna grupa.*

**Korolar 24.12** *Grupa je slobodna grupa nekog varijeteta akko je izomorfna nekoj reduciranoj slobodnoj grupi.*

**Dokaz.** Jedan pravac smo već pokazali. S druge strane, ako je $\mathbf{H}$ invarijantna podgrupa slobodne grupe $\mathbf{F}_A$, tada je, prema 24.4, $\mathbf{H} = \mathbf{F}_A(H)$, pa je $\mathbf{F}_A/\mathbf{H}$ slobodna grupa varijeteta $\mathcal{V}(H)$.□

**Korolar 24.13** *Potpuno invarijantna podgrupa slobodne grupe nekog varijeteta je verbalna podgrupa.*

**Dokaz.** Neka je $\mathbf{K}/\mathbf{H}$ potpuno invarijantna podgrupa slobodne grupe $\mathbf{F}_A/\mathbf{H}$ varijeteta $\mathcal{V}(H)$. Tada je $\mathbf{K}/\mathbf{H} = \mathbf{F}_A/\mathbf{H}(K)$. Jer, neka je $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m} \in K$ i $u_1H, \dots, u_mH \in F_A/H$, gde je $u_jH = u_kH$ ako $i_j = i_k$. Kako je $\{aH \mid a \in A\}$ slobodna baze grupe $\mathbf{F}_A/\mathbf{H}$, postoji endomorfizam $\varphi$ grupe $\mathbf{F}_A/\mathbf{H}$ koji $a_{i_j}H$ preslikava u $u_jH$, $1 \leq j \leq m$. No tada: $u_1H \dots u_mH = (a_{i_1}H \dots a_{i_m}H)\varphi = ((a_{i_1} \dots a_{i_m})H)\varphi \in K/H$.□

**Lema 24.14** *Neka je $\mathbf{N}$ normalna podgrupa slobodne grupe $\mathbf{F}_A$, $\mathbf{H}$ podgrupa grupe $\mathbf{F}_A$ generisana unijom domena svih potpuno invarijantnih podgrupa grupe $\mathbf{F}_A$ sadržanih u $\mathbf{N}$. Tada su skupovi svih zakona grupa $\mathbf{F}_A/\mathbf{N}$ i $\mathbf{F}_A/\mathbf{H}$ jednaki.*

**Dokaz.** $\mathbf{H}$ je, očigledno, potpuno invarijantna podgrupa grupe $\mathbf{F}_A$, pa je zbog toga skup svih zakona grupe $\mathbf{F}_A/\mathbf{H}$ baš $H$. Upravo smo videli: $\mathbf{F}_A/\mathbf{H} \in \mathcal{V}(H)$, a isto tako je jasno da su reči podgrupe $\mathbf{H}$ i jedini zakoni grupe $\mathbf{F}_A/\mathbf{H}$.

Pošto je $\mathbf{F}_A/\mathbf{N}$ homomorfna slika grupe $\mathbf{F}_A/\mathbf{H}$ (treća teorema o izomorfizmu), to je $H$ sadržano u skupu svih zakona grupe $\mathbf{F}_A/\mathbf{N}$. Pretpostavimo sada da je $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m}$ zakon grupe $\mathbf{F}_A/\mathbf{N}$. Onda je, za svaki niz elemenata $v_1, \dots, v_m$ grupe $\mathbf{F}_A$, gde je $v_j = v_k$ ako je $a_{i_j} = a_{i_k}$, $v_1^{\alpha_1} \dots v_m^{\alpha_m} \in N$; dakle, potpuno invarijantna podgrupa grupe $\mathbf{F}_A$ generisana vrednostima reči $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m}$ sadržana je u $\mathbf{N}$, stoga i u $\mathbf{H}$. Posebno, $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m} \in H$.□

**Korolar 24.15** *Svaka grupa je homomorfna slika reducirane slobodne grupe sa kojom ima iste zakone.*

**Dokaz.** Jasno; svaka grupa je homomorfna slika slobodne grupe, tj. izomorfna nekoj faktor grupi slobodne grupe.□

Sledeća teorema nam govori o jedinstvenosti reprezentacije reduciranih slobodnih grupa. Ali prvo malo "alata" za njen dokaz.



**Lema 24.16** *Neka je $\mathbf{H}$ potpuno invarijantna podgrupa slobodne grupe $\mathbf{F}_A$ koja nije sadržana u izvodnoj podgrupi $\mathbf{F}'_A$. Tada je, za neki pozitivan prirodan broj $n$, $\mathbf{H} = (\mathbf{F}'_A \cap \mathbf{H})\mathbf{F}_A^n$, gde je $\mathbf{F}_A^n$ podgrupa generisana $n$-tim stepenima svih elemenata grupe $\mathbf{F}_A$.*

**Dokaz.** Kako je $\mathbf{F}_A/\mathbf{F}'_A$ slobodna Abelova grupa sa slobodnom bazom $\{aF'_A \mid a \in A\}$, svaki element grupe $\mathbf{F}_A$ je oblika $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m}u$, gde je $u \in F'_A$ i gde su svi indeksi $i_1, \dots, i_m$ različiti. Neka je $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m}u \in H \setminus F'_A$. Ako je $\varphi$ endomorfizam grupe $\mathbf{F}_A$ koji ostavlja fiksnim element $a_{i_j}$, a sve ostale elemente skupa $A$ preslikava u jedinični element, tada je $(a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m}u)\varphi = a_{i_j}^{\alpha_j} \in H$ (prema 6.9, $\mathbf{F}'_A \leq \mathbf{Ker}(\varphi)$); prema tome je i $u \in H$. Zbog potpune invarijantnosti podgrupe $\mathbf{H}$ je $v^{\alpha_j} \in H$ za svako $v \in F_A$. Neka je $n$ najmanji pozitivan broj takav da je $n$-ti stepen svakog elementa iz $F_A$ u podgrupi $\mathbf{H}$; dakle, $\mathbf{F}_A^n \leq \mathbf{H}$. S druge strane, prema upravo pokazanom sledi: ako je $a_{j_1}^{\beta_1} \dots a_{j_k}^{\beta_k}w \in H$, gde je $w \in F'_A$, onda $n$ deli svaki eksponet $\beta_r$, $1 \leq r \leq k$, pa je $\mathbf{H} \leq (\mathbf{F}'_A \cap \mathbf{H})\mathbf{F}_A^n$.□

**Definicija 24.17** *Neka je $\mathbf{H}$ potpuno invarijantna podgrupa slobodne grupe $\mathbf{F}_A$. Ako podrupa $\mathbf{H}$ nije sadrža u izvodnoj podgrupi, tada je $n(\mathbf{H})$ najmanji pozitivan prirodan broj takav da je $n$-ti stepen svakog elementa iz $\mathbf{F}_A$ u $\mathbf{H}$ (videti prethodnu lemu), u suprotnom $n(\mathbf{H}) = \omega$.*

**Lema 24.18** *Neka je $\mathbf{H}$ prava potpuno invarijantna podgrupa slobodne grupe $\mathbf{F}_A$ i $|A| = \lambda$. Tada važi: faktor grupa grupe $\mathbf{F}_A/\mathbf{H}$ po izvodnoj podgrupi, $(\mathbf{F}_A/\mathbf{H})'$, direktna je suma $\lambda$ cikličnih grupa reda $n(\mathbf{H})$.*

**Dokaz.** Znamo da je $(\mathbf{F}_A/\mathbf{H})' = (\mathbf{H}\mathbf{F}'_A)/\mathbf{H}$ (6.22). Ako je $\mathbf{H} \leq \mathbf{F}'_A$, imamo trivijalno da je faktor grupa u pitanju izomorfna grupi $\mathbf{F}_A/\mathbf{F}'_A$, koja je (i to znamo) direktna suma $\lambda$ beskonačnih cikličnih grupa. Pretpostavimo stoga da podgrupa $\mathbf{H}$ nije sadržana u izvodnoj podgrupi. Tada je, prema prethodnoj lemi, $\mathbf{H}\mathbf{F}'_A = \mathbf{F}^{n(\mathbf{H})}\mathbf{F}'_A$ (pošto je $\mathbf{H}$ prava podgrupa, $n(\mathbf{H}) > 1$). No, sada je $\mathbf{F}_A/(\mathbf{F}_A^{n(\mathbf{H})}\mathbf{F}'_A)$ direktna suma cikličnih grupa $\langle aF_A^{n(\mathbf{H})}F'_A\rangle$ ($a \in A$), reda $n(\mathbf{H})$. Proverićemo da je, za dato $a_j \in A = \{a_i \mid i \in I\}$, $\langle a_jF_A^{n(\mathbf{H})}F'_A\rangle \cap \langle\{a_iF_A^{n(\mathbf{H})}F'_A \mid i \in I \setminus \{j\}\}\rangle = \mathbf{E}$ (time ćemo ujedno pokazati i da su date ciklične grupe reda $n(\mathbf{H})$). Pretpostavimo suprotno. Onda je, za neke indekse $i_1, \dots, i_m$, međusobno različite i različite od $j$, i neke pozitivne prirodne brojeve $\beta, \alpha_1, \dots, \alpha_m$ manje od $n(\mathbf{H})$, $a_j^\beta a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m} \in F_A^{n(\mathbf{H})}F'_A$. Koristeći se endomorfizmom grupe $\mathbf{F}_A$ koji $a_j$ ostavlja fiksnim, dok sve ostale simbole skupa $A$ preslikava u jedinični element, dobijamo $a_j^\beta \in F_A^{n(\mathbf{H})}F'_A$ (grupa $\mathbf{F}_A^{n(\mathbf{H})}\mathbf{F}'_A$ je potpuno invarijantna, budući da je svaka od podgrupa proizvoda potpuno invarijantna). No kako dati endomorfizam preslikava sve elemente izvodne podgrupe u jedinični, imamo zapravo $a_j^\beta \in F_A^{n(\mathbf{H})}$, što je

nemoguće, s obzirom na jedinstvenost prezentacije elemenata slobodne grupe (23.8).□

**Teorema 24.19** *Svaka reducirana slobodna grupa ima, do na izomorfizam, jedinstvenu reprezentaciju kao faktor grupa slobodne grupe po invarijantnoj podgrupi.*

**Dokaz.** Neka je $\mathbf{G}$ reducirana slobodna grupa i neka je $\mathbf{G} \cong \mathbf{F}_A/\mathbf{H} \cong \mathbf{F}_B/\mathbf{K}$, gde su $\mathbf{H}$ i $\mathbf{K}$ potpuno invarijantne podgrupe grupa, respektivno, $\mathbf{F}_A$ i $\mathbf{F}_B$. Prema prethodnoj lemi, $\mathbf{G}/\mathbf{G}'$ je direktna suma cikličnih grupa, bilo fiksnog konačnog reda ($n$) bilo beskonačnog reda. No svaka dva razlaganja Abelove grupe u direktnu sumu nerazloživih cikličnih grupa su izomorfna (35.11; imamo u vidu i 10.24($c$),($d$),($g$)), pa odatle sledi da je $|A| = |B|$, tj. $\mathbf{F}_A \cong \mathbf{F}_B$ (23.10). Jasno, možemo pretpostaviti, te ćemo tako i učiniti, da su grupe $\mathbf{F}_A$ i $\mathbf{F}_B$ jednake. Imamo, dakle, da je $\mathbf{F}_A/\mathbf{H} \cong \mathbf{F}_A/\mathbf{K}$. Prema 24.12, 24.14, skup svih zakona grupe $\mathbf{F}_A/\mathbf{H}$, pa prema tome i grupe $\mathbf{F}_A/\mathbf{K}$, je baš $H$. Stoga je, za svaku reč $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m}$ iz $\mathbf{H}$ i svaki niz elemenata $v_1, \dots, v_m$ grupe $\mathbf{F}_A$, gde su reči $v_j$ i $v_k$ jednake ako su jednaki simboli $a_{i_j}$ i $a_{i_k}$, $v_1^{\alpha_1} \dots a_m^{\alpha_m} K = K$, tj. $v_1^{\alpha_1} \dots v_m^{\alpha_m} \in K$. Posebno, $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m} \in K$, pa je, zaključujemo, $\mathbf{H} \leq \mathbf{K}$. Po simetriji stvari važi i obrnuta inkluzija.■

Naredni rezultat nam kaže da kada su u pitanju slobodne grupe varijeteta, dovoljno je samo posmatrati potpuno invarijantne podgrupe slobodnih grupa sa beskonačno prebrojivom slobodnom bazom.

**Teorema 24.20** *Neka je $A$ beskonačno prebrojiv skup, $B$ skup proizvoljne kardinalnosti i neka su $\mathbf{L}_{p.i}(\mathbf{F}_A)$ i $\mathbf{L}_{p.i}(\mathbf{F}_B)$ mreže potpuno invarijantnih podgrupa slobodnih grupa, redom, $\mathbf{F}_A$ i $\mathbf{F}_B$ (5.27). Tada postoji utapanje mreže $\mathbf{L}_{p.i}(\mathbf{F}_B)$ u mrežu $\mathbf{L}_{p.i}(\mathbf{F}_A)$; posebno, ako je $B$ beskonačan skup, onda su mreže $\mathbf{L}_{p.i}(\mathbf{F}_B)$ i $\mathbf{L}_{p.i}(\mathbf{F}_A)$ izomorfne.*

**Dokaz.** Definišimo preslikavanje $\Phi : L_{p.i}(\mathbf{F}_B) \longrightarrow L_{p.i}(\mathbf{F}_A)$ sa (za $\mathbf{H} \in L_{p.i}(\mathbf{F}_B)$) $(\mathbf{H})\Phi \stackrel{\text{def}}{=} \mathbf{F}_A(\{\mathbf{F}_B/\mathbf{H}\})$; dakle, slika potpuno invarijantne podgrupe $\mathbf{H}$ grupe $\mathbf{F}_B$ je potpuno invarijantna podgrupa grupe $\mathbf{F}_A$ čiji je domen skup svih relacija identiteta (zakona) faktor grupe $\mathbf{F}_B/\mathbf{H}$ (videti komentar pred lemu 24.5). Preslikavanje $\Phi$ je injektivno. Zaista, ako su $\mathbf{H}$ i $\mathbf{K}$ različite potpuno invarijantne podgrupe grupe $\mathbf{F}_B$, tada, prema dokazu prethodne teoreme, faktor grupe $\mathbf{F}_B/\mathbf{H}$ i $\mathbf{F}_B/\mathbf{K}$ imaju različite relacije identiteta, te ako je npr. $b_{j_1}^{\beta_1} \dots b_{j_m}^{\beta_m}$ zakon grupe $\mathbf{F}_B/\mathbf{H}$ ("ispisan" simbolima azbuke $B \cup B^{-1}$), ali ne i grupe $\mathbf{F}_B/\mathbf{K}$, onda se, pogodnom zamenom simbola $b_{j_k}$ simbolima $a_{i_k}$ azbuke $A \cup A^{-1}$, dobija reč – $a_{i_1}^{\beta_1} \dots a_{i_m}^{\beta_m}$ – grupe $\mathbf{F}_A$, koja je zakon grupe $\mathbf{F}_B/\mathbf{H}$, ali ne i grupe $\mathbf{F}_B/\mathbf{K}$. S druge strane, ako je $\mathbf{H}$ prava podgrupa grupe $\mathbf{K}$, tada je i $\mathbf{F}_A(\{\mathbf{F}_B/\mathbf{H}\})$ prava podgrupa grupe $\mathbf{F}_A(\{\mathbf{F}_B/\mathbf{K}\})$, jer su zakoni grupe $\mathbf{F}_B/\mathbf{H}$ ujedno i zakoni grupe $\mathbf{F}_B/\mathbf{K}$ (već smo konstatovali da su zakoni "originala" takođe i zakoni svake njegove homomorfne slike).



Pokažimo konačno da je $\Phi$, u slučaju da je $B$ beskonačan skup, i surjektivno preslikavanje. Naravno, ništa neće uticati na opštost razmatranja ako pretpostavimo da je $A$ podskup skupa $B$. Neka je $\mathbf{H}$ potpuno invarijantna podgrupa grupe $\mathbf{F}_A$ i $\mathbf{K}$ potpuno invarijantna podgrupa grupe $\mathbf{F}_B$ koju $\mathbf{H}$ generiše; preciznije, $\mathbf{K}$ je podgrupa generisana skupom $\{(H)\varphi \mid \varphi \in End(\mathbf{F}_B)\}$. Reči dobijene od reči grupe $\mathbf{H}$ zamenom simbola azbuke $A \cup A^{-1}$ simbolima azbuke $B \cup B^{-1}$, s tim što, jasno, iste simbole zamenjujemo istim simbolima, elementi su grupe $\mathbf{K}$. Štaviše, skup svih tako dobijenih reči je domen invarijantne podgrupe, što će reći upravo domen grupe $\mathbf{K}$. Ovo je posledica činjenice da je $A$ beskonačan skup i $\mathbf{H}$ potpuno invarijantna podgrupa grupe $\mathbf{F}_A$; jer, odatle, ako je $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m}$ iz $H$, uvek možemo naći reč $a_{j_1}^{\alpha_1} \dots a_{j_m}^{\alpha_m}$ u $H$, pri čemu su skupovi indeksa $\{i_1, \dots, i_m\}$ i $\{j_1, \dots, j_m\}$ disjunktni. Tako npr. ako smo $b_{r_1}^{\alpha_1} \dots b_{r_m}^{\alpha_m}$ dobili od $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m}$, a $b_{s_1}^{\beta_1} \dots b_{s_n}^{\beta_n}$ od $a_{j_1}^{\beta_1} \dots a_{j_n}^{\beta_n}$, onda, adekvatnim preindeksiranjem simbola, dobijamo reč u $\mathbf{H}$, $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m} a_{k_1}^{\beta_1} \dots a_{k_n}^{\beta_n}$ (gde je $\{i_1, \dots, i_m\} \cap \{k_1, \dots, k_n\} = \emptyset$), od koje se, odgovarajućom zamenom simbola dobija proizvod reči $b_{r_1}^{\alpha_1} \dots b_{r_m}^{\alpha_m}$ i $b_{s_1}^{\beta_1} \dots b_{s_n}^{\beta_n}$. Prema tome: $\mathbf{H} = \mathbf{F}_A \cap \mathbf{K}$. Ali onda je $(\mathbf{K})\Phi = \mathbf{F}_A(\{\mathbf{F}_B/\mathbf{K}\}) = \mathbf{H}$. Inkluzija $\geq$ je očigledna, a ako je (reč azbuke $A \cup A^{-1}$) $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m}$ zakon grupe $\mathbf{F}_B/\mathbf{K}$, tada je, posebno, $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m} \in K \cap F_A = H$.■

Pitanje prepoznavanje varijeteta grupa, kojih inače ima kontinuum mnogo, rešava sledeća

**Teorema 24.21** *(G. Birkhoff). Klasa grupa je varijetet akko sadrži (sve) homomorfne slike, podgrupe i kartezijanske proizvode svojih članova.*

**Dokaz.** Pravac ($\Longrightarrow$) je jasan. Trivijalno, zakoni grupe su i zakoni podgrupe, a o homomorfnim slikama je bilo reči u dokazu teoreme 24.20. Konačno, neka je klasa grupa $\mathcal{C}$ varijetet, recimo $\mathcal{C} = \mathcal{V}(R)$, i $\{\mathbf{G}_i \mid i \in I\}$ familija elemenata klase $\mathcal{C}$ ($\mathbf{G}_i = \langle G_i, \cdot_i \rangle$). Ako je $a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m} \in R$ i ako su $f_1, \dots, f_m$ elementi kartezijanskog proizvoda $\mathbf{G} = \prod_{i \in I}^{c} \mathbf{G}_i$, gde je $f_j = f_k$ ako je $i_j = i_k$, tada je, za svako $r \in I$, $(r)(f_1^{\alpha_1} \dots f_m^{\alpha_m}) = ((r)f_1)^{\alpha_1} \cdot_r \dots \cdot_r ((r)f_m)^{\alpha_m} = e_r$ (jer je $\mathbf{G}_r \in \mathcal{V}(\{a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m}\})$); dakle, $f_1^{\alpha_1} \dots f_m^{\alpha_m}$ je jedinični element grupe $\mathbf{G}$.

Pretpostavimo sada da klasa grupa $\mathcal{C}$ sadrži homomorfne slike, podgrupe i kartezijanske proizvode svojih članova i nejedinične grupe (izbegavamo trivijalan slučaj). Neka je $\mathcal{V}$ varijetet grupa određen skupom svih zakona (reči slobodne grupe $\mathbf{F}_A$ beskonačno prebrojivog ranga – $A = \{a_i \mid i \in I\}$) koji važe u svim grupama klase $\mathcal{C}$; obeležimo ga sa $R$. Očigledno, $\mathcal{C} \subseteq \mathcal{V}$. Dokazujemo da zapravo važi jednakost ovih klasa. Neka je $\mathbf{G}$ nejedinična podgrupa iz $\mathcal{V}$. Za svaku reč $v$ koja nije u $R$ izaberimo u $\mathcal{C}$ grupu $\mathbf{H}_v$ za koju $v$ nije zakon. Neka je dalje skup $B$ kardinalnosti ne manje od reda bilo koje od grupa $\mathbf{G}$, $\mathbf{H}_v$, $v \notin R$ (imamo u vidu da je $A$ beskonačno prebrojiv skup, pa je i skup reči nad azbukom $A \cup A^{-1}$ prebrojiv). Izbor skupa $B$ nam garantuje egzistenciju surjektivnog homomorfnog preslikavanja slobodne grupe $\mathbf{F}_B$ na grupu $\mathbf{G}$, te je,

za neku normalnu podgrupu $\mathbf{N}$ grupe $\mathbf{F}_B$, $\mathbf{G} \cong \mathbf{F}_B/\mathbf{N}$. Neka je $b_{j_1}^{\alpha_1} \dots b_{j_m}^{\alpha_m} \in F_B \setminus N$ (dakle, $(b_{j_1}^{\alpha_1} \dots b_{j_m}^{\alpha_m})N \neq N$). Prema tome, uz adekvatan izbor simbola iz $A$, reč $u = a_{i_1}^{\alpha_1} \dots a_{i_m}^{\alpha_m}$ nije zakon grupe $\mathbf{G}$, samim tim ni element skupa $R$. Zato imamo grupu $\mathbf{H}_u$ iz klase $\mathcal{C}$, i u njoj neke elemente $h_1, \dots, h_m$ takve da je $h_1^{\alpha_1} \dots h_m^{\alpha_m} \neq e_{H_u}$. No sada postoji surjektivno homomorfno preslikavanje (slobodne) grupe $\mathbf{F}_B$ na $\mathbf{H}_u$ koje preslikava $b_{j_r}$ u $h_r$, $1 \leq r \leq m$. Neka je $\mathbf{K}_u$ jezgro tog homomorfizma; znači: $\mathbf{F}_B/\mathbf{K}_u \cong \mathbf{H}_u$ (pa je $\mathbf{F}_B/\mathbf{K}_u \in \mathcal{C}$) i $u \notin K_u$. Odatle, $\mathbf{K} = \bigcap_{u \in F_B \setminus N} \mathbf{K}_u \leq \mathbf{N}$, te je $\mathbf{F}_B/\mathbf{N}$ homomorfna slika grupe $\mathbf{F}_B/\mathbf{K}$, koja je pak izomorfna podgrupi kartezijanskog proizvoda $\prod_{u \in F_B \setminus N}^{c} \mathbf{F}_B/\mathbf{K}_u$ (10.14). Prema datim uslovima za klasu $\mathcal{C}$ sledi: $\mathbf{G} \in \mathcal{C}$.■

Neka su $\mathsf{H}$, $\mathsf{P}^c$ i $\mathsf{S}$ *operatori* (koji klasu grupa preslikavaju u klasu grupa) definisani sa (za datu klasu grupa $\mathcal{C}$):

$\mathsf{H}(\mathcal{C}) \stackrel{\text{def}}{=} \{\mathbf{G} \mid \mathbf{G}$ je homomorfna slika neke grupe iz $\mathcal{C}\}$;

$\mathsf{P}^c(\mathcal{C}) \stackrel{\text{def}}{=} \{\mathbf{G} \mid \mathbf{G}$ je kartezijanski proizvod familije grupa iz $\mathcal{C}\}$;

$\mathsf{S}(\mathcal{C}) \stackrel{\text{def}}{=} \{\mathbf{G} \mid \mathbf{G}$ je podgrupa neke grupe iz $\mathcal{C}\}$.

Slovo S za treći operator, koje se koristi standardno u univerzalnoj algebri, dolazi od engleske reči *subalgebra* – podalgebra). Kada jezik teorije grupa pored binarnog sadrži i unarni funkcijski simbol, čija je interpretacija dodeljivanje inverznog elementa, a takav je po pravilu slučaj kada se radi o varijetetima grupa (umeće se i konstanta, nularni funkcijski simbol, za jedinični element), pojam podgrupe i podalgebre se podudaraju. U suprotnom to, naravno, ne mora biti slučaj ako grupa nije periodična; recimo, $\langle \omega, + \rangle$ je podalgebra grupe $\langle Z, + \rangle$, ali ne i njena podgrupa. Slovo P čija je upotreba takođe uobičajena u univerzalnoj algebri, ovde smo zamenili za $\mathsf{P}^c$ (ranije smo već naglasili da se u univerzalnoj algebri pod pojmom direktnog proizvoda podrazumeva ono što je u teoriji grupa kartezijanski proizvod).

Jasno, svaka klasa grupa je podklasa svoje slike za bilo koji od datih operatora. Stoga smo prethodnu teoremu mogli zapisati i sa:

*Klasa grupa $\mathcal{C}$ je varijetet akko važi: $\mathcal{C} = \mathsf{H}(\mathcal{C})$, $\mathcal{C} = \mathsf{P}^c(\mathcal{C})$ i $\mathcal{C} = \mathsf{S}(\mathcal{C})$.*

Ali postoji i jednostavniji zapis. No prvo

**Lema 24.22** *(a)* $\mathsf{H}^2 = \mathsf{H}$, *tj. za svaku klasu grupa $\mathcal{C}$ je* $\mathsf{H}(\mathsf{H}(\mathcal{C})) \stackrel{\text{def}}{=} \mathsf{H}^2(\mathcal{C}) = \mathsf{H}(\mathcal{C})$; $(\mathsf{P}^c)^2 = \mathsf{P}$; $\mathsf{S}^2 = \mathsf{S}$.

*(b) Za (svaku) klasu grupa $\mathcal{C}$ je:*

(1) $\mathsf{S}(\mathsf{H}(\mathcal{C})) \subseteq \mathsf{H}(\mathsf{S}(\mathcal{C}))$;

(2) $\mathsf{P}^c(\mathsf{H}(\mathcal{C})) \subseteq \mathsf{H}(\mathsf{P}^c(\mathcal{C}))$;

(3) $\mathsf{P}^c(\mathsf{S}(\mathcal{C})) \subseteq \mathsf{S}(\mathsf{P}^c(\mathcal{C}))$.

**Dokaz.** *(a)* Trivijalno.

*(b)* (1) Neka je $\varphi$ homomorfno preslikavanje grupe $\mathbf{G}$ klase $\mathcal{C}$ na grupu $\mathbf{H}$ i neka je $\mathbf{K}$ podgrupa grupe $\mathbf{H}$ (dakle, $\mathbf{K} \in \mathsf{S}(\mathsf{H}(\mathcal{C}))$). No tada je $((\mathbf{K})\varphi^{-1})\varphi = \mathbf{K}$ (8.7), tj. $\mathbf{K}$ je homomorfna slika podgrupe $(\mathbf{K})\varphi^{-1}$ grupe $\mathbf{G}$.



(2) Neka je $\mathbf{H} = \prod_{i \in I}^{c} \mathbf{H}_i$, gde je, za svako $i$ $(\in I)$, $\mathbf{H}_i$ homomorfna slika, za homomorfizam $\varphi_i$, grupe $\mathbf{G}_i$ iz klase $\mathcal{C}$. Onda je $\mathbf{H}$ homomorfna slika grupe $\mathbf{G} = \prod_{i \in I}^{c} \mathbf{G}_i$; (jedno) homomorfno preslikavanje $\varphi$ je dato sa (za $f \in G$): $(f)\varphi = h_f \in H$, gde je $(i)h_f \stackrel{\text{def}}{=} ((i)f)\varphi_i$. Pokažimo samo homomorfnost preslikavanja $\varphi$. Neka $f, g \in G$ i neka je $\cdot_i$ operacija grupe $\mathbf{G}_i$, a $*_i$ operacija grupe $\mathbf{H}_i$ (operacije u grupama $\mathbf{G}$ i $\mathbf{H}$ obeležićemo sa $\cdot$). Kako je, za svako $i$ iz $I$, $(i)(h_f \cdot h_g) = (i)h_f *_i (i)h_g = ((i)f)\varphi_i *_i ((i)g)\varphi_i = ((i)f \cdot_i (i)g)\varphi_i = ((i)(f \cdot g))\varphi_i = (i)(h_{f \cdot g})$, sledi: $(f \cdot g)\varphi = h_{f \cdot g} = h_f \cdot h_g = (f)\varphi \cdot (g)\varphi$.

(3) Videti dokaz tačke *(a)*.□

Primetimo: umesto, recimo, $\mathsf{H}(\mathsf{S}(\mathcal{C}))$, češće se piše jednostavno $\mathsf{HS}(\mathcal{C})$.

**Korolar 24.23** *Klasa grupa $\mathcal{C}$ je varijetet akko je $\mathcal{C} = \mathsf{HSP}^c(\mathcal{C})$.*

**Dokaz.** Neka je $\mathcal{C} = \mathsf{HSP}^c(\mathcal{C})$. Onda je, prema prethodnoj lemi, npr. $\mathsf{P}^c(\mathcal{C}) = \mathsf{P}^c\mathsf{HSP}^c(\mathcal{C}) \subseteq \mathsf{HP}^c\mathsf{SP}^c(\mathcal{C}) \subseteq \mathsf{HS}(\mathsf{P}^c)^2(\mathcal{C}) = \mathsf{HSP}^c(\mathcal{C}) = \mathcal{C}$. Analogno izvodimo: $\mathsf{H}(\mathcal{C}) = \mathcal{C}$, $\mathsf{S}(\mathcal{C}) = \mathcal{C}$, pa je $\mathcal{C}$ varijetet.

Obrat je još očigledniji.□

Ranije smo videli da je presek familije varijeteta varijetet. Međutim, kada je unija lanca u pitanju imamo

**Korolar 24.24** *Unija rastućeg lanca varijeteta grupa je varijetet akko je taj lanac konačan.*

**Dokaz.** Jasno, dovoljno je da posmatramo samo prebrojive rastuće lance. Neka je dat jedan takav, strogo rastući i beskonačan : $\mathcal{V}_0 \subset \mathcal{V}_1 \subset \dots \subset \mathcal{V}_n \subset \mathcal{V}_{n+1} \subset \dots$. Ako je $R_i$ skup svih zakona varijeteta $\mathcal{V}_i$, $i \in \omega$ ("ispisanih" prebrojivom azbukom $A \cup A^{-1}$), tada, naravno, imamo: $R_0 \supset R_1 \supset \dots \supset R_n \supset R_{n+1} \supset \dots$. Neka je, za svako $n \in \omega$, $u_n$ zakon varijeteta $\mathcal{V}_n$, ali ne i varijeteta $\mathcal{V}_{n+1}$ (dakle, $u_n \in R_n \setminus R_{n+1}$), a $\mathbf{G}_n$ element varijeteta $\mathcal{V}_{n+1}$, za koji $u_n$ nije relacija identiteta. Onda nijedna od reči $u_n$, $n \in \omega$, nije zakon grupe $\mathbf{G} = \prod_{n \in \omega}^{c} \mathbf{G}_n$ (jer $\mathbf{G}$ sadrži, kao podgrupe, izomorfne slike svake od grupa $\mathbf{G}_n$), te $\mathbf{G} \notin \bigcup_{n \in \omega} \mathcal{V}_n = \mathcal{V}$ i, prema tome, $\mathcal{V}$ nije varijetet.□

Prema 24.21 klasa cikličnih grupa nije varijetet. Isto tako, ako je dat beskonačan rastuči niz prirodnih brojeva $\langle r_n \rangle_{n \in \omega}$, gde je svaki član niza deljiv sa svim prethodnim, i ako je $\mathcal{V}_{r_n}$ varijetet određen skupom zakona $R_n = \{a^{-1}b^{-1}ab, a^{r_n}\}$, tada je, za $k < m$, $\mathcal{V}_{r_k} \subset \mathcal{V}_{r_m}$, i prema prethodnom korolaru $\bigcup_{n \in \omega} \mathcal{V}_{r_n}$ nije varijetet. Od brojnih klasa grupa sa kojima se susrećemo u ovoj knjizi tek manji deo je varijetet (videti npr. 48.7 i 49.11); mnoge nisu, jer nisu zatvorene za kartezijanske proizvode (recimo, klase konačnih, lokalno konačnih, nilpotentnih i rešivih grupa – videti napomene uz 48.9 i 49.9), no npr. klasa deljivih Abelovih grupa nije zatvorena (samo) za podgrupe.

Napomenimo na kraju da mnogi rezultati ovog paragrafa imaju svoje pandane u univerzalnoj algebri ([30], [57]). Uopšte, o varijetetima grupa pogledati u [124] (kao i u brojnim člancima o njima).

## 25 Slobodni proizvodi

Neka je data familija grupa sa disjunktnim domenima – $\{\mathbf{G}_i \mid i \in I\}$ (operacija u grupi $\mathbf{G}_i$ je $\cdot_i$, jedinični element $e_i$). Pod *rečju* ćemo ovaj put podrazumevati uređeni konačni niz $a_1 \dots a_k$, gde je $a_r$, $1 \leq r \leq k$, nejedinični element grupe $\mathbf{G}_{i_r}$ i gde nikoja dva susedna elementa nisu iz iste grupe. *Dužina reči* $u$, u oznaci $l(u)$, je broj elemenata u njoj ($l(a_1 \dots a_k) = k$). Posebno, za $k = 0$ imamo praznu reč koju ćemo opet obeležiti sa 1. Na skupu svih ovako definisanih reči, obeležimo ga sa $G$, definišimo operaciju $\bullet$ na sledeći način:

$1 \bullet a_1 \dots a_k = a_1 \dots a_k \bullet 1 = a_1 \dots a_k$;

ako su date neprazne reči $a_1 \dots a_k$ i $b_1 \dots b_m$, gde je, kao i maločas, $a_r \in A_{i_r}$ dok $b_t \in A_{j_t}$, diskutujemo:

(I) ako je $i_k \neq j_1$, onda je

$a_1 \dots a_k \bullet b_1 \dots b_m = a_1 \dots a_k b_1 \dots b_m$;

(II) ako je $a_k = b_1^{-1}, \dots, a_{k-(r-1)} = b_r^{-1}$, $0 \leq r \leq min\{k, m\}$, dakle, posebno, $i_k = j_1, \dots, i_{k-(r-1)} = j_r$ i

(*a*) $i_{k-r} = j_{r+1}$ i $a_{k-r} \cdot_{i_{k-r}} b_{k-r} = c_{k-r}$ nejedinični element grupe $\mathbf{G}_{i_{k-r}}$, onda je:

$a_1 \dots a_k \bullet b_1 \dots b_m = a_1 \dots a_{k-(r+1)} c_{k-r} b_{r+2} \dots b_m$;

(*b*) $i_{k-r} \neq j_{r+1}$, onda je:

$a_1 \dots a_k \bullet b_1 \dots b_m = a_1 \dots a_{k-r} b_{r+1} \dots b_m$;

$\langle G, \bullet \rangle$ je, tvrdimo, grupa. Sem asocijativnosti sve ostalo je očigledno (1 je jedinični element, inverzni element elementa $a_1 \dots a_k$ je $a_k^{-1} \dots a_1^{-1}$ – to ćemo uostalom još jednom pokazati). U proveri asocijativnosti koristićemo simetričnu grupu $\mathbf{S}_G = \langle S_G, \circ \rangle$. Neka je, za nejedinični element $a$ grupe $\mathbf{G}_i$, $\widehat{a}$ (notaciju, kao i dokaz preuzimamo iz [92]) preslikavanje skupa $G$ u sebe dato sa:

$$(a_1 \dots a_k)\widehat{a} = a_1 \dots a_k \bullet a.$$

Za jedinični element stavljamo: $\widehat{e_i} = \imath_G$ – identično preslikavanje skupa $G$. Lako se proverava da je $\widehat{a}$ element simetrične grupe $\mathbf{S}_G$. Ako je npr. $i_k \neq i$ element $a_1 \dots a_k$ je slika elementa $a_1 \dots a_k a^{-1}$, posebno, 1 je slika elementa $a^{-1}$. Ako je (uz ranije pretpostavke o elementima $a_r$, $b_t$) $(a_1 \dots a_k)\widehat{a} = (b_1 \dots b_m)\widehat{a}$, tj. $a_1 \dots a_k \bullet a = b_1 \dots b_m \bullet a$ i, recimo, $i_k \neq i$, tada je i $j_m \neq i$; u suprotnom bismo na levoj strani imali niz koji se završava sa $a$, dok to ne bi bio slučaj sa nizom na desnoj strani – $b_m$ je nejedinični element, a $j_{m-1} \neq i$ (dalje, trivijalno sledi: $a_1 \dots a_k = b_1 \dots b_m$). Pretpostavimo $i_k = j_m = i$. Iz $a_k a = b_m a$ sledi $a_k = b_m$ (moguće da je $a_k = b_m = a^{-1}$) i opet trivijalno: $k - 1 = m - 1$ i, za svako $r$, $1 \leq r \leq k-1$, $a_r = b_r$.

Za $a, b \in G_i$ je $\widehat{ab} = \widehat{a} \circ \widehat{b}$. Opet, ako je $i_k \neq i$ i $ab = c \neq e_i$, onda je:

$(a_1 \dots a_k)\widehat{ab} = a_1 \dots a_k c$,

ali i

$(a_1 \dots a_k)(\widehat{a} \circ \widehat{b}) = ((a_1 \dots a_k)\widehat{a})\widehat{b} = (a_1 \dots a_k a)\widehat{b} = a_1 \dots a_k c$.



Ako je $i_k = i$ i, uzmimo, $a_k = a^{-1}$, onda je:

$(a_1 \dots a_k)\widehat{ab} = a_1 \dots a_{k-1} b = ((a_1 \dots a_k)\widehat{a})\widehat{b} = (a_1 \dots a_k)(\widehat{a} \circ \widehat{b})$.

Razmatranje ostalih slučajeva je jednako tako trivijalno.

Preslikavanje $\psi_i : G_i \longrightarrow S_G$ dato sa $(a)\psi_i = \widehat{a}$ utapanje je grupe $\mathbf{G}_i$ u grupu $\mathbf{S}_G$ (ako $a, b \in G_i$ i $a \neq b$, tada je: $(1)\widehat{a} = a \neq b = (1)\widehat{b}$). Neka je $\widehat{\mathbf{G}}$ podgrupa grupe $\mathbf{S}_G$ generisana skupom $\{(G_i)\psi_i\ (= \widehat{G_i}) \mid i \in I\}$. Svaki nejedinični element (pod)grupe $\widehat{\mathbf{G}}$ se na jedinstven način predstavlja kao proizvod nejediničnih elemenata iz raznih podgrupa $\widehat{\mathbf{G}_i}$, gde nikoja dva susedna nisu iz iste podgrupe. Jer, pretpostavimo:

$\widehat{a_1} \circ \dots \circ \widehat{a_k} = \widehat{b_1} \circ \dots \circ \widehat{b_m}$.

No tada je

$a_1 \dots a_k = (1)(\widehat{a_1} \circ \dots \circ \widehat{a_k}) = (1)(\widehat{b_1} \circ \dots \circ \widehat{b_m}) = b_1 \dots b_m$,

pa je $k = m$ i $a_r = b_r$, $r = 1, \dots, k$.

"Množenje" u grupi $\widehat{\mathbf{G}}$ odgovara, uslovno rečeno, "množenju" u grupoidu $\langle G, \bullet \rangle$. Konkretno, ako je na primer

$$a_1 \dots a_k \bullet b_1 \dots b_m = a_1 \dots a_{k-(r+1)} c_{k-r} b_{r+2} \dots b_m,$$

(znači, ponavljamo: $a_k = b_1^{-1}, \dots, a_{k-(r-1)} = b_r^{-1}$ i $i_{k-r} = j_{r+1}$ i $a_{k-r} b_{r+1} = c_{k-r} \neq e_{i_{k-r}}$), onda je:

$(\widehat{a_1} \circ \dots \circ \widehat{a_k}) \circ (\widehat{b_1} \circ \dots \circ \widehat{b_m}) = \widehat{a_1} \circ \dots \widehat{a_{k-(r+1)}} \circ \widehat{c_{k-r}} \circ \widehat{b_{r+2}} \circ \dots \circ \widehat{b_m}$;

jer:

$$(1)((\widehat{a_1} \circ \dots \circ \widehat{a_k}) \circ (\widehat{b_1} \circ \dots \circ \widehat{b_m})) =$$

$$(\dots((((\dots((a_1 \dots a_k)\widehat{b_1})\dots)\widehat{b_r})\widehat{b_{r+1}})\widehat{b_{r+2}})\dots)\widehat{b_m} =$$

$$(\dots((a_1 \dots a_{k-r})\widehat{b_{r+1}})\widehat{b_{r+2}}\dots)\widehat{b_m} = (\dots((a_1 \dots a_{k-(r+1)} c_{k-r})\widehat{b_{r+2}})\dots)\widehat{b_m} =$$

$$a_1 \dots a_{k-(r+1)} c_{k-r} b_{r+2} \dots b_m = (1)(\widehat{a_1} \circ \dots \circ \widehat{a_{k-(r+1)}} \circ \widehat{c_{k-r}} \circ \widehat{b_{r+2}} \circ \dots \circ \widehat{b_m}).$$

Stoga je preslikavanje $\widehat{\varphi} : \widehat{G} \longrightarrow G$ dato sa:

$$(\widehat{a_1} \circ \dots \circ \widehat{a_k})\widehat{\varphi} = a_1 \dots a_k,$$

i, naravno, $(\imath_{\widehat{G}})\widehat{\varphi} = 1$, izomorfno preslikavanje grupe $\widehat{\mathbf{G}}$ na grupoid $\langle G, \bullet \rangle$, te je i $\langle G, \bullet \rangle$ grupa.

Grupa $\langle G, \bullet \rangle$ je tzv. *slobodni proizvod* familije grupa $\{\mathbf{G}_i \mid i \in I\}$. Analogno, kažemo da je $\langle \widehat{G}, \circ \rangle$ slobodni proizvod familije svojih podgrupa $\{\widehat{\mathbf{G}_i} \mid i \in I\}$. U tom smislu, možemo, kao i kod direktnih proizvoda, govoriti o *spoljašnjem* i *unutrašnjem slobodnom proizvodu*. Formalno (i ponovljeno)

**Definicija 25.1** *Grupa* $\mathbf{G} = \langle G, \cdot \rangle$ *je slobodni proizvod familije podgrupa* $\{\mathbf{G}_i \mid i \in I\}$ *akko se svaki nejedinični element* $g$ *iz* $\mathbf{G}$ *može na jedinstven način predstaviti kao proizvod* $g_1 \cdot \dots \cdot g_k$, *gde je* $g_r$, $r = 1, \dots, k = k(g)$ $(\geq 1)$, *nejedinični element podgrupe* $\mathbf{G}_{i_r}$ *i gde nikoja dva susedna elementa nisu iz iste podgrupe.*

$g_1 \cdot \ldots \cdot g_k$ *je tzv. normalna forma elementa* $g$. *Dogovorno, jedinični element je ujedno i sopstvena normalna forma.*

*Ako je data familija grupa* $\{\mathbf{G}_i \mid i \in I\}$ *sa disjunktnim domenima, onda je (spoljašnji) slobodni proizvod te familije grupa* $\mathbf{G} = \langle G, \bullet \rangle$, *gde je* $G$ *skup reči tj. skup konačnih uređenih nizova, eventualno dužine* 0, *nejediničnih elemenata iz* $\bigcup_{i\in I} G_i$, *gde nikoja dva susedna elementa nisu iz iste grupe, a operacija* $\bullet$ *je definisana kao gore.*

*Pisaćemo, u oba slučaja:* $\mathbf{G} = \prod^*_{i\in I} \mathbf{G}_i$ *(koristi se i* $Fr_{i\in I}\, \mathbf{G}_i$*) ili, ako je u pitanju konačna familija (podgrupa), jednostavno:* $\mathbf{G} = \mathbf{G}_1 * \cdots * \mathbf{G}_n$.

**Napomena**. Iz prethodne priče se vidi: ako je $\mathbf{G}$ slobodni proizvod familije podgrupa $\{\mathbf{G}_i \mid i \in I\}$ i, za svako $i, j \in I$, $\mathbf{G}_i \cong \mathbf{H}_i$ i $H_i \cap H_j = \emptyset$, i ako je $\mathbf{H}$ spoljašnji proizvod familije grupa $\{\mathbf{H}_i \mid i \in I\}$, tada je $\mathbf{G} \cong \mathbf{H}$. Ovo nam i dozvoljava da koristimo istu oznaku za unutrašnji i spoljašnji slobodni proizvod (ponovimo, kao i u slučaju direktnih proizvoda – videti komentar uz 10.10) i oslobađa nas naglašavanja o kojem od ovih proizvoda je reč (to će uostalom iz konteksta uvek biti jasno).

Definicija ne isključuje mogućnost da je neka od (pod)grupa $\mathbf{G}_i$ baš jedinična (pod)grupa. Trivijalno, (spoljašnji) slobodni proizvod jediničnih grupa je jedinična grupa. No naravno, grupa $\mathbf{G}$ je *nerazloživa* u slobodni proizvod akko iz $\mathbf{G} = \mathbf{H} * \mathbf{K}$ sledi da je jedna od podgrupa $\mathbf{H}$, $\mathbf{K}$ jedinična (videti, recimo, 26.10).

Naglasimo i to da se uslov da su domeni grupa kod spoljašnjeg slobodnog proizvoda disjunktni obično ne postavlja. No u svakom slučaju, za svaku datu reč $a_1 \ldots a_k$ mi moramo tačno znati iz koje grupe je svaki od elemenata $a_1, \ldots, a_k$, što opet na neki način zahteva markiranje (na poseban način) elemenata iste grupe. Stoga je jednostavnije odmah pretpostaviti da su domeni grupa disjunktni, što svakako nije nikakvo ograničenje (videti lemu prenosa – 3.24).

Iz praktičnih razloga ćemo često i kod spoljašnjeg slobodnog proizvoda $\mathbf{G} = \prod^*_{i\in I} \mathbf{G}_i$ poistovetiti grupu $\mathbf{G}_i$ sa njom izomorfnom podgrupom, grupe $\mathbf{G}$, sa domenom $(G_i \setminus \{e_i\}) \cup \{1\}$.

Dodajmo takođe, da ćemo, kao i kod direktnih proizvoda, pisati koji put samo $\prod^*_i \mathbf{G}_i$ ili, još jednostavnije, $\prod^* \mathbf{G}_i$, umesto (formalno) $\prod^*_{i\in I} \mathbf{G}_i$, ako je isključena mogućnost zabune oko indeksnog skupa.

Premda se isti izrazi, kao npr. *reč*, *dužina reči* itd., u ovom poglavlju koriste za različite pojmove, problema nema; iz teksta uvek jasno proizilazi na koju se "interpretaciju" izraza misli.

**Lema 25.2** *Neka je* $(A_i; P_i)$, $i \in I$, *prezentacija grupe* $\mathbf{G}_i$ *za preslikavanje* $\varphi_i$ *i neka je, za* $i, j \in I$, $i \neq j$, $A_i \cap A_j = \emptyset$. *Tada je* $(\bigcup_{i\in I} A_i; \bigcup_{i\in I} P_i)$ *prezentacija slobodnog proizvoda familije grupa* $\{\mathbf{G}_i \mid i \in I\}$ *(za podesno izabrano preslikavanje).*



**Dokaz**. Neka je $\mathbf{G} = \langle G, \cdot \rangle$ slobodni proizvod familije podgrupa $\{\mathbf{G}_i \mid i \in I\}$ i neka je $\varphi = \bigcup_{i\in I} \varphi_i$ preslikavanje skupa $A = \bigcup_{i\in I} A_i$ u $G$. Pretpostavka o unutrašnjem slobodnom proizvodu ne umanjuje, rekli smo, opštost razmatranja – mogli smo prvo, kao i gore, formirati spoljašnji slobodni proizvod familije grupa $\{\mathbf{G}_i \mid i \in I\}$ (uslov $G_i \cap G_j = \emptyset$ za $i \neq j$ odista nije nikakvo ograničenje), pa onda uzeti njegovu izomorfnu sliku u simetričnoj grupi. Jasno, za svaku reč (azbuke $A \cup A^{-1}$) $u \in P = \bigcup_{i\in I} P_i$ je $(u)\overline{\varphi} = e$, te se, prema 21.9$(a)$, grupa $\mathbf{G}_{(A;P)}$ homomorfno preslikava na grupu $\mathbf{G}$. Jedan surjektivni homomorfizam, $\theta$, je dat sa, podsećamo: $([v])\theta = (v)\overline{\varphi}$ (imamo u vidu i da $(A)\varphi = \bigcup_{i\in I}(A_i)\varphi_i$ generiše grupu $\mathbf{G}$). Grupe $\mathbf{G}_{(A_i;P_i)}$, $i \in I$, možemo, pa i hoćemo, smatrati podgrupama grupe $\mathbf{G}_{(A;P)}$ i, jasno, svaki nejedinični element grupe $\mathbf{G}_{(A;P)}$ se može predstaviti kao proizvod nejediničnih elemenata podgrupa $\mathbf{G}_{(A_i;P_i)}$ u kojem nikoja dva susedna elementa nisu iz iste podgrupe. Jednostavno, u ma kojoj reči $a_1^{\alpha_1} \ldots a_k^{\alpha_k}$, gde je $\alpha_r \in \{1, -1\}$, $r = 1, \ldots, k$, izvršimo koncentraciju susednih slova azbuke $A \cup A^{-1}$ koja pripadaju istoj "podazbuci" $A_i \cup A_i^{-1}$; i tako, ako je $[a_1^{\alpha_1} \ldots a_k^{\alpha_k}]$ nejedinični element i $a_1, \ldots, a_s \in A_{i_1}$, $a_{s+1}, \ldots, a_t \in A_{i_2}$, $\ldots$, $a_u, \ldots, a_k \in A_{i_l}$, imamo: $[a_1^{\alpha_1} \ldots a_k^{\alpha_k}] = [a_1^{\alpha_1} \ldots a_s^{\alpha_s}] \cdot [a_{s+1}^{\alpha_{s+1}} \ldots a_t^{\alpha_t}] \cdot \ldots \cdot [a_u^{\alpha_u} \ldots a_k^{\alpha_k}]$, gde je npr. $[a_1^{\alpha_1} \ldots a_s^{\alpha_s}] \in G_{(A_{i_1};P_{i_1})}$ i gde, naravno, ne mogu svi elementi $[a_1^{\alpha_1} \ldots a_s^{\alpha_s}]$, $\ldots$, $[a_u^{\alpha_u} \ldots a_k^{\alpha_k}]$ biti jedinični. Uočimo dalje da je $\theta|_{G_{(A_i;P_i)}} = \theta_i$ izomorfno preslikavanje grupe $\mathbf{G}_{(A_i;P_i)}$ na grupu $\mathbf{G}_i$. Odatle, prema prethodnom, sledi da je $\theta$ i injektivno. Jer, ako je $[u] = [u_1] \cdot \ldots \cdot [u_k]$, gde je $[u_r]$ nejedinični element grupe $\mathbf{G}_{(A_{i_r};P_{i_r})}$ $(r = 1, \ldots, k)$ i gde nikoja dva susedna elementa nisu iz iste podgrupe, tada je

$$([u])\theta = ([u_1])\theta_{i_1} \ldots ([u_k])\theta_{i_k} = (u_1)\overline{\varphi}_{i_1} \ldots (u_k)\overline{\varphi}_{i_k}$$

svakako nejedinični element grupe $\mathbf{G}$.□

**Korolar 25.3** *Slobodna grupa je slobodni proizvod beskonačnih cikličnih grupa.*

**Korolar 25.4** *Ako su problemi reči i konjugovanosti rešivi za grupe* $\mathbf{G}_{(A;P)}$ *i* $\mathbf{G}_{(B;Q)}$, *rešivi su i za slobodni proizvod tih grupa.*

**Dokaz**. Primetimo samo: u slučaju problema konjugovanosti dovoljno je pokazati: elementi $u$ i $v$ slobodnog proizvoda $\mathbf{G}_{(A;P)} * \mathbf{G}_{(B;Q)}$ dati nizovima koji ne počinju i ne završavaju se sa elementima iz iste grupe konjugovani su akko se $v$ dobija od $u$, uslovno rečeno, "cikličnom permutacijom" (koristimo se idejom dokaza tačke $(k)$ leme 23.3 i u osnovi "simuliramo" taj dokaz); uslov da prvi i poslednji element u nizu nije iz iste grupe nije nikakvo ograničenje s obzirom na tranzitivnost konjugovanosti.□

**Lema 25.5** *Neka je grupa* $\mathbf{G}$ *generisana unijom domena* $\bigcup_{i\in I} A_i$ *familije podgrupa* $\{\mathbf{A}_i \mid i \in I\}$. *Tada važi:*

$\mathbf{G}$ *je slobodni proizvod date familije podgrupa akko za svaku grupu* $\mathbf{H}$ *i svaki (dati) skup homomorfizama* $\{\varphi_i \in Hom(\mathbf{A}_i, \mathbf{H}) \mid i \in I\}$ *postoji homomorfno preslikavanje* $\varphi$ *grupe* $\mathbf{G}$ *u* $\mathbf{H}$ *takvo da je* $\varphi|_{A_i} = \varphi_i$ *za svako* $i \in I$.

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{G} = \prod^*_{i\in I}\mathbf{A}_i$, $\mathbf{H}$ (ma koja) grupa i, za svako $i \in I$, $\varphi_i \in Hom(\mathbf{A}_i, \mathbf{H})$. Definišimo preslikavanje $\varphi : G \longrightarrow H$ na sledeći način: ako je $x = a_1 \cdot \ldots \cdot a_k$ nejedinični element, gde je, za $r = 1, \ldots, k$, $a_r$ nejedinični element podgrupa $\mathbf{A}_{i_r}$ i gde nikoja dva susedna elementa nisu iz iste podgrupe, tada je $(x)\varphi = (a_1)\varphi_{i_1} \cdot \ldots \cdot (a_k)\varphi_{i_k}$, i, naravno, $(e_G)\varphi = e_H$. $\varphi$ je, s obzirom na jedinstvenost prezentacije nejediničnog elementa kao proizvoda nejediničnih elemenata iz datih podgrupa u kojem nikoja dva susedna nisu iz iste podgrupe, dobro definisano. Takođe, $\varphi$ je i homomorfno preslikavanje. Neka je $y = b_1 \cdot \ldots \cdot b_m$, gde $b_t \in A_{j_t}$ i neka je, s notacijom i razmatranjima iz prethodnih diskusija, $x \cdot y = a_1 \cdot \ldots \cdot a_{k-(r+1)} \cdot c_{k-r} \cdot b_{r+2} \cdot \ldots \cdot b_m$. Onda je

$$(x \cdot y)\varphi = (a_1 \cdot \ldots \cdot a_{k-(r+1)} \cdot c_{k-r} \cdot b_{r+2} \cdot \ldots \cdot b_m)\varphi =$$

$$(a_1)\varphi_{i_1} \cdot \ldots \cdot (a_{k-(r+1)})\varphi_{i_{k-(r+1)}} \cdot (c_{k-r})\varphi_{i_{k-r}} \cdot (b_{r+2})\varphi_{j_{r+2}} \cdot \ldots \cdot (b_m)\varphi_{j_m} =$$

$$(a_1)\varphi_{i_1} \cdot \ldots \cdot (a_{k-(r+1)})\varphi_{i_{k-(r+1)}} \cdot (a_{k-r})\varphi_{i_{k-r}} \cdot \ldots \cdot (a_k)\varphi_{i_k} \cdot (b_1)\varphi_{j_1} \cdot \ldots \cdot (b_m)\varphi_{j_m} =$$

$$(x)\varphi \cdot (y)\varphi;$$

ne zaboravimo: $a_k = b_1^{-1}, \ldots, a_{k-(r-1)} = b_r^{-1}$ i $i_{k-r} = j_{r+1}$ i $a_{k-r} \cdot b_{r+1} = c_{k-r}$ je nejedinični element podgrupe $\mathbf{A}_{i_{k-r}}$.

($\Longleftarrow$) Neka je $\mathbf{H} = \langle H, \bullet\rangle$ spoljašnji slobodni proizvod familije grupa $\{\mathbf{A}'_i \mid i \in I\}$, gde je, za svako $i \in I$, $\mathbf{A}'_i$ "kopija" grupe $\mathbf{A}_i$ ($a \longleftrightarrow a'$), i ako je $i \neq j$, onda je $A'_i \cap A'_j = \emptyset$. Za $i \in I$ neka je $A''_i = A'_i \setminus \{e'_i\} \cup \{1\} \subseteq H$ (1 je prazna reč). Očigledno, $\mathbf{A}''_i = \langle A''_i, \bullet\rangle$ je podgrupa grupe $\mathbf{H}$ izomorfna sa $\mathbf{A}_i$ i $\mathbf{H}$ je slobodni proizvod familije podgrupa $\{\mathbf{A}''_i \mid i \in I\}$. Neka je $\varphi_i \in Is(\mathbf{A}_i, \mathbf{A}''_i)$ "prirodni" izomorfizam: $(e_i)\varphi_i = 1$; $(a)\varphi_i = a'$ ako je $a$ nejedinični element. Prema pretpostavci postoji homomorfno preslikavanje $\varphi$ grupe $\mathbf{G}$ u $\mathbf{H}$ takvo da je $\varphi|_{A_i} = \varphi_i$. Prema prvom delu dokaza postoji homomorfno preslikavanje $\psi$ grupe $\mathbf{H}$ u $\mathbf{G}$ takvo da je $\psi|_{A''_i} = \varphi_i^{-1}$. No tada je $\varphi\circ\psi = \imath_G$, $\psi\circ\varphi = \imath_H$ (jer $\mathbf{G} = \langle \bigcup_{i\in I} A_i\rangle$ i, jasno, $\mathbf{H} = \langle \bigcup_{i\in I} A''_i)\rangle$), pa su $\varphi$ i $\psi$ bijektivna preslikavanja. Dakle, $\psi$ je izomorfno preslikavanje grupe $\mathbf{H}$ na $\mathbf{G}$ i pošto je $(\mathbf{A}''_i)\psi = \mathbf{A}_i$, sledi $\mathbf{G} = \prod^*_{i\in I}\mathbf{A}_i$.□

**Lema 25.6** ($a$) *Ako je* $\mathbf{G} = \prod^*_{i\in I}\mathbf{A}_i$ *i, za* $i \in I$, $\mathbf{A}_i = \prod^*_{j\in J_i}\mathbf{A}_{ij}$, *tada je* $\mathbf{G} = \prod^*_{i,j}\mathbf{A}_{ij}$; *slobodni proizvod* $\prod^*_{i,j}\mathbf{A}_{ij}$ *je proširenje, kazaćemo i produženje (eng. refinement), slobodnog proizvoda* $\prod^*_i \mathbf{A}_i$;

($b$) *Neka je* $\mathbf{G} = \prod^*_{i\in I}\mathbf{A}_i$ *i neka je* $\{J_k \mid k \in K\}$ *particija skupa* $I$. *Tada je* $\mathbf{G} = \prod^*_{k\in K}(\prod^*_{i\in J_k}\mathbf{A}_i)$;

($c$) *Neka je* $\mathbf{G} = \prod^*_{i\in I}\mathbf{A}_i$ *i, za* $i \in I$, $\mathbf{B}_i$ *podgrupa grupe* $\mathbf{A}_i$. *Onda je* $\langle \bigcup_{i\in I} B_i\rangle = \prod^*_{i\in I}\mathbf{B}_i$.

**Lema 25.7** ($a$) *Neka je* $\mathbf{G} = \prod^*_{i\in I}\mathbf{H}_i$ *i neka je, za* $i \in I$, $\mathbf{K}_i$ *normalna podgrupa grupe* $\mathbf{H}_i$. *Ako je* $\mathbf{K}$ *normalno zatvorenje skupa* $\bigcup_{i\in I} K_i$ *(*$\mathbf{K} = \langle\{g^{-1}xg \mid x \in \bigcup_{i\in I} K_i, g \in G\}\rangle$*), tada je* $\mathbf{G}/\mathbf{K} \cong \prod^*_{i\in I}\mathbf{H}_i/\mathbf{K}_i$;



($b$) *Neka je* $\mathbf{G} = \mathbf{H} * \mathbf{K}$ *i neka je* $\mathbf{N}$ *normalno zatvorenje podgrupe* $\mathbf{K}$. *Tada je* $\mathbf{G}/\mathbf{N} \cong \mathbf{H}$.

**Dokaz.** ($a$) Neka je $(A_i; P_i)$ prezentacija grupe $\mathbf{H}_i$ za preslikavanje $\varphi_i$ i neka je $A_i \cap A_j = \emptyset$ za $i \neq j$. Ako je $Q_i = \{u \in W_i \mid (u)\overline{\varphi}_i \in K_i\}$, gde je, kao i uvek, $W_i$ skup reči nad azbukom $A_i \cup A_i^{-1}$, tada je, prema 21.11 i 25.2, $(\bigcup_{i\in I} A_i; \bigcup_{i\in I} P_i \cup \bigcup_{i\in I} Q_i)$ prezentacija faktor grupe $\mathbf{G}/\mathbf{K}$ kao i slobodnog proizvoda familije grupa s prezentacijama $(A_i; P_i \cup Q_i)$, $i \in I$, tj. slobodnog proizvoda $\prod^*_{i\in I}\mathbf{H}_i/\mathbf{K}_i$.□

**Korolar 25.8** $\prod^*_{i\in I}\mathbf{G}_i/(\prod^*_{i\in I}\mathbf{G}_i)' \cong \prod_{i\in I}\mathbf{G}_i/(\prod_{i\in I}\mathbf{G}_i)'$.

**Dokaz.** Neka je $(G_i; P_i)$ prezentacija multiplikativnom tablicom grupe $\mathbf{G}_i$ (videti 21.6($b$) – uzimamo za $A_i$ baš $G_i$, za $\varphi_i$ identično preslikavanje). Tada je

$$\Big(\bigcup_{i\in I} G_i;\ \bigcup_{i\in I} P_i \cup \bigcup_{i\in I}\{[a_i, b_i] \mid a_i, b_i \in G_i\} \cup \cup\{[a_i, b_j] \mid i, j \in I, i \neq j, a_i \in G_i, b_j \in G_j\}\Big)$$

prezentacija faktor grupe $\prod^*_{i\in I}\mathbf{G}_i/(\prod^*_{i\in I}\mathbf{G}_i)'$, ali prema 21.6($i$), i direktnog proizvoda $\prod_{i\in I}\mathbf{G}_i/\mathbf{G}'_i$ ($\cong \prod_{i\in I}\mathbf{G}_i/(\prod_{i\in I}\mathbf{G}_i)'$); $(G_i; P_i \cup \{[a_i, b_i] \mid a_i, b_i \in G_i\})$ je prezentacija faktor grupe $\mathbf{G}_i/\mathbf{G}'_i$; mogli smo, naravno, i ovako rezonovati: $(\bigcup_{i\in I} G_i; \bigcup_{i\in I} P_i \cup \{[a_i, b_j] \mid i, j \in I, i \neq j, a_i \in A_i, b_j \in A_j\})$ je prezentacija grupe $\prod_{i\in I}\mathbf{G}_i$, a zbog $(\prod_{i\in I}\mathbf{G}_i)' = \prod_{i\in I}\mathbf{G}'_i$, gornja prezentacija je prezentacija faktor grupe $\prod_{i\in I}\mathbf{G}_i/(\prod_{i\in I}\mathbf{G}_i)'$.□

**Lema 25.9** ($a$) *Neka je* $\mathbf{G} = \prod^*_{i\in I}\mathbf{A}_i$, $|I| \geq 2$. *Ako je za nejedinični element* $a_1 \ldots a_m$, $m \geq 2$, *gde je* $a_r \in A_{i_r}$ *za* $r = 1 \ldots, m$, $i_1 \neq i_m$, *onda je on beskonačnog reda;*

($b$) *Slobodni proizvod dve ili više nejediničnih grupa sadrži element beskonačnog reda;*

($c$) *Neka je* $\mathbf{G} = \prod^*_{i\in I}\mathbf{A}_i$, $|I| \geq 2$. *Element* $g \in G$ *konačnog reda konjugovan je nekom elementu nekog od slobodnih faktora;*

($d$) *Slobodni proizvod torziono slobodnih grupa je torziono slobodna grupa.*

**Dokaz.** ($a$) i ($b$) je trivijalno.

($c$) Indukcijom po dužini reči (izraza), $m$. Slučaj $m = 1$ je trivijalan, a prema ($a$) nemamo elemenata konačnog reda dužine 2. Pretpostavimo da je tvrđenje tačno za sve reči dužine manje od $m$ ($> 2$) i neka je element $g = a_1 \ldots a_m$ konačnog reda. Opet prema ($a$), $i_1 = i_m$, a i element $a_m \bullet g \bullet a_m^{-1} = (a_m \bullet a_1) \bullet a_2 \ldots a_{m-1}$ je konačnog reda. Odatle sledi da je $a_m = a_1^{-1}$ (inače bi, prema ($a$), bilo $i_1 = i_m = i_{m-1}$, kontradikcija). Element $a_2 \ldots a_{m-1}$ je pak prema induktivnoj hipotezi konjugovan sa nekim elementom nekog slobodnog faktora.

($d$) je neposredna posledica tačke ($c$).□

**Lema 25.10** (*a*) *Neka je* $\mathbf{G} = \prod^*_{i\in I}\mathbf{G}_i$ *i* $b$ *nejedinični element grupe* $\mathbf{G}_j$. *Tada je* $\mathbf{C}(b) \leq \mathbf{G}_j$;

(*b*) *Slobodni proizvod u kojem su bar dva slobodna faktora nejedinične grupe je bez centra.*

**Dokaz**. (*a*) Neka je $1 \neq a_1 \dots a_m = a \in C(b)$, gde je $a_r \in A_{i_r}$ za $1 \leq r \leq m$. Ako je $m = 1$, trivijalno $a = a_1 \in A_j$. Očigledno u $\mathbf{C}(b)$ nemamo reči dužine 2. Pokazujemo indukcijom po $m$ da nemamo ni reči većih dužina; preciznije, pokazujemo da centralizator nijednog nejediničnog elementa bilo kog od slobodnih faktora ne sadrži reči dužine $\geq 2$. Pretpostavimo da je tvrđenje tačno za svako $k < m$ $(> 2)$. Ako su i $a_1$ i $a_m$ iz $\mathbf{A}_j$, onda je $a_m \bullet a \bullet a_m^{-1} = (a_m \cdot_j a_1) \bullet a_2 \dots a_{m-1} \in C(a_m \cdot_j b \cdot_j a_m^{-1})$; no, $a_m \cdot_j b \cdot_j a_m^{-1}$ je nejedinični element, dužina reči $(a_m \cdot a_1) \bullet a_2 \dots a_{m-1}$ je manja od $m$ i $a_2 \notin A_j$, kontradikcija. Proizilazi da bar jedan od elemenata $a_1, a_m$ nije u $\mathbf{A}_j$. Ali tada je, jasno, $b \bullet a_1 \dots a_m \neq a_1 \dots a_m \bullet b$, kontradikcija ponovo.□

**Primer 25.11** (*a*) *Beskonačna dijedarska grupa je slobodni proizvod dve ciklične grupe reda* 2.

**Dokaz**. Prezentacija beskonačne dijedarske grupe $(a, b; a^2, (ab)^2)$ (21.10(*o*)) "prevodi" se Tietzeovim transformacijama u $(x, y; x^2, y^2)$ (što se lako pokazuje), a to je, prema 25.2, prezentacija grupe $\mathbf{Z}_2 * \mathbf{Z}_2$.

(*b*) *Grupa* $\mathbf{PSL}_2(\mathbf{Z}) = \mathbf{SL}_2(\mathbf{Z})/\mathbf{Z}(\mathbf{SL}_2(\mathbf{Z}))$, *gde je* $\mathbf{SL}_2(\mathbf{Z})$ *grupa unimodularnih matrica formata* $2 \times 2$ *sa elementima iz prstena* $\langle Z, +, \cdot\rangle$ *(videti definicije* 19.36 *i* 19.42*), slobodni je proizvod cikličnih grupa reda* 2 *i* 3.

**Dokaz**. Pokažimo prvo da je grupa $\mathbf{SL}_2(\mathbf{Z})$ generisana matricama $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ i $B = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$. Za svaki ceo broj $k$ je $(AB)^k = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$ i $(BA)^k = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & 0 \\ -k & 1 \end{bmatrix}$. Ako je jedan od elemenata prve kolone matrice $C \in SL_2(\mathbf{Z})$ nula, onda je, s obzirom da je $det(C) = 1$, $C$ jednog od oblika $\pm\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$, $\pm\begin{bmatrix} 0 & 1 \\ -1 & k \end{bmatrix}$, $k \in Z$. Već smo videli: $(AB)^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$. Takođe je:

$$A^2(AB)^k = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} = -\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix},$$

$$A(AB)^{-k} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & -k \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & k \end{bmatrix},$$

$$A^3(AB)^{-k} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & -k \\ 0 & 1 \end{bmatrix} = -\begin{bmatrix} 0 & 1 \\ -1 & k \end{bmatrix}.$$



Pretpostavimo da je $\langle A, B\rangle$ prava podgrupa grupe $\mathbf{SL}_2(\mathbf{Z})$ i izaberimo među matricama van podgrupe $\langle A, B\rangle$ neku, neka je to $C = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, kod koje je zbir apsolutnih vrednosti elemenata prve kolone $(|a| + |c|)$ minimalan. Upravo smo videli da mora biti $ac \neq 0$. Ako je $|a| \geq |c|$, za podesno izbrano $k$ je $|a + kc| < |c|$, pa sledi: matrica $(AB)^k C = \begin{bmatrix} a + kc & b + kd \\ c & d \end{bmatrix}$ nije u $\langle A, B\rangle$, dok je $|a + kc| + |c| < |c| + |c| \leq |a| + |c|$, protivno izboru matrice $C$. Ako je $|c| > |a|$, tada je, za neko $k \in Z$, $|ka + c| < |a|$ i sada matrica $(BA)^{-k}C = \begin{bmatrix} a & b \\ ka + c & kb + d \end{bmatrix}$ nije u $\langle A, B\rangle$, a $|a| + |ka + c| < |a| + |c|$, kontradikcija ponovo.

Kako je $A^2 = B^3 = -I \in Z(\mathbf{SL}_2(\mathbf{Z}))$ (naravno, $Z(\mathbf{SL}_2(\mathbf{Z})) = \{I, -I\}$), generatorni elementi grupe $\mathbf{PSL}_2(\mathbf{Z})$, $\overline{A} = A\,Z(\mathbf{SL}_2(\mathbf{Z}))$ i $\overline{B} = B\,Z(\mathbf{SL}_2(\mathbf{Z}))$ su reda, respektivno 2 i 3. Neka su $\langle a\rangle$ i $\langle b\rangle$ ciklične grupe redova, redom, 2 i 3 i neka je $\varphi$ homomorfno preslikavanje grupe $\langle a\rangle * \langle b\rangle$ na grupu $\mathbf{PSL}_2(\mathbf{Z})$), određeno sa: $(a)\varphi = \overline{A}$, $(b)\varphi = \overline{B}$ (videti 25.5). Dokažimo da je $\varphi$ i injektivno preslikavanje. Neka je $u \in Ker(\varphi)$. Možemo pretpostaviti da je $u$ jednog od oblika: $b^k v$ ili $va^l$, gde je $k \in \{0, -1, 1\}$, $l \in \{0, 1\}$, dok je $v$ proizvod elemenata $ab$ i $ab^{-1}$ (ako bi npr. $u$ "počinjalo" sa $b$ i "završavalo" sa $a$, uzeli bismo njegov inverzni). Za $k \geq 1$ je $(AB^{-1})^k = (-1)^k \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix}$, što, uz već poznato $(AB)^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$, implicira da nenula proizvod matrica $(AB)^k$, $(AB)^{-r}$ nije dijagonalna matrica kao i da su svi elementi u toj matrici ili svi pozitivni ili svi negativni. Stoga su takvi proizvodi različiti od $A$, $-A$, $B$, $-B$, $B^{-1}$, $-B^{-1}$. Zbog toga mora biti $u$ jedinični element.

(*c*) *Grupa* $\mathbf{PSL}_2(\mathbf{Z})$, *pa dakle i grupa* $\mathbf{C}_2 * \mathbf{C}_3$, *ima beskonačno mnogo podgrupa konačnog indeksa i beskonačno mnogo prostih homomorfnih slika.*

**Dokaz**. Preslikavanje $\varphi : Z \longrightarrow Z_n$, $n \geq 1$, dato sa: $(k)\varphi = k - [\frac{k}{n}]n$ homomorfno je preslikavanje prstena $\langle Z, +, \cdot\rangle$ na prsten $\langle n, +_n, \cdot_n\rangle$ (videti i dopuniti 7.2(*h*)). Već smo iznimno u prošloj tački koristili $\mathbf{Z}$ da označi prsten celih brojeva. Za ovu priliku, opet iznimno, uzećemo da je $\mathbf{Z}_p$ polje $\langle p, +_p, \cdot_p\rangle$, gde je $p$ prost broj. Jasno je da je preslikavanje $\Phi : SL_2(\mathbf{Z}) \longrightarrow SL_2(\mathbf{Z}_p)$, dato sa: $(\begin{bmatrix} a & b \\ c & d \end{bmatrix})\Phi = \begin{bmatrix} (a)\varphi & (b)\varphi \\ (c)\varphi & (d)\varphi \end{bmatrix}$, surjektivno homomorfno preslikavanje grupe $\mathbf{SL}_2(\mathbf{Z})$ na grupu $\mathbf{SL}_2(\mathbf{Z}_p)$, a preslikavanje $\overline{\Phi} : PSL_2(\mathbf{Z}) \longrightarrow PSL_2(\mathbf{Z}_p)$, određeno sa: $(A\,Z(\mathbf{SL}_2(\mathbf{Z})))\overline{\Phi} = (A)\Phi\,Z(\mathbf{SL}_2(\mathbf{Z}_p))$, surjektivno homomorfno preslikavanje grupe $\mathbf{PSL}_2(\mathbf{Z})$ na grupu $\mathbf{PSL}_2(\mathbf{Z}_p)$. No prema 19.45, za svako polje $\mathbf{Z}_p$, gde je $p$ neparan prost broj, grupa $\mathbf{PSL}_2(\mathbf{Z}_p)$ je prosta (konačna) grupa, pa je i $\mathbf{Ker}(\overline{\Phi})$ normalna podgrupa konačnog indeksa.

(*d*) *Neka je* $\mathbf{G} = \mathbf{A} * \mathbf{B}$. *Tada je* $[\mathbf{A}, \mathbf{B}]$ *slobodna grupa ranga* $(|A| - 1) \cdot (|B| - 1)$.

**Dokaz**. Pretpostavićemo, naravno, da su $\mathbf{A}$ i $\mathbf{B}$ nejedinične grupe. Grupa $[\mathbf{A}, \mathbf{B}]$ je generisana skupom $X = \{[a, b] \mid a \in A \setminus \{e\},\ b \in B \setminus \{e\}\}$. Ali to je upravo i njena slobodna baza. Evidentno, $X \cap X^{-1} = \emptyset$, a lako se pokazuje da je proizvod $[a_1, b_1]^{\alpha_1} \dots [a_n, b_n]^{\alpha_n}$, gde je $n \geq 1$, $[a_i, b_i] \in X$, $\alpha_i \in \{1, -1\}$ i za $i < n$ ili je $\alpha_i = \alpha_{i+1}$ ili je uređen par $(a_i, b_i)$ različit od uređenog para $(a_{i+1}, b_{i+1})$, različit od jediničnog elementa (23.8(*a*)). Konkretno, indukcijom po $n$ se proverava da se taj proizvod završava ili sa $a_n b_n$ ili sa $b_n a_n$. Za $n = 1$ to je očigledno. Pretpostavimo da je tvrđenje tačno za svako $k < n\ (> 1)$. Prema tome, $[a_1, b_1]^{\alpha_1} \dots [a_{n-1}, b_{n-1}]^{\alpha_{n-1}}$ se završava ili sa $a_{n-1} b_{n-1}$ ili sa $b_{n-1} a_{n-1}$. Recimo da je u pitanju "završetak" $b_{n-1} a_{n-1}$, što će reći da je $\alpha_{n-1} = -1$. Ako je npr. $\alpha_n = 1$, onda je ili $a_{n-1} \neq a_n$ ili $b_{n-1} \neq b_n$, pa se u proizvodu $b_{n-1} \bullet a_{n-1} \bullet a_n^{-1} \bullet b_n^{-1} \bullet a_n \bullet b_n$ ne može "izgubiti" $a_n b_n$. Analogno bismo razmotrili ostale slučajeve.

(*e*) *Grupa* $\mathbf{PSL}_2(\mathbf{Z})'$, *tj.* $(\mathbf{C}_2 * \mathbf{C}_3)'$ *je slobodna grupa ranga* 2.

**Dokaz**. Primetimo samo: $\mathbf{C}_2$ i $\mathbf{C}_3$ su Abelove grupe, te je $(\mathbf{C}_2 * \mathbf{C}_3)' = [\mathbf{C}_2, \mathbf{C}_3]$.□

## 26 Podgrupe slobodnog proizvoda

Sledeća teorema je od suštinskog značaja za teoriju slobodnih proizvoda.

**Teorema 26.1** *(Kuroševa teorema o podgrupama). Ako je* $\mathbf{H}$ *podgrupa slobodnog proizvoda* $\mathbf{G} = \prod^*_{i \in I} \mathbf{A}_i$, *tada postoji slobodno razlaganje (dekompozicija) podgrupe* $\mathbf{H}$, $\mathbf{H} = \mathbf{F} * \prod^*_{j \in J} \mathbf{B}_j$, *gde je* $\mathbf{F}$ *slobodna grupa, a svaka od podgrupa* $\mathbf{B}_j$ *(*$j \in J$*) je konjugat neke podgrupe nekog od faktora* $\mathbf{A}_{i_j}$.

**Dokaz**. Daćemo Kurošev (dakle prvi) dokaz ove teoreme (kako je već izložen u [92] – inače, postoji još nekoliko). No za to nam je potrebno više pomoćnih stavova. Prvo par pojmova.

Ako je $a_1 \cdot \dots \cdot a_{2n}$ normalna forma nejediničnog elementa $g \in G = \prod^*_{i \in I} A_i$, onda je $a_1 \cdot \dots \cdot a_n$ *leva* i $a_{n+1} \cdot \dots \cdot a_{2n}$ *desna polovina* elementa $g$. Pisaćemo i $g = a_{-n} \dots a_{-1} a_1 \dots a_n$. Ako je pak $l(g) = 2n+1$ i $g = a_{-n} \dots a_{-1} a_0 a_1 \dots a_n$, tada je, jasno, $a_{-n} \dots a_{-1}$ leva, $a_1 \dots a_n$ desna polovina i $a_0$ *sredina* elementa $g$. Posebno, ako je $l(g) = 2n + 1$ i $a_{-i} = a_i^{-1}$ za $i = 1, \dots, n$, $g$ je, kažemo, *transform*. Naravno, u tom slučaju su $g$ i $a_0$ konjugovani elementi, stoga i istog reda. Jasno, svaki element koji nije transform je beskonačnog reda.

Definišemo u nastavku rekurzivno, po ordinalima, podgrupe grupe $\mathbf{H}$ – $\mathbf{C}_\alpha$, $\mathbf{D}_\alpha$ – na sledeći način.

$\mathbf{C}_0 = \mathbf{D}_0 = \mathbf{E}$. Pretpostavimo da su već formirane podgrupe $\mathbf{C}_\alpha$, $\mathbf{D}_\alpha$ za $\alpha < \beta$ i neka je $\mathbf{D}_\beta = \langle \bigcup_{\alpha < \beta} C_\alpha \rangle$, $H \setminus D_\beta$ neprazan slup i $l_\beta = min\{l(v) \mid v \in H \setminus D_\beta\}$. Ako u $H \setminus D_\beta$ nema transforma dužine $l_\beta$ (što će se, recimo, uvek desiti ako je $l_\beta$ paran broj), definišemo: $\overline{\mathbf{A}}_\beta = \mathbf{E}$. Ako postoje takvi transformi, biramo jedan, neka je to $g_\beta^{-1} a g_\beta$, gde je $a \in A_{i_\beta}$ i definišemo: $\overline{\mathbf{A}}_\beta = \mathbf{H} \cap g_\beta^{-1} \mathbf{A}_{i_\beta} g_\beta$; u slučaju $l_\beta = 1$ imaćemo $\overline{\mathbf{A}}_\beta = \mathbf{H} \cap \mathbf{A}_{i_\beta}$. Što se tiče samog izbora transforma, pretpostavićemo da je domen $G$ dobro uređen, $G = \{g_\gamma \mid \gamma < |G|\}$, i onda uvek uzimati elemente s najmanjim indeksom koji ispunjavaju postavljene uslove. Ako u $H \setminus \langle D_\beta, \overline{A}_\beta \rangle$ postoji element dužine $l_\beta$ čija je desna polovina $g_\beta$, a sredina element iz $A_{i_\beta}$, uzimamo jedan takav – $h_{\beta_1}$. Pošto smo već izabrali elemente $h_{\beta_\gamma}$ za $\gamma < \delta$, $h_{\beta_\delta}$ će biti izabrani element, ukoliko takav postoji, iz $H \setminus \langle D_\beta, \overline{A}_\beta, \{h_{\beta_\gamma} \mid \gamma < \delta\} \rangle$ čija je desna polovina $g_\beta$ i sredina element iz $A_{i_\beta}$. Naravno, proces mora stati za neki ordinal $\sigma_\beta$. Tada je $\mathbf{C}_\beta \stackrel{\text{def}}{=} \langle \overline{A}_\beta \cup \{h_{\beta_\delta} \mid \delta < \sigma_\beta\} \rangle$ i $\mathbf{D}_{\beta+1} = \langle D_\beta, C_\beta \rangle$ $(= \langle \bigcup_{\alpha < \beta+1} C_\alpha \rangle)$. Ako je $\overline{\mathbf{A}}_\beta = \mathbf{E}$, biramo element $h_{\beta_1}$ iz $H \setminus D_\beta$ dužine $l_\beta$ i postupak ponavljamo kao i maločas, s tim što su nam sada "reperi" desna polovina $(g_\beta)$ elementa $h_{\beta_1}$ i, kada je $l_\beta$ neparan broj, podgrupa $\mathbf{A}_{i_\beta}$ u kojoj je sredina elementa $h_{\beta_1}$.



Pod *generatorima* grupe $\mathbf{C}_\alpha$ podrazumevaćemo, specijalno za ovu priliku, elemente $h_{\alpha_\delta}$, $h_{\alpha_\delta}^{-1}$, $\delta < \sigma_\alpha$ i nejedinične elemente podgrupe $\overline{\mathbf{A}}_\alpha$. *Generatori* podgrupe $\mathbf{D}_\beta$ će biti generatori svih podgrupa $\mathbf{C}_\alpha$, $\alpha < \beta$. Generatore ćemo obeležavati (držeći se manje-više notacije iz [92]) sa $u_1, \dots, u_k, \dots$, ali i sa $v_1, \dots, v_k, \dots$, a proizvod $u_1 \dots u_k$ u kojem nikoja dva susedna generatora nisu uzajamno inverzna i ne pripadaju istoj podgrupi $\overline{\mathbf{A}}_\alpha$ zvaćemo *reč*. Reč $u_1 \dots u_k$ je *prosta* akko je njena dužina, s obzirom na razlaganje $\mathbf{G} = \prod^*_{i \in I} \mathbf{A}_i$, jednaka najvećoj od dužina faktora $u_1, \dots, u_k$: $l(u_1 \dots u_k) = max\{l(u_i) \mid 1 \leq i \leq k\}$; prema tome, dužina prostih reči podgrupe $\mathbf{C}_\alpha$ je $l_\alpha$. Proste reči označavaćemo sa $u', u'', \dots$ ili sa $u^{(1)}, u^{(2)}, \dots, u^{(m)}, \dots$ ili sa $v', v'', \dots$ (ili sa $v^{(1)}, v^{(2)}, \dots$). Među prostim rečima $u', u''$ postoji *veza prve, druge* odnosno *treće vrste* akko je, respektivno, $l(u'u'')$ veće, jednako, odnosno manje od $max\{l(u'), l(u'')\}$.

Važi

**Lema 26.2** $\mathbf{C}_\alpha$ *je slobodni proizvod podgrupe* $\overline{\mathbf{A}}_\alpha$ *i beskonačnih cikličnih podgrupa* $\langle h_{\alpha_\delta} \rangle$, $\delta < \sigma_\alpha$.

**Dokaz**. Neka je $u = u_1 \dots u_k$ reč grupe $\mathbf{C}_\alpha$ (u smislu gore datih definicija). Jasno, dovoljno je i potrebno da pokažemo da je $u$ nejedinični element grupe $\mathbf{G}$, tj. da ima netrivijalnu normalnu formu u dekompoziciji $\mathbf{G} = \prod^*_{i \in I} \mathbf{A}_i$. Konstatujmo prvo.

(*a*) *Ako je* $\gamma < \beta < \sigma_\alpha$, *onda elementi* $h_{\alpha_\gamma}$ *i* $h_{\alpha_\beta}$ *imaju različite leve polovine.*

Zaista, neka je $l_\alpha$ neparno i $h_{\alpha_\gamma} = g_1 a_1 g_\alpha$, $h_{\alpha_\beta} = g_2 a_2 g_\alpha$, gde $a_1, a_2 \in A_{i_\alpha}$. Za $g_1 = g_2 = g$ imali bismo $h_{\alpha_\gamma}^{-1} h_{\alpha_\beta} = g_\alpha^{-1} a_1^{-1} g^{-1} \cdot g a_2 g_\alpha = g_\alpha^{-1} a_1^{-1} a_2 g_\alpha \in \overline{A}_\alpha$, dakle $h_{\alpha_\beta} \in \langle \overline{A}_\alpha, h_{\alpha_\gamma} \rangle$, kontradikcija. Ako je $l_\alpha$ paran broj, slučaj je

još trivijalniji; elementi $h_{\alpha_\gamma}$, $h_{\alpha_\beta}$ već imaju jednake desne polovine, pa kao različiti ne mogu imati jednake i leve polovine.

(*b*) *Sve proste reči podgrupe* $\mathbf{C}_\alpha$ *su jedne od formi:*

(1) $u_k$;

(2) $u_iu_j$, *gde je* $g_\alpha$ *desna polovina generatora* $u_i$ *i* $g_\alpha^{-1}$ *leva polovina generatora* $u_j$;

(3) $u_iu_ju_k$, *gde je* $u_j \in \overline{A}_\alpha$ *i* $u_i = h_{\alpha_\gamma}$, $u_k = h_{\alpha_\beta}^{-1}$ *za neke, ne nužno različite, ordinale* $\gamma, \beta < \sigma_\alpha$.

Lako se proverava da su sve navedene reči proste.

U (2) bi $l(u_iu_j) < l_\alpha$ dalo $u_iu_j \in D_\alpha$, dakle, npr. $u_j \in \langle D_\alpha, u_i\rangle$, kontradikcija.

U trećem slučaju, $u_i = g_iag_\alpha$, $u_j = g_\alpha^{-1}bg_\alpha$ i $u_k = (g_kcg_\alpha)^{-1}$, gde je $a, b, c \in A_{i_\alpha}$, daju: $u_iu_ju_k = g_iabcg_k$ i ponovo, kao maločas, ne dolazi u obzir da je $abc$ jedinični element.

Važi takođe, što kompletira dokaz tačke (*b*):

*za svaku reč* $u_1 \dots u_n$ *podgrupe* $\mathbf{C}_\alpha$ *postoji distribucija zagrada*

$$u_1 \dots u_n = (u_1 \dots u_{i_1})(u_{i_1+1} \dots u_{i_2}) \dots (u_{i_{m-1}+1} \dots u_n)$$

*takva da su reči* $u^{(1)} = u_1 \dots u_{i_1}$, $u^{(2)} = u_{i_1+1} \dots u_{i_2}$, …, $u^{(m)} = u_{i_{m-1}+1} \dots u_n$ *proste a veza između svake dve susedne reči* $u^{(j)}$ *i* $u^{(j+1)}$ $(1 \le j < m)$ *je prve vrste.*

Dokaz ovog tvrđenja je indukcijom po $n$. Slučaj $n = 1$ je trivijalan. Pretpostavimo da je tvrđenje tačno za $n$ $(\ge 1)$ i neka je data reč $u_1 \dots u_nu_{n+1}$. Prema induktivnoj hipotezi je $u_1 \dots u_n = u^{(1)} \dots u^{(m)}$, gde je $u^{(k)}$, $1 \le k \le m$, prosta reč jedne od formi (1), (2), (3) i gde je veza između svake dve susedne reči prve vrste. Prema tome, desna polovina reči $u^{(m)}$ jednaka je desnoj polovini generatora $u_n$. Ako je to $g_\alpha$ (što će reći da je $u^{(m)}$ forme (1) ili (2)) i ako je $g_\alpha^{-1}$ leva polovina generatora $u_{n+1}$, onda je $u^{(m)}u_{n+1}$ prosta reč forme (2) ili (3). U ostalim slučajevima veza između $u^{(m)}$ i $u_{n+1}$ je prve vrste, te možemo uzeti $u_{n+1}$ kao novu prostu reč. Primetimo samo: neka desna polovina reči $u^{(m)}$ nije $g_\alpha$ i neka leva polovina generatora $u_{n+1}$ nije $g_\alpha^{-1}$. Tada je $u_n$ neko $h_{\alpha_\beta}^{-1}$ i $u_{n+1}$ neko $h_{\alpha_\gamma}$. Pošto je, po definiciji reči, isključeno $u_{n+1} = u_n^{-1}$, to je $\beta \ne \gamma$, pa $h_{\alpha_\beta}$ i $h_{\alpha_\gamma}$ imaju različite leve polovine, recimo $g_1$, $g_2$ i $g_1^{-1}g_2 \ne e$. Slično se diskutuju i ostali slučajevi.

Prema (*b*) direktno sledi i tvrđenje leme.□

Naredna lema (analogon upravo dokazanog tvrđenja, sada su podgrupe $\mathbf{D}_\beta$ u pitanju) i njen korolar daju dokaz teoreme.

**Lema 26.3** *Za svaku reč* $u_1 \dots u_n$ *podgrupe* $\mathbf{D}_\beta$ *postoji distribucija zagrada*

$$(u_1 \dots u_{i_1})(u_{i_1+1} \dots u_{i_2}) \dots (u_{i_{m-1}+1} \dots u_n)$$



*takva da su reči* $u^{(1)} = u_1 \dots u_{i_1}$, $u^{(2)} = u_{i_1+1} \dots u_{i_2}$, …, $u^{(m)} = u_{i_{m-1}+1} \dots u_n$ *proste i veza između svake dve susedne reči* $u^{(j)}$ *i* $u^{(j+1)}$ $(1 \le j < m)$ *je prve vrste.*

**Dokaz** Primetimo odmah, a to je ujedno i dokaz narednog korolara: ako reč $u \equiv u_1 \dots u_n$ nije prosta, onda za njeno dato razlaganje na proizvod prostih reči (gde je veza između svake dve susedne proste reči prve vrste) važi da je dužina reči $u$ veća od dužine svakog od prostog faktora $u^{(1)}, \dots, u^{(m)}$; jer, ako su, generalno, $u'$ i $u''$ proste reči između kojih je veza prve ili druge vrste, onda leva (desna) polovina normalne forme (proizvoda) $u'u''$ "sadrži" levu (desnu) polovinu normalne forme reči $u'$ $(u'')$; posebno, ako je veza prve vrste i ako je neka od reči $u'$, $u''$ neparne dužine, njena sredina ostaje element proizvoda. Formalno, dokaz primedbe bi išao indukcijom po broju prostih faktora u razlaganju $(m \ge 2)$.

Sumiramo: svaka neprazna reč grupe $\mathbf{D}_\beta$ ima nepraznu normalnu formu.

Vraćamo se na dokaz leme – indukcijom po $\beta$. Slučajevi $\beta = 0, 1$ su trivijalni (onda je $\mathbf{D}_\beta = \mathbf{E}$), a za $\beta = 2$ je $\mathbf{D}_2 = \mathbf{C}_1$ i dokaz imamo u prethodnoj lemi. Za granični ordinal $\beta$ je $\mathbf{D}_\beta = \bigcup_{\alpha<\beta} \mathbf{D}_\alpha$ i svaka reč grupe $\mathbf{D}_\beta$ je sadržana u nekoj podgrupi $\mathbf{D}_\alpha$ za neki ordinal $\alpha$ manji od $\beta$, pa se jednostavno pozivamo na induktivnu hipotezu. Preostaje "prelaz" sa $\beta$ na $\beta + 1$. Pretpostavljamo dakle da tvrđenje važi za podgrupu $\mathbf{D}_\beta$ i dajemo dokaz za podgrupu $\mathbf{D}_{\beta+1}$. No opet trebamo dosta pomočnih stavova.

**Stav 1** *Ako je* $u_1 \dots u_n$ *prosta reč podgrupe* $\mathbf{D}_\beta$, *tada su svaki njen (početni) segment* $u_1 \dots u_m$, $m \le n$, *i svaki njen (krajnji) segment* $u_k \dots u_n$, $k \ge 1$, *takođe proste reči.*

**Dokaz**. Posmatrajmo početne segmente i pretpostavimo da među njima ima onih koji nisu proste reči. Onda svakako, za neko $m < n$, postoji segment $u_1 \dots u_k$ koji nije prosta, dok je $u_1 \dots u_ku_{k+1}$ prosta reč. $u_1 \dots u_k$ je proizvod prostih reči dobijenih pogodnom distribucijom zagrada, gde je veza između svake dve susedne prve vrste, recimo: $u_1 \dots u_k = u^{(1)} \dots u^{(r)}$, $r > 1$. Upravo smo konstatovali da je dužina reči $u_1 \dots u_k$ veća od dužine svakog prostog faktora. Stoga među prostim rečima $u^{(r)}$ i $u_{k+1}$ ne može biti veza prve ili druge vrste (onda bi dužina reči $u_1 \dots u_mu_{k+1}$ bila veća od dužine svakog od generatora). Ali ako je ta veza treće vrste, onda je dužina reči $u^{(r)}u_{k+1}$ manja od dužine bar jednog od faktora, što je, opet prema lemi i gornjoj napomeni, nemoguće.

**Stav 2** *U normalnoj formi proste reči* $u_1 \dots u_n$ *podgrupe* $\mathbf{D}_\beta$ *leva polovina generatora* $u_1$ *i desna polovina generatora* $u_n$ *ostaju nepromenjeni, a što se tiče njihovih sredina (u slučaju neparnih dužina), one mogu biti eventualno zamenjene, ali samo nejediničnim elementima iz istih (slobodnih) faktora.*

**Dokaz**. Prema prethodnom stavu reč $u_1 \dots u_{n-1}$ je prosta, dakle, $l(u_1 \dots u_{n-1})$ je $max\{\, l(u_i) \mid 1 \le i \le n-1\}$. Kako je i $l(u_1 \dots u_{n-1}u_n) = max\{\, l(u_j) \mid 1 \le$

$j \leq n\}$, to je veza između prostih reči $u_1 \dots u_{n-1}$ i $u_n$ druge vrste. Odatle proizilazi da kancelacija "ne dira" desnu polovinu generatora $u_n$, dok se njegova sredina eventualno množi sa nekim elementom iz istog slobodnog faktora iz kojeg je i ona i taj proizvod mora biti nejedinični element. Analogno se rezonuje i u slučaju generatora $u_1$, koristeći se činjenicom da je $u_2 \dots u_n$ prosta reč.□

**Stav 3** *Svaka reč iz $D_\beta$ čija je normalna forma transform oblika je*

$$u_n^{-1} \dots u_1^{-1} u_0 u_1 \dots u_n,$$

*gde je $u_0$ element podgrupe $\overline{\mathbf{A}}_\alpha$ za neko $\alpha < \beta$ (dakle, i sam transform).*

**Dokaz**. Neka $v = u_1 \dots u_k \in D_\beta$ ima za normalnu formu transform. Indukcijom po $k$ dokazujemo da je $v$ datog oblika. Ako je $k = 1$, onda je, evidentno, prema izboru generatora podgrupa $\mathbf{C}_\alpha$, $\alpha < \beta$, $v$ element neke od podgrupa $\overline{\mathbf{A}}_\alpha$. Ako je $k > 1$ i $u_1 = u_k^{-1}$ ili $u_1$ i $u_k$ pripadaju istoj podgrupi $\overline{\mathbf{A}}_\alpha$, $\alpha < \beta$, tada je $u_1^{-1} v u_1$ ili $u_2 \dots u_{k-1}$ ili $u_2 \dots u_{k-1}(u_k u_1)$, te reči imaju takođe za normalnu formu transform i prema induktivnoj hipotezi tvrđenje važi za $v$. No drugi slučajevi (ako je $k > 1$) i nisu mogući. Pretpostavimo, naime, da $u_1$ i $u_k$ nisu iz iste podgrupe $\overline{\mathbf{A}}_\alpha$ i da nisu uzajamno inverzni. Razlikovaćemo slučajeve: (1) $v$ nije i (2) $v$ jeste prosta reč.

(1) Ako $v$ nije prosta reč, onda je proizvod prostih reči, recimo, $u^{(1)} \dots u^{(r)}$, $r > 1$, gde je veza između svake dve susedne proste reči prve vrste. Kako je reč $v$ transform i njena leva polovina sadrži levu polovinu proste reči $u^{(1)}$ kao i njenu sredinu, u slučaju da postoji, a desna polovina desnu polovinu proste reči $u^{(r)}$ i, za neparnu dužinu, i njenu sredinu, to je veza među prostim rečima $u^{(r)}$ i $u^{(1)}$ u proizvodu $u^{(r)}u^{(1)}$ treće vrste, pa $u^{(r)}u^{(1)}$ ne može da bude ni prosta ni "neprosta" reč, kontradikcija.

(2) Neka je $v$ prosta reč i $l(v) = l(u_i) = max\{\, l(u_j) \mid 1 \leq j \leq k\}$. Bez uticaja na opštost razmatranja možemo pretpostaviti da $u_i$ nije generator $h_{\alpha_\delta}^{-1}$, $\alpha < \beta$, $\delta < \sigma_\alpha$ – u suprotnom bismo, umesto $v$, posmatrali reč $v^{-1}$, kao i da je $i = k$ – u suprotnom bismo posmatrali reč $u_{i+1} \dots u_k v (u_{i+1} \dots u_k)^{-1} = u_{i+1} \dots u_k u_1 \dots u_i$, čija je normalna forma transform i koju, prema gore navedenom, možemo takođe smatrati prostom. Neka je $u_k \in C_\alpha$ za neko $\alpha < \beta$. Tada je, prema usvojenoj notaciji i navedenim pretpostavkama, $g_\alpha$ desna polovina generatora $u_k$, čija pak sredina pripada podgrupi $\mathbf{A}_{i_\alpha}$. Prema prethodnom stavu i navedenim pretpostavkama, desna polovina reči $v$ je isto tako $g_\alpha$, a i njena sredina je iz $\mathbf{A}_{i_\alpha}$. Pod uslovom da je $\overline{\mathbf{A}}_\alpha$ nejedinična podgrupa, i s obzirom da je $v$ transform, proizilazi: $v \in \overline{A}_\alpha$. Ako $u_k \notin \overline{A}_\alpha$, onda imamo kontradikciju: reč $u_1 \dots u_k v^{-1}$ je jednaka jediničnom elementu. No ne pomaže ni $u_k \in \overline{A}_\alpha$: sada je reč $u_1 \dots u_{k-1}(u_k v^{-1})$ jedinična reč ($u_k v^{-1} \in \overline{A}_\alpha$ i $u_{k-1} \notin \overline{A}_\alpha$). Ako je $\overline{\mathbf{A}}_\alpha = \mathbf{E}$, tada je $v$ sadržano u $\mathbf{D}_\delta$ za neko $\delta < \alpha$, pa se može predstaviti kao proizvod generatora ove podgrupe: $v = v_1 \dots v_l$. Ali opet je reč (podgrupe $\mathbf{D}_\beta$) $u_1 \dots u_k v_l^{-1} \dots v_1^{-1}$ jedinični element, kontradikcija.□



**Stav 4** $\mathbf{D}_\beta \cap \overline{\mathbf{A}}_\beta = \mathbf{E}$.

**Dokaz**. Ako je $\overline{\mathbf{A}}_\beta$ nejedinična grupa, onda, prema samoj konstrukciji, sadrži nejedinični element $v = g_\beta^{-1} a g_\beta$ (podgrupe $\mathbf{H}$) koji nije u $\mathbf{D}_\beta$. Pretpostavimo $e \neq w = g_\beta^{-1} b g_\beta \in D_\beta \cap \overline{A}_\beta$. Prema prethodnom stavu je

$$w = u_n^{-1} \dots u_1^{-1} u_0 u_1 \dots u_n,$$

gde je $u_0 \in \overline{A}_\alpha$ za neko $\alpha < \beta$. Jedina razlika među elementima $v$ i $w$ je u njihovim sredinama – to su različiti elementi neke podgrupe $\mathbf{A}_{i_\beta}$. Kako je $u_0 = g_\alpha^{-1} c g_\alpha = u_1 \dots u_n w u_n^{-1} \dots u_1^{-1} = (g_\beta u_n^{-1} \dots u_1^{-1})^{-1} b g_\beta u_n^{-1} \dots u_1^{-1}$, element $b$ je (a onda i $a$) iz podgrupe $\mathbf{A}_{i_\alpha}$ kojoj pripada $c$, dakle $\mathbf{A}_{i_\alpha} = \mathbf{A}_{i_\beta}$. Ali tada je i $u_1 \dots u_n v u_n^{-1} \dots u_1^{-1} \in \overline{A}_\alpha$ ($\subseteq D_\beta$), pa $v \in D_\beta$ (jer $u_1, \dots, u_n \in D_\beta$), kontradikcija.□

Prelazimo sada na dokaz leme za podgrupu $\mathbf{D}_{\beta+1}$. U cilju bolje preglednosti generatorni elementi podgrupa $\mathbf{D}_\beta$ i $\mathbf{C}_\beta$ će biti, respektivno, $u_1, u_2, \dots$, odnosno $v_1, v_2, \dots$, a proste reči $u', u'', \dots$, odnosno $v', v'', \dots$, ali i $u^{(1)}, u^{(2)}, \dots$, tj. $v^{(1)}, v^{(2)}, \dots$. Prema samoj konstrukciji podgrupe $\mathbf{C}_\beta$ i definiciji proste reči imamo direktno: $l(u') \leq l_\beta = l(v')$. Dalje izvodimo

**Stav 5** *Ako je $l(u') < l(v')$, onda među rečima $u'$ i $v'$ ne može postojati veza treće vrste.*

**Dokaz 5**. Pretpostavimo suprotno; neka je u proizvodu $u'v' = u'(v_1 \dots v_k)$ veza među faktorima $u'$ i $v'$ treće vrste. Inače je, prema dokazu leme 26.2, $k \leq 3$. No tada je već veza između $u'$ i $v_1$ treće vrste. To je vrlo očigledno ako je $k = 1$, u ostalim slučajevima bi veza prve ili druge vrste značila da desna polovina, sredina (u slučaju neparne dužine) i jedan krajnji segment leve polovine elementa $v_1$ ostaju "netaknuti", a prisetimo se da je desna polovina elementa $v_1$ (uvek) $g_\beta$ i leva polovina elementa $v_2$ (uvek) $g_\beta^{-1}$. Ali ako je veza između $u'$ i $v_1$ treće vrste, tj. $l(u'v_1) < l_\beta$, onda je $u'v_1 \in D_\beta$, pa je i $v_1 \in D_\beta$, što je svakako nemoguće, prema stavu 4 ako je $v_1$ element podgrupe $\overline{\mathbf{A}}_\beta$, prema samoj definiciji elemenata $h_{\beta_\delta}$, $\delta < \sigma_\beta$, ako je $v_1 = h_{\beta_\delta}^k$, $k \in \{1, -1\}$.□

**Stav 6** *Neka je $\alpha < \beta$ i $h \in H$. Ako je leva polovina elementa $h$ jednaka levoj polovini nekog od elemenata $h_{\alpha_\delta}$, dok je sredina elementa $h$ (u slučaju neparne dužine) element podgrupe $\mathbf{A}_{i_\alpha}$, tada je $h$ element podgrupe $\mathbf{D}_{\alpha+1}$, znači i podgrupe $\mathbf{D}_\beta$.*

**Dokaz**. Jasno, $l(h^{-1} h_{\alpha_\delta}) \leq l_\alpha$. Ako je baš stroga nejednakost u pitanju, onda je $h^{-1} h_{\alpha_\delta} \in D_\alpha$, a $h \in \langle D_\alpha, h_{\alpha_\delta} \rangle \subseteq D_{\alpha+1}$. Ako važi jednakost, tada je $g_\alpha$ desna polovina elementa $h^{-1} h_{\alpha_\delta}$, dok je sredina ovog elementa (za neparnu dužinu) iz podgrupe $\mathbf{A}_{i_\alpha}$. No prema konstrukciji $\mathbf{D}_{\alpha+1}$ sadrži sve takve elemente i opet je $h \in D_{\alpha+1}$.□

**Stav 7** *Ako je $l(u') = l(v') (= l_\beta)$, onda je veza među prostim rečima $u'$ i $v'$ u proizvodima $u'v'$ i $v'u'$ prve vrste.*

**Dokaz**. Posmatrajmo proizvod $u'v'$. Neka je $u' = u_1 \dots u_k$, $v' = v_1 \dots v_m$ ($m \leq 3$) i pretpostavimo da je između faktora $u'$ i $v'$ u datom proizvodu veza druge ili treće vrste. Onda je i veza među prostim rečima $u'$ i $v_1$ druge ili treće vrste; to je jasno ako je $m = 1$, a za $m = 2, 3$, imali bismo, u slučaju veze prve vrste (među $u'$ i $v_1$ u proizvodu $u'v_1$), da desna polovina, sredina (u slučaju neparne dužine) ili jedan krajnji segment leve polovine (u slučaju parne dužine) generatora $v_1$ ostaju zasigurno "čitavi", no tada bi veza između $u'$ i $v'$ bila prve vrste (imamo u vidu i da je $l(u') = l(v')$). Pretpostavimo da je $l(u') = l(u_j)$ za neko $j < k$, dok je, za $j < r \leq k$, $l(u_r) < l(u')$. Tada je u proizvodu $u_{j+1} \dots u_k v_1$ veza među prostim faktorima $u_{j+1} \dots u_k$ (videti stav 1) i $v_1$ druge vrste. Jer, stav 5 isključuje vezu treće vrste, dok bi veza prve vrste implicirala i vezu prve vrste između $u'$ i $v_1$. Dalje, prema stavu 2 (i stavu 1), desna polovina proste reči $u_1 \dots u_j$ jednaka je desnoj polovini generatora $u_j$, dok su sredine ovih reči (u slučaju neparne dužine) elementi istog slobodnog faktora. Veza među prostim rečima $u_1 \dots u_j$ i $u_{j+1} \dots u_k v_1$ je druge ili treće vrste, pa je leva polovina reči $u_{j+1} \dots u_k v_1$ inverzna desnoj polovini reči $u_1 \dots u_j$, dok im sredine pripadaju istom slobodnom faktoru (i eventualno su takođe inverzne jedna drugoj). Odatle sledi: ako je $u_j \in \overline{A}_\alpha$ ili $u_j = h_{\alpha_\delta}$ za neko $\alpha < \beta$ i $\delta < \sigma_\alpha$, dakle $u_j = g_1 a g_\alpha$, gde je $g_1$ leva polovina i $a \in A_{i_\alpha}$, onda je $u_{j+1} \dots u_k v_1 = g_\alpha^{-1} b g_2$, $b \in A_{i_\alpha}$, te je stoga $u_{j+1} \dots u_k v_1 \in C_{\alpha+1}$; ako je $u_j = h_{\alpha_\delta}^{-1}$, prema stavu 6 je ponovo $u_{j+1} \dots u_k v_1 \in C_{\alpha+1}$. Ali tada je i $v_1 \in C_{\alpha+1}$ ($\subseteq D_\beta$), kontradikcija.□

**Stav 8** *Neka je $l(u') < l_\beta$ i neka je u proizvodima $v'u'$ i $u'v''$ veza među prostim faktorima druge vrste ($l(v'u') = l_\beta = l(u'v'')$). Tada je veza među faktorima $v'u'$ i $v''$ prve vrste.*

**Dokaz**. Neka je $v' = v_{11} \dots v_{1k}$, $v'' = v_{21} \dots v_{2m}$. Ako bi među faktorima $v'u'$ i $v''$ postojala veza druge ili treće vrste, onda bi i među faktorima $v_{1k}u'$ i $v_{21}$ (kao i između $v_{1k}$ i $u'v_{21}$) postojala veza druge ili treće vrste. No ovo je, pokazaćemo, nemoguće.

Pretpostavimo prvo da je $g_\beta$ desna polovina generatora $v_{1k}$ (u tom je slučaju $k \in \{1, 2\}$ – videti dokaz leme 26.2), dok je $g_\beta^{-1}$ leva polovina generatora $v_{21}$ (sada je $m \in \{1, 2\}$). Prost račun pokazuje da se u tom slučaju pri množenju $v_{1k}u'$ sa $v_{21}$ ne bi potpuno "skratilo" $u'$.

Neka je, dalje, desna polovina generatora $v_{1k}$ različita od $g_\beta$ (onda je njegova leva polovina, obavezno, $g_\beta^{-1}$ – $v_{1k}$ je neko $h_{\beta_\delta}^{-1}$), dok je $g_\beta^{-1}$ leva polovina generatora $v_{21}$. Kako je, prema hipotezi, veza između $v_{1k}u'$ i $v_{21}$ druge ili treće vrste, mora $g_\beta$ biti desna polovina reči $v_{1k}u'$, pa je $v_{1k}u' \in \overline{A}_\beta$, a onda je $v_{1k} = h_{\beta_\delta}^{-1} \in \langle \overline{A}_\beta, D_\beta \rangle$, protivurečnost. Analogno rezonujemo i u slučaju: desna polovina generatora $v_{1k}$ je $g_\beta$, leva polovina generatora $v_{21}$ nije $g_\beta^{-1}$.

Preostaje: desna polovina generatora $v_{1k}$ nije $g_\beta$ (dakle, leva polovina je $g_\beta^{-1}$), leva polovina generatora $v_{21}$ nije $g_\beta^{-1}$ (dakle, desna polovina je $g_\beta$); ukratko, za neke ordinale $\gamma, \delta < \sigma_\beta$ je: $v_{1k} = h_{\beta_\gamma}^{-1}$, $v_{21} = h_{\beta_\delta}$. S obzirom na



$l(v'u'v'') \leq l_\beta$, proizvod $v'u'v''$ je ili transform ili jedinični element. Prema tome: $v_{1k}u'v_{21} \in \overline{A}_\beta$. Ali $v_{1k} \neq v_{21}, v_{21}^{-1}$ (jer, jasno, zbog $v_{1k}u'v_{21} \in \overline{A}_\beta$, za $v_{1k} = v_{21}^{-1}$ i $l(u')$ parno, dobili bismo da su leva i desna polovina reči $u'$ uzajamno inverzne, a za neparnu dužinu reči $u'$, bio bi konjugat njene sredine jedinični element, pa bi i sama sredina bila jedinični element – $u'$ mora u proizvodu da "nestane"), a s druge strane, ako je, recimo, $\gamma < \delta$, onda je $v_{21} = h_{\beta_\delta} \in \langle D_\beta, \overline{A}_\beta, h_{\beta_\gamma} (= v_{1k}^{-1}) \rangle$, kontradikcija.□

Konačno smo u stanju da kompletiramo dokaz leme. Tvrdimo konkretno:

*svaka reč podgrupe $\mathbf{D}_{\beta+1}$ je proizvod prostih reči jednog od oblika: $u'$, $v'$, $u'v'$, $v'u'$, $u'v'u''$, gde je veza među prostim faktorima prve vrste.*

Očigledno, prema induktivnoj hipotezi za $\mathbf{D}_\beta$ i pokazanom za $\mathbf{C}_\beta$ (lema 26.2), svaka reč iz $\mathbf{D}_{\beta+1}$ se može predstaviti kao proizvod prostih reči podgrupa $\mathbf{D}_\beta$ i $\mathbf{C}_\beta$, gde je među prostim rečima iste podgrupe veza prve vrste. Ako su $u'$ i $v'$ u tom proizvodu susedne reči i ako je $l(u') = l(v')$, onda je veza među njima (u proizvodima $u'v'$, $v'u'$) prve vrste (stav 7). Ako je $l(u') < l(v')$ i ako je veza među tim prostim faktorima u proizvodima $u'v'$, $v'u'$ druge vrste (treće ne može biti prema stavu 5), onda jednostavno te reči uzimamo kao proste reči (podgrupe $\mathbf{D}_{\beta+1}$) (naravno, ako je $l(u'v'), l(v'u') > l_\beta$, problema nema). Ako je pak $l(u') < l_\beta$ i ako je veza među $v'$ i $u'$, kao i $u'$ i $v''$, druge vrste, onda je prema poslednjem stavu veza među rečima $v'u'$ i $v''$ prve vrste. Naravno, ako je, recimo, među rečima $v'$ i $u'$ veza druge vrste, a među rečima $u'$ i $v''$ prve vrste, ponovo je među rečima $v'u'$ i $v''$ veza prve vrste.□.

**Korolar 26.4** *Podgrupa $\mathbf{D}_\beta$ je slobodni proizvod nejediničnih podgrupa $\overline{\mathbf{A}}_\alpha$ i beskonačnih cikličnih grupa $\langle h_{\alpha_\delta} \rangle$, $\delta < \sigma_\alpha$, $\alpha < \beta$.*

Sumiramo. Neka je, za neki ordinal $\alpha$, $\mathbf{H} = \mathbf{D}_\alpha$. Prema lemi 26.4 (tj. lemi 26.3), $\mathbf{H}$ je slobodni proizvod svih podgrupa $\overline{\mathbf{A}}_\beta$, $\beta < \alpha$, koje su, opet, konjugati podgrupa slobodnih faktora grupe $\mathbf{G}$ (setimo se, po definiciji je $\overline{\mathbf{A}}_\beta = \mathbf{H} \cap g_\beta^{-1} \mathbf{A}_{i_\beta} g_\beta$), i beskonačnih cikličnih grupa $\langle h_{\alpha_\delta} \rangle$, $\delta < \sigma_\alpha$.■

**Korolar 26.5** *(Teorema Nielsen-Schreiera – po drugi put). Podgrupa slobodne grupe je slobodna grupa.*

**Korolar 26.6** *Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G} = \prod_{i \in I}^* \mathbf{A}_i$ i neka je, za $g \in G$ i $i \in I$, $\mathbf{H} \cap g^{-1} \mathbf{A}_i g = \mathbf{K}$ nejedinična podgrupa. Tada u dekompoziciji podgrupe $\mathbf{H}$ dobijenoj prema prethodnoj teoremi postoji slobodni faktor koji je konjugovan sa $\mathbf{K}$ u $\mathbf{H}$.*

**Dokaz**. Neka je $e \neq b = g^{-1} a g \in K$, $a \in A_i$. Prema stavu 3, $b$ je konjugat u $\mathbf{H}$ nekom elementu neke od podgrupa $\overline{\mathbf{A}}_\alpha$, tj. postoji $h \in H$ takvo da je $b \in h^{-1} \overline{A}_\alpha h$. Odatle dalje izvodimo, držeći se notacije iz dokaza teoreme,

$h^{-1}\overline{A}_\alpha h \subseteq (g_\alpha h)^{-1} A_{i_\alpha} g_\alpha h$, pa je $a \in (g_\alpha h g^{-1})^{-1} A_{i_\alpha} g_\alpha h g^{-1}$. Stoga je $i = i_\alpha$, $c = g_\alpha h g^{-1} \in A_{i_\alpha}$ i $g = c^{-1} g_\alpha h$. Konačno:

$$\mathbf{K} = \mathbf{H} \cap g^{-1}\mathbf{A}_{i_\alpha} g = \mathbf{H} \cap (c^{-1}g_\alpha h)^{-1}\mathbf{A}_{i_\alpha}(c^{-1}g_\alpha h) =$$

$$h^{-1}(\mathbf{H} \cap g_\alpha^{-1}(c\mathbf{A}_{i_\alpha}c^{-1})g_\alpha)h = h^{-1}(\mathbf{H} \cap g_\alpha^{-1}\mathbf{A}_{i_\alpha}g_\alpha)h = h^{-1}\overline{\mathbf{A}}_\alpha h.\square$$

**Definicija 26.7** *Dve slobodne dekompozicije grupe* $\mathbf{G}$, $\mathbf{F}_1 * \prod^*_{i\in I}\mathbf{A}_i$ *i* $\mathbf{F}_2 * \prod^*_{j\in J}\mathbf{B}_j$, *gde su* $\mathbf{F}_1$, $\mathbf{F}_2$ *slobodne grupe, izomorfne su akko su* $\mathbf{F}_1$ *i* $\mathbf{F}_2$ *izomorfne grupe i ako među skupovima slobodnih faktora* $\{\mathbf{A}_i \mid i \in I\}$ *i* $\{\mathbf{B}_j \mid j \in J\}$ *postoji uzajamno jednoznačna korespondencija takva da su korespondentni faktori konjugovani u* $\mathbf{G}$.

**Korolar 26.8** *Svake dve slobodne dekompozicije grupe* $\mathbf{G}$ *imaju izomorfna proširenja.*

**Dokaz.** Neka su (1) $\prod^*_{i\in I}\mathbf{A}_i$ i (2) $\prod^*_{j\in J}\mathbf{B}_j$ dve slobodne dekompozicije grupe $\mathbf{G}$. Za svako $i \in I$ i svako $j \in J$ neka su $\mathbf{F}_i * \prod^*_{k\in K_i}\mathbf{A}_{i_k}$ i $\mathbf{F}_j * \prod^*_{m\in M_j}\mathbf{B}_{j_m}$ slobodne dekompozicije podgrupa $\mathbf{A}_i$ i $\mathbf{B}_j$ s obzirom na, respektivno, dekompozicije (2) i (1), dobijene prema "instrukcijama" prethodne teoreme. Tvrdimo: $\prod^*_{i\in I}\mathbf{F}_i * \prod^*_{i\in I}(\prod^*_{k\in K_i}\mathbf{A}_{i_k})$ i $\prod^*_{j\in J}\mathbf{F}_j * \prod^*_{j\in J}(\prod^*_{m\in M_j}\mathbf{B}_{j_m})$ su izomorfne dekompozicije grupe $\mathbf{G}$. Neka je, za $m \in M_j$, $\mathbf{B}_{j_m} = \mathbf{B}_j \cap g^{-1}\mathbf{A}_i g$. Onda je, prema prethodnom korolaru, konjugat podgrupe $\mathbf{B}_{j_m}$, $g\mathbf{B}_{j_m}g^{-1} = g\mathbf{B}_j g^{-1} \cap \mathbf{A}_i$ konjugovan (u $\mathbf{A}_i$) sa nekom od podgrupa $\mathbf{A}_{i_k}$, zapravo sa tačno jednom (očigledno, ni u jednoj slobodnoj dekompoziciji ne mogu dva različita slobodna faktora biti konjugovana); obeležimo tu podgrupu sa $\mathbf{A}_{i_{j_m}}$. Analogno, svaki faktor $\mathbf{A}_{i_k}$ je konjugovan sa tačno jednim slobodnim faktorom – $\mathbf{B}_{j_{i_k}}$. Normalna zatvorenja podgrupa $\prod^*_{i\in I}(\prod^*_{k\in K_i}\mathbf{A}_{i_k})$ i $\prod^*_{j\in J}(\prod^*_{m\in M_j}\mathbf{B}_{j_m})$ se, dakle, podudaraju, neka je to (normalna) podgrupa $\mathbf{N}$, a prema 25.7($b$) važi: $\prod^*_{i\in I}\mathbf{F}_i \cong \mathbf{G}/\mathbf{N} \cong \prod^*_{j\in J}\mathbf{F}_j.\square$

**Korolar 26.9** *Ako grupa* $\mathbf{G}$ *ima slobodnu dekompoziciju sa nerazložívim faktorima (nerazložívim u smislu da se ne mogu predstaviti kao netrivijalni slobodni proizvod), tada su svake dve takve dekompozicije grupe* $\mathbf{G}$ *izomorfne i svaka slobodna dekompozicija se može proširiti do dekompozicije sa nerazložívim faktorima.*

**Lema 26.10** *Nijedna grupa nije razloživa i u direktni i u slobodni proizvod.*

**Dokaz.** Pretpostavimo da je $\mathbf{G} = \mathbf{A} * \mathbf{B} = \mathbf{C} \times \mathbf{D}$, gde su $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ i $\mathbf{D}$ nejedinične podgrupe. Ako bi $\mathbf{A} \cap \mathbf{C}$ bila nejedinična podgrupa, onda bi, pošto nijedan nejedinični element iz $\mathbf{A}$ nije permutabilan ni sa jednim nejediničnim elementom koji nije u $\mathbf{A}$, dok su elementi podgrupa $\mathbf{C}$ i $\mathbf{D}$ uzajamno permutabilni, sledilo $\mathbf{D} \leq \mathbf{A}$, pa dakle i $\mathbf{C} \leq \mathbf{A}$, stoga i $\mathbf{A} = \mathbf{G}$, kontradikcija.



Prema tome je $\mathbf{A} \cap \mathbf{C} = \mathbf{A} \cap \mathbf{D} = \mathbf{B} \cap \mathbf{C} = \mathbf{B} \cap \mathbf{D} = \mathbf{E}$. No kako su $\mathbf{C}$ i $\mathbf{D}$ normalne podgrupe, to je i $g^{-1}\mathbf{A}g \cap \mathbf{C} = g^{-1}\mathbf{A}g \cap \mathbf{D} = g^{-1}\mathbf{B}g \cap \mathbf{C} = g^{-1}\mathbf{B}g \cap \mathbf{D} = \mathbf{E}$ za svako $g \in G$, te su prema Kuroševoj teoremi o podgrupama slobodnog proizvoda $\mathbf{C}$ i $\mathbf{D}$ slobodne grupe. Dalje, zbog $\mathbf{A} \cap \mathbf{D} = \mathbf{E}$, podgrupa $\mathbf{A}$ je izomorfna sa svojom komponentom u (pod)grupi $\mathbf{C}$ (ako je, za $x, y \in A$, $x = c_x d_x$, $y = c_y d_y$, gde $c_x, c_y \in C$, $d_x, d_y \in D$ i $c_x = c_y$, tada je $xy^{-1} = d_x d_y^{-1} \in A \cap D = \{e\}$ i $x = y$). Prema 23.19, $\mathbf{A}$ je slobodna grupa, po simetriji stvari je i $\mathbf{B}$ slobodna grupa, a onda je i sama grupa $\mathbf{G}$ slobodna. Ali $\mathbf{C}$ i $\mathbf{D}$ sadrže beskonačne ciklične grupe, recimo $\langle c\rangle$ i $\langle d\rangle$, čiji je direktan proizvod slobodna grupa, kontradikcija ($\langle c\rangle \times \langle d\rangle$ je Abelova neciklična grupa).$\square$

Naredni rezultat nam kaže da u opštem Sylowe $p$-podgrupe beskonačne grupe ne moraju biti konjugovane.

**Lema 26.11** *Ako su* $\mathbf{P}_1$ *i* $\mathbf{P}_2$ *(ma kakve dve) p-grupe i* $\mathbf{G} = \mathbf{P}_1 * \mathbf{P}_2$, *onda su* $\mathbf{P}_1$ *i* $\mathbf{P}_2$ *Sylowe p-podgrupe grupe* $\mathbf{G}$.

**Dokaz.** Pretpostavimo da je podgrupa $\mathbf{P}_1$ strogo sadržana u Sylowoj $p$-podgrupi $\mathbf{P}$ grupe $\mathbf{G}$. Grupa $\mathbf{P}$ nije razloživa u slobodni proizvod nejediničnih podgrupa (u suprotnom bi imala elemente beskonačnog reda – 25.9($a$)), te je, prema Kuroševoj teoremi, konjugovana podgrupi neke od grupa $\mathbf{P}_1$, $\mathbf{P}_2$. No evidentno $\mathbf{P}_2$ ne dolazi u obzir, pa je, za neko $g \in G$, $\mathbf{P} = g^{-1}\mathbf{P}_0 g$, gde je $\mathbf{P}_0 \leq \mathbf{P}_1$. Ali onda, pošto je $\mathbf{P}$ Sylowa $p$-podgrupa, iz $\mathbf{P} \leq g^{-1}\mathbf{P}_1 g$ ($\leq g^{-1}\mathbf{P}g$) sledi $\mathbf{P} = g^{-1}\mathbf{P}g = g^{-1}\mathbf{P}_0 g$, dakle i $\mathbf{P} = \mathbf{P}_0$ ($\leq \mathbf{P}_1$), kontradikcija.$\square$

## 27 Generalni slobodni proizvodi

Slobodni proizvodi su specijalan slučaj tzv. generalnih slobodnih proizvoda koji se još zovu i slobodni proizvodi sa amalgamiranom podgrupom (u slučaju "običnih" slobodnih proizvoda amalgamirana podgrupa je jedinična).

**Definicija 27.1** *Neka su dati familija grupa* $\mathcal{G} = \{\mathbf{G}_i \mid i \in I\}$ *i grupa* $\mathbf{H}$ *koja se utapa u svaku grupu familije* $\mathcal{G}$ *i neka je* $\{\psi_i \mid \psi_i : H \longrightarrow G_i, i \in I\}$ *familija utapanja grupe* $\mathbf{H}$ *u grupe familije* $\mathcal{G}$. *Faktor grupa grupe* $\mathbf{G} = \prod^*_{i\in I}\mathbf{G}_i$ *po normalnoj podgrupi* $\mathbf{N}$ *generisanoj skupom* $\{((h)\psi_i)^{-1}\cdot(h)\psi_j \mid h \in H, i, j \in I\}$ *zove se slobodni proizvod familije grupa* $\mathcal{G}$ *sa amalgamiranom podgrupom* $\mathbf{H}$.

Prema 21.11 i 25.2, sa notacijom preuzetom iz definicije, imamo: ako je, za $i \in I$, $(A_i; P_i)$ prezentacija grupe $\mathbf{G}_i$, recimo multiplikativnom tablicom, i $\varphi_i$ bijektivno preslikavanje skupa $A_i$ na skup $G_i$ (videti 21.5($b$)), gde je još $A_i \cap A_j = \emptyset$ za različite indekse $i, j$ iz $I$, onda je $(\bigcup_{i\in I}A_i; \bigcup_{i\in I}P_i \cup \{((a_i)\varphi_i)^{-1}(a_j)\varphi_j \mid \exists h \in H\,((a_i)\varphi_i = (h)\psi_i \wedge (a_j)\varphi_j = (h)\psi_j), a_i \in A_i, a_j \in A_j\})$ prezentacija slobodnog proizvoda familije grupa $\{\mathbf{G}_i \mid i \in I\}$ sa amalgamiranom podgrupom $\mathbf{H}$. Očigledno je isto tako da je, za svako $i, j \in I$,

$(\mathbf{H})\psi_i\mathbf{N} = (\mathbf{H})\psi_j\mathbf{N}$, pa je onda i $((\mathbf{H})\psi_i\mathbf{N})/\mathbf{N} = ((\mathbf{H})\psi_j\mathbf{N})/\mathbf{N}$ (primetimo samo: $(h)\psi_i = (h)\psi_j \cdot (((h)\psi_j)^{-1}(h)\psi_i)$).

Naredna lema nam daje uvid u strukturu slobodnih proizvoda sa amalgamiranom podgrupom (pratimo manje-više doslovno [92] i [140]).

Fiksirajmo za svaku podgrupu $(\mathbf{H})\psi_i = \mathbf{H}_i$ grupe $\mathbf{G}_i$ desnu transverzalu tako da je 1 predstavnik koseta $H_i$ (radimo u okviru grupe $\prod^*_{i\in I}\mathbf{G}_i$ - videti napomenu uz definiciju 25.1), a $\overline{g_i}$ predstavnik koseta $H_ig_i$. Prema tome, za svako $g_i \in G_i$ postoji jedinstveno $h \in H$ takvo da je $g_i = (h)\psi_i\overline{g_i}$. Neka je $u_1 \dots u_n$ normalna forma elementa $g$ slobodnog proizvoda $\mathbf{G} = \prod^*_{i\in I}\mathbf{G}_i$, gde je $u_j \in G_{i_j}$, $j = 1, \dots, n$. Definišimo redom elemente $g_j$, gde se $j$ "spušta" od $n$ do 1, na sledeći način:

$g_n = u_n$. Ako je $g_n = (h_n)\psi_{i_n}\overline{g_n}$, tada je, zbog $N(h_n)\psi_{i_n} = N(h_n)\psi_{i_{n-1}}$:

$$Ng = Nu_1 \dots Nu_{n-1}\,Nu_n = Nu_1 \dots N(u_{n-1}(h_n)\psi_{i_{n-1}})\,N\overline{g_n}.$$

Stavljamo: $g_{n-1} = u_{n-1}(h_n)\psi_{i_{n-1}}$ i ako je $g_{n-1} = (h_{n-1})\psi_{i_{n-1}}\overline{g_{n-1}}$ za $h_{n-1} \in H$, izvodimo:

$$Ng = Nu_1 \dots Nu_{n-2}(h_{n-1})\psi_{i_{n-2}}\,N\overline{g_{n-1}}\,N\overline{g_n},$$

a $g_{n-2}$ će biti, naravno, $u_{n-2}\cdot(h_{n-1})\psi_{i_{n-2}}$. Evidentno, posle ukupno $n$ koraka dobićemo

$$Ng = N(h_1)\psi_{i_1}\overline{g_1}\dots\overline{g_n}.$$

Odatle i

**Definicija 27.2** *Normalna forma elementa $g$ slobodnog proizvoda familije grupa $\{\mathbf{G}_i \mid i \in I\}$, s obzirom na slobodni proizvod te familije sa amalgamiranom grupom $\mathbf{H}$, za data utapanja $\psi_i$ ($i \in I$) grupe $\mathbf{H}$ u grupe $\mathbf{G}_i$ i date desne transverzale podgrupa $(\mathbf{H})\psi_i = \mathbf{H}_i$ grupa $\mathbf{G}_i$ koje ispunjavaju navedene uslove, formalni je izraz $h\overline{g_1}\dots\overline{g_m}$, gde je $m \geq 0$, $h \in H$, $g_j \in G_{i_j}$, $\overline{g_j} \neq 1$, $i_{j-1} \neq i_j$ za $j = 2, \dots, m$, i $Ng = N(h)\psi_{i_1}\overline{g_1}\dots\overline{g_m}$.*

**Napomena**. Isti izraz *normalna forma* (datog elementa $g$ slobodnog proizvoda $\mathbf{G} = \prod^*_{i\in I}\mathbf{G}_i$) koristi se u dve definicije - prethodnoj i 25.1. No prethodna je samo uopštenje definicije 25.1 i u osnovi se svodi na nju kada je, kako smo već rekli, amalgamirana podgrupa jedinična.

**Lema 27.3** *Svakom elementu proizvoda $\mathbf{G} = \prod^*_{i\in I}\mathbf{G}_i$ odgovara, s obzirom na data utapanja $\psi_i$ grupe $\mathbf{H}$ u grupe $\mathbf{G}_i$, $i \in I$, i "podesno" izabrane desne transverzale podgrupa $(\mathbf{H})\psi_i = \mathbf{H}_i$ grupa $\mathbf{G}_i$, jedinstvena normalna forma (s obzirom na slobodni proizvod sa amalgamiranom podgrupom).*

**Dokaz**. Ideja (kao i cela metoda) dokaza nije nova. Već smo je koristili u paragrafu 24; uostalom, kako se kaže, ista meta, isto odstojanje - sada su u pitanju generalni slobodni proizvodi.



Neka je $M$ skup svih normalnih formi svih elemenata iz $\mathbf{G}$. Prema konstrukciji koja je prethodila definiciji normalne forme, svakom elementu odgovara bar jedna. Dokaz ovoga je još brži i jednostavniji ako koristimo indukciju po dužini normalne forme elementa u slobodnom proizvodu $\mathbf{G}$. Neka je, za $i \in I$, preslikavanje $\theta_i : G_i \longrightarrow S_M$ dato sa, za $a \in G_i$: $(a)\theta_i = \widehat{a}$, gde je $(h\overline{g_1}\dots\overline{g_m})\widehat{a} \stackrel{\text{def}}{=}$ normalna forma elementa $(h)\psi_{i_1}\overline{g_1}\dots\overline{g_m}\cdot a$, dobijena prema opisanom postupku (jasno, $\widehat{1} = \imath_M$). Dokazujemo prvo: $\widehat{a\cdot b} = \widehat{a}\circ\widehat{b}$. Pretpostavljamo da je u normalnoj formi $h\overline{g_1}\dots\overline{g_m}$, kao i ranije, $\overline{g_j}$ iz $\mathbf{G}_{i_j}$. Neka je $i_m \neq i$. Tada imamo:

$$(h\overline{g_1}\dots\overline{g_m})\widehat{a} = (hh_1)\overline{g_1\,(h_2)\psi_{i_1}}\dots\overline{g_m\,(h_{m+1})\psi_{i_m}}\cdot\overline{a} \qquad (*),$$

odnosno, ako je $a \in (H)\psi_i$:

$$(h\overline{g_1}\dots\overline{g_m})\widehat{a} = (hh_1)\overline{g_1\,(h_2)\psi_{i_1}}\dots\overline{g_m\,(h_{m+1})\psi_{i_m}},$$

gde je $a = (h_{m+1})\psi_i\overline{a}$ i, za $j$, $1 \leq j \leq m$, $\overline{g_j}(h_{j+1})\psi_{i_j} = (h_j)\psi_{i_j}\overline{g_j\,(h_{j+1})\psi_{i_j}}$, $h_j \in H$ (naravno, $N(\overline{g_j}(h_{j+1})\psi_{i_j}) = N\overline{g_j\,(h_{j+1})\psi_{i_j}}$). Prema $(*)$ sledi (s dozvolom da $\overline{a}$ možda i nemamo):

$$(h\overline{g_1}\dots\overline{g_m})(\widehat{a}\circ\widehat{b}) = (hh_1k_1)\overline{g_1\,(h_2k_2)\psi_{i_1}}\dots\overline{g_m\,(h_{m+1}k_{m+1})\psi_{i_m}}\;\overline{ab},$$

gde je sada: $\overline{ab} = (k_{m+1})\psi_i\overline{ab}$ i, za $1 \leq j \leq m$, $\overline{g_j\,(h_{j+1})\psi_{i_j}}\,(k_{j+1})\psi_{i_j} = (k_j)\psi_{i_j}\overline{g_j\,(h_{j+1}k_{j+1})\psi_{i_j}}$, $k_j \in H$. S druge strane je:

$$(h\overline{g_1}\dots\overline{g_m})\widehat{ab} = (hl_1)\overline{g_1\,(l_2)\psi_{i_1}}\dots\overline{g_m\,(l_{m+1})\psi_{i_m}}\;\overline{ab};$$

ovog puta je $ab = (l_{m+1})\psi_i\,\overline{ab}$ i, za $j < m+1$, $\overline{g_j}(l_{j+1})\psi_{i_j} = (l_j)\psi_{i_j}\overline{g_j\,(l_{j+1})\psi_{i_j}}$. Iz $a = (h_{m+1})\psi_i\overline{a}$, tj. $a\overline{a}^{-1} = (h_{m+1})\psi_i$ i $\overline{ab} = (k_{m+1})\psi_i\overline{ab}$ sledi: $(a\overline{a}^{-1})(\overline{ab}) = ab = (h_{m+1}k_{m+1})\psi_i\overline{ab}$, pa je $h_{m+1}k_{m+1} = l_{m+1}$. Isto tako je, prema izvedenim jednakostima, za $j < m+1$:

$$\overline{g_j}(h_{j+1}k_{j+1})\psi_{i_j} = (\overline{g_j}(h_{j+1})\psi_{i_j})(k_{j+1})\psi_{i_j} = (h_j)\psi_{i_j}\overline{g_j\,(h_{j+1})\psi_{i_j}}(k_{j+1})\psi_{i_j} =$$

$$(h_j)\psi_{i_j}((k_j)\psi_{i_j}\overline{g_j\,(h_{j+1}k_{j+1})\psi_{i_j}}) = (h_jk_j)\psi_{i_j}\overline{g_j\,(h_{j+1}k_{j+1})\psi_{i_j}}.$$

Proizilazi: $h_jk_j = l_j$ za $j < m+1$. Provera je indukcijom po $k$, gde krećemo od $m+1-k$. Tako je npr. za $k = 1$:

$$(h_mk_m)\psi_{i_m}\overline{g_m\,(h_{m+1}k_{m+1})\psi_{i_m}} = (h_m)\psi_{i_m}\overline{g_m(h_{m+1})\psi_{i_m}}(k_{m+1})\psi_{i_m} =$$

$$\overline{g_m}(h_{m+1}k_{m+1})\psi_{i_m} = \overline{g_m}(l_{m+1})\psi_{i_m} = (l_m)\psi_{i_m}\overline{g_m\,(l_{m+1})\psi_{i_m}} =$$

$$(l_m)\psi_{i_m}\overline{g_m\,(h_{m+1}k_{m+1})\psi_{i_m}},$$

te je $h_mk_m = l_m$. Zaključujemo: za svaku normalnu formu $h\overline{g_1}\dots\overline{g_m}$, gde je $i_m \neq i$, važi: $(h\overline{g_1}\dots\overline{g_m})(\widehat{a}\circ\widehat{b}) = (h\overline{g_1}\dots\overline{g_m})\widehat{ab}$. Analogno bi se tretirao i slučaj $i_m = i$. Znači, $\theta_i$ je homomorfno preslikavanje grupe $\mathbf{G}_i$ u grupu $\mathbf{S}_M$.

Prema 25.5 postoji homomorfno preslikavanje $\theta$ grupe $\mathbf{G} = \prod^*_{i\in I}\mathbf{G}_i$ u grupu $\mathbf{S}_M$ takvo da je, za svako $i \in I$, $\theta|_{G_i} = \theta_i$. Kako je, za svako $h \in H$ i svako $i, j \in I$, $(h)(\psi_i \circ \theta_i) = (h)(\psi_j \circ \theta_j)$, jer je $((h)\psi_i)^{-1} \cdot (h)\psi_j \in N$, to je $(((h)\psi_i)^{-1}(h)\psi_j)\theta = (((h)\psi_i)^{-1})\theta_i \circ ((h)\psi_j)\theta_j = ((h)(\psi_i \circ \theta_i))^{-1} \circ (h)(\psi_j \circ \theta_j) = \imath_M$, pa se svi elementi normalne podgrupe $\mathbf{N}$ preslikavaju u jedinični element. Odatle, ako je $h\overline{g_1}\ldots\overline{g_m}$ normalna forma elementa $g$ (s obzirom na slobodni proizvod sa amalgamiranom podgrupom), te dakle i $Ng = N((h)\psi_{i_1}\overline{g_1}\ldots\overline{g_m})$, sledi $(g)\theta = ((h)\psi_{i_1}\overline{g_1}\ldots\overline{g_m})\theta$, i kako $((h)\psi_{i_1}\overline{g_1}\ldots\overline{g_m})\theta$ preslikava normalnu formu 1 u $h\overline{g_1}\ldots\overline{g_m}$, element $g$ ne može imati više različitih normalnih formi.□

**Korolar 27.4** *Neka je $\overline{\mathbf{G}}$ slobodni proizvod familije grupa $\{\mathbf{G}_i \mid i \in I\}$ sa amalgamiranom podgrupom $\mathbf{H}$ za data utapanja $\psi_i$ grupe $\mathbf{H}$ u grupe $\mathbf{G}_i$. Tada $\overline{\mathbf{G}}$ sadrži podgrupu $\overline{\mathbf{H}}$ izomorfnu sa $\mathbf{H}$ i, za svako $i \in I$, podgrupu $\overline{\mathbf{G}}_i$ izomorfnu sa $\mathbf{G}_i$, pri čemu je $\overline{\mathbf{H}}$ podgrupa svake od grupa $\overline{\mathbf{G}}_i$, $\overline{\mathbf{G}}_i \cap \langle \bigcup_{j\in I\setminus\{i\}} \overline{G}_j\rangle = \overline{\mathbf{H}}$ i $\overline{\mathbf{G}} = \langle \bigcup_{i\in I} \overline{G}_i\rangle$.*

**Dokaz.** Neka je, za $i \in I$, $\mathbf{H}_i = (\mathbf{H})\psi_i$ $(\leq \mathbf{G}_i)$ i, za $h \in H$, $(h)\psi_i = h_i$. U grupi $\overline{\mathbf{G}} = (\prod^*_{i\in I}\mathbf{G}_i)/\mathbf{N}$, gde je $\mathbf{N}$ normalna podgrupa grupe $\prod^*_{i\in I}\mathbf{G}_i$ generisana skupom $\{h_i^{-1}h_j \mid h \in H, i, j \in I\}$, neka je $\overline{\mathbf{H}} = (\mathbf{H}_i\mathbf{N})/\mathbf{N}$ $(= (\mathbf{H}_j\mathbf{N})/\mathbf{N})$ i $\overline{\mathbf{G}}_i = (\mathbf{G}_i\mathbf{N})/\mathbf{N}$. Zbog jedinstvenosti normalne forme elemenata u $\prod^*_{i\in I}\mathbf{G}_i$ imamo: $\mathbf{G}_i \cap \mathbf{N} = \mathbf{H}_i \cap \mathbf{N} = \mathbf{E}$, pa je $\overline{\mathbf{G}}_i = (\mathbf{G}_i\mathbf{N})/\mathbf{N} \cong \mathbf{G}_i/(\mathbf{G}_i \cap \mathbf{N}) \cong \mathbf{G}_i$ i, isto tako, $\overline{\mathbf{H}} \cong \mathbf{H}_i$. Jedinstvenost normalne forme elemenata daje odmah i $\mathbf{G}_i\mathbf{N} \cap \langle \bigcup_{j\in I\setminus\{i\}} G_jN\rangle = \mathbf{H}_i\mathbf{N}$ $(= \mathbf{H}_j\mathbf{N})$; relacija $\geq$ je vrlo očigledna, a ako je $ga = g_1\ldots g_mb$, gde je: $a, b \in N$, $g \in G_i$, za $k = 1, \ldots, m$, $g_k \in G_{j_k}$, $j_k \neq i$ i, za $k < m$, $j_k \neq j_{k+1}$, onda je $g^{-1}g_1\ldots g_m = ab^{-1} \in N$ i odatle $g \in H_i$ (imamo u vidu da je podgrupa $\mathbf{N}$ generisana konjugatima elemenata $h_rh_s^{-1}$, $h \in H$, $r, s \in I$). Stoga je i $\overline{\mathbf{G}}_i \cap \langle \bigcup_{j\in I\setminus\{i\}} \overline{G}_j\rangle = \overline{\mathbf{H}}$. Poslednji deo tvrđenja trivijalno važi.□

Prethodni korolar nam dozvoljava da u slobodnom proizvodu sa amalgamiranom podgrupom identifikujemo (za svako $i \in I$) podgrupu $\mathbf{G}_i$ (ponovo videti napomenu uz 25.1) sa $\overline{\mathbf{G}}_i$ i grupu $\mathbf{H}$ sa podgrupom $\overline{\mathbf{H}}$. Prema tome biće, za svaka dva različita indeksa $i, j$, $\mathbf{G}_i \cap \mathbf{G}_j = \mathbf{H}$, a elemente tog generalnog slobodnog proizvoda možemo identifikovati sa njima korespondentnim normalnim formama. Konačno, i sigurno nepotrebno, možemo biti i formalniji. Pretpostavimo, nasleđujući uvedenu notaciju, da je $\{\mathbf{K}_i \mid i \in I\}$ familija grupa koja ispunjava sledeće uslove: $\mathbf{H}$ je podgrupa svake od grupa $\mathbf{K}_i$; za svaka dva različita indeksa $i, j$ iz $I$ je $\mathbf{K}_i \cap \mathbf{K}_j = \mathbf{H}$; za svako $i \in I$ postoji izomorfno preslikavanje $\overline{\psi}_i$ grupe $\mathbf{K}_i$ na grupu $\mathbf{G}_i$ takvo da je $\overline{\psi}_i|_H = \psi_i$ (lema prenosa nam, naravno, garantuje egzistenicju jedne takve familije grupa). Da ne bismo sve još više komplikovali, neka je za grupu $\mathbf{K}_i$, $(K_i; P_i)$ njena prezentacija multiplikativnom tablicom (azbuka nam je baš $K_i \cup K_i^{-1}$, a "potrebno" bijektivno preslikavanje je, jasno, baš identično preslikavanje – 21.6($b$)). Tada je grupa $\mathbf{G}_{(\bigcup_{i\in I}K_i;\bigcup_{i\in I}P_i)}$ izomorfna grupi $\overline{\mathbf{G}}$ $(= \prod^*_{i\in I}\mathbf{G}_i/\mathbf{N})$, tj. $(\bigcup_{i\in I}K_i; \bigcup_{i\in I}P_i)$



je prezentacija grupe $\overline{\mathbf{G}}$ za preslikavanje $\Psi : \bigcup_{i\in I}K_i \longrightarrow \overline{G}$, dato sa, za $a \in K_i$: $(a)\Psi = N(a)\overline{\psi}_i$ (preslikavanje je dobro definisano, jer je, za $h \in H$ i svako $i, j$, $N(h)\overline{\psi}_i = N(h)\overline{\psi}_j$). Zaista, kako je, evidentno, za svaku reč $u$ iz $\bigcup_{i\in I}P_i$, $(u)\overline{\Psi} = N$, preslikavanje $\theta : G_{(\bigcup_{i\in I}K_i;\bigcup_{i\in I}P_i)} \longrightarrow \overline{G}$ dato sa $([u])\theta = (u)\overline{\Psi}$ surjektivni je homomorfizam. U grupi $\mathbf{K}_i$ uzmimo za desnu transverzalu podgrupe $\mathbf{H}$ onu koja korespondira (za izomorfno preslikavanje $\overline{\psi}_i$) izabranoj desnoj transverzali podgrupe $\mathbf{H}_i$ $(= (\mathbf{H})\psi_i)$ u grupi $\mathbf{G}_i$. Na način sličan već demonstriranom, lako je pokazati da je svaka reč $u$ (azbuke $\bigcup_{i\in I}K_i \cup (\bigcup_{i\in I}K_i)^{-1}$) u relaciji $\sim_P$, gde je $P = \bigcup_{i\in I}P_i$, sa rečju oblika $h\overline{a_1}\ldots\overline{a_m}$, gde je $h \in H$, $m \geq 0$, $\overline{a_j} \in K_{i_j}$ (podrazumevamo da elementi $\overline{a_j}$ pripadaju odovarajućim desnim transverzalama), $\overline{a_j} \neq e$ (sve grupe $\mathbf{K}_i$ imaju zajednički jedinični element – $e$) i, za $j = 1, \ldots, m-1$, $i_j \neq i_{j+1}$. Stoga je $([u])\theta = N(h)\psi_{i_1}\overline{g_1}\ldots\overline{g_m}$, gde je, jasno, $\overline{g_j} = (\overline{a_j})\overline{\psi}_{i_j}$. Prema 27.3, odatle sledi da je $\theta$ i injektivno preslikavanje kao i da svakoj reči $u$ odgovara jedinstvena *normalna forma* $h\overline{a_1}\ldots\overline{a_m}$. Možemo stoga umesto grupe $\mathbf{G}_{(\bigcup_{i\in I}K_i;\bigcup_{i\in I}P_i)}$ posmatrati grupu, obeležimo je sa $\mathbf{K}$, čiji je domen skup normalnih formi, a operacija, recimo $\bullet$, je adekvatno definisana: proizvod dve normalne forme $h_1\overline{a_1}\ldots\overline{a_m}$ i $h_2\overline{b_1}\ldots\overline{b_n}$ je normalna forma koja je u relaciji $\sim_P$ sa rečju $h_1\overline{a_1}\ldots\overline{a_m}\cdot h_2\overline{b_1}\ldots\overline{b_n}$. Naravno, to bi dalo, npr. u slučaju da $a_m$ i $b_1$ ne pripadaju istoj grupi $\mathbf{K}_i$:

$$h_1\overline{a_1}\ldots\overline{a_m} \bullet h_2\overline{b_1}\ldots\overline{b_n} = (h_1h_1')\overline{a_1h_2'}\ldots\overline{a_{m-1}h_m'}\,\overline{a_mh_2}\,\overline{b_1}\ldots\overline{b_n},$$

gde je, u grupi $\mathbf{K}_{i_m}$, $\overline{a_m}h_2 = h_m'\overline{a_mh_2}$ i, generalno (u odgovarajućim grupama), $\overline{a_j}h_{j+1}' = h_j'\overline{a_jh_{j+1}'}$. U svakom slučaju je preslikavanje

$$\Phi : G_{(\bigcup_{i\in I}K_i;\bigcup_{i\in I}P_i)} \longrightarrow K$$

dato sa: $([u])\Phi =$ *normalna forma koja je u relaciji $\sim_P$ sa $u$* izomorfno preslikavanje grupe $\mathbf{G}_{(\bigcup_{i\in I}K_i;\bigcup_{i\in I}P_i)}$ na $\langle K, \bullet\rangle$.

U narednoj lemi, koja je uopštenje leme 25.9, slobodni proizvod familije grupa $\{\mathbf{G}_i \mid i \in I\}$ sa amalgamiranom podgrupom $\mathbf{H}$ – neka je to sada $\mathbf{G}$, razmatraćemo u upravo predočenom obliku (podrazumevajući da je desna transverzala podgrupe $\mathbf{H}$ u svakoj od grupa $\mathbf{G}_i$ fiksirana).

**Lema 27.5** ($a$) *Ako je element $g \equiv h\overline{g_1}\ldots\overline{g_m}$ (grupe $\mathbf{G}$) takav da je $m \geq 2$ i $i_1 \neq i_m$ (podsećamo: podrazumevamo $\overline{g_j} \in G_{i_j}$), onda je on beskonačnog reda;*

($b$) *Ako su bar dve grupe $\mathbf{G}_i$ i $\mathbf{G}_j$ različite od $\mathbf{H}$, tada $\mathbf{G}$ ima element beskonačnog reda;*

($c$) *Element konačnog reda grupe $\mathbf{G}$ konjugovan je sa nekim elementom neke od grupa $\mathbf{G}_i$.*

($d$) *Centar grupe $\mathbf{G}$ je $\bigcap_{i\in I}\mathbf{Z}(\mathbf{G}_i)$ $(\leq \mathbf{H})$.*

**Dokaz.** $(a)$ Jasno; element $g^2 \equiv (hh_1)\overline{g_1h_2}\ldots\overline{g_{m-1}h_m}\,\overline{g_mh}\,\overline{g_1}\ldots\overline{g_m}$ je *dužine* $2m$ i, uopšte, element $g^k$ je dužine $km$ (ponavljamo: $\overline{g_m}h = h_m\overline{g_mh}$ i, generalno, $\overline{g_j}h_{j+1} = h_j\overline{g_jh_{j+1}}$).

$(c)$ Kao i u slučaju tačke $(a)$, i dokaz ove tačke je u potpunosti analogan dokazu tačke $(c)$ leme 25.9.□

**Korolar 27.6** *Generalni slobodni proizvod torziono slobodnih grupa je torziono slobodna grupa.*

Naredni primer pokazuje da generalni slobodni proizvod zavisi od utapanja grupe $\mathbf{H}$ u grupe $\mathbf{G}_i$.

**Primer 27.7** *Neka su* $\mathbf{G}_1$ *i* $\mathbf{G}_2$ *dve dijedarske grupe stepena* 4, *generisane, respektivno, parovima elemenata* $a, b$ *i* $x, y$, *gde je* $a^4 = b^2 = e$, $ab = ba^3$ *i* $x^4 = y^2 = e$, $xy = yx^3$, *i neka je* $\mathbf{H}$ *Kleinova podgrupa* $\langle a^2\rangle \times \langle b\rangle$ *grupe* $\mathbf{G}_1$. *Neka su, dalje,* $\varphi_2$ *i* $\psi_2$ *utapanja grupe* $\mathbf{H}$ *u* $\mathbf{G}_2$ *određena sa:* $(a^2)\varphi_2 = x^2$, $(b)\varphi_2 = y$; $(a^2)\psi_2 = yx^2$, $(b)\psi_2 = y$, *dok su* $\varphi_1$ *i* $\psi_1$ *identična utapanja (inkluzije) grupe* $\mathbf{H}$ *u* $\mathbf{G}_1$. *Tada parovi preslikavanja* $(\varphi_1, \varphi_2)$ *i* $(\psi_1, \psi_2)$ *daju različite slobodne proizvode grupa* $\mathbf{G}_1$ *i* $\mathbf{G}_2$ *sa amalgamiranom podgrupom* $\mathbf{H}$.

**Dokaz.** Neka su $\mathbf{N}_1$ i $\mathbf{N}_2$ odgovarajuće normalne podgrupe grupe $\mathbf{G}_1 * \mathbf{G}_2$ (dakle, $\mathbf{N}_1$ je normalno zatvorenje skupa $\{u^{-1}(u)\varphi_2 \mid u \in H\}$, $\mathbf{N}_2$ skupa $\{u^{-1}(u)\psi_2 \mid u \in H\}$). Prema prethodnoj lemi je $N_1 \neq a^2N_1 = x^2N_1 \in Z((\mathbf{G}_1 * \mathbf{G}_2)/\mathbf{N}_1) = Z((\mathbf{G}_1\mathbf{N}_1)/\mathbf{N}_1) \cap Z((\mathbf{G}_2\mathbf{N}_1)/\mathbf{N}_1)$, dok je, s druge strane $Z((\mathbf{G}_1 * \mathbf{G}_2)/\mathbf{N}_2) = Z((\mathbf{G}_1\mathbf{N}_2)/\mathbf{N}_2) \cap Z((\mathbf{G}_2\mathbf{N}_2)/\mathbf{N}_2) = \{N_2\}$, tj. grupa $(\mathbf{G}_1 * \mathbf{G}_2)/\mathbf{N}_2$ je bez centra ($a^2N_2 = x^2N_2$ bi impliciralo $a^2x^2 \in N_2$, a onda i $y \in N_2$, jer je $a^2(x^2y) = (a^2x^2)\cdot y \in N_2$).□

## 28 Teoreme utapanja

Naredni korolar je, istorijski gledano (1927. godina), prvi rezultat koji pokazuje da neka klasa algebri ima svojstvo amalgamiranja. No sigurno će biti od interesa i ostala tvrđenja ovog paragrafa, neka možda na prvi pogled (ali ne već i na drugi) i pomalo začujuća; pomenimo samo: postoji kontinuum mnogo grupa generisanih sa dva elementa; za svaki nenula ordinal $\alpha$ postoji $\aleph_\alpha$-univerzalna grupa.

**Definicija 28.1** *Uređena petorka* $\langle \mathbf{A}, \mathbf{B}, \mathbf{C}, \varphi, \psi\rangle$, *gde su* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ *grupe, a* $\varphi$ *i* $\psi$ *utapanja grupe* $\mathbf{A}$ *u, respektivno, grupe* $\mathbf{B}$ *i* $\mathbf{C}$, *amalgamativna je baza (kaže se i amalgamativni dijagram) teorije grupa. Data amalgamativna baza se može amalgamirati (u teoriji grupa) akko postoje grupa* $\mathbf{D}$ *i utapanja* $\varphi_1$ *i* $\psi_1$, *redom, grupa* $\mathbf{B}$ *i* $\mathbf{C}$ *u* $\mathbf{D}$ *takva da je* $\varphi\circ\varphi_1 = \psi\circ\psi_1$. *Grupu* $\mathbf{D}$, *ako takva postoji, zvaćemo i amalgamom date amalgamativne baze.*



**Korolar 28.2** *Svaka amalgamativna baza teorije grupa se može amalgamirati, drugim rečima teorija grupa ima svojstvo amalgamiranja.*

**Dokaz.** Faktički već dat. Neka je data amalgamativna baza $\langle \mathbf{A}, \mathbf{B}, \mathbf{C}, \varphi, \psi\rangle$ i neka je $\mathbf{D} = (\mathbf{B} * \mathbf{C})/\mathbf{N}$, gde je $\mathbf{N}$ normalna podgrupa generisana skupom $\{((a)\varphi)^{-1}(a)\psi \mid a \in A\}$, dakle slobodni proizvod grupa $\mathbf{B}$ i $\mathbf{C}$ sa amalgamiranom podgrupom $\mathbf{A}$. Definišimo preslikavanje $\varphi_1 : B \longrightarrow D$ na prirodan način sa: $(b)\varphi_1 = \begin{cases} bN & b \neq e \\ N & b = e \end{cases}$. Analogno definišemo preslikavanje $\psi_1$ grupe $\mathbf{C}$ u grupu $\mathbf{D}$. Prema 27.4 $\varphi_1$ i $\psi_1$ su utapanja, a evidentno je i $\varphi\circ\varphi_1 = \psi\circ\psi_1$: za $a \in A$ je $(a)(\varphi\circ\varphi_1) = (a)\varphi N = (a)\psi N = (a)(\psi\circ\psi_1)$.□

**Teorema 28.3** *(G. Higman, B. H. Neumann, H. Neumann).* $(a)$ *Neka su* $\mathbf{A}$ *i* $\mathbf{B}$ *izomorfne podgrupe grupe* $\mathbf{C}$ *i neka je* $\varphi \in Is(\mathbf{A}, \mathbf{B})$. *Tada se* $\mathbf{C}$ *može utopiti u neku grupu* $\mathbf{D}$ *tako da je izomorfizam* $\varphi$ *indukovan nekim unutrašnjim automorfizmom grupe* $\mathbf{D}$.

$(b)$ *Neka su, za svako* $\alpha < \lambda$, *gde je* $\lambda$ *ma koji kardinal,* $\mathbf{A}_\alpha$ *i* $\mathbf{B}_\alpha$ *izomorfne podgrupe grupe* $\mathbf{C}$ *i neka je* $\varphi_\alpha \in Is(\mathbf{A}_\alpha, \mathbf{B}_\alpha)$. *Tada se grupa* $\mathbf{C}$ *može utopiti u neku grupu* $\mathbf{D}$ *tako da su svi izomorfizmi* $\varphi_\alpha$, $\alpha < \lambda$, *indukovani nekim unutrašnjim automorfizmima grupe* $\mathbf{D}$.

**Dokaz.** $(a)$ Neka su $\langle u\rangle$ i $\langle v\rangle$ beskonačne ciklične grupe, $\overline{\mathbf{C}}$ "kopija" grupe $\mathbf{C}$ ($c \longleftrightarrow \overline{c}$) i $\mathbf{C}_1 = \mathbf{C} * \langle u\rangle$ i $\mathbf{C}_2 = \overline{\mathbf{C}} * \langle v\rangle$. Podgrupa $\mathbf{D}_1 = \langle C \cup u^{-1}Au\rangle$ grupe $\mathbf{C}_1$ je slobodni proizvod $\mathbf{C} * u^{-1}\mathbf{A}u$, s obzirom da je proizvod $c_1^{\alpha_1}(u^{-1}a_1u)^{\beta_1}\ldots c_n^{\alpha_n}(u^{-1}a_nu)^{\beta_n}$, gde je $c_i \in C \setminus \{e\}$, $a_i \in A \setminus \{e\}$ i gde je eventualno $\alpha_1 = 0$ ili $\beta_n = 0$ ili i jedno i drugo (što podrazumeva $n \geq 2$), inače $\alpha_i, \beta_i = 1$, uvek različit od jediničnog elementa. Isto tako je $\mathbf{D}_2 = \langle \overline{C} \cup v^{-1}\overline{B}v\rangle = \overline{\mathbf{C}} * v^{-1}\overline{\mathbf{B}}v$. Grupe $\mathbf{D}_1$ i $\mathbf{D}_2$ su izomorfne. Jedan izomorfizam – $\psi$ – određen je sa: $(c)\psi = \overline{c}$ za $c \in C$ i $(u^{-1}au)\psi = v^{-1}\overline{(a)\varphi}v$ (videti 25.5). Neka je sada $\mathbf{D}$ slobodni proizvod grupa $\mathbf{C}_1$ i $\mathbf{C}_2$ sa amalgamiranom podgrupom $\mathbf{D}_1$; podrazumevamo: $\mathbf{D}_1$ se identično preslikava na sebe, a $\psi$ je njeno izomorfno preslikavanje na grupu $\mathbf{D}_2$. Dakle, $\mathbf{D} = (\mathbf{C}_1 * \mathbf{C}_2)/\mathbf{N}$, gde je $\mathbf{N}$ normalna podgrupa generisana skupom $\{d^{-1}(d)\psi \mid d \in D_1\}$. Grupu $\mathbf{C}$ i njene podgrupe $\mathbf{A}$ i $\mathbf{B}$ poistovećujemo sa njihovim izomorfnim slikama, redom: $(\mathbf{CN})/\mathbf{N}$ $(= (\overline{\mathbf{C}}\mathbf{N})/\mathbf{N})$, $(\mathbf{AN})/\mathbf{N}$ $(= (\overline{\mathbf{A}}\mathbf{N})/\mathbf{N})$ i $(\mathbf{BN})/\mathbf{N}$ $(= (\overline{\mathbf{B}}\mathbf{N})/\mathbf{N})$. Izomorfizmu $\varphi$ korespondira preslikavanje $\overline{\varphi} \in Is((\mathbf{AN})/\mathbf{N}, (\mathbf{BN})/\mathbf{N})$, gde je $(aN)\overline{\varphi} = (a)\varphi N$ $(= \overline{(a)\varphi}N)$ i, očigledno, $\overline{\varphi}$ je indukovan unutrašnjim automorfizmom $u_{uv^{-1}N}$; zaista, zbog $(u^{-1}au)N = (v^{-1}\overline{(a)\varphi}v)N$, važi:

$$(aN)u_{uv^{-1}N} = (uv^{-1})^{-1}N\cdot aN\cdot uv^{-1}N = vN\cdot(u^{-1}au)N\cdot v^{-1}N =$$

$$vN\cdot(v^{-1}\overline{(a)\varphi}v)N\cdot v^{-1}N = \overline{(a)\varphi}N = (aN)\overline{\varphi}.$$

($b$) Formirajmo (ne nužno strogo) rastući niz grupa $\mathbf{C}_\alpha$, $\alpha < \lambda$, na sledeći način: $\mathbf{C}_0$ je ekstenzija grupe $\mathbf{C}$ u kojoj je izomorfizam $\varphi_0$ ($\in Is(\mathbf{A}_0, \mathbf{B}_0)$) indukovan nekim unutrašnjim automorfizmom (prethodna tačka garantuje egzistenciju takve grupe). Pretpostavimo da smo već dobili grupe $\mathbf{C}_\alpha$ za svako $\alpha < \beta$ ($< \lambda$) takve da je, za svako $\gamma < \delta$ ($< \beta$), $\mathbf{C}_\gamma \leq \mathbf{C}_\delta$, i u grupi $\mathbf{C}_\alpha$ su svi izomorfizmi $\varphi_\gamma$, $\gamma \leq \alpha$, indukovani nekim njenim unutrašnjim automorfizmima. Ako je $\beta = \alpha + 1$, onda za grupu $\mathbf{C}_\beta$ uzimamo ekstenziju grupe $\mathbf{C}_\alpha$ u kojoj je izomorfizam $\varphi_\beta$ indukovan nekim unutrašnjim automorfizmom. Ako je $\beta$ granični ordinal, $\mathbf{C}_\beta$ je ekstenzija grupe $\bigcup_{\alpha<\beta} \mathbf{C}_\alpha$ u kojoj je izomorfizam $\varphi_\beta$ indukovan unutrašnjim automorfizmom. Tražena grupa je naravno $\bigcup_{\alpha<\lambda} \mathbf{C}_\alpha$.

U formiranju grupa $\mathbf{C}_\alpha$ koristili smo stalno lemu prenosa (3.24). U suprotnom, ukoliko bismo doslovno sledili konstrukciju iz prethodne tačke, u slučaju graničnog ordinala $\beta$, grupu $\mathbf{C}_\beta$ dobili bismo npr. kao adekvatnu ekstenziju usmerenog limita usmerene familije grupa $\langle\langle\beta, \in\rangle, \{\mathbf{C}_\alpha \mid \alpha < \beta\}, \{\psi_{\gamma\delta} \mid \gamma < \delta\ (< \beta)\}\rangle$, gde je, naravno, $\psi_{\gamma\delta}$ utapanje grupe $\mathbf{C}_\gamma$ u grupu $\mathbf{C}_\delta$ (3.22).

Dokaz tačke ($b$) je mogao ići i nešto direktnije u odnosu na prethodni. Neka je $(C; P)$ prezentacija multiplikativnom tablicom grupe $\mathbf{C}$; opet za skup simbola uzimamo baš domen grupe $\mathbf{C}$, a preslikavanje u pitanju je, naravno, identično preslikavanje. Posmatrajmo grupu sa prezentacijom $(C \cup \{h_\alpha \mid \alpha < \lambda\}; P \cup \bigcup_{\alpha<\lambda}\{h_\alpha^{-1} a_\alpha h_\alpha \sim (a_\alpha)\varphi_\alpha \mid a_\alpha \in A_\alpha\})$, gde su $C$ i $\{h_\alpha \mid \alpha < \lambda\}$ disjunktni skupovi. Stavimo $H = \{h_\alpha \mid \alpha < \lambda\}$ i $Q = P \cup \bigcup_{\alpha<\lambda}\{h_\alpha^{-1} a_\alpha h_\alpha \sim (a_\alpha)\varphi_\alpha \mid a_\alpha \in A_\alpha\})$. Podgrupa generisana skupom $\{[h_\alpha] \mid \alpha < \lambda\}$ je slobodna grupa. Jer, neka je $\mathbf{F}_H$ slobodna grupa slobodno reduciranih reči (nad azbukom $H \cup H^{-1}$) i $\psi : C \cup H \longrightarrow F_H$ dato sa: za svako $c \in C$ je $(c)\psi = 1$ i $\psi|_H = \imath_H$. Evidentno, za svako $u \in Q$ je $(u)\overline{\psi} = 1$, pa je $\mathbf{F}_H$ homomorfna slika grupe $\mathbf{G}_{(C\cup H;Q)}$ (21.9($a$)). Ako bismo za neku slobodno reduciranu reč $v \equiv h_{\alpha_1}^{k_1} \dots h_{\alpha_m}^{k_m}$ imali $v \sim_Q 1$, dobili bismo (u $\mathbf{F}_H$): $1 = (v)\overline{\psi} = h_{\alpha_1}^{k_1} \dots h_{\alpha_m}^{k_m}$, kontradikcija.

S druge strane je preslikavanje $\phi : C \longrightarrow G_{(C\cup H;Q)}$, gde je $(c)\phi = [c]$, injektivni homomorfizam. Zaista, pretpostavimo da je $[c] = [d]$ za neka dva različita elementa $c$ i $d$ grupe $\mathbf{C}$, tj. $c \sim_Q d$, i neka je $\{h_{\alpha_1}^{-1} a_{\alpha_1} h_{\alpha_1} \sim (a_{\alpha_1})\varphi_{\alpha_1}, \dots, h_{\alpha_m}^{-1} a_{\alpha_m} h_{\alpha_m} \sim (a_{\alpha_m})\varphi_{\alpha_m}\}$ skup svih relacija iz $Q \setminus P$ koje se javljaju u dokazu relacije $c \sim_Q d$. No ako je grupa $\mathbf{K}$ ekstenzija grupe $\mathbf{C}$ koja sadrži elemente $h_{\alpha_1}, \dots, h_{\alpha_m}$ (nema potrebe da menjamo notaciju) za koje korespondentni unutrašnji automorfizmi indukuju, redom, izomorfizme $\varphi_{\alpha_1}, \dots, \varphi_{\alpha_m}$ (ponovo se pozivamo na tačku ($a$)), onda bi u njoj bilo $c = d$, kontradikcija. Zaključujemo: $\mathbf{G}_{(C\cup H;Q)}$ je tražena grupa.

**Napomena.** Ovaj dokaz nudi pojačanje stava; naime, tekst teoreme se može dopuniti zahtevom da je skup elemenata čiji korespondentni unutrašnji automorfizmi indukuju izomorfizme $\{\varphi_\alpha \mid \alpha < \lambda\}$ slobodna baza podgrupe koju generiše.



Treći dokaz koji nudimo ne treba "međukorak" – tačku ($a$). Neka su $\widehat{\mathbf{C}}$, $\overline{\mathbf{C}_\alpha}$, $\widehat{\overline{\mathbf{C}_\alpha}}$, $\alpha < \lambda$, kopije grupe $\mathbf{C}$ (podrazumevamo da su korespondentni elementi: $c$, $\hat{c}$, $\overline{c_\alpha}$, $\widehat{\overline{c_\alpha}}$) i neka su $\prod^*_{\alpha<\lambda} \langle h_\alpha\rangle$ i $\prod^*_{\alpha<\lambda} \langle k_\alpha\rangle$ slobodne grupe ranga $\lambda$. Neka je, dalje, $\theta_1$ homomorfno preslikavanje grupe $\prod^*_{\alpha<\lambda} \langle h_\alpha\rangle$ u grupu $\mathbf{Aut}(\mathbf{C} \times \prod_{\alpha<\lambda} \overline{\mathbf{C}_\alpha})$, određeno sa: $(h_\alpha)\theta_1 = \overline{h_\alpha}$, gde je $((c, \dots, \overline{d_\alpha}, \dots))\overline{h_\alpha} \stackrel{\text{def}}{=} (d, \dots, \overline{c_\alpha}, \dots)$; elemente grupe $\mathbf{C} \times \prod_{\alpha<\lambda} \overline{\mathbf{C}_\alpha}$ posmatramo kao $1 + \lambda$-nizove (radi se o ordinalnom sabiranju) kod kojih je nulta komponenta iz $\mathbf{C}$, prva iz $\overline{\mathbf{C}_0}$ i tako dalje). $\overline{h_\alpha}$ permutira, uslovno rečeno, komponente na nultom i $1+\alpha$-tom mestu (i stoga je $\overline{h_\alpha}^2 = \imath$). Homomorfizam $\theta_1$ određuje poludirektni proizvod $\mathbf{H}_1 = (\mathbf{C} \times \prod_{\alpha<\lambda} \overline{\mathbf{C}_\alpha}) \times_{\theta_1} \prod^*_{\alpha<\lambda} \langle h_\alpha\rangle$ (13.9). Analogno dobijamo poludirektni proizvod $\mathbf{H}_2 = (\widehat{\mathbf{C}} \times \prod_{\alpha<\lambda} \widehat{\overline{\mathbf{C}_\alpha}}) \times_{\theta_2} \prod^*_{\alpha<\lambda} \langle k_\alpha\rangle$. Za elemente ovih grupa uzimamo uređene parove a "množenje" se već na propisan način definiše. Podgrupu $\mathbf{N}_1$ grupe $\mathbf{H}_1$, izomorfnu grupi $\mathbf{C} \times \prod_{\alpha<\lambda} \overline{\mathbf{A}_\alpha}$, sa domenom $\{(1, (c, \dots, \overline{x_\alpha}, \dots, \overline{y_\beta}, \dots))$, gde je $x_\alpha \in A_\alpha$, $y_\beta \in A_\beta$ (jasno, skoro sve komponente su jedinični element) preslikava $\phi$, gde je $((1, (c, \dots, \overline{x_\alpha}, \dots, \overline{y_\beta}, \dots)))\phi = (1, (\hat{c}, \dots, \widehat{(x_\alpha)\varphi_\alpha}, \dots, \widehat{(y_\beta)\varphi_\beta}, \dots))$, na podgrupu $\mathbf{N}_2$ grupe $\mathbf{H}_2$ koja korespondira grupi $\widehat{\mathbf{C}} \times \prod_{\alpha<\lambda} \widehat{\mathbf{A}_\alpha}$. Neka je, konačno, $\mathbf{H} = (\mathbf{H}_1 * \mathbf{H}_2)/\mathbf{N}$ slobodni proizvod grupa $\mathbf{H}_1$ i $\mathbf{H}_2$ sa amalgamiranom podgrupom $\mathbf{N}_1$ (jasno, ta podgrupa se identično preslikava na sebe, a $\phi$ je njeno utapanje u $\mathbf{H}_2$); $\mathbf{N}$ je, znamo, normalna podgrupa generisana skupom elemenata

$$(1, (c^{-1}, \dots, (\overline{x_\alpha})^{-1}, \dots, (\overline{y_\beta})^{-1}, \dots)) \cdot (1, (\hat{c}, \dots, \widehat{(x_\alpha)\varphi_\alpha}, \dots, \widehat{(y_\beta)\varphi_\beta}, \dots)),$$

$(1, (c, \dots, \overline{x_\alpha}, \dots, \overline{y_\beta}, \dots)) \in N_1$. Preslikavanje $c \longrightarrow (1, (c, \overline{e_0}, \dots, \overline{e_\alpha}, \dots))N$ je utapanje grupe $\mathbf{C}$ u $\mathbf{H}$, a izomorfizmu $\varphi_\alpha$ odgovara preslikavanje $\overline{\varphi_\alpha}$:

$$((1, (a_\alpha, \overline{e_0}, \dots, \overline{e_\beta}, \dots))N)\overline{\varphi_\alpha} \stackrel{\text{def}}{=} (1, ((a_\alpha)\varphi_\alpha, \overline{e_0}, \dots, \overline{e_\beta}, \dots))N,$$

gde je $a_\alpha \in A_\alpha$. Elementima $h_\alpha$ i $k_\alpha$ odgovaraju, respektivno, elementi:

$$\mathbf{h}_\alpha = (h_\alpha, (e, \overline{e_0}, \dots, \overline{e_\beta}, \dots))N, \quad \mathbf{k}_\alpha = (k_\alpha, (\hat{e}, \widehat{e_0}, \dots, \widehat{e_\beta}, \dots))N.$$

Pokazujemo na kraju da je u grupi $\mathbf{H}$ izomorfizam $\overline{\varphi_\alpha}$ indukovan unutrašnjim automorfizmom određenim elementom $\mathbf{h}_\alpha \cdot \mathbf{k}_\alpha$.

$$\mathbf{k}_\alpha^{-1} \cdot \mathbf{h}_\alpha^{-1} \cdot (1, (a, \overline{e_0}, \dots, \overline{e_\beta}, \dots))N \cdot \mathbf{h}_\alpha \cdot \mathbf{k}_\alpha =$$

$$\mathbf{k}_\alpha^{-1} \cdot (1, (e, \overline{e_0}, \dots, \overline{a_\alpha}, \dots, \overline{e_\beta}, \dots))N \cdot \mathbf{k}_\alpha =$$

$$(k_\alpha^{-1}, (\hat{e}, \dots, \widehat{\widehat{e_\alpha}}, \dots))N \cdot (1, (\hat{e}, \dots, \widehat{(a_\alpha)\varphi_\alpha}, \dots))N \cdot (k_\alpha, (\hat{e}, \dots, \widehat{\widehat{e_\alpha}}, \dots))N$$

$$(\text{jer } (1, (e, \dots, \overline{a_\alpha}, \dots, \overline{e_\beta}, \dots)) \cdot (1, (\hat{e}, \dots, \widehat{(a_\alpha)\varphi_\alpha}^{-1}, \dots, \widehat{\widehat{e_\beta}}, \dots)) \in N) =$$

$$(k_\alpha^{-1}, (\widehat{e}, \ldots, \widehat{\widehat{e_\alpha}}, \ldots))N \cdot (k_\alpha, ((a_\alpha)\widehat{\varphi_\alpha}, \widehat{\widehat{e}}_0, \ldots, \widehat{\widehat{e_\alpha}}, \ldots))N =$$

$$(1, ((a_\alpha)\widehat{\varphi_\alpha}, \widehat{\widehat{e}}_0, \ldots, \widehat{\widehat{e_\alpha}}, \ldots))N = (1, ((a_\alpha)\varphi_\alpha, \overline{e_0}, \ldots, \overline{e_\alpha}, \ldots))N.\blacksquare$$

**Napomena.** Podgrupa grupe **D** iz dokaza tačke $(a)$, generisana skupom $\{(CN)/N,\ uv^{-1}N\}$, zove se *HNN-ekstenzija* grupe **C** (naravno, po "vlasnicima" gornje teoreme). Primetimo da je element $uv^{-1}N$ beskonačnog reda (27.5$(a)$) kao i da $HNN$-ekstenzija grupe **C** ima elemente konačnog reda akko ih ima grupa **C** (jer prema dokazu tačke $(a)$ i 27.5, grupa **C** ima elemente konačnog reda akko ih ima grupa **D**). Jasno, iz svega navedenog proizilazi da ako je $(C; P)$ prezentacija grupe **C**, recimo, multiplikativnom tablicom, onda je $(C \cup \{t\};\ P \cup \{t^{-1}at \sim (a)\varphi \mid a \in A\})$, gde $t \notin C$, prezentacija *HNN*-ekstenzije grupe **C**.

Iz ponuđenih konstrukcija se vidi takođe da se gornja teorema može dopuniti sa:

*Ako je* **C** *torziono slobodna i* $\mathbf{A}_\alpha, \mathbf{B}_\alpha$, $\alpha < \lambda$, *parovi njenih uzajamno inverznih podgrupa, tada za svaku familiju izomorfizama* $\{\varphi_\alpha \in Is(\mathbf{A}_\alpha, \mathbf{B}_\alpha) \mid \alpha < \lambda\}$ *postoji ekstenzija* **D** *grupe* **C** *koja je takođe torziono slobodna i takva je da je svaki izomorfizam* $\varphi_\alpha$ *indukovan nekim njenim unutrašnjim automorfizmom.*

**Korolar 28.4** *Svaka grupa* **G** *se može utopiti u neku grupu* **H** *tako da su svi automorfizmi grupe* **G** *indukovani nekim unutrašnjim automorfizmima grupe* **H**.

**Dokaz.** Podsetimo se samo: konstrukcija jedne takve grupe **H** je već data u 12.10 – radilo se o holomorfu grupe **G**.□

**Korolar 28.5** *Svaka grupa se može utopiti u grupu u kojoj su svi elementi istog reda konjugovani.*

**Dokaz.** Neka je $\mathbf{G} = \mathbf{G}_0$ data grupa. Prema prethodnoj teoremi grupa $\mathbf{G}_0$ se može utopiti u neku grupu $\mathbf{G}_1$ u kojoj su svi elementi istog reda iz $\mathbf{G}_0$ konjugovani; ako $a, b \in G_0$ i $red(a) = red(b)$, tada postoji izomorfizam $\varphi_{ab} \in Is(\langle a\rangle, \langle b\rangle)$ koji preslikava $a$ na $b$. Analogno, $\mathbf{G}_1$ se utapa u (neku) grupu $\mathbf{G}_2$ u kojoj su svi elementi istog reda iz $\mathbf{G}_2$ konjugovani. Nastavljajući postupak dobijamo lanac grupa $\mathbf{G}_0 \leq \mathbf{G}_1 \leq \cdots \leq \mathbf{G}_n \leq \cdots$, gde su, generalno, za svako $n$, svi elementi istog reda iz $\mathbf{G}_n$ konjugovani u $\mathbf{G}_{n+1}$. Evidentno, $\overline{\mathbf{G}} = \bigcup_{n\in\omega} \mathbf{G}_n$ je traženo rešenje.□

**Korolar 28.6** *Postoji grupa u kojoj su svi nejedinični elementi konjugovani.*

**Dokaz.** Krenuti od torziono slobodne grupe i imati u vidu drugi deo napomene uz prethodnu teoremu.□



**Teorema 28.7** *(G. Higman, B. H. Neumann, H. Neumann). Svaka prebrojiva grupa se može utopiti u grupu generisanu sa dva elementa beskonačnog reda.*

**Dokaz.** Neka je **G** grupa sa prebrojivim domenom $\{g_n \mid n \in \omega\}$, gde je $g_0$ jedinični element, i $\mathbf{F}_{\{a,b\}}$ slobodna grupa sa slobodnom bazom $\{a, b\}$. U grupi $\mathbf{H} = \mathbf{G} * \mathbf{F}_{\{a,b\}}$ podgrupe **A** i **B** generisane, respektivno, skupovima $\{b^{-n}ab^n \mid n \in \omega\}$ i $\{a^{-n}ba^n g_n \mid n \in \omega\}$ su slobodne, a dati generatorni skupovi su baš njihove slobodne baze. To je prilično evidentno u slučaju podgrupe **A**, po simetriji stvari to važi i za podgrupu **C** generisanu skupom $\{a^{-k}ba^k \mid k \in \omega\}$, pa se u slučaju podgrupe **B** možemo koristiti tom činjenicom i homomorfnim preslikavanjem (projekcijom) grupe **H** na $\mathbf{F}_{\{a,b\}}$ koje sve elemente iz **G** preslikava u jedinični element, a ostavlja fiksnim elemente $a$ i $b$, tj. njegova restrikcija nad grupom $\mathbf{F}_{\{a,b\}}$ je identično preslikavanje (25.5); zaista, taj homomorfizam injektivno preslikava dati generatorni skup podgrupe **B** na slobodnu bazu podgrupe **C**, što će reći da je i taj skup slobodna baza (podgrupe **B**). Neka je $\psi$ izomorfno preslikavanje slobodne grupe **A** na slobodnu grupu **B** takvo da je $(b^{-n}ab^n)\psi = a^{-n}ba^n g_n$ (23.10) i $\mathbf{K} = \langle H, c\rangle$ odgovarajuća $HNN$-ekstenzija grupe **H**; dakle, za svako $n \in \omega$, $(b^{-n}ab^n)\psi = a^{-n}ba^{-n}g_n = c^{-1}(b^{-n}ab^n)c$. No grupu **K** generišu elementi beskonačnog reda $a$ i $c$ (videti napomenu uz teoremu); zbog $(a)\psi = b = c^{-1}ac$ je $b \in \langle a, c\rangle$, a za svako $n \in \omega$ je $g_n = (a^{-n}ba^n)^{-1}(b^n c)^{-1}ab^n c$.

Konstatujmo na kraju da grupa **K** ima elemente konačnog reda akko ih ima grupa **G**, odnosno, da budemo precizniji, grupa **K** ima element datog konačnog reda akko postoji element takvog reda u **G**; jer, grupa **G** ima elemente konačnog reda akko ih ima grupa **H**, a ova ih pak ima akko ih ima njena $HNN$-ekstanzija, tj. grupa **K** (ponovo videti napomenu uz teoremu).■

**Korolar 28.8** $(a)$ *Postoji* $2^{\aleph_0}$ $(= c)$ *neizomorfnih grupa generisanih sa dva elementa.*

$(b)$ *Ne postoji prebrojiva grupa u koju bi se mogle utopiti sve prebrojive grupe.*

**Dokaz.** $(a)$ Za neprazan podskup $S$ skupa prostih brojeva $P$ neka je $\mathbf{A}_S = \sum_{p\in S} \mathbf{Z}_p$ i neka je $\mathbf{G}_S$ grupa generisana sa dva elementa beskonačnog reda u koju se utapa grupa $\mathbf{A}_S$ i koja se dobija prema prethodnom korolaru. Prema tome, grupa $\mathbf{G}_S$ ima element datog prostog reda $p$ akko je $p \in S$, a odatle sledi da za svaka dva različita neprazna podskupa $S$ i $T$ skupa $P$ grupe $\mathbf{G}_S$ i $\mathbf{G}_T$ nisu izomorfne.

$(b)$ Jasno; u svakoj prebrojivoj grupi imamo najviše prebrojivo mnogo neizomorfnih podgrupa generisanih sa dva elementa. U vezi sa ovom tačkom videti i 33.21.□

**Lema 28.9** *Za svaki beskonačan kardinal* $\lambda$ *postoji* $2^\lambda$ *neizomorfnih grupa reda* $\lambda$ *koje nisu razložive u slobodni proizvod.*

**Dokaz**. Dokaz je transfinitnom indukcijom po beskonačnim kardinalima. No prvo par napomena iz kardinalne aritmetike. Ako su $\lambda$ i $\mu$ beskonačni kardinali onda je $\lambda \cdot \mu = max\{\lambda, \mu\}$ (ovo smo već više puta koristili). Za svaki beskonačan kardinal $\lambda$ je $\sum_{\mu<\lambda} 2^{\mu} \geq \lambda$ (podrazumevamo da $\mu$ "ide" skupom kardinala manjih od $\lambda$); ovo je posledica Cantorove teoreme: za svaki kardinal $\eta$ je $2^{\eta} > \eta$. Konačno, ako je $A$ skup beskonačne kardinalnosti $\lambda$, onda on sadrži $2^{\lambda}$ podskupova kardinalnosti $\lambda$; dokaz ovog se bazira na činjenici da je $\lambda \cdot \lambda = |\lambda \times \lambda| = \lambda$ – za svaki neprazan podskup $B$ kardinala $\lambda$ je podskup $B \times \lambda$ skupa $\lambda \times \lambda$ kardinalnosti $\lambda$.

Krenimo od najmanjeg beskonačnog kardinala – $\aleph_0$. Za beskonačan podskup $S$ skupa prostih brojeva $P$ neka je $\mathbf{A}_S = \sum_{p \in S} \mathbf{Z}_p$. Već smo rekli, za različite (beskonačne) podskupove $S$ i $T$ grupe $\mathbf{A}_S$ i $\mathbf{A}_T$ nisu izomorfne, a sigurno nusu, kao Abelove, ni razložive u slobodni proizvod. Pretpostavimo dalje da je tvrđenje tačno za sve kardinale $\mu < \lambda$. Prema gornjoj napomeni postoji bar $\lambda$ neizomorfnih slobodno nerazloživih grupa reda manjeg od $\lambda$. Neka je $\{\mathbf{G}_\alpha \mid \alpha < \lambda\}$ jedna familija takvih grupa. Za podskup $S \subseteq \lambda$ kardinalnosti $\lambda$ neka je $\mathbf{H}_S = \prod^*_{\alpha \in S} \mathbf{G}_\alpha$ (jasno, $\mathbf{H}_S$ je grupa bez centra kardinalnosti $\lambda$). Prema 26.10 grupa $\mathbf{H}_S$ nije razloživa u direktni proizvod, a prema 26.9, za svaka dva različita podskupa $S$ i $T$ grupe $\mathbf{H}_S$ i $\mathbf{H}_T$ nisu izomorfne. Neka je $\mathbf{K}_S = \mathbf{H}_S \times \mathbf{S}_3$. Naravno, grupa $\mathbf{K}_S$ je bez centra i (ponovo prema 26.10) nije slobodno razloživa. Teorema 11.34 implicira da za različite podskupove $S$ i $T$ grupe $\mathbf{K}_S$ i $\mathbf{K}_T$ nisu izomorfne.□

Čitalac sada već neće imati problema da dokaže da za dati beskonačni kardinal $\lambda$ postoji $2^{\lambda}$ neizomorfnih grupa i sa raznim drugim svojstvima. Jedan takav slučaj već imamo u 28.11.

**Lema 28.10** (*a*) *Svaka prebrojiva grupa se može utopiti u prebrojivu deljivu prostu grupu.*

(*b*) *Svaka grupa se može utopiti u deljivu (prostu) grupu.*

**Dokaz**. (*a*) Neka je $\mathbf{G}$ prebrojiva grupa. Ona je (možemo smatrati) podgrupa grupe $\mathbf{H} = \mathbf{G} \times (\mathbf{Z} \oplus \sum_{n>1} \mathbf{Z}_n)$ (koja ima elemente svih redova). Grupu $\mathbf{H} * \langle a \rangle$, gde je $\langle a \rangle$ nova beskonačna ciklična grupa, utapamo u grupu $\mathbf{K}$ generisanu sa dva elementa beskonačnog reda (28.7), a ovu pak u prebrojivu grupu $\mathbf{M}$ u kojoj su svi elementi istig reda konjugovani (videti 28.5). Grupa $\mathbf{M}$ je, tvrdimo, prosta i deljiva.

Neka je $\mathbf{N}$ normalna nejedinična podgrupa grupe $\mathbf{M}$. S obzirom da su (u $\mathbf{M}$) svi elementi istog reda konjugovani, $\mathbf{N}$ sadrži nejedinični element podgrupe $\mathbf{H}$ – neka je to $b$. No tada je i element beskonačnog reda $a^{-1}b^{-1}a \cdot b = [a, b]$ u $\mathbf{N}$ i stoga, ponovo zbog konjugovanosti elemenata istog reda, $\mathbf{K} \leq \mathbf{N}$. Prema tome, $\mathbf{N}$ sadrži elemente svih redova, dakle, $\mathbf{N} = \mathbf{M}$.

Pokažimo da je $\mathbf{M}$ i deljiva grupa. Neka je $c$ jedan njen element reda $m$, gde dozvoljavamo da je $m$ oznaka i za beskonačan red, i neka je $n$ prirodan



broj veći od jedan. U grupi svakako imamo i element $d$ reda $m \cdot n$ (znači beskonačnog ako je $c$ element beskonačnog reda). No onda je $d^n$ reda $m$, te je, za neko $g \in M$, $g^{-1}d^n g = (g^{-1}dg)^n = c$.□

**Korolar 28.11** *Postoji $2^{\aleph_0}$ prebrojivih prostih grupa.*

**Dokaz**. Prebrojivih grupa generisanih sa dva elementa ima kontinuum mnogo (28.8), a svaka od njih se utapa u neku prebrojivu prostu grupu. Stoga i ovih mora biti kontinuum mnogo.□

**Definicija 28.12** *Neka je data grupa $\mathbf{G}$ i neka je $u(\overline{a}, \overline{x})$ reč po elementima konačnog niza $\overline{a}$ elemenata grupe $\mathbf{G}$ i promenljivima (nepoznanicama) konačnog niza $\overline{x}$, u kojoj se ne mora nužno javiti svaki naznačeni element grupe ili naznačena promenljiva. Konačan sistem jednačina i nejednačina oblika:*

$$\begin{aligned} u_1(\overline{a}, \overline{x}) &= e \\ &\vdots \\ u_k(\overline{a}, \overline{x}) &= e \\ v_1(\overline{a}, \overline{x}) &\neq e \\ &\vdots \\ v_r(\overline{a}, \overline{x}) &\neq e \end{aligned}$$

*konsistentan je sa grupom $\mathbf{G}$ akko postoje grupa $\mathbf{H}$ i utapanje $\varphi$ grupe $\mathbf{G}$ u $\mathbf{H}$ takvi da sistem*

$$\begin{aligned} u_1((\overline{a})\varphi, \overline{x}) &= e \\ &\vdots \\ u_k((\overline{a})\varphi, \overline{x}) &= e \\ v_1((\overline{a})\varphi, \overline{x}) &\neq e \\ &\vdots \\ v_r((\overline{a})\varphi, \overline{x}) &\neq e \end{aligned}$$

*ima rešenje u $\mathbf{H}$.*

*Grupa $\mathbf{G}$ je algebarski zatvorena akko je svaki konačan sistem jednačina i nejednačina konsistentan sa njome u njoj i rešiv.*

**Napomena**. Lema prenosa nam, jasno, dozvoljava da kažemo:

*sistem (jednačina i nejednačina) $\mathcal{S}$ je konsistentan sa grupom $\mathbf{G}$ akko postoji ekstenzija grupe $\mathbf{G}$ u kojoj taj sistem ima rešenje.*

Ovo ćemo, radi pojednostavljenja "priče", koristiti u narednoj lemi.

**Lema 28.13** *Svaka grupa se može utopiti u algebarski zatvorenu grupu; posebno, beskonačna grupa se može utopiti u algebraski zatvorenu grupu iste kardinalnosti.*

**Dokaz.** Neka je $\mathbf{G}$ beskonačnog reda $\lambda$, a $\{\mathcal{S}_\alpha \mid 1 \leq \alpha < \lambda\}$ skup svih konačnih sistema jednačina i nejednačina sa elementima iz $\mathbf{G}$ i nepoznanicama iz prebrojivog skupa $X = \{x_i \mid i \in \omega\}$). Definišemo rekurzivno, za svaki ordinal $\beta$ manji od $\lambda$, grupe $\mathbf{G}_\beta$ na sledeći način. $\mathbf{G}_0 = \mathbf{G}$. Pretpostavimo da su već određene, za svako $\gamma < \beta$, grupe $\mathbf{G}_\gamma$ koje su kardinalnosti $\lambda$ i koje obrazuju lanac. Ako je $\beta$ nasledni ordinal i ako je sistem $\mathcal{S}_\beta$ konsistentan sa grupom $\mathbf{G}_{\beta-1}$, onda za $\mathbf{G}_\beta$ biramo podgrupu ekstenzije grupe $\mathbf{G}_{\beta-1}$ u kojoj dati sistem ima rešenje, a koja je generisana unijom domena grupe $\mathbf{G}_{\beta-1}$ i konačnim skupom rešenja; u suprotnom uzimamo da je $\mathbf{G}_\beta = \mathbf{G}_{\beta-1}$. Ako je $\beta$ nasledni ordinal, onda postupamo kao i u prethodnom slučaju, s tim što što sada posmatramo grupu $\mathbf{H}_\beta = \bigcup_{\gamma<\beta} \mathbf{G}_\gamma$ i sistem $\mathcal{S}_\beta$; ponovo, ako sistem nije konsistentan sa grupom, onda je $\mathbf{G}_\beta = \mathbf{H}_\beta$, a inače je podgrupa grupe u kojoj sistem ima rešenje generisana unijom domena podgrupe $\mathbf{H}_\beta$ i skupom rešenja sistema. Evidentno, grupa $\mathbf{G}^1 = \bigcup_{\beta<\lambda} \mathbf{G}_\beta$ je grupa kardinalnosti $\lambda$ (kao unija lanca kardinalnosti $\lambda$ grupa kardinalnosti $\lambda$). Uočimo da je svaki sa njome konsistentan (konačan) sistem (jednačina i nejednačina), sa elementima iz $\mathbf{G}$ u njoj i rešiv; jer, svaki takav sistem je iz navedenog spiska, pa ako je to npr. $\mathcal{S}_\beta$, onda, budući da je konsistentan sa $\mathbf{G}^1$, svakako je konsistentan i sa $\mathbf{G}_{\beta-1}$, te su njegova rešenja sadržana u $\mathbf{G}_\beta$. Analogno bismo, startujući sada od grupe $\mathbf{G}^1$, dobili grupu $\mathbf{G}^2$, i tako redom. Konačno, $\overline{\mathbf{G}} = \bigcup_{n\geq 1} \mathbf{G}^n$ je tražena grupa. Svako dalje objašnjenje bi posle svega rečenog bilo suvišno.□

**Napomena.** Opisani postupak dobijanja algebarski zatvorene grupe, kao i njemu "srodan" postupak za dobijanje algebarski zatvorenih polja, umnogome su inspirisali opštu metodu teorije modela koja nam generalno daje:

*svaki model induktivne teorije (tj. teorije za koju važi da je unija lanca njenih modela opet njen model) sadržan je u nekom egzistencijalno kompletnom modelu te teorije.*

Čitaoca zainteresovanog za model-teoretska razmatranja algebre upućujemo na, recimo, [27] i [136].

**Lema 28.14** *Algebarske zatvorene grupe su proste i nisu konačno generisane.*

**Dokaz.** Neka je $\mathbf{G}$ algebarski zatvorena grupa i neka su $a$ i $b$ dva njena nejedinična elementa. U slobodnom proizvodu $\mathbf{G} * \langle u \rangle$ (gde, jasno, uzimamo da $u$ nije element grupe $\mathbf{G}$) elementi $a^{-1}u^{-1}au$ $(= [a, u])$ i $u^{-1}a^{-1}ub$ su beskonačnog reda. Prema 28.5, grupa $\mathbf{G} * \langle u \rangle$ se može utopiti u neku grupu $\mathbf{H}$ u kojoj su dati elementi konjugovani. Neka je, za $h \in H$, $u^{-1}a^{-1}ub = h^{-1}a^{-1}u^{-1}auh$, odnosno $b = u^{-1}au \cdot h^{-1}a^{-1}h \cdot (uh)^{-1}a(uh)$. To zapravo znači da jednačina $b^{-1}x^{-1}axy^{-1}a^{-1}x^{-1}axy = e$ ima rešenje u nekoj ekstenziji grupe $\mathbf{G}$, pa s obzirom da je $\mathbf{G}$ algebarski zatvorena grupa, rešenja jednačine postoje i u $\mathbf{G}$. Ali onda je element $b$ u normalnom zatvorenju skupa $\{a\}$, što će reći da je normalno zatvorenje bilo kog nejediničnog elementa grupe $\mathbf{G}$ upravo cela grupa.



Pokažimo da grupa $\mathbf{G}$ ne može biti ni konačno generisana. Znamo da je u grupi $\mathbf{G} * \langle u \rangle$, $au \neq ua$, tj. $a^{-1}u^{-1}au \neq e$. Rezonujući kao i maločas, zaključujemo da u grupi $\mathbf{G}$ postoji element koji nije permutabilan sa $a$; dakle, $\mathbf{G}$ ima trivijalni centar. Neka je $B = \{b_1, \ldots, b_m\}$ bilo koji konačan podskup domena grupe $\mathbf{G}$. U grupi $\mathbf{G} \times \langle v \rangle$ (gde $v \notin G$), element $v$ je permutabilan sa svakim elementom skupa $B$. Odatle opet sledi da i u grupi $\mathbf{G}$ imamo nejediničan element permutabilan sa elementima $b_1, \ldots, b_m$ (radi se o rešenju sistema: $b_1^{-1}x^{-1}b_1x = e, \ldots, b_m^{-1}x^{-1}b_mx = e$, $x \neq e$); neka je to $d$. Ali tada je $d \in C(\langle B \rangle)$, pa nije $\langle B \rangle = \mathbf{G}$.□

Tvrđenje tačke $(b)$ korolara 28.8 nije pravilo, štaviše izuzetak je. O tome u narednoj teoremi. Ali prvo

**Definicija 28.15** $(a)$ *Grupa $\mathbf{G}$ reda $\aleph_\alpha$ je $\aleph_\alpha$-univerzalna akko se svaka grupa reda manjeg od ili jednakog $\aleph_\alpha$ može u nju utopiti.*

$(b)$ *Neka je $\mathbf{H}$ podgrupa reda manjeg od $\aleph_\alpha$ grupe $\mathbf{G}$. Tada je $\mathbf{G}$ $\aleph_\alpha$-univerzalna ekstenzija podgrupe $\mathbf{H}$ akko za svaku ekstenziju grupe $\mathbf{H}$ reda manjeg od $\aleph_\alpha$ postoji utapanje u $\mathbf{G}$ čija je restrikcija nad $H$ identično preslikavanje.*

**Lema 28.16** $(GCH)$ *Svaku grupa reda $\aleph_\alpha$ ima $\aleph_{\alpha+1}$-univerzalnu ekstenziju reda $\leq \aleph_{\alpha+1}$.*

**Dokaz.** Generalna hipoteza kontinuuma $(GCH)$ je, podsećamo, uslov: za svaki ordinal $\alpha$ je $2^{\aleph_\alpha} = \aleph_{\alpha+1}$.

Neka je $\mathbf{H}$ grupa reda $\aleph_\alpha$. Konstatujmo odmah da postoji $2^{\aleph_\alpha}$ $(= \aleph_{\alpha+1})$ njenih neizomorfnih ekstenzija reda $\aleph_\alpha$; jer, prema 28.9 postoji $\aleph_{\alpha+1}$ neizomorfnih i slobodno nerazloživih grupa reda $\aleph_\alpha$, pa ako npr. neizomorfne i slobodno nerazložive grupe reda $\aleph_\alpha$ – $\mathbf{A}$ i $\mathbf{B}$ – nisu slobodni faktori grupe $\mathbf{H}$ (a takvih je sigurno $\aleph_{\alpha+1}$), onda su grupe $\mathbf{H} * \mathbf{A}$ i $\mathbf{H} * \mathbf{B}$ neizomorfne ekstenzije grupe $\mathbf{H}$ reda $\aleph_\alpha$ (naravno, grupu $\mathbf{H}$ identifikujemo sa odgovarajućom podgrupom datih slobodnih proizvoda). Neka je $\mathcal{F} = \{\mathbf{H}_\beta \mid \beta < \aleph_{\alpha+1}\}$ familija svih, do na izomorfizam, neizomorfnih ekstenzija grupe $\mathbf{H}$ reda $\aleph_\alpha$, pri čemu je, za $\beta < \gamma$ $(< \aleph_{\alpha+1})$, $\mathbf{H}_\beta \cap \mathbf{H}_\gamma = \mathbf{H}$ (lema prenosa nam dozvoljava takav izbor). Tada je, očigledno, slobodni proizvod svih grupa familije $\mathcal{F}$ sa amalgamiranom podgrupom $\mathbf{H}$ $\aleph_{\alpha+1}$-univerzalna ekstenzija grupe $\mathbf{H}$.□

**Lema 28.17** *Neka je $\mathbf{K}$ grupa reda manjeg od $\aleph_\alpha$ i $\mathbf{H}$ jedna njena podgrupa. Tada važi: ako je grupa $\mathbf{G}$ $\aleph_\alpha$-univerzalna ekstenzija grupe $\mathbf{K}$, onda je $\aleph_\alpha$-univerzalna ekstenzija i grupe $\mathbf{H}$.*

**Dokaz.** Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{M}$, reda manjeg od $\aleph_\alpha$. Možemo odmah, bez uticaja na opštost razmatranja, pretpostaviti da je $\mathbf{M} \cap \mathbf{K} = \mathbf{H}$. Prema korolaru 27.4 i komentaru uz njega, postoji grupa $\mathbf{N}$ reda manjeg od $\aleph_\alpha$, koja

je ekstenzija grupa $\mathbf{M}$ i $\mathbf{K}$. Pošto je $\mathbf{G}$ $\aleph_\alpha$-univerzalna ekstenzija grupe $\mathbf{K}$, postoji utapanje $\varphi$ grupe $\mathbf{N}$ u $\mathbf{G}$ takvo da je $\varphi|_K = \imath_K$. Jasno, $\psi = \varphi|_M$ je utapanje grupe $\mathbf{M}$ u $\mathbf{G}$ i $\psi|_H = \imath_H$.□

**Teorema 28.18** *(GCH) Za svaki nenula ordinal $\alpha$ postoji $\aleph_\alpha$-univerzalna grupa.*

**Dokaz**. Sledimo, kao i u prethodnim dvema lemama, [74]. Prvo (još) jedna definicija iz kardinalne aritmetike:

*kardinal $\lambda$ je regularan akko je veći od svakog zbira oblika $\sum_{\alpha<\mu}\kappa_\alpha$, gde su $\mu$ i, za svako $\alpha<\mu$, $\kappa_\alpha$ kardinali manji od $\lambda$; ovo je pak ekvivalentno uslovu da se nijedan kardinal manji od $\lambda$ ne može preslikati u $\lambda$ tako da je njegova slika neograničena (dakle, ako je $\mu<\lambda$ i $f$ ma kakvo preslikavanje kardinala $\mu$ u $\lambda$, onda postoji ordinal $\beta<\lambda$ takav da je $(\gamma)f<\beta$ za svako $\gamma<\mu$).*

Iz kardinalne aritmetike nam je poznato da je svaki nasledni kardinal (tj. kardinal oblika $\aleph_{\alpha+1}$) regularan.

Pokažimo prvo da postoji $\aleph_1$-univerzalna grupa. U tom cilju formiramo, za svako $\alpha,\beta,\gamma<\aleph_1$, grupe $\mathbf{G}_{\alpha\beta}$, $\mathbf{G}_\gamma$ tako da su ispunjeni sledeći uslovi:

(1) $|G_{\alpha\beta}|<\aleph_1$;

(2) $\mathbf{G}_{\alpha\beta}\leq\mathbf{G}_{\alpha'\beta'}$ kad god je $\alpha\leq\alpha'$ i $\beta\leq\beta'$;

(3) $\mathbf{G}_\gamma=\bigcup_{\alpha<\aleph_1}\mathbf{G}_{\gamma\alpha}$

i

(4) $\mathbf{G}_{\gamma+1}$ je $\aleph_1$-univerzalna ekstenzija grupe $\mathbf{G}_{\gamma\gamma}$.

Neka je $\mathbf{G}_0$ bilo koja prebrojiva grupa i neka je $\mathbf{G}_{0\alpha}=\mathbf{G}_0$ za svako $\alpha<\aleph_1$. Za $\beta>0$ grupe $\mathbf{G}_{\beta\gamma}$ dobijamo transfinitnom rekurzijom. Pretpostavimo da već imamo sve grupe $\mathbf{G}_\alpha$, $\mathbf{G}_{\alpha\delta}$ za svako $\alpha<\beta$ i svako $\delta<\aleph_1$ koje ispunjavaju postavljene uslove. Razlikujemo (standardno) slučajeve: $(I)$ $\beta$ je nasledni ordinal – $\beta=\alpha+1$ za neko $\alpha$ i $(II)$ $\beta$ je granični ordinal.

$(I)$ Neka je $\mathbf{K}$ $\aleph_1$-univerzalna ekstenzija grupe $\mathbf{G}_{\alpha\alpha}$ takva da je $\mathbf{K}\cap\mathbf{G}_\alpha=\mathbf{G}_{\alpha\alpha}$. Prema svojstvu amalgamiranja postoji grupa $\mathbf{G}_\beta$ reda $\aleph_1$ koja sadrži grupe $\mathbf{G}_\alpha$ i $\mathbf{K}$. Nju pak možemo predstaviti kao uniju rastućeg lanca prebrojivih grupa $\mathbf{H}_{\beta\delta}$, $\delta<\aleph_1$ (prebrojivi podskup grupe $\mathbf{G}_\beta$ generiše prebrojivu podgrupu). Konačno, ako za $\delta<\aleph_1$ uzmemo $\mathbf{G}_{\beta\delta}\stackrel{\text{def}}{=}\langle G_{\alpha\delta}\cup H_{\beta\delta}\rangle$ imaćemo: za svako $\delta\leq\delta'<\aleph_1$ i svako $\gamma<\beta$ važi $\mathbf{G}_{\gamma\delta}\leq\mathbf{G}_{\beta\delta'}$, $\mathbf{G}_{\beta\delta}\leq\mathbf{G}_{\beta\delta'}$ (imamo u vidu da je $\mathbf{G}_\alpha=\bigcup_{\delta<\aleph_1}\mathbf{G}_{\alpha\delta}$ podgrupa grupe $\mathbf{G}_\beta$ kao i da je, za svako $\gamma<\alpha$, $\mathbf{G}_{\gamma\delta}\leq\mathbf{G}_{\alpha\delta}$). Evidentno, grupe $\mathbf{G}_\beta$ $(=\bigcup_{\delta<\aleph_1}\mathbf{G}_{\beta\delta})$ i $\mathbf{G}_{\beta\delta}$, $\delta<\aleph_1$, ispunjavaju postavljene uslove.

$(II)$ Za granični ordinal $\beta$ uzimamo jednostavno: $\mathbf{G}_\beta=\bigcup_{\alpha<\beta}\mathbf{G}_\alpha$ i, za $\delta<\aleph_1$, $\mathbf{G}_{\beta\delta}=\bigcup_{\alpha<\beta}\mathbf{G}_{\alpha\delta}$.

Neka je $\mathbf{G}=\langle G,\cdot\rangle=\bigcup_{\alpha<\aleph_1}\mathbf{G}_\alpha$. Naravno, $\mathbf{G}$ je grupa reda $\aleph_1$. Tvrdimo i da je $\aleph_1$-univerzalna. Neka je $\mathbf{M}=\langle M,\bullet\rangle$ (ma koja) grupa reda $\aleph_1$ i $\mathbf{M}=\bigcup_{\alpha<\aleph_1}\mathbf{M}_\alpha$, gde je svaka podgrupa $\mathbf{M}_\alpha$ prebrojiva i $\mathbf{M}_\alpha\leq\mathbf{M}_\beta$ za $\alpha<\beta$ $(<\aleph_1)$. Neka je $\mathbf{N}_0$ prebrojiva grupa koja sadrži $\mathbf{M}_0$ i u koju se utapa $\mathbf{G}_{00}$



(koristimo svojstvo pridruženog utapanja, koje nam daje bilo direktni bilo slobodni proizvod, i lemu prenosa). Pošto je $\mathbf{G}_1$ $\aleph_1$-univerzalna ekstenzija grupe $\mathbf{G}_{00}$, grupa $\mathbf{N}_0$ se utapa u grupu $\mathbf{G}_1$, pa se u tu grupu utapa i njena podgrupa $\mathbf{M}_0$; neka je $\varphi_0$ utapanje grupe $\mathbf{M}_0$ u $\mathbf{G}_1$. U nastavku definišemo, opet transfinitnom rekurzijom, utapanja $\varphi_\alpha$ grupa $\mathbf{M}_\alpha$ u grupu $\mathbf{G}$ za svako $\alpha<\aleph_1$, pri čemu je ispunjeno: za svako $\alpha<\beta$ je $\varphi_\beta|_{M_\alpha}=\varphi_\alpha$. Pretpostavimo da smo već odredili za svako $\alpha<\beta$ utapanja $\varphi_\alpha$ koja ispunjavaju postavljeni uslov. Neka je $\overline{\mathbf{M}}_\beta=\bigcup_{\alpha<\beta}\mathbf{M}_\alpha$ $(\leq\mathbf{M}_\beta)$ i $\overline{\mathbf{G}}_\beta=\bigcup_{\alpha<\beta}(\mathbf{M}_\alpha)\varphi_\alpha$ $(\leq\mathbf{G})$. Naravno, $\psi=\bigcup_{\alpha<\beta}\varphi_\alpha$ je izomorfno preslikavanje grupe $\overline{\mathbf{M}}_\beta$ na grupu $\overline{\mathbf{G}}_\beta$. S obzirom da je $\overline{\mathbf{G}}_\beta$ prebrojiva podgrupa grupe $\mathbf{G}$, postoji neki ordinal $\xi\geq\beta$ za koji je $\overline{\mathbf{G}}_\beta\leq\mathbf{G}_\xi=\bigcup_{\alpha<\aleph_1}\mathbf{G}_{\xi\alpha}$, pa onda i neko $\delta$ $(<\aleph_1)$ takvo da je $\overline{\mathbf{G}}_\beta\leq\mathbf{G}_{\xi\delta}$ (imamo na umu da je $\aleph_1$ regularan kardinal). Ako je $\beta'=max\{\xi,\delta\}$, tada je $\overline{\mathbf{G}}_\beta\leq\mathbf{G}_{\beta'\beta'}$. Nalazimo sada prebrojivu ekstenziju $\mathbf{L}$ grupe $\mathbf{G}_{\beta'\beta'}$ u koju se utapa grupa $\mathbf{M}_\beta$ i to tako da je restrikcija tog utapanja nad $\overline{M}_\beta$ baš $\psi$. Neka je $\theta$ bijektivno preslikavanje skupa $M_\beta$ na skup $T=\overline{G}_\beta\cup(M_\beta\setminus\overline{M}_\beta)$ dato sa: $\theta|_{\overline{M}_\beta}=\psi$ i $(a)\theta=a$ za svako $a\in M_\beta\setminus\overline{M}_\beta$. Na skupu $T$ definišemo operaciju $*$ sa: $x*y=((x)\theta^{-1}\bullet(y)\theta^{-1})\theta$ i tako dobijamo grupu $\mathbf{T}$ izomorfnu grupi $\mathbf{M}_\beta$; prema samoj konstrukciji je $\theta\in Is(\mathbf{M}_\beta,\mathbf{T})$. Podgrupa grupe $\mathbf{T}$ sa domenom $\overline{G}_\beta$ je upravo grupa $\overline{\mathbf{G}}_\beta$; zaista, za svako $x,y\in\overline{G}_\beta$ je:

$$x*y=((x)\theta^{-1}\bullet(y)\theta^{-1})\theta=((x)\psi^{-1}\bullet(y)\psi^{-1})\psi=((x\cdot y)\psi^{-1})\psi=x\cdot y.$$

Tražena grupa $\mathbf{L}$ je onda slobodni proizvod grupa $\mathbf{T}$ i $\mathbf{G}_{\beta'\beta'}$ sa amlgamiranom podgrupom $\overline{\mathbf{G}}_\beta$, i, jasno, $\theta$ je traženo utapanje. Kako je $\mathbf{G}_{\beta'+1}$ $\aleph_1$-univerzalna ekstenzija grupe $\mathbf{G}_{\beta'\beta'}$, dakle i grupe $\overline{\mathbf{G}}_\beta$, postoji utapanje $\eta$ grupe $\mathbf{L}$ u $\mathbf{G}_{\beta'+1}$ takvo da je $\eta|_{\overline{G}_\beta}$ identično preslikavanje. Tada je $\varphi_\beta\stackrel{\text{def}}{=}\theta\circ\eta$ utapanje grupe $\mathbf{M}_\beta$ u grupu $\mathbf{G}_{\beta'+1}$ i $\varphi_\beta|_{\overline{M}_\beta}=(\theta\circ\eta)|_{\overline{M}_\beta}=\psi$. Zaključujemo: $\bigcup_{\beta<\aleph_1}\varphi_\beta$ je utapanje grupe $\mathbf{M}$ u grupu $\mathbf{G}$.

Generalno, ako je $\beta$ nasledni ordinal, onda na način analogan upravo datom, imajući u vidu lemu 28.16 i činjenicu da je $\aleph_\beta$ regularan kardinal, dokazujemo egzistenciju $\aleph_\beta$-univerzalne grupe. Razmotrimo slučaj kada je $\beta$ granični ordinal. Formirajmo prvo lanac grupa $\mathbf{G}_\alpha$, $\alpha\leq\beta$, koje ispunjavaju sledeće uslove:

$(a)$ $\mathbf{G}_0$ je $\aleph_1$-univerzalna grupa;

$(b)$ $|G_\alpha|\leq\aleph_{\alpha+1}$ za svako $\alpha\leq\beta$;

$(c)$ $\mathbf{G}_{\alpha+1}$ je $\aleph_{\alpha+2}$-univerzalna ekstenzija grupe $\mathbf{G}_\alpha$ za svako $\alpha<\beta$

i

$(d)$ $\mathbf{G}_\gamma=\bigcup_{\alpha<\gamma}\mathbf{G}_\alpha$ za svaki granični ordinal $\gamma\leq\beta$.

Pokazaćemo da je $\mathbf{G}_\beta$ $\aleph_\beta$-univerzalna grupa. Neka je $\mathbf{H}$ grupa reda $\aleph_\beta$. Predstavimo je kao uniju lanca grupa $\mathbf{H}_\alpha$, takvog da važi: $\mathbf{H}_0$ je prebrojiva grupa; za svako $\alpha$ je grupa $\mathbf{H}_\alpha$ reda manjeg od ili jednakog $\aleph_\alpha$; ako $\alpha<\gamma$ $(\leq\beta)$, onda $\mathbf{H}_\alpha\leq\mathbf{H}_\gamma$; za svaki granični ordinal $\delta\leq\beta$ je $\mathbf{H}_\delta=\bigcup_{\alpha<\delta}\mathbf{H}_\alpha$ (egzistencija lanca je očigledna). Prema $(a)$, postoji utapanje $\varphi_0$ grupe $\mathbf{H}_0$ u grupu $\mathbf{G}_0$.

Pretpostavimo da smo već, za svako $\alpha < \gamma$ $(\leq \beta)$, dobili utapanja $\varphi_\alpha$ grupa $\mathbf{H}_\alpha$ u grupe $\mathbf{G}_\alpha$, takva da je $\varphi_{\alpha'}|_{H_\alpha} = \varphi_\alpha$ za $\alpha < \alpha' (< \gamma)$. Ako je $\gamma$ granični ordinal, onda je, prema datim uslovima, $\bigcup_{\alpha<\gamma} \varphi_\alpha$ utapanje grupe $\mathbf{H}_\gamma$ u grupu $\mathbf{G}_\gamma$. Ako je $\gamma$ nasledni ordinal - $\gamma = \alpha + 1$, onda s obzirom da je $\mathbf{G}_\gamma = \mathbf{G}_{\alpha+1}$ $\aleph_{\alpha+2}$-univerzalna ekstenzija grupe $\mathbf{G}_\alpha$ možemo naći (kao što smo već videli u prethodnom delu dokaza) utapanje $\varphi_\gamma$ grupe $\mathbf{H}_\gamma$ u grupu $\mathbf{G}_\gamma$ takvo da je $\varphi_\gamma|_{H_\alpha} = \varphi_\alpha$. Jasno, $\bigcup_{\alpha<\beta} \varphi_\alpha$ je utapanje grupe $\mathbf{H}$ u grupu $\mathbf{G}$.

U vezi sa ovom teoremom videti i 33.21.■

## 29 Gruško-Neumannova teorema

Gruško-Neumannova teorema je svakako bazična teorema kada je reč o slobodnim dekompozicijama konačno generisanih grupa. Postoji više dokaza ove teoreme. Prvi su je nezavisno dokazali I. A. Gruško 1940. godine ([62]) i B. H. Neumann 1943. godine ([122]) (za dokaze s topološkim prilazom i korišćenjem teorije grafova videti u [29] i [96]). Mi sledimo Gruškov, kako je već izložen u [92].

Prvo nekoliko napomena i definicija a zatim dosta posla.

Neka je data grupa $\mathbf{G}$ sa slobodnom dekompozicijom

$$\mathbf{G} = \mathbf{G}_1 * \cdots * \mathbf{G}_k \tag{1}$$

i skupom (sistemom) generatora

$$\overline{\mathcal{G}} = \{\overline{g}_1, \ldots, \overline{g}_n\} \tag{2};$$

dozvoljavamo mogućnost da nisu svi elementi generatornog skupa različiti kao i da je među njima eventualno jedinični element.

Ako se $h \in G$ može izraziti preko elemenata generatornog skupa $\overline{\mathcal{G}}$ sa $h = \overline{g}_{i_1}^{\alpha_1} \ldots \overline{g}_{i_m}^{\alpha_m}$ tako da se među elementima $\overline{g}_{i_1}, \ldots, \overline{g}_{i_m}$ ne javlja $\overline{g}_j$, onda su očigledno i $(\overline{\mathcal{G}} \setminus \{\overline{g}_j\}) \cup \{\overline{g}_j h\}$, $(\overline{\mathcal{G}} \setminus \{\overline{g}_j\}) \cup \{h\overline{g}_j\}$ i, vrlo očigledno, $(\overline{\mathcal{G}} \setminus \{\overline{g}_j\}) \cup \{\overline{g}_j^{-1}\}$ generatorni sistemi grupe $\mathbf{G}$.

U pitanju su Nielsenove transformacije koje upravo definišemo.

**Definicija 29.1** *Neka je dat skup elemenata grupe* $\mathbf{G}$ - $V = \{g_i \mid i \in I\}$. *Elementarne Nielsenove (J. Nielsen) transformacije na* $V$ *su transformacije oblika:*

$(T_1)$ *za neko (proizvoljno)* $i \in I$ *element* $g_i$ *se zamenjuje elementom* $g_i^{-1}$;

$(T_2)$ *za različite indekse* $i, j$ *iz* $I$ *element* $g_i$ *se zamenjuje elementom* $g_i g_j$;

$(T_3)$ *eliminiše se neki element* $g_i$ *ukoliko je ovaj jedinični element.*

*Nielsenove transformacije su konačni "proizvodi" elementarnih Nielsenovih transformacija. Nielsenova transformacija je regularna akko se u njoj ne javljaju transformacije* $(T_3)$, *inače je singularna.*



Jasno, ako je $T(V)$ skup dobijen od $V$ Nielsenovom transformacijom $T$, onda $T(V)$ i $V$ generišu istu podgrupu grupe $\mathbf{G}$. Isto tako je očigledno da regularne Nielsenove transformacije obrazuju grupu (s obzirom na kompoziciju transformacija). Mi ćemo se ovde pozabaviti singularnim transformacijama, jer nas prevashodno interesuje dužina sistema na koju ne utiču jedinični elementi.

Generatorni skup koji se dobija od polaznog - (2) - konačnom primenom datih transformacija zvaćemo *dopustivi* (eng. *admissible*) generatorni skup (sistem) s obzirom na (2). Dopustivi skup generatora je *minimalan* akko je zbir dužina njegovih elemenata, tzv. *dužina sistema*, jednaka ili manja od dužine svakog drugog dopustivog sistema.

**Definicija 29.2** *Neka je* $\mathcal{G} = \{g_1, \ldots, g_n\}$ *minimalni dopustiv sistem generatora s obzirom na* (2).

(*a*) *Element* $g_i$ *iz* $\mathcal{G}$ *dužine* $l$ *veće od* 1 *zove se specijalan akko u* $\mathcal{G}$ *postoje elementi* $g_j$ *i* $g_{i_1}, \ldots, g_{i_m}$ *i eksponenti* $\beta, \alpha_1, \ldots, \alpha_m \in \{1, -1\}$ *koji ispunjavaju sledeće uslove (podsećamo još jednom:* $l(g)$ *je dužina elementa s obzirom na fiksiranu slobodnu dekompoziciju* (1)*):*

$(i)$ $j \neq i$;

$(ii)$ $l(g_j) = l\ (= l(g_i))$;

$(iii)$ $l(g_{i_p}) < l$, $p = 1, \ldots, m$;

$(iv)$ $l(g_i \cdot \prod_{p=1}^m g_{i_p}^{\alpha_p} \cdot g_j^\beta) \leq l$;

$(v)$ $l(\prod_{p=1}^m g_{i_p}^{\alpha_p} \cdot g_j^\beta) = l$;

*i*

$(vi)$ $l(\prod_{p=1}^m g_{i_p}^{\alpha_p}) < l$.

(*b*) *Neka je za element* $g$ *dužine* $l$, $g = uvw$, *gde je* $u$ *leva i* $w$ *desna polovina, a* $v$ *sredina elementa* $g$ *(dakle,* $v = 1$ *ako je* $l$ *paran broj).* $g$ *je svodljiv (reducibilan) s obzirom na sistem* $\mathcal{G}$ *akko u* $\mathcal{G}$ *postoje elementi* $g_{i_1}, \ldots, g_{i_m}$ *i eksponenti* $\alpha_1, \ldots, \alpha_m$ *takvi da važi:*

$(i)$ $l(g_{i_r}) < l$, $r = 1, \ldots, m$

*i*

$(ii)$ $g \cdot \prod_{r=1}^m g_{i_r}^{\alpha_r} = uvu^{-1}$; *posebno,* $g \cdot \prod_{r=1}^m g_{i_r}^{\alpha_r} = 1$ *ako je* $l$ *paran broj.*

**Teorema 29.3** *Neka je* $\mathcal{G} = \{g_1, \ldots, g_n\}$ *minimalni dopustiv sistem generatora grupe* $\mathbf{G}$ *sa bar jednim elementom dužine veće od* 1. *Tada* $\mathcal{G}$ *ima nesvodljiv (ireducibilan) specijalni element.*

**Dokaz.** Pošto je $\mathcal{G}$ minimalni sistem generatora, nijedan od njegovih nejediničnih elemenata se ne može izraziti preko ostalih; jer, ako bi bilo npr. $l(g_j) \geq 1$ i $g_j = g_{i_1}^{\alpha_1} \ldots g_{i_r}^{\alpha_r}$, gde $j \notin \{i_1, \ldots, i_r\}$, tada bi sistem $\mathcal{G}_1 = (\mathcal{G} \setminus \{g_j\}) \cup \{g_j^{-1} \cdot \prod_{t=1}^r g_{i_t}^{\alpha_t}\}$ bio takođe dopustiv, no manje dužine: $l(g_j^{-1} \cdot \prod_{t=1}^r g_{i_t}^{\alpha_t}) = l(1) = 0$. Odatle pak dalje sledi da u (bar) jednom slobodnom faktoru grupe $\mathbf{G}$, recimo $\mathbf{G}_m$, postoji (bar) jedan element, recimo $a$, čije sve prezentacije

(izrazi) preko elemenata sistema $\mathcal{G}$ uključiju bar jedan element dužine veće od jedan; inače bi već elementi dužine 1 sistema $\mathcal{G}$ generisali celu grupu. Među svim izrazima koje daju element $a$ biramo prvo one u kojima su maksimalne dužine elemenata iz $\mathcal{G}$ što su moguće manje, među tako odabranim biramo dalje one u kojima se elementi maksimalnih dužina javljaju najmanji broj puta, zatim u nastavku izbor sužavamo na izraze u kojima se elementi dužine za jedan manji od maksimalnih javljaju najmanji broj puta itd. Neka je

$$a = g_{j_1}^{\alpha_1} \dots g_{j_t}^{\alpha_t}, \ \alpha_i \in \{1, -1\}, \ i = 1, \dots, t \tag{3}$$

jedan tako dobijeni izraz. Jasno, $t > 1$ jer je u izrazu bar jedan element dužine veće od 1 (a $l(a) = 1$). U cilju uprošćavanja notacije uvodimo, za $1 \leq r < s \leq t$:

$$[r, s] \stackrel{\text{def}}{=} g_{j_r}^{\alpha_r} g_{j_{r+1}}^{\alpha_{r+1}} \dots g_{j_s}^{\alpha_s};$$

naravno, $l([r, s]) = l(g_{j_r}^{\alpha_r} g_{j_{r+1}}^{\alpha_{r+1}} \dots g_{j_s}^{\alpha_s})$.

Nekoliko narednih lema se odnose na svojstva izraza $[r, s]$, a s poslednjom (29.11) sledi i dokaz teoreme.

**Lema 29.4** *Postoje indeksi $r, s$, $1 \leq r < s \leq t$, takvi da važi:*

*(a)* $l(g_{j_r}) = l([r, r+1]) = \dots = l([r, s-1]) > l([r, s])$;

*(b)* $l(g_{j_r}) \geq l(g_{j_i})$, $r < i \leq s$

*i*

*(c)* $l(g_{j_r}) \geq 2$.

**Dokaz**. Neka je $r$ indeks poslednjeg faktora izraza (3) takvog da je $l([1, r-1] \cdot g_{j_r}) = l([1, r]) > l([1, r-1])$. Tada je, za $r \leq i < t$, $l([1, i]) \geq l([1; i+1])$. Očigledno, $r$ ne može biti $t$; u suprotnom bismo imali: $l([1, t-1]) = 0$, tj. $[1, t-1] = 1$ (prazna reč), i odatle $a = g_{j_t}^{\alpha_t}$, opet protivurečno sa $l(a) = 1$ i pretpostavci o izrazima koji daju $a$. Biramo sada indeks $s$ za koji je: $l([1, r]) = l([1, r+1]) = \dots = l([1, s-1]) > l([1, s])$. Egzistencija takvog $s$ sledi iz činjenice da je $l([1, r]) \geq 2$ i $l([1, t]) = l(a) = 1$. Ne dolazi u obzir da je $l([1, r]) = 1$ jer bi to impliciralo $l([1, r-1]) = 0$, a ovo, s obzirom na izbor izraza (3), $r = 1$. No onda bi, prema izboru indeksa $r$, za svako $i$ $(1 \leq i \leq t)$ bilo $l([1, i]) = 1$, pa ako bi $g_{j_u}^{\alpha_u}$ bio prvi faktor dužine veće od 1, sistem $\mathcal{G}_1 = (\mathcal{G} \setminus \{g_{j_u}\}) \cup \{[1, u]\}$ bio bi takođe generatorni dopustivi sistem ali dužine manje od dužine sistema $\mathcal{G}$.

Prelazimo na dokaze svojstava $(a)$ i $(b)$. Neka je $l(g_{j_r}) = l$. Kako je $l([1, r-1]) < l([1, r]) = l([1, r-1] \cdot g_{j_r}^{\alpha_r})$, pri "množenju" $[1, r-1]$ sa $g_{j_r}^{\alpha_r}$ ili sredina elementa $g_{j_r}^{\alpha_r}$ ostaje "netaknuta" ili se, za parno $l$, leva polovina elementa $g_{j_r}^{\alpha_r}$ ne skraćuje sasvim. Pretpostavimo da je $l(g_{j_{r+1}}) > l$. Zbog upravo navedenog i činjenice da je $l([1, r+1]) = l([1, r-1] \cdot g_{j_r}^{\alpha_r} \cdot g_{j_{r+1}}^{\alpha_{r+1}}) \leq l([1, r-1] \cdot g_{j_r}^{\alpha_r}) = l([1, r])$ sledilo bi da se u proizvodu $g_{j_r}^{\alpha_r} \cdot g_{j_{r+1}}^{\alpha_{r+1}}$ "gubi" desna polovina i sredina elementa $g_{j_r}^{\alpha_r}$, odnosno za parno $l$ "načinje" se i



njegova leva polovina. Stoga bi bilo $l(g_{j_r}^{\alpha_r} \cdot g_{j_{r+1}}^{\alpha_{r+1}}) < l(g_{j_{r+1}})$, pa bi se zamenom u sistemu $\mathcal{G}$ elementa $g_{j_{r+1}}$ elementom $g_{j_r}^{\alpha_r} \cdot g_{j_{r+1}}^{\alpha_{r+1}} = [r, r+1]$ dobio sistem manje dužine, kontradikcija. Dakle, $l(g_{j_{r+1}}) \leq l$. Ako je $r+1 < s$, tada iz $l([1, r]) = l([1, r+1])$ sledi $l(g_{j_r}^{\alpha_r} \cdot g_{j_{r+1}}^{\alpha_{r+1}}) = l([r, r+1]) = l(g_{j_r}) = l$. Jednako tako se dobija da za $r+1 = s$ mora biti $l([r, r+1]) < l$. Dokaz dalje ide indukcijom (čiju smo prvu "stepenicu" upravo proverili). Pretpostavimo da je za $i$, $r < i < s$, $l([r, r+1]) = \dots = l([r, i]) = l$, $l(g_{j_u}) \leq l$ za $u = 1, \dots, i$, i da u proizvodu $[1, r-1] \cdot [r, i]$ sredina elementa $[r, i]$ ostaje netaknuta, odnosno da se, u slučaju da je $l$ parno, njegova leva polovina ne gubi sasvim. Onda rezonujući kao maločas pokazujemo da $l(g_{j_{i+1}}) > l$ vodi u protivurečnost. Ponovo zbog $l([1, i+1]) = l([1, r-1] \cdot [r, i] \cdot g_{j_{i+1}}^{\alpha_{i+1}}) \leq l([1, i]) = l([1, r-1] \cdot [r, i])$ imamo da se pri množenju $[r, i]$ sa $g_{j_{i+1}}^{\alpha_{i+1}}$ gubi desna polovina i sredina elementa $[r, i]$, odnosno, za parno $l$, i deo njegove leve polovine, što dalje znači i da je $l([r, i+1]) < l(g_{j_{i+1}})$. Pošto je $g_{j_{i+1}}^{\alpha_{i+1}}$ jedini faktor u $[r, i+1] = g_{j_r}^{\alpha_r} \cdot \dots \cdot g_{j_i}^{\alpha_i} \cdot g_{j_{i+1}}^{\alpha_{i+1}}$ dužine veće od $l$, to je $(\mathcal{G} \setminus \{g_{j_{i+1}}\}) \cup \{[r, i+1]\}$ dopustiv sistem dužine manje od dužine sistema $\mathcal{G}$, kontradikcija. Za $i+1 < s$, stoga i $l([1, i]) = l([1, i+1])$, dobija se takođe: $l = l([r, i]) = l([r, i+1])$, a elementi $[r, i]$ i $[r, i+1]$ imaju iste leve polovine; dakle sve gore navedene pretpostavke važe i za $i+1$. Ako je $i+1 = s$, tada $l([1, i]) > l([1, s])$ implicira da se pri množenju $[1, i]$ sa $g_{j_s}^{\alpha_s}$ skraćuje leva polovina i sredina elementa $g_{j_s}^{\alpha_s}$, te je i $l([r, s]) < l$. Sada proizilazi i da ne može biti $l = 1$; u suprotnom bi bilo $l([r, s]) = 0$, tj. $[r, s]$ bi bila prazna reč, što je protivurečno sa izborom izraza (3).□

Među svim proizvodima $[r', s']$, $[r', s']^{-1}$, $1 \leq r' < s' \leq t$, koji zadovoljavaju uslove prethodne leme biramo jedan – $[r, s]$ – sa najmanjim brojem faktora. Možemo takođe pretpostaviti, a i pretpostavićemo, da je izabrani proizvod $[r, s] = g_{j_r}^{\alpha_r} \dots g_{j_s}^{\alpha_s}$ ($\alpha_i \in \{1, -1\}$ za svako $i$) ujedno i proizvod sa najmanjim brojem faktora među svim proizvodima koje daju elementi sistema $\mathcal{G}$, a koji ispunjavaju uslove leme.

S notacijom iz prethodne leme nastavljamo priču.

**Lema 29.5** *Ako se element $g_i$ dužine $l$ javlja u proizvodu $[r, s]$, onda se javlja bar dva puta.*

**Dokaz**. Pretpostavimo da se element $g_i$ dužine $l$ javlja samo jedanput u proizvodu $[r, s]$. No tada je sistem $(\mathcal{G} \setminus \{g_i\}) \cup \{[r, s]\}$ dopustivi sistem dužine manje od dužine sistema $\mathcal{G}$ (jer je $l([r, s]) < l$), kontradikcija.□

**Lema 29.6** *Neka je $r \leq r' \leq s' \leq s$. Ako proizvod $[r', s']$ ne sadrži faktor dužine $l$, onda je $l([r', s']) < l$. Ako pak proizvod $[r', s']$ sadrži faktore dužine $l$ i ako je $s' < s$, tada je $l([r', s']) = l$.*

**Dokaz**. Indukcijom po broju faktora. Slučaj $r' = s'$ je trivijalan. Pretpostavimo da tvrđenje važi za sve proizvode $[r'', s'']$ sa manje faktora od $[r', s']$. Razmatramo sve moguće slučajeve.

*I* $l([r',s'-1]) < l,\ l(g_{j_{s'}}) < l,\ s' \leq s.$

Kako je $l([r,r'-1]) = l([r,s'-1]) = l$ (uslov $(a)$ leme 29.4), u proizvodu $[r,r'-1]\cdot[r',s'-1]$ $(=[r,s'-1])$ desna polovina elementa $[r',s'-1]$ ostaje nepromenjena. Zbog toga kao i zbog $l([r,s']) \leq l$ i $l(g_{j_{s'}}) < l$, u proizvodu $[r,r'-1]\cdot[r',s'-1]\cdot g_{j_{s'}}^{\alpha_{s'}}$ $(=[r,s'])$, pri množenju $[r',s'-1]$ sa $g_{j_{s'}}^{\alpha_{s'}}$ ili se gubi desna polovina elementa $[r',s'-1]$ ili leva polovina elementa $g_{j_{s'}}^{\alpha_{s'}}$, dok se sredina korespondentnog faktora u najmanju ruku amalgamira. Odatle: $l([r',s']) \leq max\{\, l([r',s'-1]), l(g_{j_{s'}}^{\alpha_{s'}})\} < l.$

*II* $l([r',s'-1]) = l,\ l(g_{j_{s'}}) < l,\ s' < s.$

Kao i maločas, u proizvodu $[r,r'-1]\cdot[r',s'-1]$ desna polovina elementa $[r',s'-1]$ ostaje nepromenjena. Stoga i s obzirom da je $l([r,s']) = l([r,r'-1]\cdot[r',s'-1]\cdot g_{j_{s'}}^{\alpha_{s'}}) = l$ i $l(g_{j_{s'}}) < l$, proizilazi da se u proizvodu $[r',s'-1]\cdot g_{j_{s'}}^{\alpha_{s'}}$ gubi leva polovina elementa $g_{j_{s'}}^{\alpha_{s'}}$, dok mu se sredina amalgamira, pa je i $l([r',s']) = l$.

*III* $l([r',s'-1]) < l,\ l(g_{j_{s'}}) = l,\ s' < s.$

Iz $[r,s'] = [r,r'-1]\cdot[r',s'-1]\cdot g_{j_{s'}}^{\alpha_{s'}}$ $(=[r,r'-1]\cdot[r',s'])$ i $l([r,r'-1]) = l([r,s'-1]) = l([r,s']) = l$ sledi $l([r',s']) \leq l$. Jer, kao i u prethodnim slučajevima, u proizvodu $[r,r'-1]\cdot[r',s'-1]$ desna polovina elementa $[r',s'-1]$ ostaje nepromenjena, dok se sredina, ukoliko već nije prazna reč, amalgamira, pa se u proizvodu $[r',s'-1]\cdot g_{j_{s'}}^{\alpha_{s'}}$ (zbog $l([r,s']) = l$) sigurno poništava desna polovina i sredina elementa $[r',s'-1]$. Ali ne može biti $l([r',s']) < l$; u tom bismo slučaju, pošto je $g_{j_{s'}}$ jedini element dužine $l$ u $[r',s']$ (u $[r',s'-1]$ nemamo po induktivnoj pretpostavci faktor dužine $l$), mogli dobiti dopustivi sistem dužine manje od dužine sistema $\mathcal{G}$.

*IV* $l([r',s'-1]) = l,\ l(g_{j_{s'}}) = l,\ s' < s.$

$l([r,r'-1]) = l([r,s'-1]) = l([r,s']) = l$ implicira $l([r',s']) = l([r',s'-1]\cdot g_{j_{s'}}^{\alpha_{s'}}) \leq l$. Pretpostavimo: $l([r',s']) < l$. Prema induktivnoj hipotezi (i uslovu $l(g_{j_{s'}}) = l$), za svako $r''$ "između" $r'$ i $s'$ $(r' < r'' < s')$ važi $l([r'',s']) = l$, te proizvod $[r',s']^{-1} = g_{j_{s'}}^{-\alpha_{s'}}\cdot[r',s'-1]^{-1}$ ispunjava sve uslove leme 29.4, a ima manji broj faktora od proizvoda $[r,s]$, suprotno izboru proizvoda $[r,s]$.□

**Lema 29.7** $l(g_{j_s}) = l.$

**Dokaz.** Neka je $l(g_{j_s}) < l$ i neka je $g_{j_q}^{\alpha_q}$ poslednji faktor dužine $l$ proizvoda $[r,s]$. Iz $l([r,q-1]) = l([r,q]) = l(g_{j_q}) = l$ sledi da elementi $[r,q]$ i $g_{j_q}^{\alpha_q}$ imaju iste desne strane. Prema prethodnoj lemi je, za $q < u \leq s$, $l([q+1,u]) < l$. Za $q < u < s$ je, znamo, $l([r,u]) = l$, pa je, s obzirom da $[r,q]$ i $g_{j_q}^{\alpha_q}$ imaju iste desne strane, i $l([q,u]) = l$ (uostalom i ovaj rezultat direktno proizilazi iz prethodne leme). No tada proizvod $[q,s]$ ispunjava sve uslove leme 29.4, dok sadrži samo jedan element dužine $l$, protivurečno lemi 29.5.□

**Lema 29.8** *Bar jedan od faktora* $g_{j_q}^{\alpha_q}$, $r < q < s$, *je dužine* $l$.



**Dokaz.** Pretpostavimo da su faktori $g_{j_q}^{\alpha_q}$ dužine manje od $l$ za $r < q < s$. Tada su, prema lemi 29.5, elementi $g_{j_r}$ i $g_{j_s}$ jednaki, a prema lemi 29.6 je $l([r+1,s-1]) < l$. Kako je $l([r,s-1]) = l$ sledi: ako je $g_{j_r}^{\alpha_r} = uvw$, gde su $u$ i $w$, respektivno, leva i desna polovina a $v$ sredina elementa $g_{j_r}^{\alpha_r}$, onda je $[r,s-1] = uvw'$. Diskutujemo sada mogućnosti: *I* $\alpha_r = -\alpha_s$ i *II* $\alpha_r = \alpha_s$. U prvom slučaju je $g_{j_s}^{\alpha_s} = w^{-1}v^{-1}u^{-1}$, te je, zbog $l(r,s]) = l([r,s-1]\cdot g_{j_s}^{\alpha_s}) < l$, $w'w^{-1}$ prazna reč, a tada je i $[r,s] = 1$, kontradiktorno pretpostavci o izboru proizvoda (3). U drugom slučaju je $w'u = v^2 = 1$ i $[r,s] = uw$. Pošto je $w' = w\cdot[r+1,s-1]$, to je $u = [r+1,s-1]^{-1}w^{-1}$ i $[r,s] = ([r+1,s-1]^{-1}w^{-1})vw)\cdot[r+1,s-1]\cdot(([r+1,s-1]^{-1}w^{-1})vw) = [r+1,s-1]^{-1}$, opet kontradiktorno s pretpostavkom o (3) (taj proizvod bi se mogao zameniti kraćim dobijenim od njega zamenom $[r,s]$ sa $[r+1,s-1]^{-1}$).□

Za nastavak će nam trebati i ova "međulema".

**Lema 29.9** $(a)$ *Neka je* $g$ *reducibilan element s obzirom na sistem* $\mathcal{G}$ *i, za* $g_i \in \mathcal{G}$, $l(g_i^\alpha) < l(g)$ *i* $l(g\cdot g_i^\alpha) = l(g)$. *Tada je i* $g\cdot g_i^\alpha$ *reducibilan element s obzirom na* $\mathcal{G}$. *Isto tako iz* $l(g_i^\alpha\cdot g) = l(g)$ *sledi da je* $g_i^\alpha\cdot g$ *reducibilan element.*

$(b)$ *Ako je* $l(g) = l(h) = l(g\cdot h)$ *za reducibilne elemente* $g$ *i* $h$, *onda je i* $g\cdot h$ *reducibilan element.*

**Dokaz.** $(a)$ Neka je $g = uvw$ i neka je, za elemente $g_{i_1},\ldots,g_{i_m}$ sistema $\mathcal{G}$ dužine manje od dužine elementa $g$ i eksponente $\alpha_1,\ldots,\alpha_m$, $g\cdot\prod_{p=1}^m g_{i_p}^{\alpha_p} = uvu^{-1}$. Zbog $l(g_i^\alpha) < l(g)$ i $l(g\cdot g_i^\alpha) = l(g)$, $g\cdot g_i^\alpha$ je oblika $uvw'$, a $(g\cdot g_i^\alpha)\cdot(g_i^{-\alpha}\cdot\prod_{p=1}^m g_{i_p}^{\alpha_p}) = uvu^{-1}$.

Kada je u pitanju reducibilnost elementa $g_i^\alpha\cdot g$ (uz date uslove, naravno), konstatujmo prvo da je $g^{-1} = w^{-1}v^{-1}u^{-1}$ takođe reducibilan element. Zaista, iz $g\cdot\prod_{p=1}^m g_{i_p}^{\alpha_p} = uvw\cdot\prod_{p=1}^m g_{i_p}^{\alpha_p} = uvu^{-1}$ proizilazi: $(\prod_{p=1}^m g_{i_p}^{\alpha_p})^{-1} = uw$. Odatle $g^{-1}\cdot(\prod_{p=1}^m g_{i_p}^{\alpha_p})^{-1} = w^{-1}v^{-1}u^{-1}\cdot uw = w^{-1}v^{-1}w$. Prema prethodnom je $g^{-1}\cdot g_i^{-\alpha}$ reducibilan element, a onda je i $g_i^\alpha\cdot g$ reducibilan element.

$(b)$ Neka je $g = uvw$. Prema datim uslovima je $h = w^{-1}v'z$ i $g\cdot h = u(vv')z$, gde su $v$ i $v'$ elementi istog slobodnog faktora i $vv' \neq 1$, ukoliko se radi o neparnoj dužini elemenata $g$ i $h$. Ako je $g\cdot\prod_{j=1}^{m_1} g_{i_j}^{\alpha_j} = uvu^{-1}$ i $h\cdot\prod_{k=1}^{m_2} g_{l_k}^{\beta_k} = w^{-1}v'w$, tada je $gh\cdot(\prod_{k=1}^{m_2} g_{l_k}^{\beta_k}\cdot\prod_{j=1}^{m_1} g_{i_j}^{\alpha_j}) = g\cdot(h\cdot\prod_{k=1}^{m_2} g_{l_k}^{\beta_k})\cdot\prod_{j=1}^{m_1} g_{i_j}^{\alpha_j} = uvw\cdot w^{-1}v'w\cdot w^{-1}u^{-1} = u(vv')u^{-1}$.□

**Lema 29.10** *Bar jedan od faktora dužine* $l$ *proizvoda* $[r,s]$ *je ireducibilan.*

**Dokaz.** Ako je $l$ paran broj, slučaj je jasan; generalno, u sistemu $\mathcal{G}$ kao minimalnom ne može biti reducibilnih elemenata parne dužine.

Neka je $l$ neparan broj i pretpostavimo da su svi faktori $g_{j_q}$, $r < q < s$, dužine $l$ (a takvih ima prema lemi 29.8) reducibilni. Prema prethodnoj lemi i

lemi 29.6, $[r+1, s-1]$ je reducibilan element dužine $l$. Neka je $[r+1, s-1] = uvw$ i $[r+1, s-1] \cdot \prod_p g_{i_p}^{\beta_p} = uvu^{-1}$, dakle, $u \cdot w = (\prod_p g_{i_p}^{\beta_p})^{-1}$. Tada je $g_{j_r}^{\alpha_r} = u_1 v_1 u^{-1}$, $g_{j_s}^{\alpha_s} = w^{-1} v_2 w_2$ i zbog $l([r,s]) < l$, $v_1 \cdot v \cdot v_2 = 1$ i $[r,s] = u_1 \cdot w_2$. Recimo da su i elementi $g_{j_r}^{\alpha_r}$ i $g_{j_s}^{\alpha_s}$ reducibilni i neka je $g_{j_r}^{\alpha_r} \cdot \prod_q g_{l_q}^{\gamma_q} = u_1 v_1 u_1^{-1}$, $g_{j_s}^{\alpha_s} \cdot \prod_m g_{h_m}^{\delta_m} = w^{-1} v_2 w$, a onda i $u^{-1} \cdot \prod_q g_{l_q}^{\gamma_q} = u_1^{-1}$, $w_2 \cdot \prod_m g_{h_m}^{\delta_m} = w$. Prema tome, $[r,s] = u_1 \cdot w_2 = (\prod_q g_{l_q}^{\gamma_q})^{-1} \cdot u \cdot w \cdot (\prod_m g_{h_m}^{\delta_m})^{-1} = (\prod_q g_{l_q}^{\gamma_q})^{-1} \cdot (\prod_p g_{i_p}^{\beta_p})^{-1} \cdot (\prod_m g_{h_m}^{\delta_m})^{-1}$, što će reći da se element $[r,s]$ može izraziti preko elemenata sistema $\mathcal{G}$, svi dužine manje od $l$, kontradiktorno sa pretpostavkom o izrazu (3). Ako je bar jedan od elemenata $g_{j_r}^{\alpha_r}$, $g_{j_s}^{\alpha_s}$ ireducibilan, prema 29.5 elementi $g_{j_r}$ i $g_{j_s}$ su jednaki. Ako je $\alpha_r = \alpha_s$, onda je $u_1 = w^{-1}$, $w_2 = u^{-1}$ i stoga $[r,s] = u_1 \cdot w_2 = w^{-1} \cdot u^{-1} = (u \cdot w)^{-1} = \prod_p g_{i_p}^{\beta_p}$. Ako je $\alpha_r = -\alpha_s$, tada je $u_1 = w_2^{-1}$ i $[r,s] = 1$. Kako bilo, dobijamo ponovo kontradikciju s pretpostavkom o izboru izraza (3).□

**Lema 29.11** *Svaki nesvodljiv element dužine $l$ - $g_{j_p}$, $r < p < s$, specijalan je.*

**Dokaz**. Razmotrimo slučajeve: *I* $\alpha_p = 1$ i *II* $\alpha_p = -1$.

*I* Neka je $g_{j_q}^{\alpha_q}$, $p < q \leq s$, prvi element desno od $g_{j_p}$ u proizvodu $[r,s]$ dužine $l$. Uz pomoć proizvoda $[p,q]$ pokazujemo da je $g_{j_p}$ specijalan element. Uslovi $(ii)$ i $(iii)$ (definicije 29.2) su očigledno ispunjeni, a za $q < s$, prema lemi 29.6, važe i uslovi $(iv)$, $(v)$ i $(vi)$. Ako je $q = s$, uslov $(vi)$ ponovo nije sporan (prema istoj lemi). Što se tiče uslova $(iv)$ primetimo da elementi dužine $l$ $[r, s-1]$ $(= [r, p-1] \cdot [p, s-1]$ i $[p, s-1]$ imaju iste desne polovine dok njihove sredine, u slučaju neparne dužine $l$, pripadaju istom slobodnom faktoru i nisu uzajamno inverzni elementi. Pretpostavimo da je $l$ neparan broj kao i da je proizvod $[p+1, s-1]$ neparne dužine. Neka je $g_{j_p} = u_1 a w_1$, $\prod_{m=p+1}^{s-1} g_{j_m}^{\alpha_m} = u_2 b w_2$ i $g_{j_s}^{\alpha_s} = u_3 c w_3$. Zbog $l([r, s-1]) = l(g_{j_p} \cdot [p+1, s-1]) = l$ je $w_1 = z_1 d u_2^{-1}$, gde $d$ i $b$ pripadaju istom slobodnom faktoru i nisu uzajamno inverzni elementi. Dakle, $[p, s-1] = u_1 a z_1 (db) w_2$, pa je $u_3 = (z_1 (db) w_2)^{-1}$. Odatle, $[p+1, s] = [p+1, s-1] \cdot g_{j_s}^{\alpha_s} = u_2 b w_2 \cdot (w_2^{-1} (b^{-1} d^{-1}) z_1^{-1}) c w_3 = u_2 d^{-1} (z_1^{-1} c w_3)$; znači, $l([p+1, s]) = l$. Element $[p, s] = [p, s-1] \cdot g_{j_s}^{\alpha_s} = u_1 a (z_1 (db) w_2) \cdot (w_2^{-1} (db)^{-1} z_1^{-1}) c w_3 = u_1 (ac) w_3$ dužine je manje od ili jednake $l$, jer $a$ i $c$ pripadaju istom slobodnom faktoru (s obzirom da je $[r, s] = [r, s-1] \cdot g_{j_s}^{\alpha_s}$ dužine manje od $l$, sredina elementa $[r, s-1]$ i $g_{j_s}^{\alpha_s}$ pripadaju istom slobodnom faktoru i uzajamno su inverzni elementi). Analogno bismo diskutovali i ostale slučajeve.

Pokažimo i da je $j_p \neq j_q$. Pretpostavimo suprotno. Ako je $\alpha_q = 1$ $(= \alpha_p)$ i, recimo, $g_{j_p} = g_{j_q} = uvw$, gde je $v$ eventualno 1, onda zbog $l([p,q]) = l(g_{j_p} \cdot \prod_{m=p+1}^{q-1} g_{j_m}^{\alpha_m} \cdot g_{j_p}) = l(uvw \cdot \prod_{m=p+1}^{q-1} g_{j_m}^{\alpha_m} \cdot uvw) \leq l$ i $l([p, q-1]) = l(uvw \cdot \prod_{m=p+1}^{q-1} g_{j_m}^{\alpha_m}) = l$, sledi: $w \cdot \prod_{m=p+1}^{q-1} g_{j_m}^{\alpha_m} = u^{-1}$ $(w \cdot \prod_{m=p+1}^{q-1} g_{j_m}^{\alpha_m}$ je desna



polovina proizvoda $[p, q-1]$) i dalje, $g_{j_p} \cdot \prod_{m=p+1}^{q-1} g_{j_m}^{\alpha_m} = uvw \cdot \prod_{m=p+1}^{q-1} g_{j_m}^{\alpha_m} = uvu^{-1}$, suprotno pretpostavci da je $g_{j_p}$ ireducibilan element. Ako je $\alpha_q = -1$ (što za $q = p+1$ odmah daje $j_p \neq j_q$), tada, ponovo zbog $l([p,q]) = l(uvw \cdot \prod_{m=p+1}^{q-1} g_{j_m}^{\alpha_m} \cdot w^{-1} v^{-1} u^{-1}) \leq l$, sledi: $w \cdot \prod_{m=p+1}^{q-1} g_{j_m}^{\alpha_m} = w$, tj. $\prod_{m=p+1}^{q-1} g_{j_m}^{\alpha_m} = 1$, kontradiktorno sa pretpostavkama o izrazu (3).

Ako je pak $\alpha_p = -1$, nalazimo prvi element $g_{j_q}^{\alpha_q}$ dužine $l$ levo od $g_{j_p}^{-1}$ u proizvodu $[r,s]$ i u osnovi ponavljamo gornje razmatranje.□■

**Teorema 29.12** *(Gruško-Neumannova teorema). Svaki element ma kog minimalnog generatornog sistema grupe $\mathbf{G} = \mathbf{G}_1 * \cdots * \mathbf{G}_k$, dopustivog s obzirom na skup generatora $\overline{\mathcal{G}} = \{\overline{g}_1, \ldots, \overline{g}_n\}$, sadržan je u nekom slobodnom faktoru.*

**Dokaz**. Neka je $\mathcal{G} = \{g_1, \ldots, g_n\}$ minimalni dopustiv sistem generatora s obzirom na $\overline{\mathcal{G}}$. Pretpostavimo da sistem $\mathcal{G}$ sadrži (bar jedan) element dužine (s obzirom na dato razlaganje grupe u slobodni proizvod) veće od 1. Onda prema prethodnoj teoremi $\mathcal{G}$ sadrži i ireducibilan specijalan element. Neka je $g_i = uvw$ jedan od njih najmanje dužine - $l$, i neka su $g_j, g_{i_1}, \ldots, g_{i_m}$ i $\beta, \alpha_1, \ldots, \alpha_m$, respektivno, elementi i eksponenti odgovarajućih elemenata koji ispunjavaju uslove $(i)$ - $(vi)$ definicije 29.2$(a)$ (za element $g_i$). Prema $(iv)$ i $(v)$ element $\overline{g} = \prod_{p=1}^{m} g_{i_p}^{\alpha_p} \cdot g_j^{\beta}$ je oblika $w^{-1} v' w_1$, gde su $v$ i $v'$ elementi istog slobodnog faktora ili su, eventualno, oba jednaka 1. Ako je $\overline{g}$ ireducibilan element, neka je

$$g_j' = g_i \cdot \overline{g} = u \cdot (vv') w_1;$$

ako je pak $\overline{g}$ reducibilan element i $\overline{g} \cdot \prod_q g_{j_q}^{\gamma_q} = w^{-1} v' w$, gde je $l(g_{j_q}) < l$ za svako $q$, uzimamo da je

$$g_j' = g_i \cdot \overline{g} \cdot \prod_q g_{j_q}^{\gamma_q} \cdot g_i^{-1} = uvw \cdot w^{-1} v' w \cdot w^{-1} v^{-1} u^{-1} = u(vv'v^{-1}) u^{-1}.$$

Prema uslovima $(ii)$ i $(iii)$ definicije 29.2, element $g_j$ se može izraziti preko $g_j'$ i elemenata sistema $\mathcal{G} \setminus \{g_j\}$. Primetimo da je u slučaju reducibilnosti elementa $\overline{g}$, $l$ svakako neparan broj (u suprotnom bi $g_j'$ bio prazna reč, a element $g_j$ bi se mogao izraziti preko ostalih elemenata sistema $\mathcal{G}$). Znači i $\mathcal{G}' = (\mathcal{G} \setminus \{g_j\}) \cup \{g_j'\}$ je generatorni i to dopustiv minimalan sistem generatora; posebno, $l(g_j') = l$. Jer na primer, ako je $\overline{g}$ reducibilan element, dakle ako je $g_j' = g_i \cdot \prod_{p=1}^{m} g_{i_p}^{\alpha_p} \cdot g_j^{\beta} \cdot \prod_q g_{j_q}^{\gamma_q} \cdot g_i^{-1}$ i, recimo, $\beta = -1$, tada od $\mathcal{G}$ dobijamo redom dopustive skupove (imamo u vidu da je $l(\prod_{p=1}^{m} g_{i_p}^{\alpha_p} \cdot g_j^{-1}) = l$):

$\mathcal{G}_1 = (\mathcal{G} \setminus \{g_j\}) \cup \{g_j^{-1}\}$,
$\mathcal{G}_2 = (\mathcal{G}_1 \setminus \{g_j^{-1}\}) \cup \{\prod_{p=1}^{m} g_{i_p}^{\alpha_p} \cdot g_j^{-1}\}$,
$\mathcal{G}_3 = (\mathcal{G}_2 \setminus \{\prod_{p=1}^{m} g_{i_p}^{\alpha_p} \cdot g_j^{-1}\}) \cup \{(\prod_{p=1}^{m} g_{i_p}^{\alpha_p} \cdot g_j^{-1}) \cdot \prod_q g_{j_q}^{\gamma_q}\}$,
$\mathcal{G}_4 = (\mathcal{G}_3 \setminus \{\prod_{p=1}^{m} g_{i_p}^{\alpha_p} \cdot g_j^{-1} \cdot \prod_q g_{j_q}^{\gamma_q}\}) \cup \{g_i \cdot (\prod_{p=1}^{m} g_{i_p}^{\alpha_p} \cdot g_j^{-1} \cdot \prod_q g_{j_q}^{\gamma_q})\}$,

$\mathcal{G}' = \mathcal{G}_5 = (\mathcal{G}_4 \setminus \{g_i \cdot \prod_{p=1}^m g_{i_p}^{\alpha_p} \cdot g_j^{-1} \cdot \prod_q g_{j_q}^{\gamma_q}\}) \cup \{(g_i \cdot \prod_{p=1}^m g_{i_p}^{\alpha_p} \cdot g_j^{-1} \cdot \prod_q g_{j_q}^{\gamma_q}) \cdot g_i^{-1}\}$.

Ako na isti način zamenimo u sistemu $\mathcal{G}$ sve elemente koji mogu imati istu ulogu kao i $g_j$ u definiciji specijalnog elementa za $g_i$, onda u novodobijenom sistemu $\mathcal{G}''$ $g_i$ više nije specijalan element. Zaista, pretpostavimo da su za $g_j'$ i neke elemente $g_{l_z}$ dužine manje od $l$ ispunjeni uslovi definicije 29.2 za element $g_i$. Tada je, kao i ranije, s obzirom na uslove $(iv)$ i $(v)$, za neke eksponente $\delta$ i $\epsilon_z$, $\prod_z g_{l_z}^{\epsilon_z} \cdot (g_j')^{\delta} = w^{-1}v''w_2$, gde $v$ i $v''$ pripadaju istom slobodnom faktoru. Ako je $\overline{g}$ ireducibilan i $\delta = 1$ ili ako je $\overline{g}$ reducibilan i $\delta = \pm 1$, onda je $u$ leva polovina elementa $(g_j')^{\delta}$ i $\prod_z g_{l_z}^{\epsilon_z} \cdot u = w^{-1}$ (jer je $l(\prod_z g_{l_z}^{\epsilon_z}) < l = l((g_j')^{\delta}) = l(\prod_z g_{l_z}^{\epsilon_z} \cdot (g_j')^{\delta})$). Odatle, $w \cdot \prod_z g_{l_z}^{\epsilon_z} = u^{-1}$, dakle i $g_i \cdot \prod_z g_{l_z}^{\epsilon_z} = uvw \cdot \prod_z g_{l_z}^{\epsilon_z} = uvu^{-1}$, suprotno pretpostavci da je $g_i$ nesvodljiv element. Preostaje, znači, slučaj: $\overline{g}$ je ireducibilan element i $\delta = -1$. No tada $\prod_z g_{l_z}^{\epsilon_z} \cdot (g_j')^{-1} = \prod_z g_{l_z}^{\epsilon_z} \cdot w_1^{-1}(vv')u^{-1} = w^{-1}v''w_2$ daje: $\prod_z g_{l_z}^{\epsilon_z} \cdot w_1^{-1} = w^{-1}$, tj. $w = w_1 \cdot (\prod_z g_{l_z}^{\epsilon_z})^{-1}$, te sledi $w^{-1}v'w = w^{-1}v'w_1 \cdot (\prod_z g_{l_z}^{\epsilon_z})^{-1} = \overline{g} \cdot (\prod_z g_{l_z}^{\epsilon_z})^{-1}$; dakle, $\overline{g}$ je reducibilan element, kontradikcija ponovo.

Pokazujemo dalje da u sistemu $\mathcal{G}'$, pa onda i u sistemu $\mathcal{G}''$, nema novih ireducibilnih specijalnih elemenata dužine $l$ (možda smo samo neke nesvodljive specijalne elemente zamenili opet takvima). Jasno, elementi dužine $l$ koji su reducibilni u $\mathcal{G}$ reducibilni su i u sistemu $\mathcal{G}'$; elementi koji "dokazuju" njihovu nesvodljivost su dužine manje od $l$, te su zajednički za oba sistema.

Pretpostavimo prvo da je $g_j'$ specijalan element. Pokazaćemo i da je $g_j$ specijalan element.

Ako je $\overline{g} = \prod_{p=1}^m g_{i_p}^{\alpha_p} \cdot g_j^{\beta}$ ireducibilan element i $\beta = -1$, tada $(g_j')^{-1} = (g_i \cdot \overline{g})^{-1} = g_j \cdot (\prod_{p=1}^m g_{i_p}^{\alpha_p})^{-1} \cdot g_i^{-1}$ i $l(g_j') = l$ impliciraju da je $g_j$ specijalan element. Odista, sem možda petog uslova – $l((\prod_{p=1}^m g_{i_p}^{\alpha_p})^{-1} \cdot g_i^{-1}) = l$, svi ostali uslovi (definicije 29.2) su evidentno ispunjeni. Odstupajući za moment od već uvedene notacije, stavimo: $g_i = uvw$, $\prod_{p=1}^m g_{i_p}^{\alpha_p} = u_1v_1w_1$ i $g_j^{-1} = u_2v_2w_2$. Iz $l(g_i\overline{g}) = l = l(g_j^{-1})$ i $l(\prod_{p=1}^m g_{i_p}^{\alpha_p}) < l$ sledi $\prod_{p=1}^m g_{i_p}^{\alpha_p} \cdot g_j^{-1} = w^{-1}v_2w_2$, zapravo $\prod_{p=1}^m g_{i_p}^{\alpha_p} \cdot u_2 = w^{-1}$ ($v$ i $v_2$ pripadaju istom slobodnom faktoru i ukoliko nisu oba 1, nisu ni uzajamno inverzni elementi). Stoga je $w \cdot \prod_{p=1}^m g_{i_p}^{\alpha_p} = u_2^{-1}$, pa je $g_i \cdot \prod_{p=1}^m g_{i_p}^{\alpha_p} = uvu_2^{-1}$ i $l(g_i \cdot \prod_{p=1}^m g_{i_p}^{\alpha_p}) = l((\prod_{p=1}^m g_{i_p}^{\alpha_p})^{-1} \cdot g_i^{-1}) = l$. Ako je pak $\beta = 1$, $g_j$ i $g_j'$ imaju iste desne polovine a sredine im pripadaju istom slobodnom faktoru (ukoliko već nisu prazna reč), te je, očigledno, i $g_j$ specijalan element.

Pretpostavimo sada da je $\overline{g}$ reducibilan element. Tada je, podsećamo, $l(g_j') = l(g_i \cdot \prod_{p=1}^m g_{i_p}^{\alpha_p} \cdot g_j^{\beta} \cdot \prod_q g_{j_q}^{\gamma_q} \cdot g_i^{-1}) = l$, $l(g_i \cdot \prod_{p=1}^m g_{i_p}^{\alpha_p} \cdot g_j^{\beta}) \leq l$ nam je već dato, a važi i $l(g_j^{\beta} \cdot \prod_q g_{j_q}^{\gamma_q} \cdot g_i^{-1}) \leq l$. Opet za ovu priliku stavimo, nezavisno od ranije notacije: $g_i = uvw$, $\overline{g} = \prod_{p=1}^m g_{i_p}^{\alpha_p} \cdot g_j^{\beta} = u_1v_1w_1$, $g_j^{\beta} = u_2v_1w_1$ (elementi $\overline{g}$ i $g_j^{\beta}$ imaju iste sredine i desne polovine zbog $l(\prod_{p=1}^m g_{i_p}^{\alpha_p}) < l = l(g_j^{\beta})$). Kako je $\overline{g} \cdot \prod_q g_{j_q}^{\gamma_q} = u_1v_1u_1^{-1}$, tj. $v_1w_1 \cdot \prod_q g_{j_q}^{\gamma_q} = v_1u_1^{-1}$, to je i $u_2v_1w_1 \cdot \prod_q g_{j_q}^{\gamma_q} = g_j^{\beta} \cdot \prod_q g_{j_q}^{\gamma_q} = u_2v_1u_1^{-1}$. Dalje, zbog $l(g_i \cdot \overline{g}) \leq l$, mora biti $u_1^{-1} = w$, dok $v$ i $v_1$ pripadaju istom slobodnom faktoru. Odatle, $l(g_j^{\beta} \cdot \prod_q g_{j_q}^{\gamma_q} \cdot g_i^{-1}) = l(u_2v_1u_1^{-1} \cdot w^{-1}v^{-1}u^{-1}) = l(u_2(v_1v^{-1})u^{-1}) \leq l$. Prva od datih nejednačina nam pokazuje da je $g_j$ specijalan element kada je $\beta = -1$, druga kada je $\beta = 1$, jer su i ostali uslovi definicije ispunjeni. Ako je $\beta = -1$ i $\prod_{p=1}^m g_{i_p}^{\alpha_p} = u_3v_3w_3$, onda $u_1v_1w_1 = \overline{g} = \prod_{p=1}^m g_{i_p}^{\alpha_p} \cdot g_j^{-1} = u_3v_3w_3 \cdot u_2v_1w_1$ povlači $\prod_{p=1}^m g_{i_p}^{\alpha_p} \cdot u_2 = u_1 = w^{-1}$, tj. $\prod_{p=1}^m g_{i_p}^{\alpha_p} = w^{-1} \cdot u_2^{-1}$, pa je $l(g_i \cdot \prod_{p=1}^m g_{i_p}^{\alpha_p}) = l(uvw \cdot w^{-1}u_2^{-1}) = l(uvu_2^{-1}) = l$, pošto, ponavljamo, $v$ i $v_1$ pripadaju istom slobodnom faktoru. Slično rezonujemo i u drugom slučaju. Konstatujmo samo da $l(\prod_q g_{j_q}^{\gamma_q}) < l$ proizilazi iz neparnosti broja $l$ i činjenice da je $\overline{g} \cdot \prod_q g_{j_q}^{\gamma_q} = u_1v_1u_1^{-1}$.



Pretpostavimo konačno da je neki element dužine $l - g_h$, $h \neq i, j$, koji nije bio specijalan u sistemu $\mathcal{G}$, postao takvim u $\mathcal{G}''$. To bi značilo da je, za neki element $g_j'$ dužine $l$ i neke elemente $g_{h_z}$ dužine manje od $l$, kao i odgovarajuće eksponente $\theta$, $\rho_z$: $l(g_h \cdot \prod_z g_{h_z}^{\rho_z} \cdot (g_j')^{\theta}) \leq l$, $l(\prod_z g_{h_z}^{\rho_z} \cdot (g_j')^{\theta}) = l$ i $l(\prod_z g_{h_z}^{\rho_z}) < l$. No ako je $\theta = 1$ i $\overline{g}$ ireducibilan element ili ako je $\theta = \pm 1$ i $\overline{g}$ reducibilan element, element $(g_j')^{\theta}$ bi se mogao zameniti elementom $g_i$ (u tim slučajevima elementi $(g_j')^{\theta}$ i $g_i$ imaju iste leve polovine), a ako je $\theta = -1$ i $\overline{g}$ ireducibilan element, onda elementom $g_j^{-1}$; kako bilo, ispada da je $g_h$ specijalan element i sistema $\mathcal{G}$, suprotno pretpostavci.

Sumiramo. Transformacijama navedenog tipa sistem $\mathcal{G}$ se prevodi u dopustiv sistem iste dužine koji ima element dužine veće od 1, no manje specijalnih ireducibilnih elemenata dužine $l$. Na kraju će se svi takvi "izgubiti", pa ostaju eventualno ireducibilni specijalni elementi dužine veće od $l$ ($l$ je, ne zaboravimo, bila dužina "najkraćih" specijalnih ireducibilnih elemenata sistema $\mathcal{G}$). No u konačno mnogo koraka, sve ponavljajući postupak, došli bismo do dopustivog sistema minimalne dužine u kome bi bio (bar jedan) element dužine veće od 1 i ne bi bilo specijalnih ireducibilnih elemenata, kontradiktorno prethodnoj teoremi.■

Sledeću teoremu, inače vrlo važan rezultat u kombinatornoj teoriji grupa, dajemo ovde bez dokaza (koji je opet kombinatorne prirode), a koristićemo je samo u narednoj lemi. No prvo (delom ponavljamo)

**Definicija 29.13** *Neka je data slobodna grupa $\mathbf{F}_A$ slobodno reduciranih reči, nad azbukom $A \cup A^{-1}$, gde je $A = \{a_1, \ldots, a_n\}$. Transformacija uređene $n$-torke slobodno reduciranih reči $\overline{u} = (u_1, \ldots, u_n)$ je elementarna Nielsenova transformacija ranga $n$ akko*

(1) *permutura reči i eventualno neke od njih zamenjuje njima inverznim, dakle prevodi $\overline{u}$ u $n$-torku oblika $(u_{i_1}^{\alpha_1}, \ldots, u_{i_n}^{\alpha_n})$, gde je $\alpha_j \in \{1, -1\}$ i $i_k \neq i_l$ za $k \neq l$;*

(2) *zamenjuje (ma koju) reč $u_i$ jednom od reči: $u_iu_j^{\alpha}$, $u_j^{\alpha}u_i$, $u_j^{-\alpha}u_iu_j^{\alpha}$, gde je $i \neq j$ i $\alpha \in \{1, -1\}$, dok ostale ostavlja fiksnim.*

*Elementarni automorfizmi grupe* $\mathbf{F}_A$ *su automorfizmi indukovani elementarnim Nielsenovim transformacijama n-torke* $(a_1, \ldots, a_n)$.

**Napomena.** Ako je $((a_1, \ldots, a_n))\tau = (u_1, \ldots, u_n)$, gde je $\tau$ elementarna Nielsenova transformacija, onda je $B = \{u_1, \ldots, u_n\}$ takođe slobodna baza grupe $\mathbf{F}_A$. Jer, očigledno, $B$ je generatorni skup grupe, a tada, prema 23.17 i slobodna baza. S druge strane, preslikavanje $\overline{\tau} : A \longrightarrow B$, gde je $(a_i)\overline{\tau} = u_i$, određuje jedinstven automorfizam grupe $\mathbf{F}_A$ – elementarni automorfizam indukovan (generisan) elementarnom Nielsenovom transformacijom $\tau$.

S notacijom iz definicije imamo

**Teorema 29.14** *Grupa* $\mathbf{Aut}(\mathbf{F}_A)$ *je generisana (konačnim) skupom elementarnih automorfizama.*

Sada možemo objasniti i zašto se Gruško-Neumannova teorema može dati i sa

**Teorema 29.15** *Neka je* $\varphi$ *homomorfno preslikavanje slobodne konačno generisane grupe* $\mathbf{F}$ *na slobodni proizvod* $\mathbf{G}_1 * \cdots * \mathbf{G}_k$. *Tada je* $\mathbf{F}$ *slobodni proizvod grupa* $\mathbf{F}_1, \ldots, \mathbf{F}_k$, *gde je* $(\mathbf{F}_i)\varphi = \mathbf{G}_i$ *za* $i = 1, \ldots, k$.

Važi, naime

**Lema 29.16** *Teoreme* 29.12 *i* 29.15 *su ekvivalentna tvrđenja.*

**Dokaz.** 29.12 $\Longrightarrow$ 29.15 Neka je $\overline{\mathcal{A}} = \{\overline{a}_1, \ldots, \overline{a}_n\}$ slobodna baza grupe $\mathbf{F}$, $\varphi$ homomorfno preslikavanje $\mathbf{F}$ na slobodni proizvod $\mathbf{G} = \mathbf{G}_1 * \cdots * \mathbf{G}_k$ i $(\overline{a}_i)\varphi = \overline{g}_i$ za $i = 1, \ldots, n$. Neka je, dalje, $\mathcal{G} = \{g_1, \ldots, g_n\}$ minimalni dopustiv generatorni sistem grupe $\mathbf{G}$, s obzirom na $\overline{\mathcal{G}} = \{\overline{g}_1, \ldots, \overline{g}_n\}$ i dato razlaganje grupe $\mathbf{G}$ u slobodni proizvod. Sve što je potrebno da pokažemo je da će transformacijama koje $\overline{\mathcal{G}}$ prevode u $\mathcal{G}$ odgovarati transformacije sistema $\overline{\mathcal{A}}$ u opet slobodnu bazu $\mathcal{A}$ grupe $\mathbf{F}$ takvu da će se njeni elementi preslikavati na elemente sistema $\mathcal{G}$. Razmotrimo samo slučaj kada element $\overline{g}_j$ sistema $\overline{\mathcal{G}}$ zamenjujemo elementom $h\overline{g}_j$, gde je $h$ element grupe $\mathbf{G}$ koji se može predstaviti elementima sistema $\overline{\mathcal{G}}$ različitim od $\overline{g}_j$. Neka je $h = \overline{g}_{i_1}^{\alpha_1} \cdot \ldots \cdot \overline{g}_{i_m}^{\alpha_m}$ $(i_r \neq j,\ r = 1, \ldots, m)$ i $a_j = \overline{a}_{i_1}^{\alpha_1} \ldots \overline{a}_{i_m}^{\alpha_m}$. Tada je (kao generatorni skup) i $(\overline{\mathcal{A}} \setminus \{\overline{a}_j\}) \cup \{a_j\}$ slobodna baza grupe $\mathbf{F}$. Naravno, skup svih elemenata iz $\mathcal{G}$ (a svi su dužine 1) koji pripadaju slobodnom faktoru $\mathbf{G}_l$ je generatorni skup te grupe, te je $\mathbf{F} = \mathbf{F}_1 * \cdots * \mathbf{F}_k$, gde je grupa $\mathbf{F}_i$, $i = 1, \ldots, m$, generisana elementima iz $\mathcal{A}$ koji se preslikavaju u $\mathbf{G}_i$.

29.15 $\Longrightarrow$ 29.12 Neka je $\mathcal{G} = \{g_1, \ldots, g_n\}$ minimalni dopustiv generatorni sistem grupe $\mathbf{G} = \mathbf{G}_1 * \cdots * \mathbf{G}_k$, $\mathbf{F}$ slobodna grupa sa slobodnom bazom $\mathcal{A} = \{a_1, \ldots, a_n\}$ i $\varphi$ homomorfno preslikavanje grupe $\mathbf{F}$ na $\mathbf{G}$ determinisano sa $(a_i)\varphi = g_i$, $i = 1, \ldots, n$. Prema 29.15 postoji razlaganje grupe $\mathbf{F}$ u slobodni proizvod $\mathbf{F}_1 * \cdots * \mathbf{F}_k$ takvo da je $(\mathbf{F}_i)\varphi = \mathbf{G}_i$ za $i = 1, \ldots, n$. Pretpostavimo da je neki element sistema $\mathcal{G}$, recimo $g_1$, dužine (s obzirom na razlaganje u slobodni proizvod grupe $\mathbf{G}$) veće od 1. Onda je, jasno, i dužina elementa $a_1$, s obzirom na razlaganje grupe $\mathbf{F}$ u dati slobodni proizvod, veća od 1. Neka su $\mathcal{B}_1, \ldots, \mathcal{B}_k$ slobodne baze, respektivno, (slobodnih) grupa $\mathbf{F}_1, \ldots, \mathbf{F}_k$ i $\mathcal{B} = \bigcup_{i=1}^{k} \mathcal{B}_i$. Pošto je $\mathcal{B}$ slobodna baza, postoji automorfizam grupe $\mathbf{F}$ – $\psi$ – koji $\mathcal{A}$ preslikava na $\mathcal{B}$. Prema 29.14, $\psi$ je proizvod elementarnih automorfizama, recimo, $\psi = \psi_1 \circ \cdots \circ \psi_r$. Neka je $\mathcal{A}_i = (\mathcal{A})(\psi_1 \circ \cdots \circ \psi_i)$ za $1 \leq i \leq r$, i $\mathcal{G}_i = (\mathcal{A}_i)\varphi$. Tada je svaki od skupova $\mathcal{G}_i$ generatorni sistem grupe $\mathbf{G}$ i štaviše dopustiv s obzirom na $\mathcal{G}$. Pokažimo to samo za $\mathcal{G}_1$, što je i dovoljno (imajući u vidu tranzitivnost svojstva dopustivosti). Neka, na primer, $\psi_1$ zamenjuje $a_i$ sa $a_j^{-1}a_ia_j$, gde je $i \neq j$ (dok ostali elementi sistema $\mathcal{A}$ ostavlja fiksnim). Tada je $\mathcal{G}_1 = (\mathcal{G} \setminus \{g_i\}) \cup \{g_j^{-1}g_ig_j\}$ i, jasno, niz $\mathcal{G}$, $\mathcal{H}_1 = (\mathcal{G} \setminus \{g_i\}) \cup \{g_ig_j\}$, $\mathcal{H}_2 = (\mathcal{H}_1 \setminus \{g_j\}) \cup \{g_j^{-1}\}$, $\mathcal{H}_3 = (\mathcal{H}_2 \setminus \{g_ig_j\}) \cup \{g_j^{-1}g_ig_j\}$, $\mathcal{H}_4 = (\mathcal{H}_3 \setminus \{g_j^{-1}\}) \cup \{g_j\} = \mathcal{G}_1$ objašnjava kako se sistem $\mathcal{G}$ Nielsenovim transormacijama prevodi u sistem $\mathcal{G}_1$. Imajući u vidu da smo krenuli od minimalnog dopustivog skupa, u novim sistemima se ne mogu javiti jedinični elementi, dok bi, opet, dužina sistema $\mathcal{G}_r$ bila manja od sistema $\mathcal{G}$, kontradikcija.□



Jedna od vrlo korisnih posledica Gruško-Neumannove tereme je

**Korolar 29.17** *Neka je, za grupu* $\mathbf{G}$, $d(\mathbf{G}) \stackrel{\text{def}}{=} min\{\,|A| \mid A$ *je generatorni skup grupe* $\mathbf{G}\,\}$, *tzv. rang grupe* $\mathbf{G}$. *Tada važi:*

*ako je* $\mathbf{G}$ *konačno generisana grupa i* $\mathbf{G} = \mathbf{G}_1 * \cdots * \mathbf{G}_k$, *onda je* $d(\mathbf{G}) = d(\mathbf{G}_1) + \cdots + d(\mathbf{G}_k)$.

**Dokaz.** Konstatujmo ovom prilikom prvo, ako to već nismo ranije učinili, da očigledno važi:

*grupa* $\mathbf{G} = \mathbf{G}_1 * \cdots * \mathbf{G}_k$ *je konačno generisana akko je, za svako* $i = 1, \ldots, k$, $\mathbf{G}_i$ *konačno generisana grupa.*

Neka je $\varphi$ homomorfno preslikavanje slobodne grupe $\mathbf{F}$ ranga $d(\mathbf{G})$ na $\mathbf{G}$. Prema 29.15, postoji slobodno razlaganje grupe $\mathbf{F}$ – $\mathbf{F} = \mathbf{F}_1 * \cdots * \mathbf{F}_k$ – takvo da je $(\mathbf{F}_i)\varphi = \mathbf{G}_i$. Prema tome, za svako $i = 1, \ldots, k$, rang (slobodne) grupe $\mathbf{F}_i$, neka je to $r_i$, ne može biti manji od $d(\mathbf{G}_i)$. Kako je pak unija slobodnih baza grupa $\mathbf{F}_1, \ldots, \mathbf{F}_k$ slobodna baza grupe $\mathbf{F}$, to je $d(\mathbf{G}_1) + \cdots + d(\mathbf{G}_k) \leq r_1 + \cdots + r_k = d(\mathbf{G})$, a očigledno je i $d(\mathbf{G}) \leq d(\mathbf{G}_1) + \cdots + d(\mathbf{G}_k)$ (ako je $A_i$ generatorni skup grupe $\mathbf{G}_i$ kardinalnosti $d(\mathbf{G}_i)$, onda je svakako skup $A = \bigcup_{i=1}^{k} A_i$, kardinalnosti $d(\mathbf{G}_1) + \cdots + d(\mathbf{G}_k)$, generatorni skup grupe $\mathbf{G}$).□

Na ovaj korolar se nadovezuje

**Korolar 29.18** *Svaka konačno generisana grupa se može predstaviti na jedinstven način, do na broj i izomorfizam slobodnih faktora, kao slobodni proizvod konačno mnogo slobodno nerazloživih podgrupa.*

**Dokaz.** Indukcijom po rangu grupe. Slučaj grupa ranga 1, tj. cikličnih grupa, je trivijalan. Pretpostavimo da tvrđenje važi za sve grupe ranga manjeg od $r$ ($> 1$) i neka je $\mathbf{G}$ grupa ranga $r$. Ako je slobodna nerazloživa, nemamo šta dokazivati. Pretpostavimo stoga da je $\mathbf{G} = \mathbf{H} * \mathbf{K}$, gde su, jasno, $\mathbf{H}$ i $\mathbf{K}$ prave nejedinične podgrupe. Prema prethodnom korolaru rang svake od njih je manji od $r$, pa se prema induktivnoj hipotezi one (a onda i grupa $\mathbf{G}$) mogu predstaviti kao slobodni proizvod slobodno nerazloživih grupa. Jedinstvenost takvog razlaganja sledi direktno prema 26.8.□

# Glava 3

# Abelove grupe

## 30 Uvodne napomene

**Napomena.** Sve će grupe u ovom poglavlju biti Abelove, osim ako se izričito ne naglasi drugačije.

Kao što smo već ranije napomenuli, ustaljena je praksa da se u opštoj priči o Abelovim grupama koristi aditivna notacija. Konsekventno, 0 će biti neutralni element, $-a$ inverzni element elementa $a$, $\alpha a$, gde je $\alpha$ ceo broj, definisano je sa:

$$\alpha a = \begin{cases} \underbrace{a + \cdots + a}_{\alpha-puta} & \alpha > 0 \\ 0 & \alpha = 0 \\ \underbrace{(-a) + \cdots + (-a)}_{(-\alpha)-puta} & \alpha < 0 \end{cases};$$

običaj da u ovakvim slučajevima cele brojeve označavamo malim grčkim slovima, $\alpha, \beta, \ldots$, koristi se uveliko u linearnoj algebri ili, još šire gledano, u teoriji modula, o čemu je ovde upravo reč (no to ne znači da ih nećemo označavati i sa malim latiničnim slovima, obično sa sredine azbuke: $i, j, k, l, \ldots$).

$\mathbf{O}$ će biti neutralna ili nula podgrupa (sada ćemo, prirodno, pre koristiti termin *nula podgrupa* nego jedinična podgrupa, premda je i ovaj u upotrebi). Za direktne i kompletno direktne sume (tj. proizvode) koristićemo, kao što smo ranije najavili (videti komentar uz 10.1), $\sum_{i\in I} \mathbf{A}_i$, odnosno $\sum^c_{i\in I} \mathbf{A}_i$, a za njihove domene $\sum^d_{i\in I} A_i$ i $\sum_{i\in I} A_i$. Kada je reč o konačnoj direktnoj sumi pisaćemo: $\mathbf{A}_1 \oplus \cdots \oplus \mathbf{A}_n$; ako su $\mathbf{A}$ i $\mathbf{B}$ podgrupe grupe $\mathbf{G}$, onda je uvek $A + B = B + A$, tj. $A + B \stackrel{\text{def}}{=} \{a + b \mid a \in A, b \in B\}$ je domen podgrupe koju obeležavamo, u skladu sa ranijom notacijom, sa $\mathbf{A}+\mathbf{B}$. Prema tome imaćemo: $\mathbf{A} \oplus \mathbf{B}$ akko je $\mathbf{A} \cap \mathbf{B} = \mathbf{O}$. U nekim knjigama se, shodno tome, direktna suma familije grupa $\{\mathbf{A}_i \mid i \in I\}$ obeležava sa $\oplus \sum_{i\in I} \mathbf{A}_i$.

Prema 2.7($d$) suma elemenata konačnih redova i sama je konačnog reda. Kako su i uzajamno inverzni elementi istog reda, sledi da je skup svih elemenata konačnog reda u grupi $\mathbf{A}$ domen podgrupe koju ćemo zvati *maksimalnom periodičnom podgrupom* ili, jednostavnije, *periodičnim delom* grupe $\mathbf{A}$ ([50], [92]). Koristi se i termin *torziona podgrupa* ([142]) i shodno tome ta se podgrupa obeležava, a tako ćemo i mi postupati, sa $t\mathbf{A}$ ([142]). Jasno, ova podgrupa je od interesa samo kad su mešovite grupe u pitanju.

**Definicija 30.1** *Podgrupa grupe* $\mathbf{A}$ *sa domenom* $S(\mathbf{A}) \stackrel{\text{def}}{=} \{a \in A \mid red(a)$ *nije deljiv kvadratom nijednog prostog broja*$\}$, *u oznaci* $\mathbf{S(A)}$, *zove se sokla (kaže se i cokla) (engleski socle, izvorno nemački sockel).*

*Grupa* $\mathbf{A}$ *je elementarna akko je* $\mathbf{S(A)} = \mathbf{A}$.

Termin *socle* smo preveli doslovno jer (u prenosnom smislu) takav prevod upravo i odgovara; onaj koji ne zna šta znači "srpska" reč sokla (cokla) neka pita svoju majku (kao što je i autor učinio) ili oca ili baku ili dedu – neko od njih će već znati odgovor.

Prema 10.33, $p$-Abelova elementarna grupa direktna je suma cikličnih grupa (reda $p$).

**Lema 30.2** *Svaka mešovita grupa je ekstenzija periodične grupe torziono slobodnom grupom.*

**Dokaz.** Ako je $\mathbf{A}$ mešovita grupa, $\mathbf{A}/t\mathbf{A}$ je torziono slobodna grupa; ako $a \notin tA$, $n(a + tA) = tA$ bi dalo $na \in tA$, tj. $a \in tA$, kontradikcija.□

**Lema 30.3** ($a$) $t(\sum_{i\in I} \mathbf{A}_i) = \sum_{i\in I} t\mathbf{A}_i$.

($b$) $t(\sum^c_{i\in I} \mathbf{A}_i) \leq \sum^c_{i\in I} t\mathbf{A}_i$.

**Dokaz.** ($a$) Inkluzija $\geq$ je jasna. Ako je pak $0 \neq a_{i_1} + \cdots + a_{i_m} \in t(\sum^d_{i\in I} A_i)$, $a_{i_j} \neq 0$, $i_j \neq i_k$ za $j \neq k$, onda je, za neki pozitivan prirodan broj $n$, $n(a_{i_1} + \cdots + a_{i_m}) = 0$, pa je i $na_{i_1} = \cdots = na_{i_m} = 0$. Dakle, $a_{i_1} + \cdots + a_{i_m} \in \sum^d_{i\in I} tA_i$.

($b$) Neka je $\mathbf{a} = \langle a_i\rangle_{i\in I} \in t(\sum_{i\in I} A_i)$. Kao i u prethodnom slučaju je, za neki pozitivan prirodan broj $n$ i svako $i \in I$, $na_i = 0$. Stoga je $\mathbf{a} \in \sum_{i\in I} tA_i$.□

U opštem slučaju, u tački ($b$) prethodne leme nemamo inkluziju $\geq$. Sledeća lema nam pored toga kazuje i da periodični deo ne mora biti direktni sumand ([142]).

**Lema 30.4** *Periodični deo grupe* $\mathbf{A} = \sum^c_{p\in P} \mathbf{Z}_p$, *gde je* $P$ *skup svih prostih brojeva, prava je podgrupa ali ne i direktni sumand grupe.*



**Dokaz.** Elementi grupe $\mathbf{Z}_p$ će biti $k_p$, $0 \leq k \leq p-1$, gde podrazumevamo u opštem slučaju da je element $k_p$ u funkciji od indeksa $p$. Primetimo prvo da je $t(\sum^c_{p\in P} \mathbf{Z}_p) = \sum_{p\in P} \mathbf{Z}_p$. Neka je $0 \neq \mathbf{a} = \langle a_p\rangle_{p\in P}$ element konačnog reda grupe $\mathbf{A}$. Ako je $m\mathbf{a} = 0$, onda je, za svaki prost broj $p$, ili $m \equiv 0\ (mod\ p)$ ili $a_p = 0$, pa ako je $m = p^{\alpha_1}_{i_1} \ldots p^{\alpha_k}_{i_k}$, $\alpha_j \geq 1$, mora biti $a_q = 0$ za svaki prost broj $q$ koji nije u skupu $\{p_{i_1}, \ldots, p_{i_k}\}$. Stoga je $\mathbf{a} \in \sum^d_{p\in P} Z_p$.

Dalje, $\mathbf{A}$ nema nenula element deljiv svim prostim brojevima. Jer, ako je $\mathbf{a} = \langle a_p\rangle_{p\in P} = q\langle k_p\rangle_{p\in P} = \langle qk_p\rangle_{p\in P}$ za svako $q \in P$, sledi $a_q = qk_q = 0$. S druge strane, faktor grupa $\mathbf{A}/t\mathbf{A}$ ima takav element: $\mathbf{1} + \sum_{p\in P} Z_p = \langle 1_p\rangle_{p\in P} + \sum_{p\in P} Z_p$. Za dato $q \in P$ u svakoj cikličnoj grupi $\mathbf{Z}_p$, $p \neq q$, jednačina $1_p = qx$ ima rešenje $(k_p)$. Neka je $\mathbf{a}$ element čije su komponente $k_p$ za $p \neq q$, a $q$-ta komponenta mu je 0. Komponenta elementa $\mathbf{1} - q\mathbf{a}$ je 0 za $p \neq q$, a $q$-ta komponenta je $1_q$. Znači, $\mathbf{1} - q\mathbf{a} \in tA$ i odatle: $\mathbf{1} + tA = q(\mathbf{a} + tA)$.

Iz prethodnog proizilazi da $t\mathbf{A}$ ne može biti direktni sumand. U suprotnom bi grupa $\mathbf{A}$ bila izomorfna grupi $t\mathbf{A} \oplus \mathbf{A}/t\mathbf{A}$, pa bi i sama imala nenula element deljiv svim prostim brojevima.□

U grupi $\mathbf{A}$, za prost broj $p$, skup

$$A_p \stackrel{\text{def}}{=} \{a \in A \mid \text{red elementa } a \text{ je stepen broja } p\}$$

je domen $p$-podgrupe – $\mathbf{A}_p$ (setimo se da u opštem slučaju to nije važilo). Naravno, dozvoljavamo mogućnost da je naša $p$-podgrupa baš nula podgrupa. U svakom slučaju sve ove $p$-podgrupe su potpuno invarijantne.

**Lema 30.5** *Periodična grupa je direktna suma svojih (nenula) p-podgrupa.*

**Dokaz.** Jasno, $\mathbf{A}_p \cap \langle \bigcup_{q\neq p} A_q\rangle = \mathbf{O}$ (red bilo kojeg elementa iz $\langle \bigcup_{q\neq p} A_q\rangle$ je $P \setminus \{p\}$-broj, gde je $P$ skup svih prostih brojeva), a ako je $a$ element reda $p^{\alpha_1}_1 \cdot \ldots \cdot p^{\alpha_k}_k$, onda je $\langle a\rangle = \langle b_1\rangle \oplus \cdots \oplus \langle b_k\rangle$, gde je $b_i = (p^{\alpha_1}_1 \cdot \ldots \cdot p^{\alpha_{i-1}}_{i-1} p^{\alpha_{i+1}}_{i+1} \cdot \ldots \cdot p^{\alpha_k}_k)a$ element reda $p^{\alpha_i}_i$ (videti 10.24($g$)).□

U slučaju Abelovih grupa možemo govoriti i o zbiru homomorfizama. Tako se, za $\varphi, \psi \in Hom(\mathbf{A}, \mathbf{B})$, definiše:

$$(a)(\varphi + \psi) = (a)\varphi + (a)\psi.$$

Komutativnost grupa $\mathbf{A}$ i $\mathbf{B}$ garantuje da je $\varphi + \psi$ takođe homomorfizam. Posebno važi

**Lema 30.6** *Za svaku Abelovu grupu* $\mathbf{A}$ *je* $\langle End(\mathbf{A}), +, \circ\rangle$ *prsten sa jedinicom, tzv. prsten endomorfizama grupe* $\mathbf{A}$.

**Dokaz.** Trivijalno. Nula element je nula endomorfizam – endomorfizam koji sve elemente preslikava u nulu, jedinični element je identično preslikavanje i npr. (proveravamo samo desnu distributivnost):

$$(a)((\varphi+\psi)\circ\theta) = ((a)\varphi+(a)\psi)\theta = (a)(\varphi\circ\theta)+(a)(\psi\circ\theta) = (a)((\varphi\circ\theta)+(\psi\circ\theta)).\square$$

**Primer 30.7** (*a*) *Prsten endomorfizama beskonačne ciklične grupe* $\mathbf{Z}$ *izomorfan je prstenu* $\langle Z, +, \cdot\rangle$.

**Dokaz.** Endomorfizam beskonačne ciklične grupe $\mathbf{Z}$ određen je slikom generatornog elementa 1, a svaki element grupe može biti slika. Prema tome, endomorfizmi su oblika $\varphi_k$, gde je $(l)\varphi_k \stackrel{\text{def}}{=} kl$ (posebno, $(1)\varphi_k = k$), a očigledno važi:

$$\varphi_k + \varphi_m = \varphi_{k+m}, \quad \varphi_k \circ \varphi_m = \varphi_{k\cdot m}.$$

(*b*) *Prsten endomorfizama konačne ciklične grupe* $\mathbf{Z}_n = \langle n, +_n\rangle$ *izomorfan je prestenu* $\langle n, +_n, \cdot_n\rangle$.

**Dokaz.** Kao i u prethodnom slučaju, za svako $r$, $0 \leq r < n$, preslikavanje $\varphi_r : k \longrightarrow k \cdot_n r$, endomorfizam je grupe $\mathbf{Z}_n$. Dokaz se zasniva na dokazanim svojstvima operacija sabiranja i množenja po modulu $n$:

$$(k +_n l)\varphi_r = (k +_n l) \cdot_n r = k \cdot_n r +_n l \cdot_n r = (k)\varphi_r +_n (l)\varphi_r.$$

Izomorfizam prstena proizilazi iz relacija:

$$(k)(\varphi_r + \varphi_s) = (k)\varphi_r +_n (k)\varphi_s = k \cdot_n r +_n k \cdot_n s = k \cdot_n (r +_n s) = (k)\varphi_{r+_n s},$$

$$(k)(\varphi_r \circ \varphi_s) = ((k)\varphi_r)\varphi_s = (k \cdot_n r)\varphi_s = (k \cdot_n r) \cdot_n s = k \cdot_n (r \cdot_n s) = (k)\varphi_{r\cdot_n s}.$$

(*c*) *Prsten endomorfizama aditivne grupe racionalnih brojeva izomorfan je polju racionalnih brojeva.*

**Dokaz.** Videti i dopuniti 2.10($f$).

(*d*) *Prsten endomorfizama Prüferove grupe* $\mathbf{p}^\infty$ *izomorfan je tzv. prstenu p-adičnih celih brojeva, obeležimo ga sa* $\mathbf{R}$, *čiji je domen* $\{\langle k_n\rangle_{n\in N} \mid 0 \leq k_n < p^n,\ k_{n+1} \equiv k_n \ (mod\ p^n)\}$, *a sabiranje i množenje je po komponentama po modulu odgovarajućeg stepena od p:*

$$\langle k_n\rangle_{n\in N} + \langle l_n\rangle_{n\in N} \stackrel{\text{def}}{=} \langle k_n +_{p^n} l_n\rangle_{n\in N},\ \langle k_n\rangle_{n\in N} \cdot \langle l_n\rangle_{n\in N} \stackrel{\text{def}}{=} \langle k_n \cdot_{p^n} l_n\rangle_{n\in N}.$$

**Dokaz.** Lako se proverava da je $\mathbf{R}$ prsten. Recimo, ako je $k_{n+1} \equiv k_n \ (mod\ p^n)$ i $l_{n+1} \equiv l_n \ (mod\ p^n)$, onda je i $k_{n+1} +_{p^{n+1}} l_{n+1} \equiv k_n +_{p^n} l_n \ (mod\ p^n)$, $k_{n+1} \cdot_{p^{n+1}} l_{n+1} \equiv k_n \cdot_{p^n} l_n \ (mod\ p^n)$; ako je $k_n \neq 0$, onda je i $k_{n+1} \neq 0$ i $p^{n+1} - k_{n+1} \equiv p^n - k_n \ (mod\ p^n)$. Jer, na primer: $(k_{n+1} +_{p^{n+1}} l_{n+1}) - (k_n +_{p^n} l_n) = (k_{n+1} - k_n) + (l_{n+1} - l_n) - [\frac{k_{n+1}+l_{n+1}}{p^{n+1}}]p^{n+1} - [\frac{k_n+l_n}{p^n}]p^n$.

U cilju pojednostavljenja notacije, Prüferovu grupu, u oznaci $\mathbf{P}$, tretiramo kao grupu sa skupom generatornih elemenata $\{a_n \mid n \in N\}$ koje vezuju relacije: $pa_1 = 0$, $pa_{n+1} = a_n$ za svako $n \in N$ (videti 21.10($r$)). Ako je $\varphi \in End(\mathbf{P})$, onda $red((a_n)\varphi)$ deli $red(a_n)$ za svako $n \in N$, pa je $(a_n)\varphi \in \langle a_n\rangle$; neka je $(a_n)\varphi = k_n a_n$, $0 \leq k_n < p^n$. Opet, relacija $pa_{n+1} = a_n$ implicira $p(a_{n+1})\varphi = pk_{n+1}a_{n+1} = k_{n+1}a_n = (pa_{n+1})\varphi = (a_n)\varphi = k_n a_n$, te je $k_{n+1} \equiv k_n \ (mod\ p^n)$. Preslikavanje $\Phi : End(\mathbf{P}) \longrightarrow R$ dato sa:



$(\varphi)\Phi = \langle k_n\rangle_{n\in N}$, gde je $(a_n)\varphi = k_n a_n$, $0 \leq k_n < p^n$, izomorfno je preslikavanje prstena $\langle End(\mathbf{P}), +, \circ\rangle$ na prsten $\mathbf{R}$. Dobra definisanost i injektivnost su očigledni. S druge strane, svaki niz $\langle k_n\rangle_{n\in N}$, gde je $0 \leq k_n < p^n$ i $k_{n+1} \equiv k_n \ (mod\ p^n)$ određuje endomorfizam $\varphi$ grupe $\mathbf{P}$ definisan sa: $(a_n)\varphi = k_n a_n$ ili, generalno, $(ka_n)\varphi = (k \cdot_{p^n} k_n)a_n$. Zaista, za $0 \leq k, l < p$ i npr. $m < n$ važi: $(ka_m + la_n)\varphi = (kp^{n-m}a_n + la_n)\varphi = ((kp^{n-m} +_{p^n} l)a_n)\varphi$ (imamo u vidu da je $\mathbf{P}$ unija cikličnih grupa $\langle a_n\rangle$ u kojima je sabiranje, za dato $n$, po modulu $p^n$) $= ((kp^{n-m} +_{p^n} l) \cdot_{p^n} k_n)a_n = (kp^{n-m} \cdot_{p^n} k_n)a_n +_{p^n} (l \cdot_{p^n} k_n)a_n = (k \cdot_{p^n} k_n)(p^{n-m}a_n) +_{p^n} (l \cdot_{p^n} k_n)a_n = (k \cdot_{p^n} k_n)a_m +_{p^n} (l \cdot_{p^n} k_n)a_n = (k \cdot_{p^m} k_m)a_m + (l \cdot_{p^n} k_n)a_n$ (jer je $k \cdot_{p^n} k_n \equiv k \cdot_{p^m} k_m \ (mod\ p^m)$ i $p^m a_m = 0$) $= (ka_m)\varphi + (la_n)\varphi$. Homomorfnost preslikavanja $\Phi$ je očigledna. Tako je, primera radi, za $(\varphi)\Phi = \langle k_n\rangle_{n\in N}$, $(\psi)\Phi = \langle l_n\rangle_{n\in N}$ i $0 \leq k < p$, $(ka_n)(\varphi \circ \psi) = ((k \cdot_{p^n} k_n)a_n)\psi = ((k \cdot_{p^n} k_n) \cdot_{p^n} l_n)a_n = (k \cdot_{p^n} (k_n \cdot_{p^n} l_n))a_n$, i stoga je $(\varphi \circ \psi)\Phi = \langle k_n \cdot_{p^n} l_n\rangle_{n\in N} = \langle k_n\rangle_{n\in N} \cdot \langle l_n\rangle_{n\in N} = (\varphi)\Phi \cdot (\psi)\Phi$.

Uočimo uzgred da je prsten $p$-adičnih brojeva integralni domen, tj. komutativni prsten sa jedinicom bez delitelja nule (u prstenu nenula element $r$ je levi delitelj nule akko postoji nenula element $s$ takav da je $rs = 0$; analogno se definiše desni delitelj nule). Jedinični element je, jasno, niz $\langle 1\rangle$ i on odgovara identičnom automorfizmu grupe $\mathbf{P}$. Konstatujmo dalje da ako je $m$-ta komponenta elementa $\langle k_n\rangle_{n\in N}$ nula ($k_m = 0$), a $(m+1)$-va različita od nule, onda je $k_i = 0$ za $i < m$ (ovo smo već koristili) i $p^m | k_j$ za svako $j > m$, ali $p^{m+1}$ ne deli $k_j$. Ako je $m > 1$, zbog $k_m \equiv k_{m-1} \ (mod\ p^{m-1})$, tj. $0 \equiv k_{m-1} \ (mod\ p^{m-1})$ i $0 \leq k_{m-1} < p^{m-1}$, sledi $k_{m-1} = 0$; isto tako izvodimo: $k_{m-2} = \cdots = k_1 = 0$. Iz $k_{m+1} \equiv 0 \ (mod\ p^m)$ i $0 < k_{m+1} < p^{m+1}$ proizilazi: $p^m | k_{m+1}$ i $p^{m+1}$ ne deli $k_{m+1}$. Indukcijom po $j \in N = \{1, 2, \ldots\}$ pokazujemo da je $k_{m+j}$ nenula element deljiv sa $p^m$ ali ne i sa $p^{m+1}$. Slučaj $j = 1$ je upravo rešen, a ako to važi i za $k_{m+j}$, tada $k_{m+j+1} \equiv k_{m+j} \ (mod\ p^{m+j})$ i $p^m | k_{m+j}$ daju: $p^m | k_{m+j+1}$, a pretpostavka $p^{m+1} | k_{m+j+1}$ dala bi $p^{m+1} | k_{m+j}$. Sada je očigledno da ako je $k_1 = \cdots = k_{r-1} = 0$, $r \geq 1$ i $k_i \neq 0$ za $i \geq r$ (ako je $r = 1$, onda imamo da su sve komponente različite od nule) i $l_1 = \cdots = l_{s-1} = 0$, $l_j \neq 0$ za $j \geq s$, onda je $k_{r+s-1} \cdot_{p^{r+s-1}} l_{r+s-1} \neq 0$; iz $k_{r+s-1} \cdot_{p^{r+s-1}} l_{r+s-1} = 0$ sledilo bi $p^{r+s-1} | (k_{r+s-1} \cdot l_{r+s-1})$, međutim, prema navedenom, $k_{r+s-1}$ je deljivo "samo" sa $p^r$, $l_{r+s-1}$ je deljivo "samo" sa $p^s$. Primetimo da je posredno već ranije pokazano da je prsten $p$-adičnih brojeva bez delitelja nule. Jer je, za nenula endomorfizam $\varphi$, $(\mathbf{P})\varphi \cong \mathbf{P}$ (za svaku pravu podgrupu $\mathbf{H}$ grupe $\mathbf{P}$ važi $\mathbf{P}/\mathbf{H} \cong \mathbf{P}$). Primetimo na kraju da je element $\langle k_n\rangle_{n\in N}$ inverzibilan akko je $k_1 \neq 0$. Uslov $k_1 \neq 0$ je evidentno potreban. Ako je pak $k_1 \neq 0$, onda su, konstatovali smo, sve komponente različite od nule i nijedna od njih nije deljiva sa $p$. Neka je $k'_n$ inverzni element elementa $k_n$ u polugrupi $\langle p^n, \cdot_{p^n}\rangle$ (videti 2.4($c$)). Treba pokazati da je $\langle k'_n\rangle_{n\in N}$ u $R$. No pošto je $k_{n+1} \cdot k'_{n+1} = 1 + Ap^{n+1}$ i $k_n \cdot k'_n = 1 + Bp^n$ za neke cele brojeve $A$ i $B$, važi: $k_{n+1} \cdot k'_{n+1} - k_n \cdot k'_n = Cp^n$ za neki ceo broj $C$, pa je $k_{n+1} \cdot k'_{n+1} - k'_{n+1} \cdot k_n + k'_{n+1} \cdot k_n - k_n \cdot k'_n =$

$k'_{n+1} \cdot (k_{n+1} - k_n) + k_n \cdot (k'_{n+1} - k'_n) = Cp^n$. Kako je $k_{n+1} - k_n$ deljivo sa $p^n$ i $(k_n, p) = 1$, to je i $k'_{n+1} - k'_n$ deljivo sa $p^n$. Naravno, opet bi bilo jednostavnije da smo uočili da elementu $\langle k_n \rangle_{n \in N}$ odgovara endomorfizam čije je jezgro nula podgrupa; taj endomorfizam je, dakle, surjekcija (podsećamo: sve prave podgrupe Prüferove $p$-grupe su konačne), dakle automorfizam, pa ima inverzni.□

**Lema 30.8** *Ako se na skupu $Hom(\mathbf{A},\mathbf{B})$ svih homomorfnih preslikavanja Abelove grupe $\mathbf{A}$ u Abelovu grupu $\mathbf{B}$ definiše operacija $+$ sa: $(a)(\varphi+\psi) = (a)\varphi + (a)\psi$ $(\varphi,\psi \in Hom(\mathbf{A},\mathbf{B}),\ a \in A)$, onda je $\langle Hom(\mathbf{A},\mathbf{B}),+\rangle$ Abelova grupa.*

**Dokaz.** Potpuno je analogan dokazu da je, za grupu $\mathbf{A}$, $\langle End(\mathbf{A}),+\rangle$ Abelova grupa.□

**Lema 30.9** *(a)* $\langle Hom(\mathbf{Z},\mathbf{Z}),+\rangle \cong \mathbf{Z}$;

*(b)* $\langle Hom(\mathbf{Z},\mathbf{Z}_n),+\rangle \cong \mathbf{Z}_n$;

*(c)* $\langle Hom(\mathbf{Z}_{p^m},\mathbf{Z}_{p^n}),+\rangle \cong \mathbf{Z}_{p^{min\{m,n\}}}$, *$p$ prost broj;*

*(d)* $\langle Hom(\mathbf{Z}_{p^m},\mathbf{Z}_{q^n}),+\rangle \cong \mathbf{O}$, *$p,q$ različiti prosti brojevi, $\mathbf{O}$ nula podgrupa.*

**Dokaz.** Razmotrimo samo tačku *(c)* za slučaj $m < n$.

Za svako $k$, $0 \le k < p^m$, preslikavanje $\varphi_k$ dato sa: $(r)\varphi_k \stackrel{\text{def}}{=} r \cdot_{p^n} kp^{n-m}$ (posebno, $(1)\varphi_k = kp^{n-m}$) homomorfno je preslikavanje ciklične grupe $\mathbf{Z}_{p^m}$ u cikličnu grupu $\mathbf{Z}_{p^n}$: $(r +_{p^m} s)\varphi_k = (r +_{p^m} s) \cdot_{p^n} kp^{n-m} = (r +_{p^n} s) \cdot_{p^n} kp^{n-m} = r \cdot_{p^n} kp^{n-m} +_{p^n} s \cdot_{p^n} kp^{n-m} = (r)\varphi_k +_{p^n} (s)\varphi_k$ (koristili smo: $(r +_{p^m} s) \cdot_{p^n} kp^{n-m} = (r +_{p^n} s) \cdot_{p^n} kp^{n-m} = (r+s)kp^{n-m} - [\frac{(r+s)k}{p^m}]p^n$). Kako je, za $0 \le k,l < p^m$, $(1)(\varphi_k + \varphi_l) = (1)\varphi_k +_{p^n} (1)\varphi_l = kp^{n-m} +_{p^n} lp^{n-m} = (k +_{p^n} l) \cdot_{p^n} p^{n-m} = (k +_{p^m} l) \cdot_{p^n} p^{n-m} = (k +_{p^m} l)p^{n-m} = (1)\varphi_{k+_{p^m} l}$ (sada smo koristili: $(k +_{p^m} l)p^{n-m} = (k +_{p^n} l)p^{n-m} = (k+l)p^{n-m} - [\frac{k+l}{p^m}]p^n$), preslikavanje $F : Hom(\mathbf{Z}_{p^m},\mathbf{Z}_{p^n}) \longrightarrow p^m$, gde je $(\varphi_k)F = k$, izomorfno je preslikavanje grupe $\langle Hom(\mathbf{Z}_{p^m},\mathbf{Z}_{p^n}),+\rangle$ na grupu $\mathbf{Z}_{p^m}$; homomorfnost je tu: $(\varphi_k+\varphi_l)F = (\varphi_{k+_{p^m} l})F = k+_{p^m} l = (\varphi_k)F +_{p^m} (\varphi_l)F$, a ostalo je ili očigledno ili pokazano.□

**Teorema 30.10** *Neka je $\mathbf{A} = \sum_{i=1}^n \mathbf{A}_i$, $\mathbf{R}_{ii} = \langle End(\mathbf{A}_i),+,\circ\rangle$ - prsten endomorfizama Abelove grupe $\mathbf{A}_i$ i $\mathbf{R}_{ij} = \langle Hom(\mathbf{A}_i,\mathbf{A}_j),+\rangle$ - grupa homomorfnih preslikavanja grupe $\mathbf{A}_i$ u grupu $\mathbf{A}_j$ za $i \ne j$. Tada je prsten endomorfizama grupe $\mathbf{A}$ - $\mathbf{R}$ - izomorfan prstenu $\mathbf{R}'$ kvadratnih matrica $[\varphi_{ij}]_{1 \le i,j \le n}$, gde je $\varphi_{ij} \in R_{ij}$, sa "standardnim" operacijama sabiranja i množenja $([\varphi_{ij}] \cdot [\psi_{ij}] = [\theta_{ij}]$, gde je $\theta_{ij} \stackrel{\text{def}}{=} \sum_{k=1}^n \varphi_{ik} \circ \psi_{kj})$.*

**Dokaz.** Neka je $F$ preslikavanje prstena $\mathbf{R}'$ u prsten $\mathbf{R}$ definisano sa, za $\Phi = [\varphi_{ij}]$: $(\Phi)F = \varphi$, gde je, za $a = a_1 + \cdots + a_n$, $a_i \in A_i$, $(a)\varphi \stackrel{\text{def}}{=} \sum_{i=1}^n (\sum_{j=1}^n (a_j)\varphi_{ji})$. Tvrdimo da je $F$ izomorfizam datih prstena. Homomorfnost preslikavanja $F$ za aditivnu operaciju je očigledna. Opet, neka je $(\Phi)F = \varphi$, $(\Psi)F = \psi$ i $\Phi \cdot \Psi = \Theta = [\theta_{ij}]$, $\theta_{ij} = \sum_{k=1}^n (\varphi_{ik} \circ \psi_{kj})$. Tada važi:

$$(a)(\varphi \circ \psi) = ((a)\varphi)\psi = (\sum_{i=1}^n (\sum_{j=1}^n (a_j)\varphi_{ji}))\psi = \sum_{i=1}^n (\sum_{j=1}^n (\sum_{k=1}^n (a_k)\varphi_{kj})\psi_{ji}) =$$

$$\sum_{i=1}^n (\sum_{k=1}^n (a_k) \sum_{j=1}^n (\varphi_{kj} \circ \psi_{ji}))) = \sum_{i=1}^n (\sum_{k=1}^n (a_k\theta_{ki}) = (a)\theta.$$

$F$ je i injektivno preslikavanje. Jer, ako je $(\Phi)F = \varphi$ nula endomorfizam, onda je, recimo, za svako $a_1 \in A_1$, $(a_1)\varphi = (a_1)\varphi_{11} + (a_1)\varphi_{12} + \cdots + (a_1)\varphi_{1n} = 0$ (dakle, $(a_1)\varphi_{11} = \cdots = (a_1)\varphi_{1n} = 0$), pa su homomorfizmi $\varphi_{11},\ldots,\varphi_{1n}$ nula homomorfizmi. Analogno se pokazuje da je uopšte $\varphi_{ij}$ nula homomorfizam za svako $i,j$, te je $\Phi$ nula matrica. Konačno, endomorfizam $\varphi$ za koji je, za dato $j$, $1 \le j \le n$, i proizvoljan element $a_j \in A_j$, $(a_j)\varphi = \sum_{i=1}^n a_{ji}$, $a_{ji} \in A_i$, slika je matrice $\Phi = [\varphi_{ij}]$, gde je $(a_i)\varphi_{ij} = a_{ij}$. Zaista, za $a = a_1 + \cdots + a_n$ imamo:

$$(a)\varphi = (a_1 + \cdots + a_n)\varphi = (a_1)\varphi + \cdots + (a_n)\varphi =$$

$$\sum_{i=1}^n a_{1i} + \sum_{i=1}^n a_{2i} + \cdots + \sum_{i=1}^n a_{ni} = \sum_{j=1}^n (\sum_{i=1}^n a_{ji}) = \sum_{i=1}^n \sum_{j=1}^n a_{ji} =$$

$$\sum_{i=1}^n (\sum_{j=1}^n (a_j)\varphi_{ji}) = (a)((\Phi)F).\blacksquare$$



Ako je $\mathbf{A} = \mathbf{B} \oplus \mathbf{C}$, onda postoje dva idempotentna endomorfizma grupe $\mathbf{A}$ koja su uzajamno normalna (komutativna su dok je njihov proizvod nula endomorfizam), a zbir im je identično preslikavanje. Jasno, radi se o projekcijama $\pi_B$, $\pi_C$ na, respektivno, podgrupe $\mathbf{B}$ i $\mathbf{C}$: $(b+c)\pi_B \stackrel{\text{def}}{=} b$, $(b+c)\pi_C \stackrel{\text{def}}{=} c$. Lako se proverava da je $\pi_B^2 = \pi_B \circ \pi_B = \pi_B$, $\pi_C^2 = \pi_C$, $\pi_B \circ \pi_C = \pi_C \circ \pi_B = o$ - nula endomorfizam i $\pi_B + \pi_C = \imath_A$. Važi i obrat ovog stava.

**Lema 30.11** *Ako su $\varphi$ i $\psi$ uzajamno normalni, idempotentni endomorfizmi grupe $\mathbf{A}$ čiji je zbir identično preslikavanje, tada je $\mathbf{A} = (\mathbf{A})\varphi \oplus (\mathbf{A})\psi$.*

**Dokaz.** Zbog $a = (a)\imath_A = (a)(\varphi + \psi) = (a)\varphi + (a)\psi$ je $\mathbf{A} = (\mathbf{A})\varphi + (\mathbf{A})\psi$. S druge strane, ako je $a \in (A)\varphi \cap (A)\psi$, onda je, za neke elemente $a_1, a_2$, $a = (a_1)\varphi = (a_2)\psi$, pa je $(a)\varphi = ((a_2)\psi)\varphi = (a_2)(\psi \circ \varphi) = (a_2)o = 0$, i isto tako $(a)\psi = 0$; dakle i $a = 0$. Znači: $\mathbf{A} = (\mathbf{A})\varphi \oplus (\mathbf{A})\psi$.□

**Korolar 30.12** *Podgrupa $\mathbf{B}$ grupe $\mathbf{A}$ je direktni sumand akko postoji idempotentni endomorfizam grupe $\mathbf{A}$ koji je preslikava na $\mathbf{B}$, tj. akko je $\mathbf{B}$ retrakt grupe $\mathbf{A}$.*

**Dokaz**. U osnovi već dat – 12.4. Ponavljamo se vežbe radi.

Ako je $\mathbf{B}$ direktni sumand, projekcija $\pi_B$ je traženi endomorfizam. Ako je pak endomorfizam $\varphi$ grupe $\mathbf{A}$ idempotentan i $(\mathbf{A})\varphi = \mathbf{B}$, neka je $\psi = \imath_A - \varphi$. $\psi$ je, takođe, idempotentan endomorfizam: $(a)\psi^2 = ((a)(\imath_A - \varphi))(\imath_A - \varphi) = (a - (a)\varphi)(\imath_A - \varphi) = a - (a)\varphi - (a)\varphi + ((a)\varphi)\varphi = a - (a)\varphi = (a)\psi$. Jasno, $\varphi \circ \psi = \psi \circ \varphi = o$; npr. $(a)(\varphi \circ \psi) = ((a)\varphi)(\imath_A - \varphi) = (a)\varphi - (a)\varphi^2 = 0$. Prema prethodnoj lemi je $\mathbf{A} = (\mathbf{A})\varphi \oplus (\mathbf{A})\psi = \mathbf{B} \oplus (\mathbf{A})\psi$.□

**Korolar 30.13** *Podgrupa* $\mathbf{B}$ *grupe* $\mathbf{A}$ *je direktni sumand akko se identični automorfizam grupe* $\mathbf{B}$ *može proširiti do (nekog) homomorfizma* $\varphi \in Hom(\mathbf{A}, \mathbf{B})$.

**Dokaz**. ($\Longleftarrow$) Primetimo samo da je $\varphi$ idempotentan endomorfizam: $(a)\varphi^2 = ((a)\varphi)\varphi = ((a)\varphi)\imath_B = (a)\varphi$.□.

**Lema 30.14** *Neka je* $\mathbf{B}$ *podgrupa grupe* $\mathbf{A}$. *Tada su sledeći uslovi ekvivalentni:*

(1) $\mathbf{B}$ *je direktni sumand grupe* $\mathbf{A}$;

(2) *Ako je* $\mathbf{C}$ *podgrupe grupe* $\mathbf{D}$ *i ako se homomorfno preslikavanje* $\varphi$ *grupe* $\mathbf{C}$ *u* $\mathbf{B}$ *može proširiti do homomorfnog preslikavanja* $\psi$ *grupe* $\mathbf{D}$ *u* $\mathbf{A}$, *onda postoji i homomorfno preslikavanje* $\theta$ *grupe* $\mathbf{D}$ *u* $\mathbf{B}$ *koje je proširenje homomorfizma* $\varphi$.

**Dokaz**. (1) $\Longrightarrow$ (2) Neka je $\mathbf{A} = \mathbf{B} \oplus \mathbf{B}_1$, $\mathbf{C} \leq \mathbf{D}$, $\varphi \in Hom(\mathbf{C}, \mathbf{B})$, $\psi \in Hom(\mathbf{D}, \mathbf{A})$ i $\psi|_C = \varphi$. Ako je $\pi_B$ projekcija grupe $\mathbf{A}$ na $\mathbf{B}$, onda je $\theta = \psi \circ \pi_B \in Hom(\mathbf{D}, \mathbf{B})$ i, za $c \in C$, je $(c)\theta = (c)(\psi \circ \pi_B) = ((c)\psi)\pi_B = ((c)\varphi)\pi_B = (c)\varphi$ (jer je $(c)\varphi \in B$).

(2) $\Longrightarrow$ (1) Neka je grupa $\mathbf{A}$ generisana skupom $B \cup \{a_\alpha \mid \alpha < \lambda\}$, $B \cap \{a_\alpha \mid \alpha < \lambda\} = \emptyset$, i neka je $\mathbf{F} = \sum_{\alpha<\lambda} \mathbf{Z}_\alpha$ slobodna grupa ranga $\lambda$. Preslikavanje baze grupe $\mathbf{F}$ u $\mathbf{A}$ dato sa $1_\alpha \longrightarrow a_\alpha$ proširuje se, znamo, do homomorfizma $\psi \in Hom(\mathbf{F}, \mathbf{A})$. Neka je, dalje, $\mathbf{F}_1 = (\mathbf{B} \cap (\mathbf{F})\psi)\psi^{-1}$ i $\varphi = \psi|_{F_1}$. Prema uslovu (2) postoji homomorfizam $\theta \in Hom(\mathbf{F}, \mathbf{B})$ takav da je $\theta|_{F_1} = \varphi$. Preslikavanje $b \longrightarrow b$ za svako $b \in B$, i $a_\alpha \longrightarrow (1_\alpha)\theta$ indukuje idempotentno homomorfno preslikavanje $\phi$ grupe $\mathbf{A}$ na podgrupu $\mathbf{B}$:

$$(b + k_1 a_{\alpha_1} + \cdots + k_r a_{\alpha_r})\phi \stackrel{\text{def}}{=} b + (k_1 1_{\alpha_1} + \cdots + k_r 1_{\alpha_r})\theta.$$

Zaista, $\phi$ je dobro definisano, jer ako je $b + k_1 a_{\alpha_1} + \cdots + k_r a_{\alpha_r} = b_1 + m_1 a_{\beta_1} + \cdots + m_s a_{\beta_s}$, $b, b_1 \in B$, tj. $b + (k_1 1_{\alpha_1} + \cdots + k_r 1_{\alpha_r})\psi = b_1 + (m_1 1_{\beta_1} + \cdots + m_s 1_{\beta_s})\psi$, tada je $b - b_1 = (m_1 1_{\beta_1} + \cdots + m_s 1_{\beta_s} - k_1 1_{\alpha_1} - \cdots - k_r 1_{\alpha_r})\psi \in B \cap (F)\psi$, te je $m_1 1_{\beta_1} + \cdots + m_s 1_{\beta_s} - k_1 1_{\alpha_1} - \cdots - k_r 1_{\alpha_r} \in F_1$. Stoga je $(m_1 1_{\beta_1} + \cdots + m_s 1_{\beta_s} - k_1 1_{\alpha_1} - \cdots - k_r 1_{\alpha_r})\theta = (m_1 1_{\beta_1} + \cdots + m_s 1_{\beta_s} - k_1 1_{\alpha_1} - \cdots - k_r 1_{\alpha_r})\psi = b - b_1$, dakle, i $b + (k_1 1_{\alpha_1} + \cdots + k_r 1_{\alpha_r})\theta = b_1 + (m_1 1_{\beta_1} + \cdots + m_s 1_{\beta_s})\theta$. $\phi$ je, evidentno, homomorfizam, a važi i $\phi^2 = \phi$:

$$(b + k_1 a_{\alpha_1} + \cdots + k_r a_{\alpha_r})\phi^2 = (b + (k_1 1_{\alpha_1} + \cdots + k_r 1_{\alpha_r})\theta)\phi =$$



$$b + (k_1 1_{\alpha_1} + \cdots + k_r 1_{\alpha_r})\theta = (b + k_1 a_{\alpha_1} + \cdots + k_r a_{\alpha_r})\phi.$$□

**Lema 30.15** *Neka je, za podgrupe* $\mathbf{B}$ *i* $\mathbf{C}$ *grupe* $\mathbf{A}$, $\mathbf{B} \cap \mathbf{C} = \mathbf{O}$ *i neka je* $\mathbf{B}$ *maksimalna podgrupa (grupe* $\mathbf{A}$*) čiji je presek sa* $\mathbf{C}$ *nula podgrupa (znači, ako je* $\mathbf{B}$ *prava podgrupa grupe* $\mathbf{D} \leq \mathbf{A}$, *onda je* $\mathbf{D} \cap \mathbf{C} \neq \mathbf{O}$*); za* $\mathbf{B}$ *se kaže i da je* $\mathbf{C}$*-visoka podgrupa. Tada važi:*

($a$) *ako je, za* $a \in A$ *i neki prost broj* $p$, $pa \in B$, *onda je* $a \in B + C$;

($b$) $\mathbf{A} = \mathbf{B} \oplus \mathbf{C}$ *akko iz* $pa = b + c$, $b \in B$, $c \in C$, $p$ *prost broj, sledi da je* $c = pc_1$ *za neko* $c_1 \in C$.

**Dokaz**. ($a$) Ako je, s notacijom iz teksta leme i uz pretpostavku da je ispunjen uslov tačke ($a$), $a \in B$, nemamo šta dokazivati. Ako $a \notin B$, onda $\langle B, a\rangle \cap \mathbf{C} \neq \mathbf{O}$, pa je, za neko $k$, $0 < k < p$, i neke elemente $b \in B$, $c \in C$, $b + ka = c \neq 0$. Dakle, $ka \in B + C$, ali je, po uslovu, i $pa \in B + C$. Stoga je, za cele brojeve $u$ i $v$ takve da je $uk + vp = 1$, $a = (uk + vp)a = u(ka) + v(pa) \in B + C$.

($b$) ($\Longrightarrow$) Ako je $\mathbf{A} = \mathbf{B} \oplus \mathbf{C}$, $pa = b + c$ i $a = b_1 + c_1$, odmah dobijamo: $c = pc_1$.

($\Longleftarrow$) Neka je ispunjen dati uslov i neka je, za $a \in A$ i neki prost broj $p$, $pa = b + c \in B + C$. Onda je, za neko $c_1 \in C$, $c = pc_1$, pa je $p(a - c_1) = b \in B$, i prema prethodnoj tački, $a - c_1 \in B + C$; prema tome je i $a \in B + C$. Zaključujemo da je faktor grupa $\mathbf{A}/(\mathbf{B} \oplus \mathbf{C})$ ili nula ili torziono slobodna grupa. Ali, $a_1 \in A \setminus (B + C)$ bi dalo: $\langle B, a_1\rangle \cap \mathbf{C} \neq \mathbf{O}$, te bi, za neki nenula ceo broj $m$ i neko $b_1 \in B$, $c_1 \in C$, bilo $c_1 = b_1 + ma_1 \neq 0$, tj. $ma_1 = c_1 - b_1 \in B + C$, odnosno $m(a_1 + (B + C)) = B + C$, kontradikcija.□

Sledeće konstrukcije, premda ih mi nećemo mnogo koristiti, od velikog su interesa u teoriji Abelovih grupa (i, još šire gledano, imajući u vidu njihove analogone, u teoriji modula, homološkoj algebri, teoriji kategorija). Definicija koja sledi (za teoriju Abelovih grupa) zahteva manje od njoj odgovarajuće za teoriju (svih) grupa – 27.5, utoliko što pomenuta preslikavanja nisu nužno injektivna.

**Definicija 30.16** *Uređena petorka* $\langle \mathbf{A}, \mathbf{B}, \mathbf{C}, \phi, \psi\rangle$, *gde su* $\mathbf{A}$, $\mathbf{B}$ *i* $\mathbf{C}$ *Abelove grupe i* $\phi \in Hom(\mathbf{A}, \mathbf{B})$, $\psi \in Hom(\mathbf{A}, \mathbf{C})$ *je amalgamativna baza (dijagram) teorije Abelovih grupa. Data baza se može amalgamirati u teoriji Abelovih grupa akko postoji Abelova grupa* $\mathbf{D}$ *i homomorfizmi* $\phi_1 \in Hom(\mathbf{B}, \mathbf{D})$, $\psi_1 \in Hom(\mathbf{C}, \mathbf{D})$ *takvi da je* $\phi \circ \phi_1 = \psi \circ \psi_1$.

**Teorema 30.17** *Za svaku amalgamativnu bazu* $\langle \mathbf{A}, \mathbf{B}, \mathbf{C}, \phi, \psi\rangle$ *postoji jedinstvena, do na izomorfizam, Abelova grupa* $\mathbf{D}$ *i homomorfizmi* $\phi_1 \in Hom(\mathbf{B}, \mathbf{D})$, $\psi_1 \in Hom(\mathbf{C}, \mathbf{D})$ *takvi da je* $\phi \circ \phi_1 = \psi \circ \psi_1$ *i* $\mathbf{D}$ *je maksimalna takva, u smislu da ako i za neku Abelovu grupu* $\mathbf{G}$ *postoje homomorfizmi* $\phi_2 \in Hom(\mathbf{B}, \mathbf{G})$, $\psi_2 \in Hom(\mathbf{C}, \mathbf{G})$ *sa svojstvom* $\phi \circ \phi_2 = \psi \circ \psi_2$, *onda postoji jedinstveni homomorfizam* $\theta \in Hom(\mathbf{D}, \mathbf{G})$ *takav da je* $\phi_1 \circ \theta = \phi_2$, $\psi_1 \circ \theta = \psi_2$.

**Dokaz.** Odmah da kažemo (a što nije bilo teško ni pogoditi, kad već znamo 27.6): $\mathbf{D} = (\mathbf{B} \oplus \mathbf{C})/\mathbf{H}$, gde je $\mathbf{H}$ podgrupa sa domenom $H = \{((a)\phi, -(a)\psi) \mid a \in A\}$ (očigledno, $H$ je domen podgrupe). Definišimo preslikavanja $\phi_1 : B \longrightarrow D$ i $\psi_1 : C \longrightarrow D$ sa: $(b)\phi_1 = (b,0)+H$, $(c)\psi_1 = (0,c)+H$. Jasno, $\phi_1$, $\psi_1$ su homomorfizmi, a za $a \in A$ imamo: $(a)(\phi \circ \phi_1) = ((a)\phi)\phi_1 = ((a)\phi, 0) + H$, $(a)(\psi \circ \psi_1) = ((a)\psi)\psi_1 = (0,(a)\psi)+H$. No, $((a)\phi, 0) + H = (0,(a)\psi) + H$ jer je $((a)\phi, -(a)\psi) \in H$.

Pokažimo sada maksimalnost (u gore definisanom smislu) grupe $\mathbf{D}$. Neka je, dakle, data grupa $\mathbf{G}$ i homomorfizmi $\phi_2 \in Hom(\mathbf{B},\mathbf{G})$, $\psi_2 \in Hom(\mathbf{C},\mathbf{G})$ takvi da je $\phi \circ \phi_2 = \psi \circ \psi_2$. Neka je preslikavanje $\theta : \mathbf{D} \longrightarrow \mathbf{G}$ dato sa: $((b,c)+H)\theta = (b)\phi_2+(c)\psi_2$. $\theta$ je dobro definisano, jer ako važi $(b,c)+H = (b_1,c_1)+H$, tj. $(b-b_1, c-c_1) \in H$, tada je, za neko $a \in A$, $b-b_1 = (a)\phi$, $c-c_1 = -(a)\psi$ $(= (-a)\psi)$, pa je $((b,c)+H)\theta = (b)\phi_2 + (c)\psi_2 = (b_1+(a)\phi)\phi_2 + (c_1-(a)\psi)\psi_2 = (b_1)\phi_2 + (a)(\phi\circ\phi_2) + (c_1)\psi_2 - (a)(\psi\circ\psi_2) = (b_1)\phi_2 + (c_1)\psi_2 = ((b_1,c_1)+H)\theta$. Naravno, $\theta$ je i homomorfizam, a za $b \in B$ je $(b)(\phi_1 \circ \theta) = ((b,0)+H)\theta = (b)\phi_2 + (0)\psi_2 = (b)\phi_2$. Znači, $\phi_1 \circ \theta = \phi_2$, a analogno sledi i $\psi_1 \circ \theta = \psi_2$. Pretpostavimo da je i za $\theta_1 \in Hom(\mathbf{D},\mathbf{G})$, $\phi_1 \circ \theta_1 = \phi_2$, $\psi_1 \circ \theta_1 = \psi_2$. Tada je $((b,c)+H)\theta_1 = (((b,0)+H)+((0,c)+H))\theta_1 = ((b,0)+H)\theta_1 + ((0,c)+H)\theta_1 = ((b)\phi_1)\theta_1 + ((c)\psi_1)\theta_1 = (b)\phi_2 + (c)\psi_2 = ((b,c)+H)\theta$, te je $\theta = \theta_1$.

Preostaje nam još da pokažemo i jedinstvenost (do na izomorfizam) grupe $\mathbf{D}$. Da ne bismo uvodili nove oznake neka grupa $\mathbf{G}$ (sa homomorfizmima $\phi_2$, $\psi_2$) i sama ima svojstva grupe $\mathbf{D}$. Onda postoji jedinstveni homomorfizam $\overline{\theta} \in Hom(\mathbf{G},\mathbf{D})$ takav da je $\phi_2 \circ \overline{\theta} = \phi_1$, $\psi_2 \circ \overline{\theta} = \psi_1$. Iz $\phi_2 \circ \overline{\theta} = \phi_1$ dobijamo $\phi_1 \circ \theta \circ \overline{\theta} = \phi_1$; isto tako je i $\psi_1 \circ \theta \circ \overline{\theta} = \psi_1$. Ali, prema konstatovanom, postoji jedinstveni endomorfizam grupe $\mathbf{D}$ – $\chi$ – takav da je $\phi_1 \circ \chi = \phi_1$, $\psi_1 \circ \chi = \psi_1$. Kako i identično preslikavanje $\imath_D$ i $\theta \circ \overline{\theta}$ zadovoljavaju tu ulogu, to je $\theta \circ \overline{\theta} = \imath_D$. Slično dobijamo: $\overline{\theta} \circ \theta = \imath_G$. Iz prve od ovih relacija sledi da je $\theta$ injektivno a iz druge da je surjektivno. Sumiramo: $\theta \in Is(\mathbf{D},\mathbf{G})$.■

**Korolar 30.18** *Svaka amalgamativna baza teorije Abelovih grupa se može amalgamirati, tj. teorija Abelovih grupa ima svojstvo amalgamiranja.*

**Dokaz.** Sa oznakama iz prethodne leme imamo: ako su $\phi, \psi$ injektivna preslikavanja, onda su i $\phi_1, \psi_1$ injektivna preslikavanja. Jer, ako je npr. za $b_1, b_2 \in B$ $(b_1)\phi_1 = (b_2)\phi_1$, tj. $(b_1,0) + H = (b_2,0) + H$, onda je $(b_1-b_2,0) \in H$, pa je, za neko $a \in A$, $b_1 - b_2 = (a)\phi$, $0 = -(a)\psi$. Zbog injektivnosti preslikavanja $\psi$ je $a = 0$, stoga je i $b_1 - b_2 = 0$, odnosno $b_1 = b_2$.□

**Definicija 30.19** *Neka su* $\mathbf{A}$, $\mathbf{B}$ *i* $\mathbf{C}$ *Abelove grupe,* $\phi \in Hom(\mathbf{B},\mathbf{A})$, $\psi \in Hom(\mathbf{C},\mathbf{A})$. *Povratni dijagram je uređena petorka* $\langle \mathbf{B},\mathbf{C},\mathbf{A},\phi,\psi\rangle$.

**Teorema 30.20** *Za svaki povratni dijagram* $\langle \mathbf{B},\mathbf{C},\mathbf{A},\phi,\psi\rangle$ *postoji jedinstvena do na izomorfizam Abelova grupa* $\mathbf{D}$ *i homomorfizmi* $\phi_1 \in Hom(\mathbf{D},\mathbf{B})$, $\psi_1 \in Hom(\mathbf{D},\mathbf{C})$ *takvi da je* $\phi_1 \circ \phi = \psi_1 \circ \psi$ *i* $\mathbf{D}$ *je najmanja takva grupa*



*u smislu da ako i za neku Abelovu grupu* $\mathbf{G}$ *postoje homomorfizmi* $\phi_2 \in Hom(\mathbf{G},\mathbf{B})$, $\psi_2 \in Hom(\mathbf{G},\mathbf{C})$ *takvi da je* $\phi_2 \circ \phi = \psi_2 \circ \psi$, *onda postoji jedinstveni homomorfizam* $\theta \in Hom(\mathbf{G},\mathbf{D})$ *takav da je* $\phi_2 = \theta \circ \phi_1$, $\psi_2 = \theta \circ \psi_1$.

**Dokaz.** Kao i u slučaju amalgamativnog dijagrama odmah da kažemo: $\mathbf{D}$ je podgrupa grupe $\mathbf{B}\oplus\mathbf{C}$ sa domenom $D = \{(b,c) \mid (b)\phi = (c)\psi\}$. Homomorfizmi $\phi_1, \psi_1$ su projekcije: $(b,c)\phi_1 = b$, $(b,c)\psi_1 = c$. Očigledno je, za $(b,c) \in D$, $((b,c))(\phi_1 \circ \phi) = (b)\phi = (c)\psi = ((b,c))(\psi_1 \circ \psi)$. Ako je i za homomorfizme Abelove grupe $\mathbf{G}$ $\phi_2 \in Hom(\mathbf{G},\mathbf{B})$ i $\psi_2 \in Hom(\mathbf{G},\mathbf{C})$ ispunjeno $\phi_2 \circ \phi = \psi_2 \circ \psi$, definišimo preslikavanje $\theta : G \longrightarrow D$ sa: $(g)\theta = ((g)\phi_2, (g)\psi_2)$. Naravno, $((g)\phi_2, (g)\psi_2) \in D$ (jer je, po pretpostavci, $\phi_2 \circ \phi = \psi_2 \circ \psi$). S obzirom da su $\phi_2$, $\psi_2$ homomorfizmi, to je i $\theta$ homomorfizam, a za $g \in G$ je $(g)(\theta \circ \phi_1) = ((g)\phi_2, (g)\psi_2)\phi_1 = (g)\phi_2$. Dakle, $\theta \circ \phi_1 = \phi_2$, a analogno se proverava i da je $\theta \circ \psi_1 = \psi_2$. Pokažimo da je $\theta$ i jedinstveni homomorfizam (sa datim svojstvima). Neka je npr. i za $\theta_1 \in Hom(\mathbf{G},\mathbf{D})$ $\theta_1 \circ \phi_1 = \phi_2$, $\theta_1 \circ \psi_1 = \psi_2$ i neka je $(g)\theta_1 = (b,c)$. Iz $\theta_1 \circ \phi_1 = \phi_2$ sledi: $(g)(\theta_1 \circ \phi_1) = ((b,c))\phi_1 = b = (g)\phi_2$; slično: $(g)(\theta_1 \circ \psi_1) = c = (g)\psi_2$, te je $(g)\theta_1 = ((g)\phi_2, (g)\psi_2) = (g)\theta$. Što se tiče jedinstvenosti (do na izomorfizam) grupe $\mathbf{D}$ dokaz je idejno isti onom za amalgamativni dijagram. Opet, da se ne bismo zamarali novim oznakama, neka grupa $\mathbf{G}$ (sa homomorfizmima $\phi_2$, $\psi_2$) ima svojstva grupe $\mathbf{D}$ i neka je $\overline{\theta} \in Hom(\mathbf{D},\mathbf{G})$ jedinstveni homomorfizam za koji je $\overline{\theta} \circ \phi_2 = \phi_1$, $\overline{\theta} \circ \psi_2 = \psi_1$. Odatle, $(\overline{\theta} \circ \theta) \circ \phi_1 = \phi_1$, $(\overline{\theta} \circ \theta) \circ \psi_1 = \psi_1$, ali i $\imath_D \circ \phi_1 = \phi_1$, $\imath_D \circ \psi_1 = \psi_1$, a znamo da postoji samo jedan endomorfizam grupe $\mathbf{D}$ koji je "levi jedinični" za preslikavanja $\phi_1$, $\psi_1$. Stoga je $\overline{\theta} \circ \theta = \imath_D$. Analogno, $\theta \circ \overline{\theta} = \imath_G$. $\overline{\theta}$ je, dakle, bijektivno, a grupe $\mathbf{D}$ i $\mathbf{G}$ su izomorfne.■

**Napomena.** Grupu $\mathbf{D}$ (povratnog dijagrama $\langle \mathbf{B},\mathbf{C},\mathbf{A},\phi,\psi\rangle$) iz prethodne teoreme zvaćemo, dogovorno, *povratna grupa*

## 31 Rang Abelovih grupa

Pojam sistema linearno nezavisnih elemenata je od posebnog interesa za Abelove grupe kao modula nad prstenom celih brojeva; kada je o vektorskim prostorima reč, analogoni su, naravno, sistemi linearno nezavisnih vektora. Stoga će onima koji su već upoznatima sa elementima linearne algebre preostati manje-više samo da se podsete na odgovarajuće poznate stavove (o bazama vektorskih prostora) i generalizuju ih.

**Definicija 31.1** *Konačni sistem (familija, skup) elemenata* $\{a_1, \ldots, a_n\}$ *grupe* $\mathbf{A}$ *je linearno nezavisan akko je:*

$$\alpha_1 a_1 + \cdots + \alpha_n a_n = 0 \Longleftrightarrow \alpha_1 = \cdots = \alpha_n = 0.$$

*Beskonačan sistem elemenata je linearno nezavisan akko je svaki njegov konačan podsistem linearno nezavisan.*

*Linearno nezavisan sistem elemenata je maksimalan linearno nezavisan sistem elemenata akko nije strogo sadržan ni u jednom drugom linearno nezavisnom sistemu elemenata.*

*Sistem (konačan ili beskonačan) elemenata je linearno zavisan akko nije linearno nezavisan.*

*Element $a$ je linearno zavisan od sistema elemenata $\{a_i \mid i \in I\}$ akko je $\alpha a \in \langle\{a_i \mid i \in I\}\rangle$ za neki nenula ceo broj $\alpha$, tj. u slučaju da je $I \neq \emptyset$, akko postoji konačna podfamilija $\{a_{i_1}, \ldots, a_{i_k}\}$ date familije i neki celi brojevi $\alpha \neq 0$, $\alpha_1, \ldots, \alpha_k$, takvi da je $\alpha a = \alpha_1 a_{i_1} + \cdots + \alpha_k a_{i_k}$.*

*Jedan sistem je linearno zavisan od drugog akko je svaki njegov element linearno zavisan od tog drugog sistema.*

*Dva sistema su ekvivalentna akko je svaki od njih linearno zavisan od onog drugog.*

**Lema 31.2** *(a) Linearno nezavisan sistem ne sadrži elemente konačnog reda; element konačnog reda je linearno zavisan od svakog sistema.*

*(b) Podsistem linearnog nezavisnog sistema je linearno nezavisan.*

*(c) U grupi uvek postoji maksimalan linearno nezavisan sistem elemenata (dozvoljavamo da to može biti i prazan skup).*

*(d) Svaki element sistema je linearno zavisan od tog sistema. Ako je sistem $\mathcal{I}$ linearno nezavisan i $a \in \mathcal{I}$, onda je $a$ linearno nezavisan od sistema $\mathcal{I} \setminus \{a\}$.*

*Linearno nezavisan sistem je maksimalan linearno nezavisan sistem akko je svaki element linearno zavisan od njega.*

*(e) Sistem elemenata $\mathcal{I} = \{g_i \mid i \in I\}$ torziono slobodne grupe $\mathbf{G}$ je linearno nezavisan akko je $\langle\mathcal{I}\rangle = \sum_{i\in I}\langle g_i\rangle$.*

*(f) Svojstvo linearne zavisnosti sistema je tranzitivno. Svojstvo ekvivalentnosti sistema je relacija ekvivalencije.*

**Dokaz.** (c) Direktna posledica leme Zorna – unija lanca linearno nezavisnih sistema i sama je linearno nezavisan sistem.

(e) Neka je $\mathcal{I}$ linearno nezavisan sistem. Kako, za ma koji ceo broj $\alpha$, $\alpha g_i \notin \langle\mathcal{I} \setminus \{g_i\}\rangle$, evidentno je $\langle\mathcal{I}\rangle = \sum_{i\in I}\langle g_i\rangle$.

Ako je pak $\langle\mathcal{I}\rangle = \sum_{i\in I}\langle g_i\rangle$ i $\alpha_1 g_{i_1} + \cdots + \alpha_{i_n} g_{i_n} = 0$, gde je $i_j \neq i_k$ za $j \neq k$ i $n \geq 1$, onda sledi, s obzirom na jedinstvenost prezentacije elemenata u direktnoj sumi: $\alpha_k g_{i_k} = 0$ za svako $k$ $(1 \leq k \leq n)$, tj. $\alpha_1 = \cdots = \alpha_n = 0$.

(f) Neka su $\mathcal{I} = \{a_i \mid i \in I\}$, $\mathcal{J} = \{b_j \mid j \in J\}$ i $\mathcal{K} = \{c_k \mid k \in K\}$ tri sistema takvi da je $\mathcal{I}$ linearno zavisan od $\mathcal{J}$ i $\mathcal{J}$ linearno zavisan od $\mathcal{K}$. No ako je, za $a \in \mathcal{I}$,

$$\alpha a = \beta_{j_1} b_{j_1} + \cdots + \beta_{j_k} b_{j_k},$$

a za $b_{j_l}$ $\beta_l b_{j_l} \in \langle\mathcal{K}\rangle$, gde su $\alpha$, $\beta_l$ $(1 \leq l \leq k)$ nenula celi brojevi, onda je $(\alpha\beta_1 \cdot \ldots \cdot \beta_k)a \in \langle\mathcal{K}\rangle$.□



**Teorema 31.3** *(Steinitz). Neka je u grupi $\mathbf{A}$ $\{a_1, \ldots, a_m\}$ linearno nezavisan sistem koji je linearno zavisan od sistema $\{b_1, \ldots, b_n\}$. Tada je $n \geq m$ i postoji podsistem $\{b_{i_1}, \ldots, b_{i_m}\}$ sistema $\{b_1, \ldots, b_n\}$ takav da su sistemi $(\{b_1, \ldots, b_n\} \setminus \{b_{i_1}, \ldots, b_{i_m}\}) \cup \{a_1, \ldots, a_m\}$ i $\{b_1, \ldots, b_n\}$ ekvivalentni.*

**Dokaz.** Indukcijom po $m$. Pretpostavićemo odmah da je $\{a_1, \ldots, a_m\}$ neprazan skup, tj. da je $m \geq 1$. Slučaj $m = 1$ treba, naravno, proveriti, no dokaz za njega se u osnovi ponavlja u opštem razmatranju pa ćemo ga izostaviti. Neka je, stoga, $m > 1$, i neka je, po induktivnoj hipotezi, tvrđenje tačno za $m - 1$. Prema tome je $m - 1 \leq n$ i postoji podsistem $\{b_{i_1}, \ldots, b_{i_{m-1}}\}$ sistema $\{b_1, \ldots, b_n\}$ takav da su sistemi (1) $\{b_1, \ldots, b_n\}$ i (2) $(\{b_1, \ldots, b_n\} \setminus \{b_{i_1}, \ldots, b_{i_{m-1}}\}) \cup \{a_1, \ldots, a_{m-1}\}$ ekvivalentni. U daljem, da bismo pojednostavili notaciju, uzećemo da je indeks $i_k$ baš $k$ – ovo se, konačno, može uvek postići adekvatnom prenumeracijom indeksa. Prema tački $(f)$ prethodne leme element $a_m$ je linearno zavisan od sistema (2), dakle, za neki nenula ceo broj $\alpha$ i neke cele brojeve $\alpha_i$, $1 \leq i \leq n$ imamo:

$$\alpha a_m = \alpha_1 a_1 + \cdots + \alpha_{m-1} a_{m-1} + \alpha_m b_m + \cdots + \alpha_n b_n.$$

Odavde direktno sledi da je $n > m - 1$ kao i da je bar jedan od brojeva $\alpha_m, \ldots, \alpha_n$ različit od nule, recimo $\alpha_m$ (u suprotnom bi element $a_m$ bio linearno zavisan od sistema $\{a_1, \ldots, a_{m-1}\}$). No tada je element $b_m$ linearno zavisan od sistema (3) $\{a_1, \ldots, a_m\} \cup \{b_{m+1}, \ldots, b_n\}$, pa su sistemi (2) i (3) ekvivalentni, a onda i (1) i (3).■

**Korolar 31.4** *Ako grupa ima jedan konačan maksimalan linearno nezavisan sistem, onda su svi maksimalno linearno nezavisni sistemi te grupe konačni i iste kardinalnosti.*

**Dokaz.** Evidentno je da grupa ne može imati i konačan, $\mathcal{I} = \{a_1, \ldots, a_n\}$, i beskonačan, $\mathcal{J} = \{b_j \mid j \in J\}$, $|J| \geq \aleph_0$, maksimalan linearno nezavisan sistem. U protivnom bismo imali da je, za $1 \leq i \leq n$ i

$$\alpha_i a_i = \beta_1^i b_{j_1}^i + \cdots + \beta_{n_i}^i b_{j_{n_i}}^i,\ \alpha_i \neq 0,$$

svaki element familije $\mathcal{J}$ linearno zavisan od konačne podfamilije $\bigcup_{i=1}^n \{b_{j_k}^i \mid 1 \leq k \leq n_i\}$, suprotno pretpostavci o linearnoj nezavisnosti familije $\mathcal{J}$.

Ostalo direktno sledi prema prethodnoj teoremi i i tački $(d)$ leme 31.2.□

**Lema 31.5** *Ako torziono slobodna grupa $\mathbf{G}$ ima jedan beskonačan maksimalan linearno nezavisan sistem, onda su i svi ostali maksimalni linearno nezavisni sistemi beskonačni i svi su iste kardinalnosti – reda grupe.*

**Dokaz.** Upravo smo videli da nijedan maksimalan linearno nezavisan sistem ne može biti konačan. Analognim kardinalnim argumentom se dokazuje

da su svi beskonačni maksimalni linearno nezavisni sistemi iste kardinalnosti. Pokazaćemo da je u pitanju baš kardinal $|G|$. U osnovi ovog dokaza je poznata činjenica da konačnih podskupova beskonačnog skupa kardinalnosti $\lambda$ ima takođe $\lambda$.

Neka je $\mathcal{I} = \{g_i \mid i \in I\}$, $|I| = \lambda$, jedan maksimalan linearno nezavisan sistem, i neka je, za dato $g \in G$, $\alpha_g$ najmanji ceo pozitivan broj takav da je $\alpha_g g \in \langle \mathcal{I} \rangle$ (videti 31.2(*d*)), a $\mathcal{I}_g$ konačna podfamilija familije $\mathcal{I}$ takva da se svi njeni elementi netrivijalno javljaju u prezentaciji elementa $\alpha_g g$, tj. ako je $\mathcal{I}_g = \{g_{i_1}, \ldots, g_{i_{n_g}}\}$, tada je, za neke nenula cele brojeve $\alpha_1, \ldots, \alpha_{n_g}$, $\alpha_g g = \alpha_1 g_{i_1} + \cdots + \alpha_{n_g} g_{i_{n_g}}$. Jasno, za dati element $g$, $\alpha_g$, podfamilija $\mathcal{I}_g$, kao i svi umnošci $\alpha_k$, $1 \leq k \leq n_g$, jednoznačno su određeni. Stoga je preslikavanje

$$\varphi : g \longrightarrow \langle \alpha_g, \mathcal{I}_g, \{\alpha_1, \ldots, \alpha_{n_g}\} \rangle$$

injektivno preslikavanje domena grupe $\mathbf{G}$ u skup svih uređenih trojki sa komponentama, redom: ceo pozitivan broj, konačna podfamilija familije $\mathcal{I}$ i konačan podskup nenula celih brojeva. Kako je kardinalnost ovog skupa trojki manja od ili jednaka $\aleph_0 \cdot \lambda \cdot \aleph_0 = \lambda = |\mathcal{I}|$, sledi da je $|G| \leq |\mathcal{I}|$, a (odveć) trivijalno je $|\mathcal{I}| \leq |G|$.□

**Lema 31.6** *Neka je* $\mathbf{A}$ *podgrupa grupe* $\mathbf{G}$ *i neka su* $\mathcal{I} = \{a_i \mid i \in I\}$ *i* $\mathcal{J} = \{b_j + A \mid j \in J\}$ *(maksimalni) linearno nezavisni skupovi grupa, respektivno,* $\mathbf{A}$ *i* $\mathbf{G/A}$. *Tada je* $\{a_i \mid i \in I\} \cup \{b_j \mid j \in J\}$ *(maksimalan) linearno nezavisan skup grupe* $\mathbf{G}$.

*Posebno,* $\{g_i \mid i \in I\}$ *je (maksimalan) linearno nezavisan skup grupe* $\mathbf{G}$ *akko je* $\{g_i + tG \mid i \in I\}$ *(maksimalan) linearno nezavisan skup grupe* $\mathbf{G}/t\mathbf{G}$.

**Dokaz**. Neka je

$$\alpha_1 a_{i_1} + \cdots + \alpha_m a_{i_m} + \beta_1 b_{j_1} + \cdots + \beta_n b_{j_n} = 0$$

za neke cele brojeve $\alpha_k, \beta_j$, $a_k \in \mathcal{I}$, $b_j \in \mathcal{J}$. Odatle proizilazi

$$\beta_1(b_{j_1} + A) + \cdots + \beta_n(b_{j_n} + A) = A,$$

pa je $\beta_1 = \cdots = \beta_n = 0$, a onda je i $\alpha_1 = \cdots = \alpha_m = 0$.

Ako su $\mathcal{I}$ i $\mathcal{J}$ maksimalni linearno nezavisni skupovi, onda je i $\mathcal{I} \cup \mathcal{J}$ maksimalan linearno nezavisan skup grupe G. Jer je, za $g \in G$, za neki nenula ceo broj $\beta$. neke cele brojeve $\beta_1, \ldots, \beta_n$ i neke elemente $b_{j_1}, \ldots, b_{j_n}$ familije $\mathcal{J}$:

$$\beta(g + A) = \beta_1(b_{j_1} + A) + \cdots + \beta_n(b_{j_n} + A),$$

tj. $\beta g - (\beta_1 b_{j_1} + \cdots + \beta_n b_{j_n}) \in A$. Prema tome je, za neki nenula ceo broj $\alpha$, neke cele brojeve $\alpha_1, \ldots, \alpha_m$ i neke elemente $a_{i_1}, \ldots, a_{i_m}$ familije $\mathcal{I}$:

$$\alpha[\beta g - (\beta_1 b_{j_1} + \cdots + \beta_n b_{j_n})] = \alpha_1 a_{i_1} + \cdots + \alpha_m a_{i_m},$$



i odatle

$$(\alpha\beta)g = \alpha_1 a_{i_1} + \cdots + \alpha_m a_{i_m} + (\alpha\beta_1) b_{j_1} + \cdots + (\alpha\beta_n) b_{j_n}.$$

Zaključujemo: svaki element grupe je linearno zavisan od sistema $\{a_i \mid i \in I\} \cup \{b_j \mid j \in J\}$.□

**Korolar 31.7** *Ako je* $\mathbf{G}$ *grupa sa beskonačnim linearno nezavisnim sistemom, onda su svi njeni maksimalni linearno nezavisni sistemi kardinalnosti* $|G/tG|$.

**Dokaz**. Direktna posledica prethodnih lema.□

Korolari 31.4 i 31.7 stoje iza sledeće definicije

**Definicija 31.8** *Torziono slobodni rang grupe* $\mathbf{A}$, *u oznaci* $r_0(\mathbf{A})$, *je kardinalnost (ma kog) maksimalnog linearno nezavisnog sistema grupe. Grupa je konačnog torziono slobodnog ranga akko je taj kardinal konačan, u suprotnom je beskonačnog torziono slobodnog ranga.*

**Korolar 31.9** *Torziono slobodni rang grupe* $\mathbf{G}$ *jednak je torziono slobodnom rangu njene faktor grupe* $\mathbf{G}/t\mathbf{G}$.

*Ako je* $\mathbf{A}$ *podgrupa grupe* $\mathbf{G}$, *konačnog torziono slobodnog ranga, onda su i* $\mathbf{A}$ *i* $\mathbf{G/A}$ *grupe konačnog torziono slobodnog ranga i zbir njihovih torziono slobodnih rangova jednak je torziono slobodnom rangu grupe* $\mathbf{G}$.

*Ako je torziono slobodna grupa* $\mathbf{A}$ *reda* $\lambda$ *većeg od* $\aleph_0$, *onda je i* $r_0(\mathbf{A}) = \lambda$.

**Lema 31.10** *Torziono slobodni rang direktne sume jednak je sumi torziono slobodnih rangova (direktnih) sumanada.*

**Dokaz**. Neka je $\mathbf{G} = \sum_{\alpha \in \mu} \mathbf{A}_\alpha$ i neka je $\lambda_\alpha$ torziono slobodni rang grupe $\mathbf{A}_\alpha$. Ako su $\mathcal{I}_\alpha = \{a_i^\alpha \mid i \in I_\alpha\}$, $|I_\alpha| = \lambda_\alpha$, $\alpha \in \mu$, maksimalni linearno nezavisni skupovi podgrupa $\mathbf{A}_\alpha$, $\alpha \in \mu$, onda je $\bigcup_{\alpha \in \mu} \mathcal{I}_\alpha$ maksimalan linearno nezavisan skup grupe G (naravno, $\mathcal{I}_\alpha \cap \mathcal{I}_\beta = \emptyset$ za $\alpha \neq \beta$).

Provera linearne nezavisnosti se oslanja na činjenicu da je zbir nenula komponenata iz različitih sumanada (direktne sume) različit od nule. Dokaz maksimalnosti analogan je onima iz prethodnih slučajeva. Ako je, za $g \in G$, $g = b_{\alpha_1} + \cdots + b_{\alpha_n}$, gde je $b_{\alpha_j} \in A_{\alpha_j}$, i ako je, za dato $j$ $(1 \leq j \leq n)$ i $\beta_j \in Z \setminus \{0\}$, $\beta_j b_{\alpha_j} = \gamma_1 a_{i_1}^{\alpha_j} + \cdots + \gamma_k a_{i_k}^{\alpha_j}$, onda je, očigledno, $(\beta_1 \cdot \ldots \cdot \beta_n) g \in \langle \bigcup_{\alpha \in \mu} \mathcal{I}_\alpha \rangle$.

Ako je $\mu \geq \aleph_0$ i ako je $\lambda_\alpha \geq 1$ za svako $\alpha \in \mu$, tada je $\sum_{\alpha \in \mu} \lambda_\alpha = \mu \cdot sup\{\lambda_\alpha \mid \alpha \in \mu\}$.□

**Primer 31.11** (*a*) *Sve periodične grupe su torziono slobodnog ranga* 0.

(*b*) *Torziono slobodni rang aditivnih grupa celih i racionalnih brojeva je* 1.

**Dokaz.** U oba slučaja za bilo koja dva nenula elementa $a, b$ postoje nenula celi brojevi $\alpha, \beta$ takvi da je $\alpha a = \beta b$.

(*c*) *Torziono slobodni rang slobodne Abelove grupe jednak je broju sumanada u direktnoj sumi (setimo se da je slobodna Abelova grupa direktna suma beskonačnih cikličnih grupa).*

(*d*) *Torziono slobodni rang multiplikativne grupe nenula racionalnih brojeva je* $\aleph_0$.

**Dokaz.** Jedan maksimalan linearno nezavisan sistem je skup svih prostih brojeva; jasno:

$$p_{i_1}^{\alpha_1} \cdot \ldots \cdot p_{i_k}^{\alpha_k} = 1 \text{ akko je } \alpha_1 = \cdots = \alpha_k = 0.$$

Ranije smo već naveli multiplikativnu grupu pozitivnih racionalnih brojeva kao primer slobodne Abelove grupe; sada još možemo dodati – i to torziono slobodnog ranga $\aleph_0$.

(*e*) *Torziono slobodni rang aditivne grupe realnih brojeva je kontinuum – c.*

**Dokaz.** Videti 31.9 (pogledati i 33.19).

(*f*) *Torziono slobodni rang multiplikativne grupe nenula realnih brojeva je kontinuum.*

**Dokaz.** Periodični deo ove grupe je $\langle\{1,-1\},\cdot\rangle$, a njemu odgovarajuća faktor grupa izomorfna je sa multiplikativnom grupom pozitivnih realnih brojeva.□

Primetimo da ako grupa $\mathbf{G}$ ima beskonačan torziono slobodni rang $\lambda$, onda ima $2^\lambda$ maksimalnih linearno nezavisnih sistema. Jer, ako je $\{a_i \mid i \in I\}$ ($|I| = \lambda$) jedan od njih i ako je $J \subseteq I$, tada je i $\{a_i \mid i \in I \setminus J\} \cup \{2a_j \mid j \in J\}$ takođe maksimalan linearno nezavisan sistem. S druge strane, više od $2^\lambda$ maksimalnih linearno nezavisnih sistema i ne može biti – postoji bijekcija između skupova svih maksimalnih linearno nezavisnih sistema, respektivno, grupa $\mathbf{G}$ i $\mathbf{G}/t\mathbf{G}$ (31.6), a grupa $\mathbf{G}/t\mathbf{G}$ je kardinalnosti $\lambda$.

Ako je grupa konačnog torziono slobodnog ranga, onda ima $\aleph_0$ maksimalnih linearno nezavisnih sistema.

Pojam linearne nezavisnosti se prirodno uopštava.

**Definicija 31.12** *Konačan skup nenula elemenata $\{a_1, \ldots, a_n\}$ grupe $\mathbf{G}$ je slabo linearno nezavisan akko važi: $\alpha_1 a_1 + \cdots + \alpha_n a_n = 0$ akko je (za svako $i$, $i = 1, \ldots, n$) $\alpha_i = 0$ ako je $a_i$ element beskonačnog reda, odnosno $\alpha_i$ je deljivo sa $red(a_i)$ ako je $a_i$ element konačnog reda.*

*Skup nenula elemenata je slabo linearno nezavisan akko je svaki njegov konačan podskup slabo linearno nezavisan.*



**Napomena.** Termin *slaba linearna nezavisnost* nije u upotrebi u literaturi. Autori se opredeljuju za jednu od dve ponuđene opcije; mi smo pak smatrali da je u radu sa slobodnim i konačno generisanim Abelovim grupama praktičnija prva definicija linearne nezavisnosti (i tu smo sledili [92] – u toj knjizi torziono slobodni rang se zove rangom), dok ćemo se kasnije više koristiti novom ([50]). Izrazom *slabo* hteli smo naglasiti da sada nisu nužno svi koeficijenti $\alpha_i$ jednaki 0, kako je to "strogo" zahtevala definicija linearne nezavisnosti – ako je element $a_i$ konačnog reda – $k$, koeficijent $\alpha_i$ je ceo broj deljiv sa $k$. Jasno, u slučaju torziono-slobodne grupe skup je linearno nezavisan akko je slabo linearno nezavisan. Sledeća fakta su analogoni već poznatih (za linearnu nezavisnost), pa se analogno i dokazuju.

**Lema 31.13** (*a*) *Svaka grupa sadrži maksimalan (s obzirom na inkluziju) slabo linearno nezavisan sistem;*

(*b*) *Svaki slabo linearno nezavisan skup sadržan je u nekom maksimalnom slabo linearno nezavisnom skupu.*

(*c*) *Podskup $\{g_i \mid i \in I\}$ nenula elemenata domena grupe $\mathbf{G}$ je slabo linearno nezavisan akko je $\langle\{g_i \mid i \in I\}\rangle = \sum_{i\in I} \langle g_i\rangle$.*

**Definicija 31.14** *Rang Abelove grupe, u oznaci $r(\mathbf{A})$, je kardinalnost maksimalnog slabo linearno nezavisnog sistema čiji je svaki element ili beskonačnog reda ili mu je red stepen nekog prostog broja.*

Naravno, odmah se postavlja pitanje korektnosti ovako uvedene relacije. Neka je za dati maksimalan slabo linearno nezavisan sistem (sa navedenim svojstvom) grupe $\mathbf{A}$ – $\mathcal{I}$:

$\mathcal{I}_0 \stackrel{\text{def}}{=} \{a \in \mathcal{I} \mid a \text{ je beskonačnog reda }\}$,

i za prost broj $p$

$\mathcal{I}_p \stackrel{\text{def}}{=} \{a \in \mathcal{I} \mid \text{red elementa } a \text{ je stepen broja } p\}$.

Na nama je da pokažemo da su $|\mathcal{I}_0|$, $|\mathcal{I}_p|$ (za svaki prost broj $p$) invarijantne veličine, tj. da ne zavise od izbora sistema.

Već znamo da je $|\mathcal{I}_0| = r_0(\mathbf{A})$ = torziono slobodni rang grupe $\mathbf{A}$.

Fiksirajmo sada prost broj $p$. Evidentno, $\mathcal{I}_p$ je maksimalan slabo linearno nezavisan sistem podgrupe $\mathbf{A}_p$. Stoga ćemo se skoncentrisati na $\mathbf{A}_p$. Ranije smo pokazali (10.33) da je $\mathbf{A}_p[p]$ (gde je $A_p[p] \stackrel{\text{def}}{=} \{a \in A_p \mid pa = 0\}$ – videti uvodni deo odeljka o deljivim grupama) direktna suma cikličnih grupa reda $p$, pa ako je $\mathbf{A}_p[p] = \sum_{\alpha<\lambda} \langle a_\alpha\rangle$, gde je $\lambda$ kardinal, onda je $|A_p[p]| = p^\lambda$ ako je $\lambda$ konačan kardinal, u suprotnom je $|A_p[p]| = \lambda$. Jasno, $\{a_\alpha \mid \alpha < \lambda\}$ je maksimalan slabo linearno nezavisan sistem grupe $\mathbf{A}_p[p]$ – slabo je linearno nezavisan i generiše celu grupu. Pokazaćemo da je $|\mathcal{I}_p| = \lambda$. Neka je, za element $b_\beta \in \mathcal{I}_p$, $red(b_\beta) = p^{m_\beta}$, $m_\beta \in N$. Tada je $\mathcal{I}'_p \stackrel{\text{def}}{=} \{p^{m_\beta - 1} b_\beta\ (= b'_\beta) \mid b_\beta \in \mathcal{I}_p\}$ maksimalan slabo linearno nezavisan sistem grupe $\mathbf{A}_p[p]$. Trivijalno,

iz $\sum_{i=1}^{n} k_i p^{m_{\beta_i}-1} b_{\beta_i} = 0$ sledi: $p^{m_{\beta_i}}$ deli $k_i p^{m_{\beta_i}-1}$, tj. $p$ deli $k_i$, $i = 1, \ldots, n$. Neka je $b \in A_p[p]$. Onda je, za neki ceo broj $k$, $0 < k < p$, $kb \in \langle \mathcal{I}_p \rangle$, dakle, $kb = r_1 b_{\beta_1} + \cdots + r_s b_{\beta_s}$. Kako je $(k, p) = 1$, to je $uk + vp = 1$ za neke cele brojeve $u$ i $v$, te je $b = ukb = ur_1 b_{\beta_1} + \cdots + ur_s b_{\beta_s}$. No, $pb = 0$ implicira: za svako $i$, $1 \leq i \leq s$, $p^{m_{\beta_i}}$ deli $pur_i$, odnosno $p^{m_{\beta_i}-1}$ deli $ur_i$, odnosno $p^{m_{\beta_i}-1}$ deli $r_i$ (jer je $(u, p) = 1$). Prema tome, $\mathcal{I}'_p$ generiše celu grupu $\mathbf{A}_p[p]$ - $\mathbf{A}_p[p] = \sum_{b'_\beta \in \mathcal{I}'_p} \langle b'_\beta \rangle$, pa je i maksimalan slabo linearno nezavisan sistem. Zaključujemo: $|\mathcal{I}_p| = |\mathcal{I}'_p| = \lambda$. U skladu sa prethodnim, $|\mathcal{I}_p|$ ćemo obeležiti sa $r_p(\mathbf{A})$. Prema tome:

$$r(\mathbf{A}) = r_0(\mathbf{A}) + \sum_{p \in P} r_p(\mathbf{A}).$$

Ponavljamo: u torziono slobodnoj grupi $\mathbf{A}$ je $r(\mathbf{A}) = r_0(\mathbf{A})$, pa se, ukoliko je iz konteksta jasno da se radi o torziono slobodnoj grupi, kaže i samo rang, umesto torziono slobodni rang. Slična konvencija se usvaja kada je u pitanju $p$-primarna grupa - $\mathbf{B}$: onda je $r(\mathbf{B}) = r_p(\mathbf{B})$.

**Definicija 31.15** ($a$) *Baza slobodne Abelove grupe je maksimalan linearno nezavisan sistem koji generiše celu grupu.*

($b$) *Baza Abelove grupe je maksimalan slabo linearno nezavisan sistem koji generiše celu grupu (ukoliko takav postoji).*

Konstatujmo odmah da tačka ($a$) prethodne definicije ima smisla, tj. da uvek postoji baza. Jer, ako je $\mathbf{F} = \sum_{i \in I} \mathbf{Z}_i$, gde je, za svako $i \in I$, $\mathbf{Z}_i$ kopija aditivne grupe celih brojeva, onda je jedna baza npr. $\{1_i \mid i \in I\}$ - obično ćemo nju i imati u vidu kad govorimo o bazi, drugim rečima nju ćemo smatrati, za dato razlaganje grupe $\mathbf{F}$ u direktnu sumu, "standardnom" bazom. Naravno, to nije i jedina baza ako je $|I| \geq 1$. Preciznije: ako je $|I| \geq \aleph_0$, grupa $\mathbf{F}$ ima $2^{|I|}$ baza; ako je $2 \leq |I| < \aleph_0$, grupa $\mathbf{F}$ ima $\aleph_0$ baza; ako je $|I| = 1$, imamo dve baze.

Ilustracije radi, recimo da je u grupi $\mathbf{F} = \mathbf{Z}_0 \oplus \mathbf{Z}_1$ za svaki ceo broj $m$ skup $\{1_0, m1_0 + 1_1\}$ baza; ili, ekvivalentno tome, za svako $m \in Z$ postoji razlaganje grupe $\mathbf{F}$ u direktnu sumu $\mathbf{Z}_0 \oplus \langle m1_0 + 1_1 \rangle$.

Jasno, nije svaki maksimalan linearno nezavisan sistem u slobodnoj Abelovoj grupi baza. U grupi $\mathbf{Z}$ ih imamo samo dve - $\{1\}$ i $\{-1\}$, dok je svaki jednoelementni skup $\{m\}$, $m \neq 0$, maksimalan linearno nezavisan skup.

Naglasimo, za svaku eventualnost, i očiglednu činjenicu:

*svaki element slobodne Abelove grupe se na jedinstven način može pretstaviti kao linearna kombinacija elemenata date baze.*

**Korolar 31.16** *Svaki maksimalan slabo linearno nezavisan sistem p-Abelove elementarne grupe je ujedno i njena baza.*



Kao i u opštem slučaju (videti 23.5) možemo celu stvar i ovako postaviti.

**Definicija 31.17** *Generatorni skup $\mathcal{A}$ Abelove grupe $\mathbf{A}$ je slobodni generatorni skup grupe $\mathbf{A}$ akko za svako preslikavanje $\varphi$ skupa $\mathcal{A}$ u domen (ma koje) Abelove grupe $\mathbf{B}$ postoji njegova jedinstvena ekstenzija $\overline{\varphi} \in Hom(\mathbf{A}, \mathbf{B})$ $(\overline{\varphi}|_{\mathcal{A}} = \varphi)$.*

**Lema 31.18** *Abelova grupa $\mathbf{A}$ je slobodna Abelova grupa akko ima slobodni generatorni skup.*

**Dokaz.** Ako je $\mathbf{A} = \sum_{\alpha < \lambda} \langle a_\alpha \rangle$ slobodna Abelova grupa ($\langle a_\alpha \rangle$, $\alpha < \lambda$, su beskonačne ciklične grupe), onda je, to smo već pokazali, $\mathcal{A} = \{a_\alpha \mid \alpha < \lambda\}$ njen slobodni generatorni skup; recimo samo: jedinstvenost ekstenzije je zagarantovana jedinstvenošću prezentacije elemenata kao linearnih kombinacija elemenata skupa $\{a_\alpha \mid \alpha < \lambda\}$. Čitalac može, vežbe radi, da pokaže: ako je $(a_\alpha)\varphi = b_\alpha$ i ako je $b_\alpha$ konačnog reda $k$, tada je $(ma_\alpha + na_\alpha)\overline{\varphi} = ((m+n)a_\alpha)\overline{\varphi} = (m+n)b_\alpha = (m + n - [\frac{m+n}{k}]k)b_\alpha = (ma_\alpha)\overline{\varphi} + (na_\alpha)\overline{\varphi} = mb_\alpha + nb_\alpha = (m - [\frac{m}{k}]k)b_\alpha + (n - [\frac{n}{k}]k)b_\alpha)$.

Ako je, s druge strane, $\mathcal{A} = \{a_\alpha \mid \alpha < \lambda\}$ slobodni generatorni skup grupe $\mathbf{A}$, tada za preslikavanje $\varphi$ skupa $\mathcal{A}$ u domen slobodne grupe $\mathbf{B} = \sum_{\alpha < \lambda} \mathbf{Z}_\alpha$, gde je $(a_\alpha)\varphi = 1_\alpha$ ($\mathbf{Z}_\alpha$ je kopija aditivne grupe celih brojeva generisana elementom $1_\alpha$), postoji jedinstvena homomorfna ekstenzija $\overline{\varphi} \in Hom(\mathbf{A}, \mathbf{B})$. Analogno, preslikavanje $\psi : 1_\alpha \longrightarrow a_\alpha$ se na jedinstven način proširuje do homomorfizma $\overline{\psi} \in Hom(\mathbf{B}, \mathbf{A})$. Proizilazi: $\overline{\varphi} \circ \overline{\psi} = \imath_{\mathbf{A}}$, $\overline{\psi} \circ \overline{\varphi} = \imath_{\mathbf{B}}$, pa je $\overline{\varphi}$ bijekcija i prema tome je $\mathbf{A} \cong \mathbf{B}$.□

**Napomena.** Iz dokaza leme ujedno sledi i da se u slučaju slobodnih Abelovih grupa pojmovi *baza* i *slobodni generatorni skup* podudaraju. Koristi se i termin *slobodna baza* koji se, kao i termin *slobodni generatorni skup*, češće koristi u univerzalnoj algebri.

U priči o slobodnim Abelovim grupama dozvolićemo, u opštem, da skup indeksa $I$ direktnih sumanada može biti i prazan skup, tj. i nula grupu $\mathbf{O}$ ćemo smatrati slobodnom Abelovom grupom. Ovo će nas osloboditi suvišnih naknadnih diskusija u pojedinim razmatranjima.

Podsetimo se i da smo već pokazali da je svaka Abelova grupa reda $\lambda$ (generisana skupom kardinalnosti $\lambda$) homomorfna slika slobodne Abelove grupe ranga $\lambda$ - 21.10($i$).

**Teorema 31.19** *Podgrupa $\mathbf{H}$ slobodne Abelove grupe $\mathbf{F}$ je slobodna Abelova grupa ranga manjeg od ili jednakog rangu grupe $\mathbf{F}$ $(r(\mathbf{H}) \leq r(\mathbf{F}))$.*

**Dokaz.** Neka je $\mathbf{F} = \sum_{\alpha \in \lambda} \mathbf{Z}_\alpha$, gde je $\lambda$ ordinal (dozvoljeno nam je, kao što smo već pokazali u odeljku o direktnim proizvodima, da za indeksni skup uzmemo dobro uređen skup). U dokazu ćemo se koristiti standardnom bazom $\{1_\alpha \mid \alpha \in \lambda\}$.

Neka je $\mathbf{H}$ netrivijalna podgrupa grupe $\mathbf{F}$. U jedinstvenoj prezentaciji elementa $h \in H \setminus \{0\}$:

$$h = k_1 1_{\alpha_1} + \cdots + k_n 1_{\alpha_n},$$

gde je $k_i$, $1 \leq i \leq n$, nenula ceo broj i $\alpha_1 \in \cdots \in \alpha_n (\in \lambda)$, $\alpha_n$ ćemo zvati poslednjim indeksom, a $k_n$ poslednjim koeficijentom elementa $h$. U skupu $A_0 \stackrel{\text{def}}{=} \{\alpha \in \lambda \mid \alpha$ je poslednji indeks nekog elemenenta iz $H \setminus \{0\}\}$ izaberimo najmanji element (takav postoji, jer je $A_0 \subseteq \lambda$, a $\lambda$ je dobro uređen relacijom pripadanja $\in$); neka je to $\alpha_0$. Dalje, u skupu $H_1 \stackrel{\text{def}}{=} \{h \in H \mid h$ je nula ili je njegov poslednji koeficijent $\alpha_0\}$ izaberimo element sa najmanjim pozitivnim poslednjim koeficijentom; neka je to $h_0$ sa poslednjim koeficijentom $k_0$. Nije teško proveriti da je $H_1$ domen beskonačne ciklične grupe generisane sa $h_0$. Jer, ako je $h \in H_1 \setminus \{0\}$ sa poslednjim koeficijentom $k$, pri čemu je $k = k_0 r + t$, $0 \leq t < k_0$, onda je $h - rh_0$ element grupe $\mathbf{H}$, koji bi, ukoliko bi $t$ bilo različito od nule, imao poslednji indeks $\alpha_0$ i poslednji koeficijent manji od $k_0$, kontradikcija. Stoga je $t = 0$, dakle i $h = rh_0$; u protivnom, $h - rh_0$ $(\neq 0)$ bi bio nenula element grupe $\mathbf{H}$ sa poslednjim indeksom manjim od $\alpha_0$. Trivijalno je pak $\langle h_0 \rangle \subseteq H_1$.

Pretpostavimo sada da smo za dati ordinal $\beta$ odredili elemente $h_\gamma$ za svako $\gamma \in \beta$, sa poslednjim indeksima $\alpha_\gamma$, takve da važi: za $\gamma_1 \in \gamma_2$ $(\in \beta)$ je $\alpha_{\gamma_1} \in \alpha_{\gamma_2}$, skup $\{h_\gamma \mid \gamma \in \beta\}$ je linearno nezavisan i svaki element podgrupe $\mathbf{H}$ sa poslednjim indeksom manjim od $sup\{\alpha_\gamma \mid \gamma \in \beta\}$ je element podgrupe $\mathbf{H}_\beta \stackrel{\text{def}}{=} \langle \{h_\gamma \mid \gamma \in \beta\} \rangle = \sum_{\gamma \in \beta} \langle h_\gamma \rangle$ (31.2(e)). Ako je $\mathbf{H}_\beta = \mathbf{H}$ dokaz je gotov, u suprotnom iz skupa $A_\beta = A_0 \setminus \{\alpha_\gamma \mid \gamma \in \beta\}$ izaberimo najmanji element $\alpha_\beta$, a $h_\beta$ neka je element iz $H$ sa poslednjim indeksom $\alpha_\beta$ i najmanjim pozitivnim poslednjim koeficijentom među elementima iz $H$ sa istim poslednjim indeksom. Jasno, $\mathbf{H}_\beta \cap \langle h_\beta \rangle = \mathbf{O}$, te je $\mathbf{H}_{\beta+1} \stackrel{\text{def}}{=} \langle H_\beta \cup \{h_\beta\} \rangle = \mathbf{H}_\beta \oplus \langle h_\beta \rangle$. S druge strane, svaki element $h$ iz $H$ sa poslednjim indeksom $\alpha_\beta$ mora biti u $H_{\beta+1}$, jer ako su $p, q$ poslednji koeficijenti elemenata, respektivno, $h_\beta$, $h$ i ako je $q = up + v$, $0 \leq v < p$, element $h - uh_\beta$ bi, u slučaju $v \neq 0$, imao poslednji indeks $\alpha_\beta$ i poslednji koeficijent pozitivan i manji od $p$, protivno pretpostavci o izboru elementa $h_\beta$; sledi da je $v = 0$, pa je $h - uh_\beta \in H_\beta$, tj. $h \in H_\beta + \langle h_\beta \rangle$. Ukoliko je i $\mathbf{H}_{\beta+1} \neq \mathbf{H}$ postupak se ponavlja. Konačno ćemo, za neki ordinal $\delta \leq \lambda$, dobiti $\mathbf{H} = \mathbf{H}_\delta$, gde je $\mathbf{H}_\delta$ slobodna Abelova grupa sa bazom $\{h_\gamma \mid \gamma \in \delta\}$.■

**Korolar 31.20** *(a) Ako je slobodna Abelova grupa* $\mathbf{B}$ *podgrupa konačnog indeksa* $n$ *torziono slobodne Abelove grupe* $\mathbf{A}$*, onda je i* $\mathbf{A}$ *slobodna Abelova grupa i* $r(\mathbf{A}) = r(\mathbf{B})$.

*(b) Podgrupa konačnog indeksa slobodne Abelove grupe* $\mathbf{A}$ *je slobodna Abelova grupa ranga jednakog rangu grupe* $\mathbf{A}$.

**Dokaz.** *(a)* Preslikavanje $\varphi : A \longrightarrow B$ dato sa $(a)\varphi = na$ izomorfno je preslikavanje grupe $\mathbf{A}$ u (pod)grupu $\mathbf{B}$ ($\mathbf{A}/\mathbf{B}$ je grupa reda $n$, injektivnost preslikavanja $\varphi$ je posledica činjenice da je $\mathbf{A}$ torziono slobodna grupa; naravno, komutativnost obezbeđuje homomorfnost). $(\mathbf{A})\varphi$ je, kao podgrupa (slobodne Abelove) grupe $\mathbf{B}$, slobodna Abelova grupa, pa je i $\mathbf{A}$ $(\cong (\mathbf{A})\varphi)$ slobodna Abelova grupa, a prema prethodnoj teoremi je

$$r(\mathbf{A}) = r((\mathbf{A})\varphi) \leq r(\mathbf{B}) \leq r(\mathbf{A}),$$

te je $r(\mathbf{A}) = r(\mathbf{B})$.□



**Lema 31.21** *Slobodna Abelova grupa je rezidualno p-konačna grupa za svaki prost broj p.*

**Dokaz.** Neka je $\mathbf{A} = \sum_{i \in I} \mathbf{Z}_i$, gde su, kao i obično, $\mathbf{Z}_i$, $i \in I$, kopije aditivne grupe celih brojeva, sa domenima $\{k_i \mid k \in Z\}$, i neka je $0 \neq a = p_{i_1}^{l_1} m_{i_1} + \cdots + p_{i_n}^{l_n} m_{i_n}$ $((m_{i_j}, p_{i_j}) = 1)$. Ako je $\mathbf{B} = p_{i_1}^{l_1+1}\mathbf{Z}_{i_1} \oplus \cdots \oplus p_{i_n}^{l_n+1}\mathbf{Z}_{i_n} \oplus \sum_{i \notin \{i_1,\ldots,i_n\}} \mathbf{Z}_i$, onda $a \notin B$ i, prema 10.3(c), $\mathbf{A}/\mathbf{B}$ $(\cong \mathbf{Z}_{p_{i_1}^{l_1+1}} \oplus \cdots \oplus \mathbf{Z}_{p_{i_n}^{l_n+1}})$ je konačna $p$-grupa.□

Naredna lema nam daje još jednu karakterizaciju slobodnih Abelovih grupa.

**Definicija 31.22** *Abelova grupa* $\mathbf{A}$ *je projektivna u klasi Abelovih grupa akko za svako homomorfno preslikavanje* $\varphi$ *grupe* $\mathbf{A}$ *u Abelovu grupu* $\mathbf{C}$ *i svako surjektivno homomorfno preslikavanje* $\psi$ *Abelove grupe* $\mathbf{B}$ *na* $\mathbf{C}$ *postoji* $\theta \in Hom(\mathbf{A}, \mathbf{B})$ *takvo da je* $\theta \circ \psi = \varphi$.

**Lema 31.23** *Abelova grupa je slobodna akko je projektivna (u klasi Abelovih grupa).*

**Dokaz.** $(\Longrightarrow)$ Neka je $\mathbf{A} = \sum_{\alpha < \lambda} \mathbf{Z}_\alpha$ slobodna Abelova grupa i neka su $\mathbf{B}$, $\mathbf{C}$ Abelove grupe, $\varphi \in Hom(\mathbf{A}, \mathbf{C})$, $\psi \in Hom(\mathbf{B}, \mathbf{C})$, s tim što je $\psi$ i surjektivno. Ako je $(1_\alpha)\varphi = c_\alpha$ za $\alpha < \lambda$, fiksirajmo po jedan element $(b_\alpha)$ iz svakog skupa $(\{c_\alpha\})\psi^{-1}$, $\alpha < \lambda$ (skup $(\{c_\alpha\})\psi^{-1}$ je neprazan jer je $\psi$ surjektivno). Već znamo da je preslikavanje $\theta : A \longrightarrow B$ definisano sa $(m_1 1_{\alpha_1} + \cdots + m_k 1_{\alpha_k})\theta = m_1 b_{\alpha_1} + \cdots + m_k b_{\alpha_k}$ homomorfizam, a očigledno je $\theta \circ \psi = \varphi$.

$(\Longleftarrow)$ Neka je $\mathbf{A}$ projektivna i $\mathbf{B}$ slobodna Abelova grupa koju homomorfizam $\psi$ preslikava na $\mathbf{A}$. Onda, uzimajući inkluziju $\imath_A$ za homomorfno preslikavanje grupe $\mathbf{A}$ u sebe, postoji homomorfizam $\theta \in Hom(\mathbf{A}, \mathbf{B})$ takav da je $\theta \circ \psi = \imath_A$. $\theta$ je injektivno (jer je i $\imath_A$ injektivno), a $\mathbf{B} = \mathbf{Ker}(\psi) \oplus (\mathbf{A})\theta$; jer, ako je, za $b \in B$, $(b)\psi = a = (a)(\theta \circ \psi)$, sledi $(b - (a)\theta)\psi = 0$, tj. $b - (a)\theta \in Ker(\psi)$, pa je $\mathbf{B} = \mathbf{Ker}(\psi) + (\mathbf{A})\theta$, a očigledno je $\mathbf{Ker}(\psi) \cap (\mathbf{A})\theta = \mathbf{O}$. Kao podgrupa (izomorfna podgrupi) slobodne Abelove grupe, $\mathbf{A}$ je i sama slobodna Abelova grupa.□

**Lema 31.24** *Ako je faktor grupa Abelove grupe* $\mathbf{G}$ *po podgrupi* $\mathbf{B}$ *slobodna Abelova grupa, onda je* $\mathbf{G}$ *direktna suma grupe* $\mathbf{B}$ *i jedne slobodne Abelove grupe.*

**Dokaz.** Neka je $\mathbf{G/B} = \sum_{\alpha\in\lambda}\langle a_\alpha+B\rangle$, gde je, za $\alpha\in\lambda$, $\langle a_\alpha+B\rangle$ beskonačna ciklična grupa. Ako je $\mathbf{A} = \langle\{a_\alpha \mid \alpha\in\lambda\}\rangle$, onda je, evidentno, $\mathbf{A}$ slobodna Abelova grupa i $\mathbf{G} = \mathbf{A}+\mathbf{B}$; iz $g+B = k_1(a_{\alpha_1}+B)+\cdots+k_m(a_{\alpha_m}+B)$, $k_i\in Z$, sledi: $g\in(k_1a_{\alpha_1}+\cdots+k_ma_{\alpha_m})+B$, pa je $g\in A+B$. Analogno se pokazuje da je $\mathbf{A}\cap\mathbf{B} = \mathbf{O}$: ako je $b = l_1a_{\alpha_1}+\cdots+l_na_{\alpha_n}\in A\cap B$ ($\alpha_i\neq\alpha_j$ za $i\neq j$), tada je i $B = l_1(a_{\alpha_1}+B)+\cdots+l_n(a_{\alpha_n}+B)$, dakle $l_1 = \cdots = l_n = 0$.□

**Lema 31.25** *Prsten endomorfizama slobodne Abelove grupe ranga n izomorfan je prstenu kvadratnih matrica reda n sa celobrojnim koeficijentima.*

*Grupa automorfizama slobodne Abelove grupe* $\mathbf{A}$ *ranga* $n$ ($\langle Aut(\mathbf{A}),\circ\rangle$) *izomorfna je multiplikativnoj grupi regularnih matrica reda n sa celobrojnim koeficijentima i determinantama* $\pm1$.

**Dokaz.** Direktna posledica leme 30.9 i teoreme 30.10. Recimo samo, automorfizmima odgovaraju inverzibilne matrice, a s obzirom da se radi o matricama sa celobrojnom koeficijentima, determinante inverzibilnih matrica su ili 1 ili -1.□

## 32 Konačno generisane Abelove grupe

Kad je o konačno generisanim Abelovim grupama reč ključna je sledeća teorema (koja upotpunjuje teoremu 31.19).

**Teorema 32.1** *Neka je* $\mathbf{H}$ *nenula podgrupa slobodne Abelove grupe* $\mathbf{F}$ *ranga* $n$. *Tada je i* $\mathbf{H}$ *slobodna Abelova grupa čiji je rang (k) manji od ili jednak n i u (slobodnim) grupama* $\mathbf{F}$ *i* $\mathbf{H}$ *mogu se naći baze, respektivno,* $\{u_1,\ldots,u_n\}$ *i* $\{v_1,\ldots,v_k\}$ *takve da je, za* $i = 1,\ldots,k$, $v_i = \alpha_iu_i$, *gde su* $\alpha_i$ *pozitivni celi brojevi, i za* $i\leq k-1$, $\alpha_{i+1}$ *je deljivo sa* $\alpha_i$.

**Dokaz.** Dokaz dajemo indukcijom po $n$, rangu grupe $\mathbf{F}$.

Slučaj $n = 1$ je poznat – radi se o beskonačnoj cikličnoj grupi čije su sve nenula podgrupe i same beskonačne ciklične grupe. Pretpostavimo, stoga, da tvrđenje važi za sve slobodne grupe (i njihove nenula podgrupe) ranga $\leq n-1$, ($n>0$) i neka je $\mathbf{F}$ slobodna Abelova grupa ranga $n$, a $\mathbf{H}$ njena nenula podgrupa. Za svaku datu bazu B grupe $\mathbf{F}$ skup $\{\alpha \mid \alpha$ je ceo pozitivan broj koji se javlja kao koeficijent nekog elementa iz $H\}$ ima najmanji element. Izaberimo među bazama jednu kojoj odgovara najmanji takav broj ($\alpha_1$); naravno, ona ne mora biti jednoznačno određena. Neka je to $\mathcal{B}_1 = \{w_1,\ldots,w_n\}$. S obzirom na moguću prenumeraciju elemenata baze, možemo pretpostaviti da je za neko $v_1\in H$ baš:

$$v_1 = \alpha_1w_1+\beta_2w_2+\cdots+\beta_nw_n.$$



Ako je $\beta_i = \alpha_1q_i+r_i$, $0\leq r_i<\alpha_1$, $i = 2,\ldots,n$, onda se u bazi $\mathcal{B}_2 = \{w_1+q_2w_2+\cdots+q_nw_n(=u_1), w_2,\ldots,w_n\}$ element $v_1$ predstavlja u obliku:

$$v_1 = \alpha_1u_1+r_2w_2+\cdots+r_nw_n,$$

te prema izboru elementa $\alpha_1$ mora biti $r_2 = \cdots = r_n = 0$. Dakle, $v_1 = \alpha_1u_1$. Neka je $H_1 = \{h\in H \mid$ koeficijent od $h$ uz $u_1$ u bazi $\mathcal{B}_2$ je $0\}$. $H_1$ je, očigledno, domen podgrupe ($\mathbf{H}_1$) i važi: $\mathbf{H} = \langle v_1\rangle\oplus\mathbf{H}_1$; jer, ako je za $h\in H$:

$$h = \gamma_1u_1+\gamma_2w_2+\cdots+\gamma_nw_n$$

i $\gamma_1 = \alpha_1r+t$, $0\leq t<\alpha_1$, tada je

$$h-rv_1 = tu_1+\gamma_2w_2+\cdots+\gamma_nw_n\in H,$$

pa mora biti $t = 0$. Prema tome:

$$h = rv_1+(\gamma_2w_2+\cdots+\gamma_nw_n)\in\langle v_1\rangle+H_1.$$

Ako je $\mathbf{H}_1$ nula podgrupa dokaz je završen: $\mathbf{H} = \langle v_1\rangle$. U suprotnom, $\mathbf{H}_1$ je nenula podgrupa slobodne grupe $\mathbf{F}_1$ sa bazom $\{w_2,\ldots,w_n\}$ i, prema induktivnoj pretpostavci, ona je slobodna grupa ranga, recimo $k-1$, manjeg od ili jednakog $n-1$ i postoje baze $\{u_2,\ldots,u_n\}$ i $\{v_2,\ldots,v_k\}$, respektivno, grupa $\mathbf{F}_1$ i $\mathbf{H}_1$ takve da je $v_i = \alpha_iu_i$, $2\leq i\leq k$, $\alpha_i>0$ i $\alpha_i|\alpha_{i+1}$ za $2\leq i\leq k-1$. No i $\alpha_1$ deli $\alpha_2$ (čime je ujedno i dokaz kompletiran). Naime, ako je $\alpha_2 = \alpha_1q+s$, $0\leq s<\alpha_1$, tada je, u bazi $\{u_1-qu_2(=\overline{u}_1), u_2,\ldots,u_n\}$, element $v_2-v_1 = (-\alpha_1)\overline{u}_1+su_2$, te mora biti $s = 0$.■

**Korolar 32.2** *(Fundamentalna teorema o konačno generisanim Abelovim grupama)*

*(a) Konačno generisana Abelova grupa je direktna suma (konačnog broja) nerazloživih cikličnih grupa;*

*(b) Konačna Abelova grupa je direktna suma konačnog broja primarnih cikličnih grupa.*

**Dokaz.** Abelova grupa $\mathbf{G}$ generisana skupom od $n$ elemenata homomorfna je slika slobodne Abelove grupe $\mathbf{F}_n$ ranga $n$. Neka je $\varphi$ dati homomorfizam. Prema prvoj teoremi o izomorfizmu je $\mathbf{G}\cong\mathbf{F}_n/\mathbf{Ker}(\varphi)$, a prema prethodnoj teoremi $\mathbf{Ker}(\varphi)$ je slobodna Abelova grupa ranga $k\leq n$ i postoje baze $\{u_1,\ldots,u_n\}$ i $\{v_1,\ldots,v_k\}$, respektivno, grupa $\mathbf{F}_n$ i $\mathbf{Ker}(\varphi)$ takve da je $v_i = \alpha_iu_i$, $\alpha_i>0$, $i\leq k$ i $\alpha_i|\alpha_{i+1}$. Prema tome, $h = \beta_1u_1+\cdots+\beta_nu_n\in Ker(\varphi)$ akko $\alpha_i|\beta_i$ za $1\leq i\leq k$ i $\beta_i = 0$ za $k<i\leq n$ (ukoliko je $k<n$). Element $u_i+Ker(\varphi)$ faktor grupe $\mathbf{F}_n/\mathbf{Ker}(\varphi)$ reda je $\alpha_i$ za $i\leq k$, odnosno beskonačnog reda za $k<i\leq n$; jer, $\alpha_i(u_i+Ker(\varphi)) = \alpha_iu_i+Ker(\varphi) = v_1+Ker(\varphi) = Ker(\varphi)$, a ako je $m_i(u_i+Ker(\varphi)) = Ker(\varphi)$, tj. $m_iu_i\in Ker(\varphi)$, onda

$\alpha_i | m_i$. Analogno je, za $i > k$, $m_i(u_i + Ker(\varphi)) \neq Ker(\varphi)$ za svako $m_i > 0$. Grupa $\mathbf{F}_n/\mathbf{Ker}(\varphi)$ generisana je skupom $\{u_i + Ker(\varphi) \mid 1 \leq i \leq n\}$ i zapravo je direktna suma cikličnih grupa $\langle u_i + Ker(\varphi)\rangle$, gde, s obzirom na rečeno, dozvoljavamo mogućnost da je neki od sumanada nula grupa. Zaista, svaki nejedinični element faktor grupe $\mathbf{F}_n/\mathbf{Ker}(\varphi)$ se na jedinstven način predstavlja kao zbir nejediničnih elemenata (nenula) cikličnih grupa. Pretpostavimo da je $u_i + Ker(\varphi) \neq Ker(\varphi)$ za $l \leq i \leq k$ i neka je

$$g + Ker(\varphi) = \beta_l(u_l + Ker(\varphi)) + \cdots + \beta_n(u_n + Ker(\varphi)) =$$

$$\gamma_l(u_l + Ker(\varphi)) + \cdots + \gamma_n(u_n + Ker(\varphi)),$$

gde je $0 \leq \beta_i, \gamma_i < \alpha_i$ za $l \leq i \leq k$. No onda je $(\beta_l - \gamma_l)u_l + \cdots + (\beta_n - \gamma_n)u_n \in Ker(\varphi)$, pa, za $l \leq i \leq k$; $\alpha_i | (\beta_i - \gamma_i)$ i, za $k < j \leq n$, $\beta_j - \gamma_j = 0$. U svakom slučaju je $\beta_j = \gamma_j$ za svako $j$, $l \leq j \leq n$.

Kao grupa izomorfna grupi $\mathbf{F}_n/\mathbf{Ker}(\varphi)$ i $\mathbf{G}$ je direktna suma cikličnih grupa.

Dokaz završavamo podsećanjem da su jedine nerazložive ciklične grupe primarne (reda $p^m$, $p$ -prost broj) i beskonačne ciklične grupe.□

Naravno, u tačkama $(a)$ i $(b)$ prethodnog korolara dozvoljavamo mogućnost i da imamo samo jedan sumand. Primetimo, s druge strane, da je svaka torziono-slobodna konačno generisana Abelova grupa slobodna.

Jedan direktni dokaz prethodnog korolara bazira se na sledećoj lemi.

**Lema 32.3** *Ako je Abelova grupa* $\mathbf{G}$ *generisana skupom* $\mathcal{G} = \{a_1, \ldots, a_k\}$ *i ako su* $n_1, \ldots, n_k$ *celi brojevi takvi da je* $NZD(n_1, \ldots, n_k) = 1$, *tada postoji generatorni skup* $\{b_1, \ldots, b_k\}$ *grupe* $\mathbf{G}$, *gde je* $b_1 = n_1a_1 + \cdots + n_ka_k$.

**Dokaz**. Dokaz je indukcijom po $n = |n_1| + \cdots + |n_k|$. Za $n = 1$ lema očigledno važi (za samo jedno $i$ je $|n_i| = 1$, a $(\mathcal{G} \setminus \{a_i\}) \cup \{-a_i\}$ je takođe generatorni skup). Pretpostavimo stoga da je tvrđenje tačno kad god je zbir datih celih brojeva manji od $n$ i neka je $|n_1| + \cdots + |n_k| = n$ $(> 1)$. Sada su bar dva od njih različita od nule; neka je $n_1, n_2 \neq 0$ i $|n_1| \geq |n_2|$. Ako su $n_1$ i $n_2$ suprotnog znaka, onda je $|n_1 + n_2| < |n_1|$; ako su istog znaka, onda je $|n_1 - n_2| < |n_1|$. Ne želeći ništa da specifikujemo pisaćemo: $|n_1 \pm n_2| < |n_1|$. Znači, $|n_1 \pm n_2| + |n_2| + \cdots + |n_k| < n$, a ostaje $NZD(n_1 \pm n_2, n_2, \ldots, n_k) = 1$, te za generatorni skup $\mathcal{G}_1 = \{a_1, a_2 \mp a_1, \ldots, a_k\}$ postoji, prema induktivnoj hipotezi, generatorni skup $\{b_1, b_2, \ldots, b_k\}$, gde je $b_1 = (n_1 \pm n_2)a_1 + n_2(a_2 \mp a_1) + \cdots + n_ka_k = n_1a_1 + n_2a_2 + \cdots + n_ka_k$.□

**Drugi dokaz korolara** 32.2$(a)$. Neka je $\mathbf{G}$ konačno generisana Abelova grupa i neka je $k = min\{|\mathcal{G}| \mid \mathcal{G} \subseteq G$ je konačan generatorni skup grupe $\mathbf{G}\}$. Elemente skupa $\mathcal{B} = \{\mathcal{G} \mid |\mathcal{G}| = k$ i $\langle\mathcal{G}\rangle = \mathbf{G}\}$ uredimo leksikografski $(\preceq)$ na sledeći način: ako je $\mathcal{C} = \{c_1, \ldots, c_k\}$, $\mathcal{D} = \{d_1, \ldots, d_k\} \in \mathcal{B}$, $red(c_1) \leq \cdots \leq red(c_k)$, $red(d_1) \leq \cdots \leq red(d_k)$, onda je $\mathcal{C} \preceq \mathcal{D}$ akko je ili za svako $i$, $1 \leq i \leq k$, $red(c_i) = red(d_i)$ ili postoji $i$ takvo da je $red(c_j) = red(d_j)$ za svako $j < i$ i $red(c_i) < red(d_i)$. Ako je $\mathcal{A} = \{a_1, \ldots, a_k\}$ minimalni element (ne nužno jedinstven) skupa $\mathcal{B}$ (s obzirom na dato uređenje), tada je $\mathbf{G} = \langle a_1\rangle \oplus \cdots \oplus \langle a_k\rangle$. Jer, ako je $m_ja_j + \cdots + m_ka_k = 0$, $1 \leq j$, $0 < m_j < red(a_j)$, $m = NZD(m_1, \ldots, m_k)$, $m_i = mn_i$, onda je $(n_1, \ldots, n_k) = 1$, te postoji generatorni skup $\{b_j, \ldots, b_k\}$ grupe $\langle a_j, \ldots, a_k\rangle$, gde je $b_j = n_ja_j + \cdots + n_ka_k$. No, skup $\{a_1, \ldots, a_{j-1}, b_j, \ldots, b_k\}$ je generatorni skup grupe $\mathbf{G}$, dok je $mb_j = m_ja_j + \cdots + m_ka_k = 0$, dakle, $red(b_j) \leq m \leq m_j < red(a_j)$, kontradikcija s pretpostavkom o izboru generatornog skupa $\mathcal{A}$ (skup $\{a_1, \ldots, a_{j-1}, b_j, \ldots, b_k\}$ je "strogo manji" od $\mathcal{A}$).□



**Korolar 32.4** *Konačno generisana Abelova grupa* $\mathbf{G}$ *je oblika:*

$$\sum_{i=1}^{k} \mathbf{C}_{n_i} \oplus \sum_{j=1}^{m} \mathbf{A}_j,$$

*gde je* $\mathbf{A}_j$, $j = 1, \ldots, m$, *beskonačna ciklična grupa,* $\mathbf{C}_{n_i}$, $i = 1, \ldots, k$, *ciklična grupa reda* $n_i$ *i, za* $i = 2, \ldots, k$, $n_i$ *deli* $n_{i-1}$ *(ako je* $k = 0$ *ili* $m = 0$, *podrazumevamo da je odgovarajuća "suma" nula podgrupa).*

**Dokaz**. Posmatramo samo periodični deo grupe $\mathbf{G}$. Neka je

$$t(\mathbf{G}) = \sum_{i=1}^{k_1} \mathbf{C}_{p_1^{\alpha_{1,i}}} \oplus \cdots \oplus \sum_{i=1}^{k_r} \mathbf{C}_{p_r^{\alpha_{r,i}}},$$

i neka je, za svako $t$, $t = 1, \ldots, r$, $\alpha_{t,1} \geq \cdots \geq \alpha_{t,k_t} \geq 1$. Prema 10.45$(a)$ je:

$$\mathbf{H}_1 = \mathbf{C}_{p_1^{\alpha_{1,1}}} \oplus \cdots \oplus \mathbf{C}_{p_r^{\alpha_{r,1}}} \cong \mathbf{Z}_{p_1^{\alpha_{1,1}} \ldots p_r^{\alpha_{r,1}}},$$

$$\mathbf{H}_2 = \mathbf{C}_{p_1^{\alpha_{1,2}}} \oplus \cdots \oplus \mathbf{C}_{p_r^{\alpha_{r,2}}} \cong \mathbf{Z}_{p_1^{\alpha_{1,2}} \ldots p_r^{\alpha_{r,2}}},$$

i tako dalje, dok je za $k = max\{k_1, \ldots, k_r\}$

$$\mathbf{H}_k = \mathbf{C}_{p_1^{\alpha_{1,k}}} \oplus \cdots \oplus \mathbf{C}_{p_r^{\alpha_{r,k}}} \cong \mathbf{Z}_{p_1^{\alpha_{1,k}} \ldots p_r^{\alpha_{r,k}}};$$

pretpostavljamo, naravno: $\alpha_{t,s} = 0$ ako je $s > k_i$, odnosno u tom slučaju je $\mathbf{C}_{p_t^{\alpha_{t,s}}}$ jedinična grupa. Evidentno, $|H_t|$ deli $|H_{t-1}|$ za $t = 2, \ldots, r$.□

**Korolar 32.5** *Grupa automorfizama konačne neciklične Abelove grupe nije Abelova.*

**Dokaz**. Prema prethodnom korolaru dovoljno je razmotriti samo slučaj direktne sume $\mathbf{Z}_m \oplus \mathbf{Z}_n$, gde $(2 \leq) m$ deli $n$. Uočimo prvo da su preslikavanja (za $(a, b) \in Z_m \times Z_n$): $\varphi : (a, b) \longrightarrow (a +_m (b - [\frac{b}{m}]m), b)$ i $\psi : (a, b) \longrightarrow (a, -b)$

automorfizmi grupe $\mathbf{Z}_m \oplus \mathbf{Z}_n$. Proveru dajemo za $\varphi$ ($\psi$ je jasno automorfizam). Bijektivnost je očigledna i pošto $m$ deli $n$, to je:

$$((a,b)+(a_1,b_1))\varphi = ((a +_m a_1, b +_n b_1))\varphi =$$

$$((a +_m a_1) +_m ((b +_n b_1 - [\frac{b +_n b_1}{m}]m), b +_n b_1) =$$

$$((a +_m a_1) +_m (b + b_1 - [\frac{b + b_1}{m}]m), b +_n b_1).$$

Isto tako je:

$$((a,b))\varphi + ((a_1,b_1))\varphi = (a +_m (b - [\frac{b}{m}]m), b) + (a_1 +_m (b_1 - [\frac{b_1}{m}]m), b_1) =$$

$$((a +_m (b - [\frac{b}{m}]m) +_m (a_1 +_m (b_1 - [\frac{b_1}{m}]m), b +_n b_1) =$$

$$((a +_m a_1) +_m ((b - [\frac{b}{m}]m) +_m (b_1 - [\frac{b_1}{m}]m), b +_n b_1) =$$

$$(a +_m a_1 +_m (b + b_1 - [\frac{b + b_1}{m}]m), b +_n b_1).$$

Sada je

$$((1,1))(\varphi \circ \psi) = ((1 +_m 1, 1))\psi = (1 +_m 1, n-1)$$

i

$$((1,1))(\psi \circ \varphi) = ((1, n-1))\varphi = (1 +_m ((n-1) - [\frac{(n-1)}{m}]m), n-1),$$

pa ako je $m > 2$, onda je $(n-1) - [\frac{(n-1)}{m}]m \neq 1$, stoga i $\varphi \circ \psi \neq \psi \circ \varphi$. Lako se proverava da je za $m = 2$ (i $n = 2k$) $((a,b))(\varphi \circ \psi) = ((a,b))(\psi \circ \varphi)$ za svako $(a,b) \in Z_2 \times Z_n$.

Ako je $m = 2$, možemo odmah pretpostaviti da je $n = 2^k$ za neko $k > 1$ – već smo rekli da je grupa automorfizama Kleinove grupe $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ simetrična grupa $\mathbf{S}_3$ (videti komentar uz 8.23), a uopšte je, ponavljamo, za neparno $j$: $\mathbf{Z}_{2^i \cdot j} \cong \mathbf{Z}_{2^i} \oplus \mathbf{Z}_j$. Uvodimo, jer moramo, još jedan automorfizam – $\theta$ – grupe $\mathbf{Z}_2 \oplus \mathbf{Z}_{2^k}$:

$$((a,b))\theta \stackrel{\text{def}}{=} \begin{cases} (0,b) & a = 0 \\ (1, 2^{k-1} +_{2^k} b) & a = 1; \end{cases}$$

Bijektivnost a i svojstvo homomorfnosti su gotovo očigledni. Tako je na primer:

$$((1,b)+(0,b_1))\theta = ((1, b +_{2^k} b_1))\theta = (1, 2^{k-1} +_{2^k} b +_{2^k} b_1) =$$

$$(1, 2^{k-1} +_{2^k} b) + (0, b_1) = ((1,b))\theta + ((0,b_1))\theta.$$



S obzirom da je $((1,1))(\varphi \circ \theta) = ((0,1))\theta = (0,1)$ i

$$((1,1))(\theta \circ \varphi) = (1, 2^{k-1} +_{2^k} 1))\varphi =$$

$$(1 +_2 (2^{k-1} + 1 - [\frac{2^{k-1}+1}{2}]2), 2^{k-1} +_{2^k} 1) = (0, 2^{k-1}+1),$$

ovog puta automorfizmi $\varphi$ i $\theta$ nisu permutabilni.□

**Korolar 32.6** *Konačno generisane Abelove grupe su rezidualno konačne.*

Direktna posledica leme 10.22, s obzirom da je $\mathbf{Z}$ rezidualno konačna grupa (videti komentar uz definiciju 5.19 ili 23.3($h$)).□

**Korolar 32.7** *Podgrupa* $\mathbf{H}$ *konačno generisane Abelove grupe* $\mathbf{G}$ *i sama je konačno generisana.*

**Dokaz.** Ako je $\mathbf{G}$ generisana skupom od $n$ elemenata, onda je $\mathbf{G} \cong \mathbf{F}_n/\mathbf{Ker}(\varphi)$, gde je $\mathbf{F}_n$ slobodna Abelova grupa ranga $n$ i $\varphi$ homomorfno preslikavanje grupe $\mathbf{F}_n$ na grupu $\mathbf{G}$. Prema 8.7, podgrupa $\mathbf{H}$ je izomorfna nekoj grupi $\mathbf{U}/\mathbf{Ker}(\varphi)$, gde je $\mathbf{U}$ podgrupa grupe $\mathbf{F}_n$ koja sadrži $\mathbf{Ker}(\varphi)$. No, rang grupe $\mathbf{U}$ je manji od ili jednak $n$, pa je i faktor grupa $\mathbf{U}/\mathbf{Ker}(\varphi)$ konačno generisana.□

Podsetimo se još da smo ranije pokazali da gornje tvrđenje ne važi u opštem za nekomutativne grupe (videti npr. 28.7).

**Korolar 32.8** *Abelova grupa ispunjava uslov maksimalnosti podgrupa akko je konačno generisana.*

**Dokaz.** Direktna posledica prethodnog korolara i leme 5.15.□

**Lema 32.9** *Neka je* $\mathbf{H}$ *konačna normalna podgrupa grupe* $\mathbf{G}$ *i neka je* $\mathbf{G}/\mathbf{H}$ *slobodna Abelova grupa ranga* $r$. *Onda postoji karakteristična podgrupa* $\mathbf{M}$ *grupe* $\mathbf{G}$ *koja je slobodna Abelova grupa ranga* $r$ *i čija je faktor grupa* – $\mathbf{G}/\mathbf{M}$ – *konačna.*

**Dokaz.** Prema prethodnom korolaru i 8.15, grupa $\mathbf{G}$ ispunjava uslov maksimalnosti podgrupa. Pokazujemo prvo da $\mathbf{G}$ ima za podgrupu slobodnu Abelovu grupu $\mathbf{F}$ konačnog indeksa. Prema $N/C$-teoremi (8.27), grupa $\mathbf{N}(\mathbf{H})/\mathbf{C}(\mathbf{H}) = \mathbf{G}/\mathbf{C}(\mathbf{H})$ izomorfna je podgrupi grupe $\mathbf{Aut}(\mathbf{H})$, dakle konačna je. Dalje je, prema drugoj i trećoj teoremi o izomorfizmu, $\mathbf{C}(\mathbf{H})/(\mathbf{C}(\mathbf{H}) \cap \mathbf{H}) \cong (\mathbf{H} \cdot \mathbf{C}(\mathbf{H}))/\mathbf{H} \leq \mathbf{G}/\mathbf{H}$, $(\mathbf{G}/\mathbf{H})/(\mathbf{H} \cdot \mathbf{C}(\mathbf{H})/\mathbf{H}) \cong \mathbf{G}/(\mathbf{H} \cdot \mathbf{C}(\mathbf{H})$, i jasno, $[\mathbf{G} : \mathbf{H} \cdot \mathbf{C}(\mathbf{H})] \leq [\mathbf{G} : \mathbf{H}]$, pa je, prema 31.20, $(\mathbf{H} \cdot \mathbf{C}(\mathbf{H}))/\mathbf{H}$, a onda i $\mathbf{C}(\mathbf{H})/(\mathbf{C}(\mathbf{H}) \cap \mathbf{H})$, slobodna Abelova grupa ranga $r$. Ako je $\mathbf{K} = \mathbf{H} \cap \mathbf{C}(\mathbf{H}) = \mathbf{E}$, dobili smo traženu podgrupu – $\mathbf{F} = \mathbf{C}(\mathbf{H})$. Ako je $\mathbf{K} \neq \mathbf{E}$, polazimo od podgrupa $\mathbf{K}$ i $\mathbf{C}(\mathbf{H})$ kao polaznih (svi uslovi leme su tu). Neka je $\mathbf{K}$ reda $n$. Pošto

je $\mathbf{C(H)}' \leq \mathbf{K}$, za svako $a, b \in C(\mathbf{H})$ je $[a,b] \in K$, tj. za neko $c \in K$ je $a^{-1}b^{-1}ab = c$. Odatle, $b^{-1}ab = ac$ i $(b^{-1}ab)^n = b^{-1}a^nb = (ac)^n = a^n$ ($a$ je permutabilno sa $c$), te je $b \in C(a^n)$. Stoga $\{a^n \mid a \in C(\mathbf{H})\}$ generiše normalnu Abelovu podgrupu $(\mathbf{L})$ koja je i konačno generisana (sve podgrupe grupe $\mathbf{G}$ su konačno generisane – 5.15). Prema 32.2($a$), $\mathbf{L}$ je direktna suma konačne (Abelove) grupe i slobodne Abelove grupe – $\mathbf{F}$. Prema tome, $[\mathbf{L} : \mathbf{F}] < \infty$. Grupa $\mathbf{C(H)/(KL)}$ ($\cong \mathbf{(C(H)/K)/((KL)/K)}$) je pak kao periodična, konačno generisana Abelova grupa konačna (za $a \in C(\mathbf{H})$ je $(aK)^n = a^nK \in KL/K$, dakle, $((aK)\,KL/K)^n = KL/K$). Zbog $\mathbf{(KL)/K} \cong \mathbf{K/(K \cap L)}$ i $\mathbf{(KL)/K}$ je konačna grupa. Sledi:

$$[\mathbf{G} : \mathbf{F}] = [\mathbf{G} : \mathbf{C(H)}] \cdot [\mathbf{C(H)} : \mathbf{KL}] \cdot [\mathbf{KL} : \mathbf{L}] \cdot [\mathbf{L} : \mathbf{F}] < \infty;$$

znači, slobodna Abelova grupa $\mathbf{F}$ podgrupa je grupe $\mathbf{G}$ konačnog indeksa. Prema 9.41, $\mathbf{F}$ sadrži karakterističnu podgrupu $\mathbf{M}$ konačnog indeksa u $\mathbf{G}$ (dakle i konačnog indeksa u $\mathbf{F}$), pa je, ponovo prema 31.20, $\mathbf{M}$ slobodna Abelova grupa ranga $r$.

**Teorema 32.10** *(Teorema o podgrupama). Neka je* $\mathbf{H}$ *podgrupa konačno generisane Abelove grupe* $\mathbf{G}$ *i neka je* $\mathbf{G}$ *direktna suma, za dati prost broj* $p$, $k_p$ *p-primarnih cikličnih grupa redova, za* $k_p > 0$, *respektivno,* $p^{\alpha_{p_1}}, \ldots, p^{\alpha_{p_{k_p}}}$, *gde je* $\alpha_{p_1} \geq \cdots \geq \alpha_{p_{k_p}}$ $(\geq 1)$, *i* $r$ $(\geq 0)$ *beskonačnih cikličnih grupa. Neka je, dalje,* $\mathbf{H}$ *direktna suma* $l_p$ *p-primarnih cikličnih grupa, redova, za* $l_p > 0$, $p^{\beta_{p_1}}, \ldots, p^{\beta_{p_{l_p}}}$, *gde je* $\beta_{p_1} \geq \cdots \geq \beta_{p_{l_p}}$ $(\geq 1)$, *i* $s$ *beskonačnih cikličnih grupa. Tada je* $s \leq r$, *za svaki prost broj* $p$ *je* $l_p \leq k_p$, *i ako je* $l_p > 0$, *onda je* $\beta_{p_m} \leq \alpha_{p_m}$ *za* $1 \leq m \leq l_p$.

**Dokaz**. $r$ i $s$ su torziono slobodni rangovi grupa, respektivno, $\mathbf{G}$ i $\mathbf{H}$, te je i $r \geq s$ (jasno, torziono slobodni rang podgrupe ne može biti veći od torziono slobodnog ranga grupe).

Neka je $\mathbf{G}_p$ suma $p$-cikličnih sumanada grupe $\mathbf{G}$. Tada je $t\mathbf{G} = \sum_{p \in P} \mathbf{G}_p$ ($P$ je skup prostih brojeva; naravno, samo za konačno mnogo prostih brojeva $p$ je $\mathbf{G}_p$ nenula podgrupa). S druge strane je $t\mathbf{H} = \sum_{p \in P}(\mathbf{G}_p \cap \mathbf{H})$. Inkluzija $\geq$ je očigledna. Ako je pak $h = la + kb \in H$, $a, b \in G$, $l, k \in Z$, gde je red elementa $a$ stepen od $p$, recimo $p^m$, $red(b) = n$ uzajamno prost sa $p$, tada je, za neke cele brojeve $u, v$, $up^m + vn = 1$, pa je $(vn)h = (1 - up^m)la + (vn)kb = la \in H\,(\cap G_p)$. Prema tome, ako je $\mathbf{H}_p$ suma $p$-cikličnih sumanada podgrupe $\mathbf{H}$, onda je $\mathbf{H}_p = \mathbf{G}_p \cap \mathbf{H}$, a $t\mathbf{H} = \sum_{p \in P} \mathbf{H}_p = \sum_{p \in P}(\mathbf{G}_p \cap \mathbf{H})$.

Kako je $\mathbf{G}_p$ $(\mathbf{H}_p)$ direktna suma $k_p$ $(l_p)$ cikličnih $p$-podgrupa, to je njena podgrupa čiji su elementi (sem jediničnog) reda $p$, reda $p^{k_p}$ $(p^{l_p})$; ta podgrupa je direktna suma cikličnih podgrupa reda $p$ svakog od $k_p$ $(l_p)$ sumanda. Stoga je $l_p \leq k_p$. Dalje, uočimo da je u grupi $\mathbf{G}_p$ $(\mathbf{H}_p)$ skup elemenata $(a)$ deljivih sa nekim stepenom od $p$, recimo $p^m$ (u smislu da jednačina $a = p^m x$ ima rešenje u grupi) domen podgrupe; 0 je, jasno, deljivo sa $p^m$, a ako su $a$ i $b$ deljivi sa



$p^m$, onda su, opet očigledno, i elementi $-a$, $a + b$ deljivi sa $p^m$. Obeležimo, za ovu priliku, te podgrupe sa, respektivno, $\mathbf{G}_p^{p^m}$, $\mathbf{H}_p^{p^m}$. Primetimo još da ako je $\mathbf{A} = \langle a \rangle$ ciklična grupa reda $p^k$ i $k > m$, onda je $\mathbf{A}^{p^m} = \langle p^m a \rangle$ (koristimo aditivnu notaciju). Trivijalno, $\langle p^m a \rangle \subseteq A$, a ako je $b = ua$ $(0 < u < p^k)$ deljivo sa $p^m$, tj. ako je, za neko $c = va\,(\in A)$, $b = ua = p^m(va) = (p^m \cdot_{p^k} v)a$, sledi $p^m | u$. Neka su (vraćamo se dokazu) $\{a_1, \ldots, a_{k_p}\}$ i $\{b_1, \ldots, b_{l_p}\}$ baze grupa $\mathbf{G}_p$ i $\mathbf{H}_p$, gde je $a_i$ reda $p^{\alpha_{p_i}}$, $b_j$ reda $p^{\beta_{p_j}}$. Ako bismo pretpostavili da je za neko $j \leq l_p$ $\alpha_{p_1} \geq \beta_{p_1}, \ldots, \alpha_{p_{j-1}} \geq \beta_{p_{j-1}}$, ali $\alpha_{p_j} < \beta_{p_j}$, dobili bismo da je baza grupe $\mathbf{G}_p^{p^{\alpha_{p_j}}} = \langle p^{\alpha_{p_j}} a_1 \rangle \oplus \cdots \oplus \langle p^{\alpha_{p_j}} a_{j-1} \rangle$ kardinalnosti $j - 1$, dok je baza grupe $\mathbf{H}_p^{p^{\alpha_{p_j}}} = \langle p^{\alpha_{p_j}} b_1 \rangle \oplus \cdots \oplus \langle p^{\alpha_{p_j}} b_j \rangle \oplus \cdots$ kardinalnosti $\geq j$, što je, već smo pokazali, nemoguće (rezonujemo, naime, kao u dokazu da je $k_p \geq l_p$).■

**Korolar 32.11** *(Teorema o izomorfizmu dekompozicija). Neka su date dve dekompozicije konačno generisane Abelove grupe* $\mathbf{G}$ *u direktnu sumu nerazloživih cikličnih grupa. Ako su* $r$ *i* $s$ *broj beskonačnih cikličnih sumanada, redom datih dekompozicija,* $k_p$ *i* $l_p$ *broj p-cikličnih sumanada redova, respektivno,* $p^{\alpha_{p_1}}, \ldots, p^{\alpha_{p_{k_p}}}$, *odnosno* $p^{\beta_{p_1}}, \ldots, p^{\beta_{p_{l_p}}}$, *gde je* $\alpha_{p_1} \geq \cdots \geq \alpha_{p_{k_p}}$, $\beta_{p_1} \geq \cdots \geq \beta_{p_{l_p}}$, *tada je:* $r = s$, $k_p = l_p$ *i* $\alpha_{p_j} = \beta_{p_j}$ *za svako* $j \leq k_p$ $(= l_p)$.

**Dokaz**. Direktna posledica prethodne teoreme (svaka grupa je ujedno i svoja podgrupa).□

**Napomena** Sistem (skup) brojeva $r, k_p, p^{\alpha_{p_1}}, \ldots, p^{\alpha_{p_{k_p}}}$ (za $p \in P$) iz prethodnog korolara, gde je $r$ broj beskonačnih cikličnih sumanada, $k_p$ broj $p$-cikličnih sumanada sa redovima, redom, $p^{\alpha_{p_1}}, \ldots, p^{\alpha_{p_{k_p}}}$ u razlaganju date konačno generisane Abelove grupe $\mathbf{G}$ u direktnu sumu nerazloživih cikličnih grupa zove se *kompletni sistem invarijanata* grupe $\mathbf{G}$. Jasno je da kompletni sistem invarijanata određuje do na izomorfizam grupu – svake dve grupe sa istim kompletnim sistemom invarijanata izomorfne su.

Konstatujmo takođe da je lemom 30.9 i teoremom 30.10 potpuno određen prsten endomorfizama svake konačno generisane Abelove grupe.

**Teorema 32.12** *(L. S. Pontrjagin). Prebrojiva Abelova torziono slobodna grupa* $\mathbf{A}$ *je slobodna Abelova grupa akko je svaka njena podgrupa konačnog ranga slobodna Abelova grupa.*

**Dokaz**. Jasno, samo je pravac ($\Leftarrow$) u pitanju. Neka je $X = \{a_n \mid n \in \omega\}$ prebrojiv generatorni skup grupe $\mathbf{A}$ (bez nula elementa) i neka je $\mathbf{A}_0$ podgrupa grupe $\mathbf{A}$ sa domenom $\{a \in A \mid ma \in \langle a_0 \rangle$ za neki pozitivan prirodan broj $m\}$. $\mathbf{A}_0$ je, po uslovu teoreme, kao grupa ranga 1 beskonačna ciklična grupa generisana, recimo, elementom $b_0$. Ako je $\mathbf{A} = \mathbf{A}_0$ dokaz je završen. U suprotnom, faktor grupa $\mathbf{A}/\mathbf{A}_0$ isto tako ispunjava uslove teoreme. Očigledno je torziono

slobodna i svaka njena podgrupa konačnog ranga je slobodna. Zaista, ako je $\overline{\mathbf{B}} = \mathbf{B}/\mathbf{A}_0$ podgrupa konačnog ranga, onda je i $\mathbf{B}$ podgrupa konačnog ranga grupe $\mathbf{A}$ (npr. ako je $\{c_0+A,\dots,c_r+A\}$ jedan maksimalno linearno nezavisan sistem grupe $\overline{\mathbf{B}}$, tada je $\{c_0,\dots,c_r,a_0\}$ maksimalan linearno nezavisan skup grupe $\mathbf{B}$), dakle i slobodna Abelova konačno generisana grupa; stoga je i $\overline{\mathbf{B}}$ konačno generisana torziono slobodna grupa, prema tome i slobodna Abelova grupa. Neka je $a_{i_1}$ prvi element skupa $X$ koji nije u $\mathbf{A}_0$ i $\mathbf{A}_1/\mathbf{A}_0$ podgrupa grupe $\mathbf{A}/\mathbf{A}_0$ sa domenom $\{a+A_0 \mid m(a+A_0) \in \langle a_{i_1}+A_0\rangle$ za neki pozitivan prirodan broj $m\}$. Kao i maločas, zaključujemo da je $\mathbf{A}_1/\mathbf{A}_0$ beskonačna ciklična grupa, generisana, recimo, elementom $b_1+A_0$. $\mathbf{A}_1$ je slobodna Abelova grupa ranga 2 sa bazom $\{b_0,b_1\}$ – videti dokaz leme 31.24, a faktor grupa $\mathbf{A}/\mathbf{A}_1$, ako već nije $\mathbf{A}=\mathbf{A}_1$, ispunjava uslove teoreme; ako bismo za $a \notin A_1$ pretpostavili da je, za neki pozitivan prirodan broj $k$, $ka \in A_1$, to bi značilo: za neki pozitivan prirodan broj $m$ je $m(ka+A_0) = (mk)(a+A_0) \in \langle a_{i_1}+A_0\rangle$, tj. $a+A_0 \in A_1/A_0$, odnosno $a \in A_1$, kontradikcija. Ako je pak $\mathbf{B}/\mathbf{A}_1$ konačnog ranga $s$, opet je $\mathbf{B}$ konačnog ranga $(s+2)$, znači slobodna Abelova konačno generisana grupa, te je i $\mathbf{B}/\mathbf{A}_1$, kao konačno generisana torziono slobodna grupa, slobodna. Dalje formiramo podgrupu $\mathbf{A}_2$, gde je $\mathbf{A}_2/\mathbf{A}_1$ beskonačna ciklična podgrupa grupe $\mathbf{A}/\mathbf{A}_1$, sa domenom $\{a+A_1 \mid m(a+A_1) \in \langle a_{i_2}+A_1\rangle$ za neki pozitivan prirodan broj $m$, $a_{i_2}$ je prvi element skupa $X$ koji nije u $\mathbf{A}_1\}$. Tako za neki element $b_2$ dobijamo: $\mathbf{A}_2 = \langle b_2\rangle \oplus \mathbf{A}_1 = \langle b_2\rangle \oplus \langle b_1\rangle \oplus \langle b_0\rangle$. Nastavljajući postupak dobijamo eventualno beskonačan lanac podgrupa

$$\mathbf{A}_0 < \mathbf{A}_1 < \cdots < \mathbf{A}_n < \cdots$$

čija je unija cela grupa $\mathbf{A}$ i gde je, za svako $i \in \omega$, $\mathbf{A}_{i+1}/\mathbf{A}_i$ beskonačna ciklična grupa generisana elementom $b_{i+1}+A_i$ (što će reći: $\mathbf{A}_{i+1} = \langle b_{i+1}\rangle \oplus \mathbf{A}_i$). Zaključujemo: $\{b_i \mid i \in \omega\}$ je baza (slobodne Abelove) grupe $\mathbf{A}$.

U vezi ove teoreme videti i 44.17.■

## 33 Deljive grupe

U 14.7 smo definisali deljivost elementa grupe prirodnim brojem (većim od nule); s obzirom na aditivnu notaciju sada imamo:

*element $a$ (Abelove) grupe $\mathbf{A}$ deljiv je sa pozitivnim prirodnim brojem $n$ akko jednačina $a = nx$ ima rešenje u $\mathbf{A}$ (tj. postoji element $b \in A$ takav da je $a = nb = \underbrace{b+\cdots+b}_{n-puta}$).*

U tom smislu moglo bi se govoriti i o deljivosti elemenata grupe negativnim celim brojevima, no svakako ništa novo i interesantno se ne bi time dobilo. Ranije je već pokazano (videti 7.2($f$)) da rešenje, ukoliko postoji, ne mora, u opštem, biti jedinstveno. Zapravo važi: ako je, za datu grupu $\mathbf{A}$, $A[n] \overset{\text{def}}{=} \{d \in A \mid nd = 0\}$ i ako je, za $a,b \in A$, $a = nb$, onda je

$$a = nc \text{ akko } c \in b + A[n].$$



$A[n]$ je, jasno, domen podgrupe ($\mathbf{A}[n]$), pa gornju činjenicu možemo i ovako formulisati: ako jednačina $a = nx$ ima jedno rešenje – $b$, onda je skup svih rešenja koset podgrupe $\mathbf{A}[n]$ određen elementom $b$. Odatle sledi da je u torziono-slobodnim grupama rešenje jednačine $a = nx$, ukoliko postoji, jedinstveno (sada je $\mathbf{A}[n] = \mathbf{O}$ za svako $n > 0$). Videli smo već (ista referenca kao gore) i da ako je $n$ uzajamno prost sa redom elementa $a$, onda je $a$ deljivo sa $n$.

Uočimo i sledeće:

Ako je $\varphi$ homomorfno preslikavanje grupe $\mathbf{A}$ u grupu $\mathbf{B}$ i ako je element $a$ grupe $\mathbf{A}$ deljiv sa $n$, onda je i njegova homomorfna slika $(a)\varphi$ deljiva sa $n$;

Ako je $a$ deljivo sa $m$ i $n$, onda je deljivo i sa $NZS(m,n)$; jer, $NZS(m,n)\cdot NZD(m,n) = mn$, i ako su $u$ i $v$ celi brojevi takvi da je $um+vn = NZD(m,n)$, a $a = mb = nc$, tada je:

$$NZS(m,n)(vb+uc) = \frac{mn}{NZD(m,n)}(vb+uc) =$$

$$\frac{nv}{NZD(m,n)}a + \frac{mu}{NZD(m,n)}a = a;$$

Skup elemenata grupe deljivih sa $n(>0)$ domen je podgrupe – $n\mathbf{A}$ – sa domenom $nA \overset{\text{def}}{=} \{na \mid a \in A\}$. Element $a$ grupe $\mathbf{A}$ deljiv je sa $n$ akko je $a \in nA$.

Prema tome:

**$\mathbf{A}$ *je deljiva grupa akko je* $\mathbf{A} = n\mathbf{A}$ *za svaki pozitivan prirodan broj* $n$.**

Jasno, direktna (kartezijanska) suma je deljiva grupa akko je svaki sumand deljiva grupa.

Odmah sledi da osim nula grupe nijedna druga deljiva grupa nije konačna (jer, ako je $|A| = n$, onda je, jasno, $nA = \{0\}$). S obzirom da nula grupa nije od interesa, obično ćemo kada govorimo o (Abelovoj) deljivoj grupi podrazumevati da se radi o beskonačnoj grupi.

Kako je i homomorfna slika deljive grupe deljiva, to je, za pravu podgrupu $\mathbf{B}$ deljive grupe $\mathbf{A}$, faktor grupa $\mathbf{A}/\mathbf{B}$ deljiva, dakle i beskonačna. Proizilazi da $\mathbf{A}$ nema podgrupa konačnog indeksa, stoga nema ni maksimalnih podgrupa. Prema korolaru 5.13 sledi: nenula deljiva grupa nije konačno generisana i svaki njen element se može eliminisati iz svakog generatornog skupa koji ga sadrži. Ovo smo već ranije imali u slučaju aditivne grupe racionalnih brojeva i Prüferovih grupa, a uskoro ćemo pokazati da su to, na neki način, i ključne deljive grupe.

Grupa $\mathbf{Ra}$ je, jasno, deljiva. Da bismo pokazali da je i grupa $\mathbf{p}^\infty$, $p$ prost broj, deljiva koristićemo sledeće činjenice:

**Lema 33.1** *(a) Grupa* **A** *je deljiva akko je* $pA = A$ *za svaki prost broj* $p$.

*(b) Grupa* **A** *generisana skupom* $X$ *je deljiva akko je svaki element iz* $X$ *deljiv svim pozitivnim prirodnim brojevima.*

**Dokaz.** *(a)* Pravac ($\Longrightarrow$) je deo definicije, a ako je $n = p_1 \cdot \ldots \cdot p_r$ (gde ne isključujemo mogućnost da su neki od prostih faktora jednaki), onda je, uz pretpostavku da je $pA = A$ za svaki prost broj $p$:

$$nA = (p_1 \cdot \ldots \cdot p_{r-1})(p_r A) = (p_1 \cdot \ldots \cdot p_{r-1})A =$$

$$(p_1 \cdot \ldots p_{r-2})(p_{r-1}A) = (p_1 \cdot \ldots \cdot p_{r-2})A = \cdots = A.$$

*(b)* Jasno; ako je $c = k_1a_1 + \cdots + k_ma_m$, $k_i \in Z$, $a_i \in X$, i ako je, za $i = 1, \ldots, m$, $a_i = nb_i$, onda je $c = n(k_1b_1 + \cdots + k_mb_m)$.□

Grupa $\mathbf{p}^\infty$ je, podsetimo se, generisana skupom $\{a_n \ (= e^{\frac{2\pi}{p^n}i}) \mid n = 1, 2, \ldots\}$, gde je $a_n$ reda $p^n$ i $a_n = a_{n+1}^p$. Prema tome, svaki element $a_n$ je deljiv svim stepenima prostog broja $p$, a ako je $(m, p) = 1$, jednačina $a_n = x^m$ je rešiva u okviru ciklične grupe $\langle a_n \rangle$ $(7.2(f))$.

Recimo još da ćemo u 33.19 ponovo dokazati da su Prüferove grupe deljive. Iz te teoreme slede i gotova sva dosad navedena zapažanja, no dali smo ih ovim redom jer se svojom očiglednošću , takoreći, "nameću".

Provera da li je $p$-grupa deljiva svodi se u osnovi na proveru da li su svi njeni elementi reda $p$ deljivi sa svakim stepenom broja $p$. Objasnićemo to, no prvo

**Definicija 33.2** *Soklu Abelove p-grupe* **A** - $\mathbf{A}[p]$ - *zovemo najnižim slojem grupe* **A**. *Podgrupa* $\mathbf{A}[p^n]$, $n > 1$, *je n-ti sloj grupe* **A**.

*Element* $a \in A$ *je beskonačne visine u* **A** *akko je deljiv svim stepenima broja p; element a je visine n akko jednačina* $a = p^n x$ *ima rešenje u* **A** *ali ne i jednačina* $a = p^{n+1}x$. *Analogno se definiše visina elementa u podgrupi* **B** *grupe* **A** *(sam element ne mora biti i element podgrupe).*

*Grupa* **A** *je ograničena akko je skup redova njenih elemenata ograničen (sa gornje strane u skupu prirodnih brojeva).*

Visinu elementa $a$ u **A** (u podgrupi **B**) obeležavaćemo sa $h(a)$ $(h_{\mathbf{B}}(a))$, pa ćemo, ako je $a$ beskonačne visine, pisati $h(a) = \infty$. Trivijalno, $h(0) = \infty$. Ako je 0 i jedini element grupe beskonačne visine, kazaćemo da je grupa bez elemenata beskonačne visine (uporediti sa pojmom: grupa bez centra).

Sledeće činjenice, verujemo, ne treba obrazlagati:

*Ako je* **B** *podgrupa p-grupe* **A** *i* $a \in A$, *tada je* $h(a) \geq h_{\mathbf{B}}(a)$. *Ako je* $\mathbf{A} = \sum_{i \in I} \mathbf{A}_i$ *i ako je* $a_i \in \mathbf{A}_i$, *onda je* $h(a_i) = h_{\mathbf{A}_i}(a_i)$. *Ako je* $a = a_{i_1} + \cdots + a_{i_k}$, *tada je* $h(a) = min\{h(a_{i_1}), \ldots, h(a_{i_k})\}$. *Analogna tvrđenja važe i za kartezijanske sume.*



*Generalno, ako su dva elementa, a i b, različite visine, onda je* $h(a + b) = min\{h(a), h(b)\}$ *(naravno,* $\infty > n$ *za svako n). Ako su elementi iste visine* $(h(a) = h(b))$, *onda je* $h(a + b) \geq h(a)$. *Ako je* $a = mb$ *i* $(m, p) = 1$, *onda je* $h(a) = h(b)$.

*Grupa* **A** *je ograničena akko je skup visina svih njenih nenula elemenata ograničen.*

**Lema 33.3** *p-grupa* **A** *je deljiva akko je svaki element njenog najnižeg sloja beskonačne visine.*

**Dokaz.** Grupa **A** je unija rastućeg niza podgrupa $\mathbf{A}[p^n]$. Indukcijom po $n$ $(\geq 1)$ pokazujemo da je svaki element podgrupe $\mathbf{A}[p^n]$ beskonačne visine. Za $n = 1$ imamo upravo uslov leme. Pretpostavimo da je tvrđenje tačno za svako $k \leq n$ i neka je $a$ element reda $p^{n+1}$. Element $b = pa$ je reda $p^n$ te je, po induktivnoj pretpostavci, $h(b) = \infty$. Ali tada je i $h(a) = \infty$, jer ako bi bilo $h(a) = l$, onda bismo za $m > l + 1$ i neko $c \in A$ imali: $b = p^m c = pa$, pa bi iz $p(a - p^{m-1}c) = 0$ sledilo da je ili $a - p^{m-1}c = 0$ ili da je element $a - p^{m-1}c$ reda $p$, koji bi, kao takav, imao beskonačnu visinu. Oba slučaja bi implicirala $h(a) \geq m - 1$ $(> l)$, kontradiktorno pretpostavci o visini elementa $a$.□

**Lema 33.4** *Svaka (Abelova) grupa je podgrupa neke deljive grupe.*

**Dokaz.** Abelova grupa **A** generisana skupom $\{a_\alpha \mid \alpha < \lambda\}$ homomorfna je slika slobodne Abelove grupe $\sum_{\alpha<\lambda} \mathbf{Z}_\alpha$, gde je svako $\mathbf{Z}_\alpha$ kopija aditivne grupe celih brojeva. Prema tome, ako je $\varphi$ dati homomorfizam, onda $\mathbf{A} \cong \sum_{\alpha<\lambda} \mathbf{Z}_\alpha / \mathbf{Ker}(\varphi)$. Aditivna grupa celih brojeva podgrupa je pak aditivne grupe racionalnih brojeva, pa se $\sum_{\alpha<\lambda} \mathbf{Z}_\alpha$ može utopiti u direktni sumu aditivnih grupa racionalnih brojeva $\sum_{\alpha<\lambda} \mathbf{R}a_\alpha$. Naravno, nema razloga da ne smatramo da je $\sum_{\alpha<\lambda} \mathbf{Z}_\alpha$ baš podgrupa grupe $\sum_{\alpha<\lambda} \mathbf{R}a_\alpha$. Sledi da je **A** izomorfna podgrupi grupe $\sum_{\alpha<\lambda} \mathbf{R}a_\alpha / \mathbf{Ker}(\varphi)$, koja je kao homomorfna slika deljive grupe i sama deljiva.□

**Definicija 33.5** *Abelova grupa* **A** *je injektivna u klasi Abelovih grupa akko za svake dve Abelove grupe* **B** *i* **C**, *svako homomorfno preslikavanje* $\varphi$ *grupe* **B** *u* **A** *i svako injektivno homomorfno preslikavanje* $\psi$ *grupe* **B** *u* **C** *(ukoliko takvo postoji) imamo homomorfno preslikavanje* $\theta$ *grupe* **C** *u* **A** *takvo da je* $\varphi = \psi \circ \theta$.

**Definicija 33.6** *Abelova grupa* **B** *je (prava) esencijalna ekstenzija svoje podgrupe* **A** *akko je* $(A \subset B$ *i)* $\mathbf{A} \cap \mathbf{C} \neq \mathbf{O}$ *za svaku nenula podgrupu* **C** *grupe* **B**.

Svojstva injektivnosti, deljivosti i nemanja pravih esencijalnih ekstenzija podudaraju se u klasi Abelovih grupa. Važi naime:

**Teorema 33.7** *Sledeći uslovi su ekvivalentni za grupu* $\mathbf{A}$*:*

($a$) $\mathbf{A}$ *je deljiva grupa;*

($b$) $\mathbf{A}$ *je injektivna grupa;*

($c$) $\mathbf{A}$ *je direktni sumand svake grupe koja je sadrži kao podgrupu;*

($d$) $\mathbf{A}$ *nema pravih esencijalnih ekstenzija;*

($e$) $\mathbf{A}$ *nema maksimalnih podgrupa;*

($f$) $\mathbf{A}$ *nema netrivijalnih konačnih homomorfnih slika.*

**Dokaz.** ($a$) $\Longrightarrow$ ($b$) Neka je $\mathbf{A}$ deljiva grupa, $\varphi$ homomorfno preslikavanje grupe $\mathbf{B}$ u $\mathbf{A}$ i $\psi$ injektivno homomorfno preslikavanje grupe $\mathbf{B}$ u $\mathbf{C}$. Da bismo stvar pojednostavili možemo pretpostaviti, bez uticaja na opštost razmatranja, da je $\psi$ baš inkluzija ($B \subseteq C$). Na skupu $\mathcal{P}$ svih uređenih parova $(\mathbf{D}, \theta)$, gde je $\mathbf{B} \leq \mathbf{D} \leq \mathbf{C}$, $\theta \in Hom(\mathbf{D}, \mathbf{A})$ i $\theta|_B = \varphi$ (skup $\mathcal{P}$ je neprazan jer barem $(\mathbf{B}, \varphi) \in \mathcal{P}$), definišemo uređenje $\preceq$ sa

$$(\mathbf{D}_1, \theta_1) \preceq (\mathbf{D}_2, \theta_2) \text{ akko } \mathbf{D}_1 \leq \mathbf{D}_2 \text{ i } \theta_2|_{D_1} = \theta_1.$$

Očigledno, $\preceq$ je parcijalno uređenje i $\langle \mathcal{P}, \preceq \rangle$ je zatvoreno za unije lanaca. Ako je, za $\alpha < \beta$ ($< \lambda$), $(\mathbf{D}_\alpha, \theta_\alpha) \preceq (\mathbf{D}_\beta, \theta_\beta)$, onda je:

$$\bigcup_{\alpha<\lambda} (\mathbf{D}_\alpha, \theta_\alpha) = (\bigcup_{\alpha<\lambda} \mathbf{D}_\alpha, \bigcup_{\alpha<\lambda} \theta_\alpha);$$

Provera da je $\bigcup_{\alpha<\lambda} \theta_\alpha \in Hom(\bigcup_{\alpha<\lambda} \mathbf{D}_\alpha, \mathbf{A})$ trivijalna je; dobra definisanost sledi iz činjenice da je $\theta_\beta|_{D_\alpha} = \theta_\alpha$ za $\alpha < \beta$, a kako su $\theta_\alpha$, $\alpha < \lambda$, homomorfizmi, to je i $\bigcup_{\alpha<\lambda} \theta_\alpha$ homomorfizam. Prema Zornovoj lemi $(\mathcal{P}, \preceq)$ ima (bar jedan) maksimalni element, neka je to $(\mathbf{D}, \theta)$. Pokazaćemo, a time i kompletirati dokaz, da je $D = C$. Pretpostavimo suprotno i neka je $c \in C \setminus D$. Ako je $\langle c \rangle \cap D = \{0\}$, onda je $(\mathbf{D} \oplus \langle c \rangle, \overline{\theta})$, gde je $\overline{\theta}|_D = \theta$ i $(mc)\overline{\theta} = 0$ za svako $m \in Z$ (ne ulazimo u to da li je $c$ konačnog ili beskonačnog reda), u $\mathcal{P}$ i $(\mathbf{D}, \theta)$ je "strogo manje" ($\prec$) od $(\mathbf{D} \oplus \langle c \rangle, \overline{\theta})$, kontradikcija. Ako je pak $\langle c \rangle \cap D \neq \{0\}$, neka je $m$ najmanji pozitivan "umnožak" od $c$ koji "upada" u $D$; $0 \neq mc = d_0 \in D$ i $kc \notin D$ za svako pozitivno $k$ manje od $m$. Neka je $(d_0)\theta = a_0$ i $a_0 = mb_0$ ($b_0 \in A$); takvo $b_0$ postoji pošto je $\mathbf{A}$ deljiva grupa. Elementi grupe $\langle D, c \rangle$ su oblika $d + kc$, $d \in D$, $0 \leq k < m$, a za $0 \leq k_1, k_2 < m$ je:

$$(d_1 + k_1 c) + (d_2 + k_2 c) = (d_1 + d_2 + [\frac{k_1 + k_2}{m}]d_0) + (k_1 +_m k_2)c.$$

Sada se lako proverava da je preslikavanje $\overline{\theta} : \langle D, c \rangle \longrightarrow A$ definisano sa $(d + kc)\overline{\theta} = (d)\theta + kb_0$ homomorfno preslikavanje. Zaista:

$$((d_1 + k_1 c) + (d_2 + k_2 c))\overline{\theta} = (d_1 + d_2 + [\frac{k_1 + k_2}{m}]d_0 + (k_1 +_m k_2)c)\overline{\theta} =$$



$$(d_1 + d_2 + [\frac{k_1 + k_2}{m}]d_0)\theta + (k_1 +_m k_2)b_0 =$$

$$(d_1)\theta + (d_2)\theta + [\frac{k_1 + k_2}{m}]a_0 + (k_1 +_m k_2)b_0 =$$

$$(d_1)\theta + (d_2)\theta + ([\frac{k_1 + k_2}{m}]m + (k_1 +_m k_2))b_0 = (d_1)\theta + (d_2)\theta + (k_1 + k_2)b_0 =$$

$$((d_1)\theta + k_1 b_0) + ((d_2)\theta + k_2 b_0) = (d_1 + k_1 c)\overline{\theta} + (d_2 + k_2 c)\overline{\theta}.$$

Dakle, $(\mathbf{D}, \theta) \prec (\langle D, c \rangle, \overline{\theta})$, i opet kontradikcija.

($b$) $\Longrightarrow$ ($c$) Neka je $\mathbf{A}$ injektivna grupa i $\mathbf{A} \leq \mathbf{B}$. Za (iste) inkluzije $\imath_A : A \longrightarrow A$, $\imath_A : A \longrightarrow B$ (gde je $\forall a \in a\ (a)\imath_A = a$) postoji $\varphi \in Hom(\mathbf{B}, \mathbf{A})$ takvo da je $\varphi|_A = \imath_A$. No tada je $\mathbf{B} = \mathbf{A} \oplus \mathbf{Ker}(\varphi)$. Jer, ako je, za $b \in B$, $(b)\varphi = a$ ($= (a)\imath_A = (a)\varphi$), tada je $(b - a)\varphi = 0$, tj. $b - a \in Ker(\varphi)$, odnosno $b \in a + Ker(\varphi)$. Znači, $\mathbf{B} = \mathbf{A} + \mathbf{Ker}(\varphi)$, a očigledno je $\mathbf{A} \cap \mathbf{Ker}(\varphi) = \mathbf{O}$ (za $a \in A \cap Ker(\varphi)$ je $(a)\varphi = a = 0$). Recimo još da smo analogan gornjeg razmatranja (za sve grupe) već imali u 10.45($h$).

($c$) $\Longrightarrow$ ($d$) (Vrlo) očigledno.

($d$) $\Longrightarrow$ ($a$) Neka je $\mathbf{A}$ podgrupa deljive grupe $\mathbf{B}$ i neka je $A \subset B$ (u protivnom nemamo šta dokazivati). Neka je, dalje, $\mathbf{C}$ maksimalni element parcijalno uređenog skupa $\langle \{\mathbf{D} \leq \mathbf{B} \mid \mathbf{D} \neq \mathbf{O}, \mathbf{D} \cap \mathbf{A} = \mathbf{O}\}, \leq \rangle$ (skup $\{\mathbf{D} \leq \mathbf{B} \mid \mathbf{D} \neq \mathbf{O}, \mathbf{D} \cap \mathbf{A} = \mathbf{O}\}$ je po pretpostavci neprazan, a lema Zorna garantuje egzistenciju maksimalnog elementa). Tvrdimo: $\mathbf{A} \oplus \mathbf{C} = \mathbf{B}$. Zaista, u suprotnom bi, s obzirom na izbor podgrupe $\mathbf{C}$, grupa $\mathbf{B}/\mathbf{C}$ bila prava esencijalna ekstenzija grupe $(\mathbf{A} \oplus \mathbf{C})/\mathbf{C}$ ($\cong \mathbf{A}$), kontradikcija. Proizilazi: grupa $\mathbf{A}$ je direktni sumand deljive grupe $\mathbf{B}$, znači, i sama je deljiva.

($a$) $\Longrightarrow$ ($e$) Već pokazano.

($e$) $\Longrightarrow$ ($f$) Ako bi grupa $\mathbf{B}$ bila konačna netrivijalna homomorfna slika grupe $\mathbf{A}$ za homomorfno preslikavanje $\varphi$, imala bi maksimalnu podgrupu, pa bi, prema 8.7, i $\mathbf{A}$ imala maksimalnu podgrupu (koja sadrži $\mathbf{Ker}(\varphi)$), protivno uslovu ($e$).

($f$) $\Longrightarrow$ ($a$) Neka važi ($f$) i neka je $\mathbf{A}$ nenula grupa. Pretpostavka da nije deljiva značila bi da je $nA \neq A$ za neki pozitivan prirodan broj $n$. Neka je $p$ najmanji takav broj. Jasno, $p$ mora biti prost broj (videti dokaz tačke ($a$) leme 33.1). No tada je faktor grupa $\mathbf{A}/p\mathbf{A}$ nenula Abelova grupa čiji su svi nenula elementi reda $p$, pa je direktna suma cikličnih grupa reda $p$ – 10.33. Ako već sama nije konačna, onda je bilo koji od njenih sumanada njena konačna homomorfna slika (radi se o "projekciji" na njega), pa je ujedno i netrivijalna konačna homomorfna slika grupe $\mathbf{A}$ (za kompoziciju homomorfizama), suprotno našoj pretpostavci.■

**Korolar 33.8** *Neka je deljiva grupa* $\mathbf{A}$ *prava podgrupa grupe* $\mathbf{B}$ *i neka je* $\mathbf{C}$ *nenula podgrupa grupe* $\mathbf{B}$ *takva da je* $\mathbf{A} \cap \mathbf{C} = \mathbf{O}$*. Tada postoji podgrupa* $\mathbf{D}$ *grupe* $\mathbf{B}$ *takva da je* $\mathbf{B} = \mathbf{A} \oplus \mathbf{D}$ *i* $\mathbf{C} \leq \mathbf{D}$.

**Dokaz**. Primetimo da je ovo uopštenje tačke $(c)$ prethodne teoreme u smislu slobode izbora "drugog direktnog sumanda". Utoliko je i dokaz donekle ponavljanje dokaza implikacije $(b) \Longrightarrow (c)$. Posmatrajmo sledeća homomorfna preslikavanja grupe $\mathbf{A} \oplus \mathbf{C}$: $\varphi : A + C \longrightarrow A$, gde je, za $a \in A$, $c \in C$, $(a + c)\varphi = a$ i $\imath_{A+C} : A + C \longrightarrow B$. Pošto je $\mathbf{A}$ injektivna grupa, postoji homomorfizam $\psi \in Hom(\mathbf{B}, \mathbf{A})$ takav da je $\varphi = \imath_{A+C} \circ \psi$. Opet se lako pokazuje (da se ne ponavljamo) da je $\mathbf{B} = \mathbf{A} \oplus \mathbf{Ker}(\psi)$ i, naravno, $\mathbf{C} \leq \mathbf{Ker}(\psi)$.□

Prethodni korolar se može dalje uopštiti. Ali prvo

**Definicija 33.9** *Podgrupa* $\mathbf{A}$ *grupe* $\mathbf{C}$ *je apsolutni direktni sumand akko za svaku podgrupu* $\mathbf{B}$ *grupe* $\mathbf{C}$, *maksimalnu s obzirom na svojstvo:* $\mathbf{A} \cap \mathbf{B} = \mathbf{O}$, *važi* $\mathbf{C} = \mathbf{A} \oplus \mathbf{B}$.

**Lema 33.10** *Neka je* $\mathbf{A}$ *podgrupa grupe* $\mathbf{C}$ *i* $\mathbf{B}$ *maksimalna podgrupa grupe* $\mathbf{C}$ *s obzirom na svojstvo* $\mathbf{A} \cap \mathbf{B} = \mathbf{O}$. *Tada važi:*

$(a)$ $\mathbf{C}/(\mathbf{A} \oplus \mathbf{B})$ *je periodična grupa;*

$(b)$ $\mathbf{C}/(\mathbf{A} \oplus \mathbf{B})[p] \cong (\langle pC, B\rangle \cap \mathbf{A})/p\mathbf{A}$.

**Dokaz**. $(a)$ Neka je $A + B \neq c + (A + B) \in C/(A + B)$. Prema uslovu maksimalnosti $\langle c, B\rangle$ ima nenula presek sa $\mathbf{A}$, pa je, za neki pozitivan prirodan broj $k$, za neko $b \in B$ i neko $a \in A$, $kc + b = a$, a odatle je $k(c + (A + B)) = A + B$.

$(b)$ Neka je $c + (A + B) \in C/(A + B))[p]$. Tada je $pc = a + b$ za neko $a \in A$ i neko $b \in B$ (elementi $a$ i $b$ su jednoznačno određeni jer je $\mathbf{A} \cap \mathbf{B} = \mathbf{O}$), i stoga je $a = pc - b \in \langle pC, B\rangle \cap A$. Definišimo preslikavanje $\phi : C/(A + B)[p] \longrightarrow (\langle pC, B\rangle \cap A)/pA$ sa $(c + (A + B))\phi = a + pA$. Jasno, moramo prvo pokazati da je definicija korektna, tj. da ne zavisi od izbora predstavnika koseta. Neka je $c + (A + B) = c_1 + (A + B) \in C/(A + B)[p]$, $pc = a + b$, $pc_1 = a_1 + b_1$ i $c - c_1 = a_2 + b_2$. Elementi $a, a_1$ su iz $\langle pC, B\rangle$, a iz $pa_2 + pb_2 = pc - pc_1 = (a - a_1) + (b - b_1)$ sledi $a - a_1 = pa_2$, tj. $a + pA = a_1 + pA$; znači: $(c + (A + B))\phi = (c_1 + (A + B))\phi$. Zadržavajući oznake pokazujemo da $\phi$ ima svojstvo homomorfizma. Iz $pc = a + b$, $pc_1 = a_1 + b_1$ izvodimo $p(c + c_1) = (a + a_1) + (b + b_1)$, i dalje, $((c + c_1) + (A + B))\phi = (a + a_1) + pA = (a + pA) + (a_1 + pA) = (c + (A + B))\phi + (c_1 + (A + B))\phi$. Preslikavanje $\phi$ je bijekcija. $\phi$ je "na", jer ako je $a + pA \neq pA$, $a \in \langle pC, B\rangle \cap A$, onda je, za neke elemente $c \in C \setminus (A + B)$, $b \in B$, $a = pc - b$ $(c \in A + B$, tj. $c = a_1 + b_1$, impliciralo bi, redom: $a = p(a_1 + b_1) - b$, $a - pa_1 = pb_1 - b \in A \cap B = O$, $a \in pA$, kontradikcija), a prema definiciji preslikavanja $\phi$ je $(c + (A + B))\phi = a + pA$. $\phi$ je i injektivno. Ako je $pc = a + b$, $pc_1 = a_1 + b_1$, $a + pA = (c + (A + B))\phi = (c_1 + (A + B))\phi = a_1 + pA$, a $a - a_1 = pa_2$, dakle i $p(c - c_1 - a_2) = b - b_1 \in B$, diskutujemo: ako je $c - c_1 - a_2 \in B$ dobijamo odmah $c + (A + B) = c_1 + (A + B)$; ako $c - c_1 - a_2 \notin B$, tada je $\langle B, c - c_1 - a_2\rangle \cap A \neq O$.



Neka je, za neko $a_3 \in A$, $b_3 \in B$ i neki ceo broj $k$ takav da je $(k, p) = 1$, $a_3 = b_3 + k(c - c_1 - a_2)$. Tada je, za cele brojeve $u$ i $v$ takve da je $uk + vp = 1$, $c - c_1 - a_2 = (ku + vp)(c - c_1 - a_2) = ku(c - c_1 - a_2) + vp(c - c_1 - a_2) \in A + B$, dakle i $c - c_1 \in A + B$, odnosno $c + (A + B) = c_1 + (A + B)$.□

**Lema 33.11** *Direktni sumand* $\mathbf{A}$ *grupe* $\mathbf{C}$ *je apsolutni direktni sumand akko je jedan od sledeća dva uslova ispunjen:*

$(a)$ $\mathbf{A}$ *je deljiva grupa;*

$(b)$ $\mathbf{C}/\mathbf{A}$ *je periodična grupa i* $p^m(\mathbf{C}/\mathbf{A})_p = \mathbf{O}$, *ukoliko postoji element* $a \in A \setminus pA$ *reda* $p^m$ *(*$(\mathbf{C}/\mathbf{A})_p$ *je maksimalna p-podgrupa grupe* $\mathbf{C}/\mathbf{A}$*).*

**Dokaz**. $(\Longrightarrow)$ Neka je $\mathbf{A}$ apsolutni direktni sumand i $\mathbf{A} \oplus \mathbf{B} = \mathbf{C}$. Ako je $\mathbf{A}$ i deljiva grupa, nemamo što dokazivati. Pretpostavimo stoga da $\mathbf{A}$ nije deljiva grupa i neka je $p\mathbf{A} \neq \mathbf{A}$ za prost broj $p$. Pokazujemo prvo da je $\mathbf{C}/\mathbf{A}$ $(\cong \mathbf{B})$ periodična grupa. Ako je $a \in A \setminus pA$, onda je $\langle a - pb\rangle \cap \mathbf{A} \neq \mathbf{O}$ za svako $b \in B$. U suprotnom, ako bi $\mathbf{D}$ bio maksimalni element parcijalno uređenog skupa $\langle\{\langle a - pb\rangle \leq \mathbf{G} \leq \mathbf{C} \mid \mathbf{A} \cap \mathbf{G} = \mathbf{O}\}, \leq\rangle$, imali bismo, s jedne strane, $\mathbf{C} = \mathbf{A} \oplus \mathbf{D}$, a s druge, $a = pb + (a - pb) \in A \cap \langle pC, D\rangle$ i $a + pA \neq pA$, te bi prema prethodnoj lemi bilo $\mathbf{C}/(\mathbf{A} \oplus \mathbf{D})[p] \neq \mathbf{O}$, kontradikcija. Sledi da je $0 \neq n(a - pb) \in A$ za neki pozitivan prirodan broj $n$, i odatle je $npb = 0$, te je $b$ konačnog reda. Pretpostavimo sada da je $a \in A \setminus pA$ reda $p^m$ i $b \in B_p$ $(\cong (C/A)_p)$. Prema upravo rečenom, $p$-ciklična grupa $\langle a - pb\rangle$ ima nenula presek sa podgrupom $\mathbf{A}$. Ako je $0 \neq p^r(a - pb) \in A$, onda je $p^r a \neq 0$ i $p^{r+1}b = 0$. Stoga je $r \leq m - 1$, pa je svakako $p^m b = 0$.

$(\Longleftarrow)$ Neka je $\mathbf{A}$ deljiva grupa i $\mathbf{D}$ maksimalna podgrupa takva da je $\mathbf{A} \cap \mathbf{D} = \mathbf{O}$. Prema prethodnoj lemi je $\mathbf{C}/(\mathbf{A} \oplus \mathbf{D})$ periodična grupa. No, za svaki prost broj $p$ je $p\mathbf{A} = \mathbf{A}$, pa je $\mathbf{C}/(\mathbf{A} \oplus \mathbf{D})[p] \cong (\langle pC, D\rangle \cap \mathbf{A})/p\mathbf{A} = (\langle pC, D\rangle \cap \mathbf{A})/\mathbf{A}$ nula grupa. Proizilazi: $\mathbf{C}/(\mathbf{A} \oplus \mathbf{D})$ je nula grupa, tj. $\mathbf{C} = \mathbf{A} \oplus \mathbf{D}$.

Neka je sada ispunjen uslov $(b)$ i neka je $\mathbf{C} = \mathbf{A} \oplus \mathbf{B}$. Ako $\mathbf{A}$ ne bi bila apsolutni direktni sumand, postojala bi podgrupa $\mathbf{D}$ maksimalna s obzirom na svojstvo da joj je presek sa $\mathbf{A}$ nula grupa i takva da je $\mathbf{A} \oplus \mathbf{D} \neq \mathbf{C}$. Kao homomorfna slika grupe $\mathbf{C}/\mathbf{A}$ (ili prema prethodnoj lemi, svejedno) $\mathbf{C}/(\mathbf{A} \oplus \mathbf{D})$ je nenula periodična grupa, te je, za neki prost broj $p$, $(\mathbf{C}/(\mathbf{A} \oplus \mathbf{D}))_p \neq \mathbf{O}$. Zbog $\mathbf{C}/(\mathbf{A} \oplus \mathbf{D})[p] = (\mathbf{C}/(\mathbf{A} \oplus \mathbf{D}))_p[p] \neq \mathbf{O}$, dakle i $(\langle pC, D\rangle \cap \mathbf{A})/p\mathbf{A} \neq \mathbf{O}$, postoji element $a = pc + d \in A \cap \langle pC, D\rangle$, $a \in A$, $d \in D$, koji nije u $pA$, reda, recimo, $p^m$. Možemo odmah pretpostaviti da je $c \in B$ (ukoliko je $c = a_1 + b_1$, onda je $a - pa_1 = pb_1 + d$ opet element iz $(A \cap \langle pC, D\rangle) \setminus pA$). Red elementa $c$ je neki broj $p^r s$, $r \leq m$, $(s, p) = 1$ (zbog $p^m \mathbf{B}_p = \mathbf{O}$). Sada je $a_2 = sa = p(sc) + sd \in (A \cap \langle pC, D\rangle) \setminus pA$, a red elementa $sc$ je $p^r$. Naravno, $r \geq 2$ (inače, $0 \neq a_2 = sd \in A \cap D$), no $0 \neq p^{r-1}(sa) = p^r(sc) + p^r d = p^r d \in A \cap D$, kontradikcija. Mora biti, zaključujemo, $\mathbf{C} = \mathbf{A} \oplus \mathbf{D}$; prema tome, $\mathbf{A}$ je apsolutni direktni sumand.□

Naredna definicija je inspirisana analognom iz teorije polja.

**Definicija 33.12** *Neka je* $\mathbf{A}$ *podgrupa grupe* $\mathbf{B}$. *Element* $b \in B$ *je algebarski nad* $\mathbf{A}$ *akko je rešenje jednačine oblika* $kx = a$, $k \in Z$, $a \in A \setminus \{0\}$, *u suprotnom je transcedentan. Grupa* $\mathbf{B}$ *je algebarska ekstenzija svoje podgrupe* $\mathbf{A}$ *akko je svaki njen element algebarski nad* $\mathbf{A}$.

*Grupa* $\mathbf{A}$ *je algebarski zatvorena akko ne postoji njena prava algebarska ekstenzija.*

**Lema 33.13** (*a*) *Grupa* $\mathbf{B}$ *je algebarska nad svojom podgrupom* $\mathbf{A}$ *ako i samo ako je* $\mathbf{B/A}$ *periodična grupa i* $\sum_{p\in P}\mathbf{B}[p] \leq \mathbf{A}$ *(*$P$ *je skup prostih brojeva).*

(*b*) $\mathbf{A}$ *je algebarski zatvorena grupa akko je deljiva.*

**Dokaz.** (*a*) ($\Longrightarrow$) Neka je grupa $\mathbf{B}$ algebarska nad $\mathbf{A}$, $b \in B[q]$ ($qb = 0$) i neka je $b$ rešenje jednačine $mx = a \in A \setminus \{0\}$. Onda je $(m, q) = 1$, pa ako su $u$ i $v$ celi brojevi takvi da je $mu + vq = 1$, sledi: $b = (um + vq)b = ua \in A$. Dakle, $\mathbf{B}[q] \leq \mathbf{A}$ i, uopšte, $\sum_{p\in P}\mathbf{B}[p] \leq \mathbf{A}$. Ako je $b + A \neq A$ i $mb = a\ (\neq 0)$, tada je $m(b + A) = a + A = A$; $\mathbf{B/A}$ je, znači, periodična grupa.

($\Longleftarrow$) Ako je element $b$ reda $p_1p_2 \dots p_k$, $k \geq 2$, $p_i$ – prost broj (moguće je da su neki faktori jednaki), onda je $0 \neq (p_2 \dots p_k)b \in B[p_1] \leq A$. Pretpostavimo sada da je $b$ beskonačnog reda i $m(b + A) = A$. Tada je $mb = a \in A \setminus \{0\}$. Treba li još dodati da je svaki element iz $\mathbf{A}$ algebarski nad $\mathbf{A}$.

(*b*) ($\Longleftarrow$) Neka je deljiva grupa $\mathbf{A}$ podgrupa grupe $\mathbf{B}$. Ako je $\mathbf{A}$ prava podgrupa, onda je, za neku nenula podgrupu $\mathbf{C}$, $\mathbf{B} = \mathbf{A} \oplus \mathbf{C}$ i nijedan nenula element $c$ iz $C$ nije algebarski nad $\mathbf{A}$.

($\Longrightarrow$) Pretpostavimo da $\mathbf{A}$ nije deljiva grupa i neka je $\mathbf{B}$ njena prava esencijalna ekstenzija. No, $\mathbf{B}$ je i algebarska ekstenzija grupe $\mathbf{A}$; jer je, za $b \in B\setminus\{0\}$, $\langle b\rangle \cap \mathbf{A} \neq \mathbf{O}$.□

**Napomena**. Svojstvo "biti algebarska ekstenzija" je tranzitivno: ako je $\mathbf{B}$ algebarska ekstenzija podgrupe $\mathbf{A}$ i $\mathbf{C}$ algebarska ekstenzija svoje podgrupe $\mathbf{B}$ i ako je $mc = b \neq 0$, $nb = a \neq 0$, onda je $(mn)c = a$. Odatle proizilazi: ako je dat lanac grupa $\mathbf{D}_\alpha$, $\alpha < \lambda$, gde je $\mathbf{D}_{\alpha+1}$ algebarska ekstenzija grupe $\mathbf{D}_\alpha$, a za granični ordinal $\gamma$ je $\mathbf{D}_\gamma = \bigcup_{\alpha<\gamma}\mathbf{D}_\alpha$, tada je $\mathbf{D}_\lambda = \bigcup_{\alpha<\lambda}\mathbf{D}_\alpha$ algebarska ekstenzija grupe $\mathbf{D}_0$.

**Lema 33.14** *Neka je* $\mathbf{A}$ *podgrupa grupe* $\mathbf{C}$. *Tada postoji podgrupa* $\mathbf{B}$ *grupe* $\mathbf{C}$ *koja je algebarska ekstenzija grupe* $\mathbf{A}$ *i maksimalna je takva (moguće je da je* $\mathbf{B} = \mathbf{C}$*). Pored toga, za svaki prost broj* $p$ *i svako* $a \in A$ *jednačina* $px = a$ *je rešiva u* $\mathbf{B}$ *akko je rešiva u* $\mathbf{C}$.

**Dokaz**. Parcijalno uređen skup $\langle \mathcal{P}, \leq\rangle$, gde je $\mathcal{P} = \{\mathbf{D} \leq \mathbf{C} \mid \mathbf{D}$ je algebarska ekstenzija grupe $\mathbf{A}\}$ ($\mathcal{P} \neq \emptyset$ jer je $\mathbf{A} \in \mathcal{P}$), zatvoren je za unije lanaca i prema lemi Zorna ima maksimalni element – $\mathbf{B}$. Pretpostavimo da je za $a \in A \setminus \{0\}$



i prost broj $p$ jednačina $a = px$ rešiva u $\mathbf{C}$ ali ne i u $\mathbf{B}$. Neka je $a = pc$. Ali tada je $\langle B, c\rangle = \langle\{b + kc \mid 0 \leq k < p, b \in B\}, +\rangle$ prava algebarska ekstenzija grupe $\mathbf{B}$ (dakle i grupe $\mathbf{A}$); jer, $p(kc + b) = ka + pb \in B$ i ako je $ka + pb = 0$, tj. $ka = -pb$, onda za cele brojeve $u$ i $v$ takve da je $uk + vp = 1$ dobijamo $a = uka + vpa = p(-ub + va) \in pB$ (suprotno pretpostavci $a \notin pB$). Polazna pretpostavka o rešivosti jednačine $a = px$ u $\mathbf{C}$ ali ne i u $\mathbf{B}$ vodi, dakle, u kontradikciju.□

Injektivnost (deljivost) Abelove grupe implicira i rešivost svakog "razumnog" sistema linearnih jednačina u njoj. No prvo

**Definicija 33.15** *Sistem linearnih jednačina nad grupom* $\mathbf{A}$ *je skup jednačina oblika:*

$$k_{\alpha_1}x_{\beta_1} + \dots + k_{\alpha_{m_\alpha}}x_{\beta_{m_\alpha}} = a_\alpha,\quad k_{\alpha_j} \in Z,\ a_\alpha \in A,\ \alpha < \mu \qquad (*).$$

*U opštem, taj skup može biti beskonačan* ($\mu \geq \aleph_0$) *i u tom slučaju je moguće da je i skup nepoznatih* $\{x_\beta \mid \beta < \lambda\}$ *beskonačan* ($\lambda \geq \aleph_0$).

*Sistem je kompatibilan akko kad god je linearna kombinacija levih strana jednaka nuli, onda je i odgovarajuća linearna kombinacija desnih strana jednaka nuli; drugim rečima, ako je* $l_\alpha(x)$ *leva strana jednačine* $(*)$, *tada:*

$$m_1l_{\alpha_1}(x) + \dots + m_kl_{\alpha_k}(x) = 0 \Longrightarrow m_1a_{\alpha_1} + \dots + m_ka_{\alpha_k} = 0.$$

*Sistem je rešiv u* $\mathbf{A}$ *akko postoji podskup* $\{b_\beta \mid \beta < \lambda\}$ *domena* $A$ *takav da je za svako* $\alpha < \mu$:

$$k_{\alpha_1}b_{\beta_1} + \dots + k_{\alpha_{m_\alpha}}b_{\beta_{m_\alpha}} = a_\alpha.$$

Naravno, pod "razumnim" sistemom linearnih jednačina podrazumevamo upravo kompatibilan sistem, jer je uslov kompatibilnosti, trivijalno, potreban uslov za rešivost sistema; nažalost, u opštem, nije i dovoljan. Ali

**Lema 33.16** *Svaki kompatibilan sistem linearnih jednačina nad deljivom grupom* $\mathbf{A}$ *je rešiv u* $\mathbf{A}$.

**Dokaz**. Ostajemo pri već uvedenoj notaciji. Skup nepoznatih $\{x_\beta \mid \beta < \lambda\}$ posmatrajmo kao slobodni generatorni skup (bazu) slobodne Abelove grupe $\mathbf{F}$ (ranga $\lambda$). Neka je $\mathbf{G}$ podgrupa grupe $\mathbf{F}$ generisana skupom $\{l_\alpha(x) \mid \alpha < \mu\}$. Preslikavanje $\varphi : l_\alpha(x) \longrightarrow a_\alpha$, $\alpha < \mu$, generatornog skupa grupe $\mathbf{G}$ u $A$ može se proširiti do homomorfizma $\overline{\varphi} \in Hom(\mathbf{G}, \mathbf{A})$ akko je sistem jednačina kompatibilan. Ako postoji takvo $\overline{\varphi}$ ($(l_\alpha(x))\overline{\varphi} = (l_\alpha(x))\varphi = a_\alpha$ za svako $\alpha < \mu$) i ako je $m_1l_{\alpha_1}(x) + \dots + m_kl_{\alpha_k}(x) = 0$, onda je i:

$$(m_1l_{\alpha_1}(x) + \dots + m_kl_{\alpha_k}(x))\overline{\varphi} = m_1(l_{\alpha_1}(x))\varphi + \dots + m_k(l_{\alpha_k}(x))\varphi =$$

$$m_1a_{\alpha_1} + \dots + m_ka_{\alpha_k} = (0)\overline{\varphi} = 0.$$

S druge strane, ako je sistem kompatibilan, preslikavanje $\overline{\varphi}: G \longrightarrow A$ definisano sa $(m_1 l_{\alpha_1}(x) + \cdots + m_k l_{\alpha_k}(x))\overline{\varphi} = m_1(l_{\alpha_1}(x))\varphi + \cdots + m_k(l_{\alpha_k}(x))\varphi = m_1 a_{\alpha_1} + \cdots + m_k a_{\alpha_k}$ je homomorfno. Jasno, samo je dobra definisanost u pitanju, no ako je $m_1 l_{\alpha_1}(x) + \cdots + m_k l_{\alpha_k}(x) = n_1 l_{\gamma_1}(x) + \cdots + n_l l_{\gamma_l}(x)$, po uslovu kompatibilnosti je $m_1 a_{\alpha_1} + \cdots + m_k a_{\alpha_k} = n_1 a_{\gamma_1} + \cdots + n_l a_{\gamma_l}$, tj. $(m_1 l_{\alpha_1}(x) + \cdots + m_k l_{\alpha_k}(x))\overline{\varphi} = (n_1 l_{\gamma_1}(x) + \cdots + n_l l_{\gamma_l}(x))\overline{\varphi}$.

Za homomorfizme $\overline{\varphi}: G \longrightarrow A$ i $\imath_G: G \longrightarrow F$ postoji, s obzirom da je $\mathbf{A}$ injektivna grupa, homomorfizam $\psi \in Hom(\mathbf{F}, \mathbf{A})$ takav da je $\overline{\varphi} = \imath_G \circ \psi$ (dakle, $\psi|_G = \overline{\varphi}$), pa je $\{b_\beta\ (= (x_\beta)\psi) \mid \beta < \lambda\}$ rešenje sistema:

$$(k_{\alpha_1} x_{\beta_1} + \cdots + k_{\alpha_m} x_{\beta_m})\psi = k_{\alpha_1}(x_{\beta_1})\psi + \cdots + k_{\alpha_m}(x_{\beta_m})\psi =$$

$$k_{\alpha_1} b_{\beta_1} + \cdots + k_{\alpha_m} b_{\beta_m} = (l_\alpha(x))\overline{\varphi} = (l_\alpha(x))\varphi = a_\alpha.\square$$

**Korolar 33.17** *Sistem linearnih jednačina nad deljivom grupom* $\mathbf{A}$ *je rešiv u* $\mathbf{A}$ *akko je svaki njegov konačan podsistem rešiv u* $\mathbf{A}$.

**Dokaz.** Direktna posledica prethodne leme i očigledne činjenice da je sistem kompatibilan akko je svaki njegov konačan podsistem kompatibilan. I recimo za svaki slučaj, ovo tvrđenje ne važi u opštem. Čitalac upoznat sa osnovama teorije modela lako će naći i drugi dokaz ovog tvrđenja koristeći teoremu kompaktnosti (naravno, i u osnovi tog dokaza ostaje činjenica da je deljiva grupa direktni sumand svake "nadgrupe").$\square$

Razmatranja iz prethodne leme iskoristićemo za dokaz sledećeg stava.

**Lema 33.18** *Podgrupa* $\mathbf{A}$ *grupe* $\mathbf{B}$ *je direktni sumand akko je svaki sistem linearnih jednačina nad* $\mathbf{A}$ *(u* $(*)$ *je* $a_\alpha$ *iz* $A$*) koji je rešiv u* $\mathbf{B}$ *rešiv i u* $\mathbf{A}$.

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{A}$ direktni sumand grupe $\mathbf{B}$ i neka je sistem jednačina oblika $(*)$ (koristimo notaciju iz 33.15) rešiv u $\mathbf{B}$. Neka je, opet, $\mathbf{F}$ slobodna Abelova grupa generisana skupom nepoznatih $\{x_\beta \mid \beta < \lambda\}$, $\mathbf{G}$ njena podgrupa generisana skupom $\{l_\alpha(x) \mid \alpha < \mu\}$, $\{b_\beta \mid \beta < \lambda\}$ rešenje sistema u $\mathbf{B}$. Preslikavanje $x_\beta \longrightarrow b_\beta$ proširuje se do homomorfnog preslikavanja $\psi: F \longrightarrow B$, a $\varphi = \psi|_G$ je homomorfno preslikavanje grupe $\mathbf{G}$ u $\mathbf{A}$ ($(l_\alpha(x))\psi = k_{\alpha_1} b_{\beta_1} + \cdots + k_{\alpha_m} b_{\beta_m} = a_\alpha \in A$). Prema 30.14 postoji tada i homomorfno preslikavanje $\theta$ grupe $\mathbf{F}$ u $\mathbf{A}$ koje je ekstenzija preslikavanja $\varphi$, pa je $\{(x_\beta)\theta \mid \beta < \lambda\}$ rešenje sistema u $\mathbf{A}$:

$$a_\alpha = (l_\alpha(x))\varphi = (l_\alpha(x))\theta = k_{\alpha_1}(x_{\beta_1})\theta + \cdots + k_{\alpha_m}(x_{\beta_m})\theta.$$

Ovaj pravac se lako i direktno dokazuje.

($\Longleftarrow$) Neka je grupa $\mathbf{B}$ generisana skupom $A \cup \{b_\beta \mid \beta < \lambda\}$ i $\mathbf{F}$ slobodna Abelova grupa ranga $\lambda$ sa bazom $\{x_\beta \mid \beta < \lambda\}$. Preslikavanje $x_\beta \longrightarrow b_\beta$, $\beta < \lambda$, proširuje se do homomorfizma $\psi \in Hom(\mathbf{F}, \mathbf{B})$. Neka je $\mathbf{F}_1 = (\mathbf{A} \cap (\mathbf{F})\psi)\psi^{-1}$ i $\varphi = \psi|_{F_1}$. Jasno, $\varphi \in Hom(\mathbf{F}_1, \mathbf{A})$. $\mathbf{F}_1$ je i sama slobodna Abelova grupa ranga $\mu \leq \lambda$, recimo sa bazom $\{l_\alpha(x) \mid \alpha < \mu\}$, gde je $l_\alpha(x) = k_{\alpha_1} x_{\beta_1} + \cdots + k_{\alpha_m} x_{\beta_m}$. Ako je $a_\alpha = (l_\alpha(x))\varphi = (l_\alpha(x))\psi = k_{\alpha_1}(x_{\beta_1})\psi + \cdots + k_{\alpha_m}(x_{\beta_m})\psi$, vidimo da je sistem linearnih jednačina $\{l_\alpha(x) = a_\alpha \mid \alpha < \mu\}$ nad $\mathbf{A}$ rešiv u $\mathbf{B}$, pa je, po uslovu, rešiv i u $\mathbf{A}$. Neka je skup rešenja, pretpostavljamo da je $\kappa\ (\geq \mu)$ nepoznatih, $\{a'_\beta \mid \beta < \kappa\}$. Sada je moguće naći homomorfno preslikavanje $\theta \in Hom(\mathbf{F}, \mathbf{A})$ takvo da je $\theta|_{F_1} = \varphi$. Naravno, stavićemo $x_{\beta_i} \longrightarrow a'_{\beta_i}$, a ostale elemente baze, ukoliko ima preostalih, možemo preslikati u proizvoljne elemente podgrupe $\mathbf{A}$. $\theta$ je onda inducirani homomorfizam (zbog $(l_\alpha(x))\theta = a_\alpha = (l_\alpha(x))\varphi$ važi i $\theta|_{F_1} = \varphi$). Dalje rezonujemo kao u 30.14.$\square$



Sledeća teorema daje potpun opis deljivih grupa i ujedno objašnjava zašto su $\mathbf{Ra}$ i Prüferove grupe ključne deljive grupe.

**Teorema 33.19** *Svaka nenula deljiva grupa je direktna suma grupa izomorfnih bilo aditivnoj grupi racionalnih brojeva bilo nekoj Prüferovoj grupi.*

**Dokaz.** Neka je $\mathbf{A}$ deljiva grupa. Periodični deo $t\mathbf{A}$ grupe $\mathbf{A}$ je takođe deljiva grupa, jer ako je $a \in tA$ i $a = nb$, onda je i $b$ konačnog reda. Stoga je, prema prethodnoj teoremi, $\mathbf{A} = t\mathbf{A} \oplus \mathbf{B}$, gde je podgrupa $\mathbf{B}$ ($\cong \mathbf{A}/t\mathbf{A}$) torziono slobodna i deljiva (kao direktni sumand ali i kao homomorfna slika deljive grupe). Opet, $t\mathbf{A}$ je direktna suma primarnih grupa: $t\mathbf{A} = \sum_{p \in Q} \mathbf{A}_p$ ($Q$ je podskup skupa prostih brojeva), koje su, ponavljamo, kao direktni sumandi deljive grupe i same deljive grupe. Prema tome, dovoljno je razmotriti samo slučajeve primarnih i torziono slobodnih deljivih grupa.

Neka je $a \in A_p$ reda $p^n$ i neka je: $a_1 = p^{n-1}a$, $a_2 = p^{n-2}a$, ..., $a_{n-1} = pa$, $a_n = a$, $a_{n+1}$ rešenje jednačine $a_n = px$, $a_{n+2}$ rešenje jednačine $a_{n+1} = px$ itd. Skup $\{a_k \mid k \in \omega \setminus \{0\}\}$ generiše, s obzirom na navedene relacije (videti 21.10($r$)), grupu $\mathbf{p}^\infty_a$, koja je, kao deljiva, direktni sumand grupe $\mathbf{A}_p$. Neka je $b \in A_p \setminus p^\infty_a$. Ako je $\langle b \rangle \cap p^\infty_a = \{0\}$, konstruišemo na isti način grupu $\mathbf{p}^\infty_b$, pa smo tako dobili podgrupu $\mathbf{p}^\infty_a \oplus \mathbf{p}^\infty_b$ grupe $\mathbf{A}_p$. Ako je $\langle b \rangle \cap p^\infty_a \neq \{0\}$, a $p^k$ najmanji "umnožak" elementa $b$ koji "upada" u $p^\infty_a$, nalazimo u $\mathbf{p}^\infty_a$ rešenje jednačine $p^k b = p^k x$, neka je to $c$, pa radimo sa elementom $b - c = d$ ($\notin p^\infty_a$). Očigledno, $\langle d \rangle \cap p^\infty_a = \{0\}$ i $\mathbf{p}^\infty_a \cap \mathbf{p}^\infty_d = \mathbf{O}$. Nastavljajući postupak konačno bismo iscrpli sve elemente, a grupa $\mathbf{A}_p$ se javlja kao direktna suma Prüferovih $\mathbf{p}^\infty$ grupa. Formalno, možemo pretpostaviti da je skup $A_p$ dobro uređen (aksioma izbora nam to dozvoljava), npr. $\mathbf{A}_p = \{c_\alpha \mid \alpha < \lambda\}$; naš prvi element $a$ bi bio $c_0$, element $b$ bi bio prvi element (s obzirom na dato uređenje) koji se ne javlja u $\mathbf{p}^\infty_a = \mathbf{p}^\infty_{c_0}$ i tako redom.

Pređimo sada na torziono slobodni direktni sumand $\mathbf{B}$ grupe $\mathbf{A}$. Neka je $\{b_\alpha \mid \alpha < \mu\}$ maksimalan linearno nezavisan sistem grupe $\mathbf{B}$. Svaki od elemenata $b_\alpha$ odrediće jednu podgrupu izomorfnu aditivnoj grupi racionalnih brojeva. Uzmimo, primera radi, element $b_0 = d_1$. Neka je $d_2$ rešenje jednačine $d_1 = 2x$, $d_3$ rešenje jednačine $d_2 = 3x$, ..., $d_{n+1}$ rešenje jednačine $d_n = (n +$

$1)x$ (sva ova rešenja su jedinstvena jer smo u torziono slobodnoj grupi). Skup $\{d_k \mid k \in \omega \setminus \{0\}\}$ generiše, prema datim relacijama, grupu $\mathbf{Ra}_{b_0}$ izomorfnu aditivnoj grupi racionalnih brojeva (21.10($p$)), a $\mathbf{Ra}_{b_\alpha} \cap \langle \bigcup_{\beta \neq \alpha} Ra_{b_\beta} \rangle = \mathbf{O}$ (u racionalnoj grupi za svaka dva nenula elementa $c, d$ postoje nenula celi brojevi $m, n$ takvi da je $mc = nd$, a skup $\{b_\alpha \mid \alpha < \mu\}$ je linearno nezavisan). Sledi: $\mathbf{B} = \sum_{\alpha<\mu} \mathbf{Ra}_{b_\alpha}$; jer, za $b \in B \setminus \sum_{\alpha<\mu} Ra_{b_\alpha}$, $mb = k_1 b_{\alpha_1} + \cdots + k_n b_{\alpha_n}$, $m \in Z \setminus \{0\}$ i $k_1 b_{\alpha_1} + \cdots + k_n b_{\alpha_n} = mc$, $c \in \sum_{\alpha\in\mu} Ra_{b_\alpha}$ (takav element postoji jer je $\sum_{\alpha<\mu} \mathbf{Ra}_{b_\alpha}$ deljiva grupa), imali bismo $mb = mc$, tj. $b = c$, kontradikcija.■

**Korolar 33.20** ($a$) *Svake dve dekompozicije deljive grupe u direktnu sumu grupa tipa* $\mathbf{Ra}$ *i* $\mathbf{p}^\infty$, $p$ *prost broj, izomorfne su.*

($b$) *Sve torziono slobodne deljive grupe fiksnog reda većeg od* $\aleph_0$ *su izomorfne; Dve prebrojive torziono slobodne deljive grupe su izomorfne akko su istog torziono slobodnog ranga.*

($c$) *Sve $p$-primarne deljive grupe fiksnog reda većeg od* $\aleph_0$ *su izomorfne; Dve prebrojive $p$-primarne deljive grupe* $\mathbf{A}$ *i* $\mathbf{B}$ *su izomorfne akko su njihove podgrupe* $\mathbf{A}[p]$ *i* $\mathbf{B}[p]$ *istog reda, konačnog ili beskonačnog.*

**Dokaz.** ($a$) Napomenimo samo: torziono slobodni rang deljive grupe $\mathbf{C}$ određen je brojem sumanada tipa $\mathbf{Ra}$, a red podgrupe $\mathbf{C}[p]$ određen je brojem sumanada tipa $\mathbf{p}^\infty$ – red podgrupe $\mathbf{C}[p]$ je $p^m$ akko ima $m$ sumanada tipa $\mathbf{p}^\infty$; $|C[p]| = \lambda \geq \aleph_0$ akko ima $\lambda$ sumanada tipa $\mathbf{p}^\infty$.□

Prema korolaru sledi da, do na izomorfizam, postoji (beskonačno) prebrojivo mnogo prebrojivih torziono slobodnih i $p$-primarnih ($p$-prost broj) deljivih grupa. Prebrojivih deljivih grupa ima kontinuum (imati u vidu da toliko već ima podskupova skupa prostih brojeva).

Za fiksni kardinal $\lambda > \aleph_0$ postoje po jedna torziono slobodna i $p$-primarna deljiva grupa reda $\lambda$. Deljiva grupa reda $\lambda$ direktna je suma $\lambda$ nerazloživih deljivih grupa tipa $\mathbf{Ra}$ i $\mathbf{p}^\infty$, $p$ prost broj. Aditivna grupa realnih brojeva jedina je (do na izomorfizam) torziono slobodna deljiva grupa reda kontinuum: $\mathbf{Re} \cong \sum_{\alpha<c} \mathbf{Ra}_\alpha$, gde je $c = 2^{\aleph_0}$ – kontinuum, $\mathbf{Ra}_\alpha$ kopija aditivne grupe racionalnih brojeva.

**Korolar 33.21** *Za svaki ordinal* $\alpha$ *postoji Abelova* $\aleph_\alpha$*-univerzalna grupa.*

**Dokaz.** Prema 33.4 i prethodnoj teoremi, za dati ordinal $\alpha$ jedna Abelova $\aleph_\alpha$-univerzalna grupa je

$$\sum_{\beta<\aleph_\alpha} \mathbf{Ra}_\beta \oplus \sum_{p\in P} \Big( \sum_{\gamma<\aleph_\alpha} \mathbf{p}^\infty_\gamma \Big),$$

gde su, za $\beta, \gamma < \aleph_\alpha$, $\mathbf{Ra}_\beta$ i $\mathbf{p}^\infty_\gamma$ "kopije", respektivno, aditivne grupe racionalnih brojeva i Prüferove $p$-grupe, a $P$ je skup svih prostih brojeva.□



**Korolar 33.22** *Ako je polje* $\mathbf{F} = \langle F, +, \cdot \rangle$ *karakteristike* 0, *onda je grupa* $\langle F, + \rangle$ *direktna suma kopija aditivne grupe racionalnih brojeva.*

**Dokaz.** Pokazujemo, a to je i dovoljno, da je $\langle F, + \rangle$ deljiva grupa. Neka je $a \in F \setminus \{0\}$ i $1 < m \in N$. Onda je

$$m((m1)^{-1}a) = \underbrace{(m1)^{-1}a + \cdots + (m1)^{-1}a}_{m-puta} = \underbrace{(1 + \cdots + 1)}_{m-puta}(m1)^{-1}a =$$

$$(m1)(m1)^{-1}a = a;$$

dakle, jednačina $a = mx$ je rešiva za svako $a \in F$ i svako $m \in N$.□

**Teorema 33.23** *Svaka Abelova grupa* $\mathbf{A}$ *je podgrupa injektivne (deljive) grupe* $\mathbf{D}$ *koja je ujedno i njena esencijalna ekstenzija. Štaviše, takva ekstenzija je jedinstvena do na izomorfizam.*

**Dokaz.** Ako je $\mathbf{A}$ deljiva grupa, onda za $\mathbf{D}$ uzimamo baš $\mathbf{A}$ (prema prethodnoj teoremi $\mathbf{A}$ nema pravih esencijalnih ekstenzija). Pretpostavimo stoga da $\mathbf{A}$ nije deljiva grupa i neka je podgrupa deljive grupe $\mathbf{B}$. Parcijalno uređen skup $\langle \{\mathbf{C} \leq \mathbf{B} \mid \mathbf{C}$ je esencijalna ekstenzija podgrupe $\mathbf{A}\}$ $(= \mathcal{P}), \leq \rangle$ zatvoren je za unije lanca; jer, ako je, za $\alpha < \beta$ $(< \lambda)$, $\mathbf{C}_\alpha \leq \mathbf{C}_\beta$, $\mathbf{C}_\alpha, \mathbf{C}_\beta \in \mathcal{P}$, i ako je $\mathbf{C}$ nenula podgrupe grupe $\bigcup_{\alpha<\lambda} \mathbf{C}_\alpha$, onda za $0 \neq c \in C$ postoji $\gamma$ $(< \lambda)$ tako da je $\langle c \rangle \leq \mathbf{C}_\gamma$, i pošto je $\mathbf{C}_\gamma \in \mathcal{P}$, $\langle c \rangle \cap \mathbf{A} \neq \mathbf{O}$. Prema Zornovoj lemi $\langle \mathcal{P}, \leq \rangle$ ima (bar jedan) maksimalni element; neka to bude $\mathbf{D}$. No, $\mathbf{D}$ je bez pravih esencijalnih ekstenzija, stoga je i deljiva grupa. Zaista, ako bi $\mathbf{G}$ bila prava esencijalna ekstenzija grupe $\mathbf{D}$, tada bismo za identična utapanja $\imath_D : D \longrightarrow G$ i $\imath_D : D \longrightarrow B$ imali, s obzirom da je $\mathbf{B}$ injektivna grupa, homomorfno preslikavanje $\varphi : G \longrightarrow B$ takvo da je $\varphi|_D = \imath_D$. Sledilo bi: $\mathbf{Ker}(\varphi) \cap \mathbf{D} = \mathbf{O}$ (za $d \in D \cap Ker(\varphi)$ je $(d)\varphi = d = 0$), pa mora biti $\mathbf{Ker}(\varphi) = \mathbf{O}$. $\varphi$ je, prema tome, injektivni homomorfizam, te je $(\mathbf{G})\varphi \cong \mathbf{G}$ i $(\mathbf{G})\varphi$ $(\leq \mathbf{B})$ je, kao prava esencijalna ekstenzija podgrupe $\mathbf{D}$, element skupa $\mathcal{P}$, kontradiktorno pretpostavci o izboru podgrupe $\mathbf{D}$. Uočimo da je $\mathbf{D}$ i minimalna deljiva podgrupa grupe $\mathbf{B}$ koja sadrži $\mathbf{A}$; za deljivu podgrupu $\mathbf{D}_1$ takvu da je $\mathbf{A} \leq \mathbf{D}_1 \leq \mathbf{D}$ imali bismo $\mathbf{D} = \mathbf{D}_1 \oplus \mathbf{C}$ (za neku podgrupu $\mathbf{C}$), pa ako $\mathbf{C}$ ne bi bila nula grupa, $\mathbf{D}$ ne bi bila esencijalna ekstenzija grupe $\mathbf{A}$.

Neka je i deljiva grupa $\mathbf{F}$ esencijalna ekstenzija grupe $\mathbf{A}$. Za identična utapanja $\imath_A : A \longrightarrow D$ i $\imath_A : A \longrightarrow F$ postoji (pošto je $\mathbf{F}$ injektivna grupa) $\psi \in Hom(\mathbf{D}, \mathbf{F})$ takvo da je $\psi|_A = \imath_A$. Kao i u prethodnim razmatranjima trivijalno sledi $Ker(\psi) \cap A = \{0\}$, dakle i $\mathbf{Ker}(\psi) = \mathbf{O}$ ($\mathbf{D}$ je, imamo na umu, esencijalna ekstenzija grupe $\mathbf{A}$). $\psi$ je, znači, utapanje (injektivni homomorfizam), pa je onda i surjektivno preslikavanje; u suprotnom bi za deljivu grupu $(\mathbf{D})\psi$ bilo $A \subseteq (D)\psi \subset F$, opet protivno pretpostavci da je $\mathbf{F}$ esencijalna ekstenzija grupe $\mathbf{A}$.■

**Definicija 33.24** *Esencijalna deljiva ekstenzija grupe* $\mathbf{A}$ *zove se injektivni ili deljivi omotač grupe* $\mathbf{A}$.

Injektivni omotač grupe $\mathbf{A}$ obeležićemo sa $\mathbf{I}(\mathbf{A})$ (koriste se i druge oznake, npr. $\mathbf{E}(\mathbf{A})$, po engleskoj reči *envelope* = omot). Svaka deljiva ekstenzija grupe $\mathbf{A}$ sadrži bar jedan njen injektivni omotač. S druge strane, injektivni omotač grupe $\mathbf{A}$ je najmanja deljiva grupa koja sadrži $\mathbf{A}$. Ako je $\mathbf{A}$ deljiva grupa, ona je jednaka svom injektivnom omotaču.

**Lema 33.25** *Abelova grupa* $\mathbf{A}$ *je ranga* 1 *akko je njen injektivni omotač izomorfan ili aditivnoj grupi racionalnih brojeva* $\mathbf{Ra}$ *ili nekoj Prüferovoj grupi (akko je grupa* $\mathbf{A}$ *izomorfna ili nekoj podgrupi grupe* $\mathbf{Ra}$ *ili nekoj kockičnoj grupi).*

**Dokaz.** Pravac($\Longleftarrow$) je jasan; $\mathbf{Ra}$ i $\mathbf{p}^\infty$ su grupe ranga 1.

($\Longrightarrow$) Neka je $\mathbf{I}(\mathbf{A}) = \sum_{\alpha<\lambda} \mathbf{D}_\alpha$, gde je $\mathbf{D}_\alpha$ izomorfna ili grupi $\mathbf{Ra}$ ili nekoj Prüferovoj grupi. Ako je $\lambda \geq 2$, onda je, za nenula elemente $a_0 \in D_0$, $a_1 \in D_1$, $\langle a_i\rangle \cap \mathbf{A} \neq \mathbf{O}$ $(i = 0,1)$. Ako su $k_0$, $k_1$ najmanji pozitivni celi brojevi takvi da je $k_i a_i \in A$, $i = 0,1$, dobijamo da je $\{k_0a_0, k_1a_1\}$ linearno nezavisan ili slabo linearno nezavisan sistem (ako je bar jedan od elemenata $a_0, a_1$ konačnog reda), pa je i $r(\mathbf{A}) \geq 2$.□

**Lema 33.26** *Deljiva grupa* $\mathbf{A}$ *je injektivni omotač svoje podgrupe* $\mathbf{B}$ *akko je* $\mathbf{A}/\mathbf{B}$ *periodična grupa i* $A[p] = B[p]$ *za svaki prost broj* $p$.

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{A}$ injektivni omotač podgrupe $\mathbf{B}$. Trivijalno je, za svaki prost broj $p$, $A[p] = B[p]$; u suprotnom bismo, za $a \in A[p] \setminus B[p]$, imali $\langle a\rangle \cap \mathbf{B} = \mathbf{O}$. Isto tako $\mathbf{A}/\mathbf{B}$ mora biti periodična grupa; jer ako je $n(a + B) \neq B$ (tj. $na \notin B$) za svaki pozitivan prirodan broj $n$, ponovo je $\langle a\rangle \cap \mathbf{B} = \mathbf{O}$.

($\Longleftarrow$) Pretpostavimo da su ispunjeni uslovi leme ali da grupa $\mathbf{A}$ nije injektivni omotač podgrupe $\mathbf{B}$. Onda postoji prava deljiva podgrupa $\mathbf{C}$ takva da je $B \subseteq C \subset A$. No tada je $\mathbf{A} = \mathbf{C} \oplus \mathbf{D}$ za neku (nenula) podgrupu $\mathbf{D}$, pa ako je $0 \neq d \in D$ element konačnog – možemo odmah pretpostaviti prostog reda $p$, to protivureči uslovu $A[p] = B[p]$, a ako je beskonačnog reda, homomorfna slika grupe $\mathbf{A}/\mathbf{B}$ – $\mathbf{A}/\mathbf{C} \cong (\mathbf{A}/\mathbf{B})/(\mathbf{C}/\mathbf{B})$ $(\cong \mathbf{D})$ – nije periodična, pa samim tim ni $\mathbf{A}/\mathbf{B}$ nije periodična, kontradikcija opet. □.

**Lema 33.27** *Ako je* $\mathbf{B}_i$ *esencijalna ekstenzija grupe* $\mathbf{A}_i$ *za svako* $i \in I$, *onda je i* $\sum_{i\in I} \mathbf{B}_i$ *esencijalna ekstenzija grupe* $\sum_{i\in I} \mathbf{A}_i$.

**Dokaz.** Koristimo se sledećom očiglednom činjenicom:

*Grupa* $\mathbf{B}$ *je esencijalna ekstenzija grupa* $\mathbf{A}$ *akko je* $\langle b\rangle \cap \mathbf{A} \neq \mathbf{O}$ *za svaki nenula element* $b$ *iz* $B$.



Dokaz sada dajemo indukcijom po kardinalnosti nosača elemenata. Tvrđenje trivijalno važi za $n = 1$. Pretpostavimo da je tačno i za svako $k \leq n$ $(\geq 1)$ i neka je $|S(b)| = n+1$, $b = b_{i_1} + \cdots + b_{i_n} + b_{i_{n+1}}$. Kako je $\langle b_{i_{n+1}}\rangle \cap A_{i_{n+1}} \neq \{0\}$, to je, za neki pozitivan prirodan broj $k$, $0 \neq kb_{i_{n+1}} = a_{i_{n+1}} \in A_{i_{n+1}}$. Ako je $c = kb_{i_1} + \cdots + kb_{i_n} = 0$, sledi $kb = kb_{i_{n+1}} = a_{i_{n+1}}$, u suprotnom je, po induktivnoj pretpostavci, za neki pozitivan prirodan broj $l$, $0 \neq lc = (lk)b_{i_1} + \cdots + (lk)b_{i_n} \in A_{i_1} + \cdots + A_{i_n}$, pa je $0 \neq (lk)b \in A_{i_1} + \cdots + A_{i_{n+1}} \subseteq \sum_{i\in I}^{d} A_i$.□

**Korolar 33.28** $\mathbf{I}(\sum_{i\in I} \mathbf{A}_i) = \sum_{i\in I} \mathbf{I}(\mathbf{A}_i)$.

**Primer 33.29** (*a*) *Grupa* $\mathbf{Ra}$ *se ne preslikava homomorfno ni na jednu svoju pravu nenula podgrupu.*

**Dokaz.** Ako bi se grupa $\mathbf{Ra}$ homomorfno preslikala na svoju nenula pravu podgrupu $\mathbf{A}$, ta bi bila deljiva, pa stoga i direktni sumand (nerazložive) grupe $\mathbf{Ra}$, kontradikcija.

Dokaz smo mogli bazirati i na 2.10($f$). Videli smo: ako je $\varphi \in End(\mathbf{Ra})$ i $(1)\varphi = \frac{m}{n}$, onda je $(a)\varphi = \frac{m}{n}a$ za svako $a \in Ra$. No, svako takvo preslikavanje je i surjektivno za $\frac{m}{n} \neq 0$.

(*b*) *Grupa* $\mathbf{p}^\infty$ *je izomorfna svim svojim nenula homomorfnim slikama.*

**Dokaz.** Homomorfna nenula slika grupe $\mathbf{p}^\infty$ je, trivijalno, deljiva $p$-grupa sa $p-1$ elemenata reda $p$ – ako je jezgro homomorfnog preslikavanja $\langle e^{\frac{2\pi}{p^n}i}\rangle$, u faktor grupi $\mathbf{p}^\infty/\langle e^{\frac{2\pi}{p^n}i}\rangle$ (jedini) elementi reda $p$ su $e^{\frac{2k\pi}{p^{n+1}}i}\langle e^{\frac{2\pi}{p^n}i}\rangle$, $0 < k < p$.

(*c*) *Beskonačna grupa je Prüferova* $\mathbf{p}^\infty$ *grupa za neki prost broj* $p$ *akko su sve njene podgrupe linearno uređene inkluzijom.*

**Dokaz.** Pravac $\Longleftarrow$ nam je već poznat. Ako su pak u grupi $\mathbf{A}$ sve podgrupe linearno uređene inkluzijom, odmah sledi da je $\mathbf{A}$ Abelova (za $a, b \in A$ je ili $\langle a\rangle \subseteq \langle b\rangle$ ili $\langle b\rangle \subseteq \langle a\rangle$, u svakom slučaju elementi $a$ i $b$ su komutativni) i periodična (podgrupe beskonačne ciklične grupe nisu linearno uređene inkluzijom). Dalje, $\mathbf{A}$ je $p$-grupa za neki prost broj $p$, jer ni u cikličnog grupi čiji red sadrži dva različita prosta faktora podgrupe nisu linearno uređene – videti 10.24($g$). S obzirom na beskonačnost grupe $\mathbf{A}$ i linearnu uređenost podgrupa, za svaki prirodan broj $n$ je $A[p^n] \neq A$; $\mathbf{A}$ je stoga, kao unija lanca cikličnih podgrupa $\langle a_n\rangle$, gde je $a_n$ reda $p^n$ i $a_{n+1}^p = a_n$ (grupa reda $p^n$ sadrži podgrupe reda $p^m$ za svako $m$, $0 \leq m < n$), izomorfna podgrupi reda $\mathbf{p}^\infty$.

(*d*) $\mathbf{Ra}/\mathbf{Z} \cong \sum_{p\in P} \mathbf{p}^\infty$, *$P$ – skup prostih brojeva.*

**Dokaz.** $Ra/Z = \{\frac{m}{n} + Z \mid m \in \omega, n \in \omega \setminus \{0\}, 0 \leq m < n, (m,n) = 1\}$. Radi se, dakle, o periodičnoj deljivoj grupi, i kako je, za svaki prost broj $p$, svega $p-1$ elemenata reda $p$ $(\frac{m}{p} + Z,\ 1 \leq m \leq p-1)$, to postoji (za svaki prost broj $p$) po samo jedan sumand tipa $\mathbf{p}^\infty$.

Podgrupa grupe $\mathbf{Ra}/\mathbf{Z}$ je pak izomorfna direktnoj sumi kockičnih grupa, po jedne za svaki prost broj $p$. $p$-sumand je ili konačna ciklična grupa, eventu-

alno nula grupa, ili Prüferova (kvaziciklična) grupa $\mathbf{p}^\infty$ (videti dokaz teoreme 32.10)

(*e*) $\mathbf{I}(\mathbf{Z}) = \mathbf{Ra}$, $\mathbf{I}(\mathbf{C}_{p^k}) \cong \mathbf{p}^\infty$ *(za* $k \geq 1$*).*

(*f*) $\mathbf{I}((Ra^+, \cdot)) \cong \sum_{\alpha\in\omega} \mathbf{Ra}_\alpha$, $\mathbf{I}((Ra \setminus \{0\}, \cdot)) \cong \sum_{\alpha\in\omega} \mathbf{Ra}_\alpha \oplus \mathbf{2}^\infty$.

**Dokaz.** Ova tačka je direktna posledica prethodne i leme 33.27. $(Ra^+, \cdot)$ je slobodna Abelova grupa ranga $\aleph_0$. $(Ra \setminus \{0\}, \cdot) = (Ra^+, \cdot) \times (\{1, -1\}, \cdot)$, a $-1$ je jedini element konačnog reda – dva.

(*g*) *U opštem ne važi:* $\mathbf{I}(\mathbf{A}/\mathbf{B}) \cong \mathbf{I}(\mathbf{A})/\mathbf{B}$.

**Dokaz.** Recimo, za prost broj $p$ je $\mathbf{I}(\mathbf{Z}/p\mathbf{Z}) \cong \mathbf{p}^\infty$, ali, jasno, $\mathbf{p}^\infty \ncong \mathbf{Ra}/p\mathbf{Z}$ (za svaki prost broj $q$ različit od $p$ grupa $\mathbf{Ra}/p\mathbf{Z}$ ima element reda $q$ – $\frac{p}{q} + pZ$).

(*h*) $\mathbf{Re}/\mathbf{Z} \cong \sum_{p\in P} \mathbf{p}^\infty \oplus \sum_{\alpha<c} \mathbf{Ra}_\alpha$, $\mathbf{Re}/\mathbf{Ra} \cong \mathbf{Re}$.

**Dokaz.** $\mathbf{Re}/\mathbf{Z}$ je deljiva grupa reda kontinuum, a njen periodični deo – $\mathbf{Ra}/\mathbf{Z}$ – je prebrojiv. Stoga je $\mathbf{Re}/\mathbf{Z}$ torziono slobodnog ranga kontinuum. Znači, $\mathbf{Re}/\mathbf{Z}$ je direktna suma svog periodičnog dela $\mathbf{Ra}/\mathbf{Z}$ i torziono slobodne deljive grupe torziono slobodnog ranga kontiuum, pa prvi deo tvrđenja sledi prema tački (*d*) i 33.19.

Grupa $\mathbf{Re}/\mathbf{Ra}$ je deljiva torziono slobodna grupa reda kontinuum i time je sve rečeno.

(*i*) $\sum^c_{n<\omega} \mathbf{p}^\infty_n \cong \sum_{\alpha<c} \mathbf{Ra}_\alpha \oplus \sum_{\alpha<c} \mathbf{p}^\infty$ *(dole u indeksima c je kontinuum* $= 2^{\aleph_0}$*, a* $\mathbf{p}^\infty_n$ *je kopija grupe* $\mathbf{p}^\infty$ *generisana elementima* $e_n^{\frac{2\pi}{p^k}i}$, $k = 1, 2, \ldots$*).*

**Dokaz.** Imamo u vidu: periodični deo grupe $\sum^c_{n<\omega} \mathbf{p}^\infty_n$ je kardinalnosti kontinuum; za svaki podskup $X$ skupa $\omega$ element $\mathbf{a}_X = \langle a_n \rangle$, gde je

$$a_n = \begin{cases} e_n^{\frac{2\pi}{p}i} & n \in X \\ 0 & \text{inače} \end{cases},$$

reda je $p$ (a takvih već ima kontinuum). No i elemenata beskonačnog reda ima kontinuum. Dovoljno je pokazati da ima bar jedan – zbir elemenata, jednog sa konačnim redom i jednog beskonačnog reda, beskonačnog je reda. Očigledno, $\mathbf{b} = \langle b_n \rangle$, gde je $b_n = e_n^{\frac{2\pi}{p^n}i}$, beskonačnog je reda.

(*j*) *Neka je* $\mathbf{A}$ *prava podgrupa deljive grupe* $\mathbf{B}$*. Svaki automorfizam grupe* $\mathbf{A}$ *može se proširiti do automorfizma grupe* $\mathbf{B}$.

**Dokaz.** Možemo odmah pretpostaviti da je $\mathbf{B}$ injektivni omotač grupe $\mathbf{A}$ (jer ako je $\mathbf{A} \leq \mathbf{C} < \mathbf{B}$, gde je $\mathbf{C}$ deljiva grupa, dakle i direktni sumand, imamo, za neku nenula podgrupu $\mathbf{D}$, $\mathbf{B} = \mathbf{C} \oplus \mathbf{D}$, i problem se, jasno, svodi na proširenje automorfizma grupe $\mathbf{A}$ do automorfizma grupe $\mathbf{C}$). Neka je $\varphi \in Aut(\mathbf{A})$. Onda za preslikavanja $\varphi : A \longrightarrow B$ i $\imath_A : A \longrightarrow B$ postoji, s obzirom da je $\mathbf{B}$ injektivna grupa, endomorfizam $\overline{\varphi}$ grupe $\mathbf{B}$, takav da je $\varphi \circ \overline{\varphi} = \imath_A$.



$\overline{\varphi}$ je surjektivno, u protivnom bismo imali $B \supset (B)\overline{\varphi} \supseteq (A)\overline{\varphi} = ((A)\varphi)\overline{\varphi} = A$, dok je $(\mathbf{B})\overline{\varphi}$ kao homomorfna slika deljive grupe takođe deljiva grupa, kontradikcija. $\overline{\varphi}$ je i injektivno, jer ako bi bilo $Ker(\overline{\varphi}) \neq O$, onda bi bilo i $\mathbf{A} \cap \mathbf{Ker}(\overline{\varphi}) \neq \mathbf{O}$, pa bismo za $0 \neq a \in A \cap Ker(\overline{\varphi})$ i $a = (b)\varphi$, $b \in A$, imali: $0 = (a)\overline{\varphi} = ((b)\varphi)\overline{\varphi} = b$, stoga i $a = 0$, protivurečnost. Kako je $\overline{\varphi} \in Aut(\mathbf{B})$, to je i $\overline{\varphi}^{-1} \in Aut(\mathbf{B})$, a $\overline{\varphi}^{-1}|_A = \varphi$ (iz $((a)\varphi)\overline{\varphi} = (a)\imath_A = a$ sledi $(a)\varphi = (a)\overline{\varphi}^{-1}$).

(*k*) *Neka je* $\varphi \in Is(\mathbf{A}, \mathbf{B})$*. Tada postoji izomorfno preslikavanje* $\overline{\varphi}$ *grupe* $\mathbf{I}(\mathbf{A})$ *na grupu* $\mathbf{I}(\mathbf{B})$ *takvo da je* $\overline{\varphi}|_A = \varphi$.

**Dokaz.** Videti dokaz prethodne tačke.

(*l*) *Svaka od grupa* $\mathbf{A} = \sum_{i=0}^\infty \mathbf{2}_i^\infty$, $\mathbf{B} = \mathbf{Z}_2 \oplus \mathbf{A}$ *izomorfna je (nekoj) podgrupi one druge, ali te grupe nisu izomorfne (jasno, kao i u tački* (*i*)*,* $\mathbf{2}_i^\infty$ *je kopija Prüferove grupe* $\mathbf{2}^\infty$ *sa domenom* $\{z_i \mid z \in C,\ z^{2^n} = 1,\ i = 1, 2, \ldots\}$*).*

**Dokaz.** Grupa $\mathbf{B}$ izomorfna je podgrupi $\mathbf{A}_1 = \langle \{1_0, -1_0\}, \cdot \rangle \oplus \sum_{i=1}^\infty \mathbf{2}_i^\infty$ grupe $\mathbf{A}$. S druge strane, $\mathbf{A}$ je deljiva grupa, a $\mathbf{B}$ nije.□

**Lema 33.30** *Neka je faktor grupa* $\mathbf{B}/\mathbf{A}$ *izomorfna podgrupi* $\mathbf{H}$ *grupe* $\mathbf{G}$*. Tada postoji grupa* $\mathbf{C}$ *koja sadrži* $\mathbf{B}$ *i čija je faktor grupa* $\mathbf{C}/\mathbf{A}$ *izomorfna grupi* $\mathbf{G}$.

**Dokaz.** Neka je $\mathbf{I}(\mathbf{B}/\mathbf{A})$ injektivni omotač grupe $\mathbf{B}/\mathbf{A}$ sadržan u faktor grupi $\mathbf{I}(\mathbf{B})/\mathbf{A}$ i neka je $\mathbf{I}(\mathbf{H})$ injektivni omotač grupe $\mathbf{H}$ sadržan u izabranom injektivnom omotaču grupe $\mathbf{G}$ – $\mathbf{I}(\mathbf{G})$. Prema tome je, za neku deljivu (eventualno nula) grupu $\mathbf{D}_2$, $\mathbf{I}(\mathbf{G}) = \mathbf{I}(\mathbf{H}) \oplus \mathbf{D}_2$. Neka je, dalje, $\varphi \in Is(\mathbf{B}/\mathbf{A}, \mathbf{H})$, a $\overline{\varphi} \in Is(\mathbf{I}(\mathbf{B}/\mathbf{A}), \mathbf{I}(\mathbf{H}))$ njegova ekstenzija (videti poslednju tačku u poslednjem primeru). Za inkluziju $\imath_{\mathbf{I}(\mathbf{B}/\mathbf{A})} : I(\mathbf{B}/\mathbf{A}) \longrightarrow I(\mathbf{B})/\mathbf{A}$ i izomorfizam $\overline{\varphi} : I(\mathbf{B}/\mathbf{A}) \longrightarrow I(\mathbf{H})$ postoji homomorfno preslikavanje $\psi : I(H) \longrightarrow I(\mathbf{B})/A$ takvo da je $\overline{\varphi} \circ \psi = \imath_{\mathbf{I}(\mathbf{B})/\mathbf{A}}$. $\psi$ je, jasno, injektivno (jer je $\overline{\varphi}$ surjektivno i $\imath_{\mathbf{I}(\mathbf{B}/\mathbf{A})}$ injektivno). Neka je $\mathbf{I}(\mathbf{B})/\mathbf{A} = (\mathbf{I}(\mathbf{H}))\psi \oplus \mathbf{D}_1$ i neka je $\psi_1$ izomorfno preslikavanje grupe $\mathbf{D}_1$ na $\sum_{\alpha<\mu} \mathbf{Ra}_\alpha \oplus \sum_{p\in P}(\sum_{\beta<\mu_p} \mathbf{p}^\infty)$, a $\psi_2$ grupe $\mathbf{D}_2$ na $\sum_{\alpha<\lambda} \mathbf{Ra}_\alpha \oplus \sum_{p\in P}(\sum_{\beta<\lambda_p} \mathbf{p}^\infty)$, gde su $\mu$, $\mu_p$, $\lambda$ i $\lambda_p$ kardinali ($\geq 0$). Ako je $\underline{D} = \sum_{\alpha<\min\{\mu,\lambda\}} \mathbf{Ra}_\alpha \oplus \sum_{p\in P}(\sum_{\beta<min\{\mu_p,\lambda_p\}} \mathbf{p}^\infty)$, onda je, za neke (deljive) (pod)grupe $\mathbf{D}_1'$, $\mathbf{D}_2'$, $\mathbf{D}_1 = (\underline{\mathbf{D}})\psi_1^{-1} \oplus \mathbf{D}_1'$ i $\mathbf{D}_2 = (\underline{\mathbf{D}})\psi_2^{-1} \oplus \mathbf{D}_2'$. Evidentno, za neku deljivu (eventualno nula) grupu $\mathbf{F}$ grupa $\mathbf{D}_2'$ se može utopiti u grupu $\mathbf{D}_1' \oplus \mathbf{F}$. Neka je $\theta$ jedno takvo utapanje. Tada se $\mathbf{I}(\mathbf{G})$ može utopiti u grupu $\mathbf{I}(\mathbf{B})/\mathbf{A} \oplus \mathbf{F}$, recimo tako da se za $h \in I(\mathbf{H})$, $g_1 \in (\underline{D})\psi_2^{-1}$ i $g_2 \in D_2'$ element $h + g_1 + g_2$ preslikava u $(h)\psi + (g_1)\psi_2\psi_1^{-1} + (g_2)\theta$. Za tako izabrano utapanje izomorfna slika grupe $\mathbf{I}(\mathbf{G})$ sadrži $\mathbf{I}(\mathbf{B}/\mathbf{A})$ (pa stoga i grupu $\mathbf{B}/\mathbf{A}$).

U grupi $\mathbf{I}(\mathbf{B}) \oplus \mathbf{F}$ nalazimo konačno podgrupu $\mathbf{C}$ takvu da je $\mathbf{C}/\mathbf{A} \cong \mathbf{G}$ (videti 10.17).□

**Definicija 33.31** *Abelova grupa je reducirana akko je nula podgrupa njena jedina deljiva podgrupa.*

**Lema 33.32** *Svaka Abelova grupa je direktna suma jedne deljive i jedne reducirane podgrupe (dozvoljavamo mogućnost da je neka od ovih podgrupa nula grupa).*

**Dokaz**. Neka je data grupa $\mathbf{A}$ i neka je $\mathbf{B}$ podgrupa generisana unijom domena svih deljivih podgrupa grupe $\mathbf{A}$. Ali onda je i $\mathbf{B}$ deljiva podgrupa, jer su svi elementi generatornog skupa deljivi svim pozitivnim prirodnim brojevima. Stoga je, za neku podgrupu $\mathbf{C}$, $\mathbf{A} = \mathbf{B} \oplus \mathbf{C}$ i, jasno, $\mathbf{C}$ je reducirana podgrupa.□

S obzirom da nam je struktura deljivih grupa poznata (33.19), iz prethodne leme proizilazi da su u ispitivanju Abelovih grupa jedino reducirane grupe od interesa.

**Lema 33.33** *Direktna suma nenula grupa je reducirana grupa akko je svaki sumand reducirana grupa.*

**Dokaz**. Pravac ($\Longrightarrow$) je trivijalan. Neka je, s druge strane, $\mathbf{A} = \sum_{\alpha<\lambda} \mathbf{A}_\alpha$, gde je svaka podgrupa $\mathbf{A}_\alpha$ nenula reducirana. Ako bismo pretpostavili da je $\mathbf{D}$ nenula deljiva podgrupa grupe $\mathbf{A}$, onda bi, za svaku projekciju $\pi_\alpha$ grupe $\mathbf{A}$ na sumand $\mathbf{A}_\alpha$, $(\mathbf{D})\pi_\alpha$ bilo deljiva podgrupa grupe $\mathbf{A}_\alpha$ i, stoga, $(\mathbf{D})\pi_\alpha = \mathbf{O}$. No, $\mathbf{D} \leq \sum_{\alpha<\lambda}(\mathbf{D})\pi_\alpha = \mathbf{O}$, kontradikcija.□

**Lema 33.34** *Ako je $\mathbf{A} = \mathbf{B} \oplus \mathbf{C}$, gde je $\mathbf{B}$ deljiva a $\mathbf{C}$ reducirana podgrupa, onda je $\mathbf{B}$ i maksimalna deljiva podgrupa grupe $\mathbf{A}$.*

**Dokaz**. Očigledno (videti i 10.17).□

**Lema 33.35** *Abelova grupa ispunjava uslov minimalnosti podgrupa akko je direktna suma konačno mnogo Prüferovih grupa i primarnih cikličnih grupa.*

**Dokaz**. ($\Longleftarrow$) Ovaj pravac je već dokazan – 13.4.

($\Longrightarrow$) Neka grupa $\mathbf{A}$ ispunjava uslov minimalnosti podgrupa. $\mathbf{A}$ je, odmah konstatujemo, periodična grupa (beskonačna ciklična grupa ne ispunjava uslov minimalnosti podgrupa), pa je $\mathbf{A} = \sum_{p\in P} \mathbf{A}_p$, gde je, za $p \in P$, $\mathbf{A}_p$ $p$-podgrupa grupe $\mathbf{A}$. Jasno, konačno je mnogo nenula $p$-podgrupa (videti 5.22). Neka je, za prost broj $q$, $\mathbf{A}_q \neq \mathbf{O}$ i $\mathbf{A}_q = \mathbf{B}_q \oplus \mathbf{D}_q$, gde je $\mathbf{D}_q$ deljiva $q$-grupa, dakle direktna suma konačnog broja Prüferovih $q$-grupa (opet zbog 5.22), a $\mathbf{B}_q$ reducirana $q$-grupa. Ako bi $\mathbf{B}_q$ bila beskonačna grupa, zbog uslova minimalnosti podgrupa, imala bi i minimalnu beskonačnu podgrupu, neka je to $\mathbf{C}_q$. Ako bi, dalje, važilo $\mathbf{C}_q = q\mathbf{C}_q$, tada bi $\mathbf{C}_q$ bila deljiva grupa (33.1), kontradikcija. Stoga je $q\mathbf{C}_q$ prava podgrupa (pod)grupe $\mathbf{C}_q$, znači konačna grupa. No, onda je i faktor grupa $\mathbf{C}_q/\mathbf{C}_q[q]$ ($\cong q\mathbf{C}_q$) konačna, te je $\mathbf{C}_q[q]$ beskonačna grupa, preciznije, beskonačna direktna suma cikličnih grupa reda



$q$ (10.33), kontradikcija ponovo. Zaključujemo: $\mathbf{B}_q$ je konačna $q$-grupa, prema tome (i prema 32.2) direktna suma konačnog broja cikličnih $q$-grupa.

Drugi jedan jednostavniji dokaz koristi 5.23 (i 32.2). Jedinstvena minimalna podgrupa konačnog indeksa grupe $\mathbf{A}$ – konačni ostatak grupe $\mathbf{A}$, neka je to $\mathbf{B}$, deljiva je grupa; jer $[\mathbf{B} : p\mathbf{B}] < \infty$ ($\mathbf{B}/p\mathbf{B}$ je elementarna Abelova $p$-grupa, dakle direktna suma cikličnih grupa reda $p$, a zbog uslova minimalnosti tih sumanada je konačno mnogo – 8.7), pa je $\mathbf{B} = p\mathbf{B}$.□

Iako u ovoj knjizi neće biti reči o uređenim grupama (o njima videti u, recimo, [6], [81], [82]), dajemo na kraju ovog paragrafa jedan interesantan rezultat O. Höldera koji se na njih odnosi.

**Definicija 33.36** *Grupa $\mathbf{G} = \langle G, \cdot \rangle$ je parcijalno (linearno) uređena relacijom $\leq$ akko je $\leq$ parcijalno (linearno) uređenje skupa $G$ saglasno sa operacijom grupe: $\forall a, b, c \in G\ (a \leq b \Longrightarrow ac \leq bc \wedge ca \leq cb)$; pisaćemo, po potrebi, $\mathbf{G} = \langle G, \cdot, \leq \rangle$.*

*Element $a$ uređene grupe $\mathbf{G}$ je pozitivan (strogo pozitivan) akko je $e \leq a$ ($e < a$, tj. $e \leq a \wedge e \neq a$). Skup pozitivnih elemenata grupe $\mathbf{G}$ obeležavaćemo sa $P(\mathbf{G})$.*

*U linearno uređenoj grupi moduo elementa $a$, u oznaci $|a|$, je $\max\{a, a^{-1}\}$.*

*Nejedinična parcijalno uređena grupa $\mathbf{G} = \langle G, \cdot, \leq \rangle$ je Arhimedova akko za svaka dva njena elementa $a, b$, iz $a^n \leq b$ za svaki ceo broj $n$ sledi $a = e$.*

*Podgrupa $\mathbf{H}$ parcijalno uređene grupe je konveksna akko za svako $a, b$ iz $\mathbf{H}$ i svako $c$ iz $\mathbf{G}$, iz $a \leq c \leq b$ sledi $c \in H$.*

*Podskup $P$ domena grupe $\mathbf{G}$ je čist akko je $P \cap P^{-1} \subseteq \{e\}$, gde je $P^{-1} \stackrel{\text{def}}{=} \{g^{-1} \mid g \in P\}$.*

*Podskup $P$ domena grupe $\mathbf{G}$ je linearan akko je $P \cup P^{-1} = G$.*

Sledeća fakta su očigledna.

**Lema 33.37** *(a) U parcijalno uređenoj grupi $\mathbf{G}$ (za bilo koje njene elemente $a, b, c, d$) važi:*

$$\begin{array}{ll} a \leq b \Longrightarrow c^{-1}ac \leq c^{-1}bc & a < b \Longrightarrow c^{-1}ac < c^{-1}bc \\ a \leq b \Longrightarrow b^{-1} \leq a^{-1} & a < b \Longrightarrow b^{-1} < a^{-1} \\ a \leq b \wedge c \leq d \Longrightarrow ac \leq bd & a < b \wedge c \leq d \Longrightarrow ac < bd; \end{array}$$

*(b) Linearno uređena nejedinična grupa je torziono slobodna;*

*(c) U linearno uređenoj grupi $\mathbf{G}$ je $e < |g|$ za svaki nejedinični element $g$;*

*(d) Linearno uređena grupa je Arhimedova akko za svaka dva njena nejedinična elementa $a, b$ postoji pozitivan prirodan broj $n$ takav da je $|b| < |a|^n$.*

**Lema 33.38** (*a*) *Postoji uzajamno jednoznačna korespondencija između svih parcijalnih uređenja grupe* **G** *i svih njenih čistih normalnih podskupova koji sadrže jedinični element i zatvoreni su za "množenje" (i prema tome su domeni podpolugrupa sa jediničnim elementom).*

(*b*) *Postoji uzajamno jednoznačna korespondencija između svih linearnih uređenja grupe* **G** *i svih njenih čistih linearnih normalnih podskupova koji sadrže jedinični element i zatvoreni su za množenje.*

**Dokaz.** (*a*) Obeležimo sa $\mathcal{U}$ skup svih parcijalnih uređenja grupe **G** (koji može biti i prazan), a sa $\mathcal{P}$ skup svih njenih čistih normalnih podskupova koji sadrže jedinični element i zatvoreni su za množenje. Ako je $\leq \in \mathcal{U}$, obeležićemo odgovarajući skup pozitivnih elemenata kratko sa $P_{\leq}$. Evidentno, prema tački (*a*) prethodne leme, $P_{\leq}$ je normalan čist skup koji sadrži jedinični element i zatvoren je za množenje. Opet, ako je $P$ čist normalan skup koji sadrži jedinični element i zatvoren je za množenje, tada je relacija $\leq_P \stackrel{\text{def}}{=} \{(a,b) \in G \times G \mid a^{-1}b \in P\}$ parcijalno uređenje grupe; refleksivnost je očigledna; antisimetričnost: ako je $a \leq_P b$ i $b \leq_P a$, odnosno, $a^{-1}b \in P$ i $b^{-1}a = (a^{-1}b)^{-1} \in P$, onda je $a^{-1}b \in P \cap P^{-1}$, dakle $a^{-1}b = e$, tj. $a = b$; tranzitivnost: ako je $a \leq_P b$ i $b \leq_P c$, onda je, zbog $a^{-1}b, b^{-1}c \in P$, i $a^{-1}b \cdot b^{-1}c = a^{-1}c \in P$, pa je $a \leq_P c$; saglasnost sa operacijom grupe: ako je $a \leq_P b$, pošto je $P$ normalan podskup, to je i, za svako $c$ ($\in G$), $c^{-1}(a^{-1}b)c = (ac)^{-1}bc \in P$, znači $ac \leq_P bc$; s druge strane, $a^{-1}b = a^{-1}c^{-1}cb = (ca)^{-1}cb \in P$ daje $ca \leq_P cb$.

Konačno, nije teško proveriti ni sledeće: $\leq = \leq'$ akko $P_{\leq} = P_{\leq'}$, $\leq_{P_{\leq}} = \leq$, $P_{\leq_P} = P$, što nam kaže da je (jedna) tražena korespondencija među elemetima skupova $\mathcal{U}$ i $\mathcal{P}$ data sa $\leq \longleftrightarrow P_{\leq}$.

U vezi s tačkom (*b*) treba samo primetiti da linearnost skupa $P$ obezbeđuje linearnost uređenja $\leq_P$.□

**Lema 33.39** *Postoje samo dva linearna uređenja aditivne grupe racionalnih brojeva – "standardno" $\leq$ i njemu inverzno.*

**Dokaz.** Neka je $\leq'$ linearno uređenje grupe **Ra**. Razlikujemo slučajeve: (*i*) $0 <' 1$ i (*ii*) $1 <' 0$.

(*i*) Kako je $0 <' 1$, to je i $0 <' n = \underbrace{1 + \cdots + 1}_{n-puta}$ za svaki prirodan broj $n$ veći od 1, a iz $0 <' 1 = n \cdot \frac{1}{n}$ sledi i $0 <' \frac{1}{n}$, pa su i svi (strogo) pozitivni, u smislu standardnog uređenja, racionalni brojevi strogo pozitivni s obzirom na uređenje $\leq'$; prema tome je $\leq = \leq'$.

U slučaju (*ii*) imamo, što se analogno pokazuje, inverznu relaciju relacije $\leq$ ($\leq^{-1}$, gde je $a \leq^{-1} b$ akko je $b \leq a$).□

**Lema 33.40** *Linearno uređena grupa* **G** *je Arhimedova akko nema netrivijalnih konveksnih podgrupa.*



**Dokaz.** ($\Longrightarrow$) Pretpostavimo da **G** ima netrivijalnu kompleksnu podgrupu **H** i neka je $g \in G \setminus H$. Onda je, za svako $h \in H$, $h < |g|$ (inače bismo, za neko $h \in H$, imali $e < |g| \leq |h|$ i $|g| \in H$, kontradikcija). Ali tada je, za svako $h$ iz $H$ i svaki pozitivan prirodan broj $n$, $|h|^n < |g|$ i **G** nije Arhimedova grupa.

($\Longleftarrow$) Neka **G** nije Arhimedova i neka je, za strogo pozitivne elemente $a, b$ i za svaki pozitivan prirodan broj $n$, $a^n < b$. Tada je $H = \{g \in G \mid$ postoji pozitivan prirodan broj $n = n_g$ takav da je $|g| \leq a^n\}$ domen netrivijalne konveksne podgrupe. Jer, ako je $c, d \in H$ i $|c| \leq a^m$, $|d| \leq a^n$, tada je $c \cdot d^{-1} \leq |c| \cdot |d^{-1}| = |c| \cdot |d| \leq a^{m+n}$ i, isto tako, $dc^{-1} \leq a^{m+n}$. Trivijalno se proverava i konveksnost podgrupe.□

**Lema 33.41** *Linearno uređena Arhimedova grupa je Abelova.*

**Dokaz.** Neka je $\mathbf{G} = \langle G, \cdot, \leq \rangle$ linearno uređena Arhimedova grupa. Razlikujemo slučajeve: (*i*) **G** ima najmanji strogo pozitivan element i (*ii*) **G** je bez takvog elementa.

(*i*) Neka je $a$ najmanji strogo pozitivan element grupe **G** i $b$ ma koji njen nejedinični element. Ako je $n$ najmanji pozitivan prirodan broj za koji je $a^n \leq |b| < a^{n+1}$, onda je $e \leq a^{-n} \cdot |b| < a$, pa je $|b| = a^n$. Prema tome, **G** je beskonačna ciklična grupa.

(*ii*) Primetimo prvo da je dovoljno samo da pokažemo da su strogo pozitivni elementi permutabilni (ako je, recimo, $e < a$ i $b < e$, onda iz $ab^{-1} = b^{-1}a$ sledi, "množenjem" s leva i s desna sa $b$, $ab = ba$). Dalje, za svaki strogo pozitivan element $a$ postoji strogo pozitivan element $b$ takav da je $b^2 < a$; jer, ako je $e < c < a$, onda je $e < c^{-1}a$, pa ako je $e < b < min\{c, c^{-1}a\}$, imamo: $b^2 < c \cdot c^{-1}a = a$. Pretpostavimo sada da je, za strogo pozitivne elemente $a$ i $b$, $ba < ab$, tj. $e < [a,b]$, i neka je $c$ strogo pozitivan element za koji je $c^2 < [a,b]$ i $c < a, b$. Kako je u pitanju Arhimedova grupa, postoje pozitivni prirodni brojevi $m$ i $n$ takvi da je $c^m \leq a < c^{m+1}$, $c^n \leq b < c^{n+1}$, a odatle je $ab < c^{m+n+2}$, $a^{-1}b^{-1} \leq c^{-(m+n)}$ i, stoga, $[a,b] = a^{-1}b^{-1} \cdot ab \leq c^2$, kontradikcija.□

**Lema 33.42** *Deljiva linearno uređena Arhimedova grupa je izomorfna podgrupi aditivne grupe realnih brojeva uređenoj standardnom relacijom $\leq$ (podrazumevamo, jasno, da se radi o izomorfnom preslikavanju i s obzirom na relacije uređenja).*

**Dokaz.** Neka je $\mathbf{A} = \langle A, +, \leq' \rangle$ deljiva linearno uređena Arhimedova grupa. S obzirom da je torziono slobodna i deljiva, **A** je direktna suma kopija aditivne grupe racionalnih brojeva. Neka je **B** jedna od "kopija" sa indukovanim uređenjem, zapravo zašto da ne pretpostavimo da je **B** baš **Ra** sa standardnim uređenjem $\leq$, dakle, $\leq = \leq' \cap Ra^2$ (ništa ne gubimo od opštosti – tu je uvek lema prenosa, a kad je u pitanju uređenje, na volju nam je da biramo između

$\leq'$ i $\leq'^{-1}$; očigledno: $\langle A,+,\leq'\rangle \cong \langle A,+,\leq'^{-1}\rangle$ - jedan izomorfizam preslikava elemente u njima inverzne).

Pokazujemo prvo: skup $Ra$ je *gust* u skupu $A$, tj. između svaka dva različita elementa postoji jedan racionalni (dokaz se ne razlikuje od poznatog dokaza da je skup $Ra$ gust u skupu $Re$). Neka $a,b \in A$ i $a <' b$, odnosno $0 <' b-a$. Onda je, za neki pozitivan prirodan broj $n$, $1 <' n(b-a)$, pa je i $\frac{1}{n} <' b-a$ $(*)$. Neka je, dalje, $m$ $(\in Ra)$ ceo broj takav da je $m \leq' a$ (takav uvek postoji: ako je $0 \leq' a$, možemo uzeti $m = 0$, a ako je $a <' 0$, onda je $0 <' -a$, te je, za neki pozitivan prirodan broj $m$, $-a <' m \cdot 1 = \underbrace{1+\cdots+1}_{m-puta}$, dakle, $-m <' a$). Opet, pošto je grupa Arhimedova, postoji pozitivan prirodan broj $p$ takav da je $a - m <' p \cdot \frac{1}{n}$. Neka je $p_0$ najmanji takav. Ako je $1 < p_0$, tada je $(p_0-1)\cdot\frac{1}{n} \leq' a-m$, što "sabiranjem" sa $(*)$ daje $p_0 \cdot \frac{1}{n} <' b-m$. Ako je $p_0 = 1$, tj. $a - m <' \frac{1}{n}$, "sabiranjem" nejednačine $0 \leq' a-m$ sa $(*)$ dobijamo ponovo $\frac{1}{n}$ $(= p_0 \cdot \frac{1}{n}) <' b-m$. Proizilazi: $a <' m + p_0 \cdot \frac{1}{n} <' b$.

Neka je, za $a \in A$, $X_a \stackrel{\text{def}}{=} \{x \in Ra \mid x <' a\}$, $Y_a \stackrel{\text{def}}{=} \{y \in Ra \mid a \leq' y\}$. Evidentno, $X_a$ je Dedekindov presek (skupa $Ra$), koji pak određuje jedinstven realan broj $r_a = X_a$ (videti donju napomenu). Jasno, ako je, za $a,b \in A$, $a <' b$, tada je, prema gore navedenom, i $X_a$ pravi podskup skupa $X_b$, odnosno, $r_a < r_b$ (gde je $\leq$ standardno uređenje realnih brojeva). Preslikavanje $\varphi : A \longrightarrow Re$ dato sa $(a)\varphi = r_a$ je, prema tome, injektivno, a očigledno je, s obzirom na definiciju zbira realnih brojeva kao Dedekindovih preseka, da se u stvari radi o utapanju uređene grupe $\mathbf{A}$ u uređenu grupu $\mathbf{Re}$.□

**Napomena**. U (jednoj) priči o realnim brojevima Dedekindov presek je pravi neprazan podskup skupa racionalnih brojeva bez maksimalnog elementa i "zatvoren naniže". Realni broj se definiše kao Dedekindov presek, sabiranje realnih brojeva je dato sa:

$$r + s \stackrel{\text{def}}{=} \{a+b \mid a,b \in Ra,\ a \in r,\ b \in s\},$$

a uređenje realnih brojeva je upravo relacija inkluzije.

**Teorema 33.43** *(O. Hölder). Arhimedova linearno uređena grupa je izomorfna podgrupi aditivne grupe realnih brojeva uređenoj prirodnom relacijom* $\leq$.

**Dokaz**. Neka je $\mathbf{A} = \langle A,+,\leq'\rangle$ Arhimedova linearno uređena grupa i neka je $\mathbf{I(A)}$ njen injektivni omotač. Naš zadatak se, prema prethodnoj lemi, svodi na proširenje relacije $\leq'$ do (neke) relacije s obzirom na koju će $\mathbf{I(A)}$ biti Arhimedova linearno uređena grupa. Neka je $P \stackrel{\text{def}}{=} \{a \in I(\mathbf{A}) \mid \exists n \in N\ a^n \in P_{\leq'}\}$ (koristimo notaciju iz 33.38). Proveravamo prvo da $P$ ispunjava uslove tačke $(b)$ leme 33.38. Očigledno, $e \in P$ i ako je $a \in P$, onda su i svi konjugati elementa $a$ u $P$ (jer je $P_{\leq'}$ normalan podskup). Kako je $\mathbf{I(A)/A}$ periodična grupa, to je, za (ma koje) $a \in I(\mathbf{A})$, za neki prirodan broj $n$ koji je u funkciji



elementa $a$, $a^n \in A = P_{\leq'} \cup P_{\leq'}^{-1}$ i, stoga, $a \in P$ ili $a \in P^{-1}$; drugim rečima, $P$ je linearan skup. Ako su $a,b$ iz $P$, onda je, za neke prirodne brojeve $m,n$, $a^m, b^n \in P_{\leq'}$, pa je i $(ab)^{mn} = (a^m)^n(b^n)^m \in P_{\leq'}$, te je $P$ zatvoreno za množenje. Ako je pak $a \in P \cap P^{-1}$ i ako je za prirodne brojeve $m,n$, $a^m, a^{-n} \in P_{\leq'}$, tada je i $a^{mn}, a^{-mn} = (a^{mn})^{-1} \in P_{\leq'}$, dakle, $a^{mn} \in P_{\leq'} \cap P_{\leq'}^{-1} = \{e\}$, tj. $a = e$ (A je, kao linearno uređena grupa, torziono slobodna, pa je i njen injektivni omotač, budući njena esencijalna ekstenzija, torziono slobodna grupa); $P$ je, znači i čist podskup. Proizilazi da je $\leq_P$ linearno uređenje grupe $\mathbf{I(A)}$ i, jasno, radi se o ekstenziji relacije $\leq'$. Ali u pitanju je baš Arhimedova grupa. Jer, neka je $e \leq_P a \leq_P b$. Onda je, za neki prirodan broj $m$, $a^m, b^m \in P_{\leq'} \setminus \{e\}$, i dalje, za neki prirodan broj $n$, $b^m <' (a^m)^n = a^{mn}$. Odatle sledi: $(b^{-1}a^n)^m \in P_{\leq'} \setminus \{e\}$, $b^{-1}a^n \in P$ i $b <_P a^n$.■

## 34 Lokalno ciklične grupe

Već je pokazano da je grupa $\mathbf{Ra}$ lokalno ciklična, prema tome su i sve njene podgrupe lokalno ciklične. Upoznajmo se prvo sa njima. Pratimo [146].

Neka je, za prost broj $p$, $v_p$ preslikavanje, tzv. *valuacija*, skupa $Ra \setminus \{0\}$ u $Z$, dato sa $(\prod_{q\in P} q^{\alpha_q})v_p = \alpha_p$ (jasno, u proizvodu $\prod_{q\in P} q^{\alpha_q}$ samo je konačno mnogo stepena $\alpha_q$ različito od nule). Posebno, za svaki prost broj $p$ je $(1)v_p = 0$ i (za $a,b \in Ra \setminus \{0\}$) važi:

$$(a\cdot b)v_p = (a)v_p + (b)v_p \tag{1}$$

i, za $a \neq -b$,

$$(a+b)v_p \geq min\{(a)v_p, (b)v_p\} \tag{2}.$$

(1) je očigledno, a (2) se lako proverava diskusijom po znacima $(a)v_p$, $(b)v_p$ (jedan slučaj je, recimo, $(a)v_p \geq 0$, $(b)v_p < 0$). *Vrednost podgrupe* $\mathbf{G}$ *grupe* $\mathbf{Ra}$ *u* $p$, u oznaci $v_p(\mathbf{G})$, definišemo sa

$$v_p(\mathbf{G}) = inf\{(g)v_p \mid g \in G \setminus \{0\}\}.$$

Za svaku podgrupu $\mathbf{G}$ je, očigledno, $-\infty \leq v_p(\mathbf{G}) < \infty$, a za samo konačno mnogo prostih brojeva $p$ je $v_p(\mathbf{G}) > 0$. Jer, pretpostavimo da je za sve elemente beskonačnog podskupa $Q = \{p_i \mid i \in \omega\}$ skupa $P$ ($p_i$ ovde ne označava $i$-ti po redu prost broj) $v_{p_i}(\mathbf{G}) > 0$. Ali ako je $p_{i_1}^{\alpha_1} \ldots p_{i_m}^{\alpha_m} q_{j_1}^{-\beta_1} \ldots q_{j_n}^{-\beta_n} \in G$, $\alpha_i, \beta_j > 0$, onda je i $a = p_{i_1}^{\alpha_1} \ldots p_{i_m}^{\alpha_m} \in G$. Neka je $p \in Q \setminus \{p_{i_1}, \ldots, p_{i_m}\}$ i neka je $b = p^{\gamma} p_{k_1}^{\gamma_1} \ldots p_{k_r}^{\gamma_r} \in G$. Ako je $(a,b) = c$, tada je, po Euklidovoj teoremi, i $c \in G$, no jasno, $(p,c) = 1$ i stoga $(c)v_p = 0$, kontradikcija.

**Lema 34.1** *Neka je* $\mathbf{G}$ *podgrupa aditivne grupe racionalnih brojeva. Tada je*

$$G = \{0\} \cup \{a \in Ra \setminus \{0\} \mid \textit{za svaki prost broj } p \textit{ je } (a)v_p \geq v_p(\mathbf{G})\}.$$

**Dokaz.** Neka je $P_{\mathbf{G}} \stackrel{\text{def}}{=} \{p \in P \mid v_p(\mathbf{G}) > 0\} = \{p_1, \ldots, p_k\}$ i $n_{\mathbf{G}} = \prod_{p \in P_{\mathbf{G}}} p^{v_p(\mathbf{G})}$ (upravo smo konstatovali da je $P_{\mathbf{G}}$ konačan skup). Sigurno, $n_{\mathbf{G}}$ deli svaki ceo broj iz $\mathbf{G}$ i, uopšte, ako je, za svako $p \in P_{\mathbf{G}}$, $(n,p) = 1$ i $\frac{m}{n} \in G$, tada $n_{\mathbf{G}} | m$. Pokazaćemo da je i $n_{\mathbf{G}} \in G$, dakle i najmanji pozitivan ceo broj u $G$. Izaberimo, za $p \in P_{\mathbf{G}}$, ceo broj $m_p$ iz $G$ takav da je $(m_p)v_p = v_p(\mathbf{G})$ i neka je $(m_{p_1}, \ldots, m_{p_k}) = n_{\mathbf{G}} \cdot a$. Ako je $a = 1$, odmah dobijamo $n_{\mathbf{G}} \in G$ (prema Euklidovoj teoremi postoje celi brojevi $u_1, \ldots, u_k$, takvi da je $u_1 m_{p_1} + \cdots + u_k m_{p_k} = n_{\mathbf{G}}$). U svakom slučaju je, po istoj logici, $a \cdot n_{\mathbf{G}} \in G$. Ako je pak $a = q_1^{\beta_1} \ldots q_r^{\beta_r}$, gde, naravno, nijedno $q_i$ nije iz $P_{\mathbf{G}}$, izaberimo za svako $q_i$, $1 \leq i \leq r$, ceo broj $n_i \in G$ takav da je $(n_i)v_{q_i} = 0$ (egzistencija ovakvog broja zagarantovana je činjenicom da je $v_{q_i}(\mathbf{G}) \leq 0$). No tada je $(a \cdot n_{\mathbf{G}}, n_1, \ldots, n_r) = n_{\mathbf{G}}$ i opet je $n_{\mathbf{G}} \in G$. Dalje sledi da je, za svaki prost broj $q \notin P_{\mathbf{G}}$ i svaki ceo broj $k \geq v_q(\mathbf{G})$ $(\leq 0)$, $q^k n_{\mathbf{G}} \in G$. Ako je $k \geq 0$, nemamo šta dokazivati ($n_{\mathbf{G}} \in G \Longrightarrow q^k n_{\mathbf{G}} \in G$). Neka je zato $k < 0$ i $q^k m \in G$, $m \in Z$ i $(m,q) = 1$ (stalno imamo u vidu: ako je $q^k \frac{m}{n} \in G$, onda je i $q^k m \in G$). Za neke cele brojeve $u$ i $v$ je $uq^{-k} + vm = 1$, te je $q^k n_{\mathbf{G}} = q^k n_{\mathbf{G}}(uq^{-k} + vm) = un_{\mathbf{G}} + (vn_{\mathbf{G}})(q^k m) \in G$. Konačno, ako $q_1, \ldots, q_n \notin P_{\mathbf{G}}$ i $0 > k_i \geq v_{q_i}(\mathbf{G})$, onda je, za neke cele brojeve $v_1, \ldots, v_n$, $q_1^{k_1} \ldots q_n^{k_n} = v_1 q_1^{k_1} + \cdots + v_n q_n^{k_n}$; jer je, za $a_i = q_1^{-k_1} \ldots q_{i-1}^{-k_{i-1}} q_{i+1}^{-k_{i+1}} \ldots q_n^{-k_n}$, $i = 1, \ldots n$, $(a_1, \ldots, a_n) = 1$, pa je, za neke cele brojeve $v_1, \ldots, v_n$, $v_1 a_1 + \cdots + v_n a_n = 1$ i (posle množenja sa $q_1^{k_1} \ldots q_n^{k_n}$), $q_1^{k_1} \ldots q_n^{k_n} = v_1 q_1^{k_1} + \cdots + v_n q_n^{k_n}$. Prema tome, za svaki ceo broj $m$, $mq_1^{k_1} \ldots q_n^{k_n} \in G$ akko $n_{\mathbf{G}} | m$, čime je dokaz kompletiran.□

**Definicija 34.2** *Tip je funkcija ($\varphi$) koja preslikava skup prostih brojeva $P$ u skup $Z \cup \{-\infty\}$ i koja je za samo konačno mnogo prostih brojeva pozitivna* ($|\{p \in P \mid (p)\varphi > 0\}| < \infty$).

**Korolar 34.3** *Postoji jedan-jedan korespondencija između skupa svih nenula podgrupa aditivne grupe racionalnih brojeva i skupa svih tipova.*

**Dokaz.** Korespondencija je data sa $\mathbf{G} \longrightarrow \varphi_{\mathbf{G}}$, gde je $(p)\varphi_{\mathbf{G}} = v_p(\mathbf{G})$ za $p \in P$. Ako je $\mathbf{G} \neq \mathbf{H}$, mora, prema prethodnoj lemi, biti i $\varphi_{\mathbf{G}} \neq \varphi_{\mathbf{H}}$ (ako bi bilo $v_p(\mathbf{G}) = v_p(\mathbf{H})$ za svako $p \in P$, imali bismo $G = \{0\} \cup \{a \in Ra \setminus \{0\} \mid (a)v_p \geq v_p(\mathbf{G}) = v_p(\mathbf{H}) \text{ za svako } p \in P\} = H$). Što se tiče surjektivnosti korespondencije, dati tip $\varphi$, gde je $(p)\varphi = k_p$, odgovara podgrupi $\mathbf{G}$ sa domenom $G = \{0\} \cup \{a \in Ra \setminus \{0\} \mid \forall p \in P\ (a)v_p \geq k_p\}$; lako se proverava da je $G$ domen podgrupe: ako je $a \in G \setminus \{0\}$, onda je očigledno i $-a \in G$, a ako je i $b \in G \setminus \{0, -a\}$, prema već konstatovanom je $(a+b)v_p \geq min\{(a)v_p, (b)v_p\} \geq k_p$.□

**Lema 34.4** *Podgrupe $\mathbf{G}$ i $\mathbf{H}$ grupe $\mathbf{Ra}$ izomorfne su akko je*

$$\sum_{p \in P} |v_p(\mathbf{G}) - v_p(\mathbf{H})| < \infty.$$



**Dokaz.** ($\Longrightarrow$) Neka je $\varphi \in Is(\mathbf{G}, \mathbf{H})$. Fiksirajmo jedno $g \in G \setminus \{0\}$ i neka je $r_\varphi = (g)\varphi \cdot g^{-1}$. Svaki element iz $\mathbf{G}$ je oblika $\frac{m}{n}g$, $m \in Z$, $n \in Z \setminus \{0\}$, pa imamo: $n(\frac{m}{n}g)\varphi = m(g)\varphi = (mg)r_\varphi$, tj. $(\frac{m}{n}g)\varphi = (\frac{m}{n}g)r_\varphi$. Stoga je $H = Gr_\varphi$, i ako je $r_\varphi = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$, onda je, za $p \notin \{p_1, \ldots, p_m\}$, $v_p(\mathbf{G}) = v_p(\mathbf{H})$, a za $i \in \{1, \ldots, m\}$ je:

$$v_{p_i}(\mathbf{H}) = \begin{cases} v_{p_i}(\mathbf{G}) & \text{ako je } v_{p_i}(\mathbf{G}) = -\infty \\ v_{p_i}(\mathbf{G}) + \alpha_i & \text{inače;} \end{cases}$$

pretpostavljamo, naravno, $-\infty - (-\infty) = 0$, $-\infty - m = -\infty$, $m - (-\infty) = \infty$.

($\Longleftarrow$) Neka je $\sum_{p \in P} |v_p(\mathbf{G}) - v_p(\mathbf{H})| < \infty$. Mora, dakle, za skoro sve proste brojeve $q$ biti $v_q(\mathbf{G}) = v_q(\mathbf{H})$. Ako je za sve, nemamo šta dokazivati. Pretpostavimo stoga da je $\{p \in P \mid v_p(\mathbf{G}) \neq v_p(\mathbf{H})\} = \{p_1, \ldots, p_m\}$; jasno, za svako $i$ $(1 \leq i \leq m)$ je $v_p(\mathbf{G}), v_p(\mathbf{H}) \neq -\infty$. Stavimo: $v_{p_i}(\mathbf{H}) = v_{p_i}(\mathbf{G}) + \alpha_i$, $\alpha_i \in Z \setminus \{0\}$, i $r = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$. Tada je preslikavanje $\varphi : G \longrightarrow H$ dato sa $(g)\varphi = gr$ izomorfno preslikavanje grupe $\mathbf{G}$ na $\mathbf{H}$. Ako je $g \in G \setminus \{0\}$, onda je prema 34.1 $(g)v_p \geq v_p(\mathbf{G})$ za svako $p \in P$, a tada je i $((g)\varphi)v_p = (gr)v_p \geq v_p(\mathbf{H})$; znači $(g)\varphi = gr \in H$. Opet, ako je $h \in H \setminus \{0\}$ (dakle $(h)v_p \geq v_p(\mathbf{H})$ za svako $p \in P$) biće

$$(hr^{-1})v_p = \begin{cases} (h)v_p & \text{ako } p \notin \{p_1, \ldots, p_m\} \\ (h)v_p - \alpha_i & \text{ako } p = p_i. \end{cases}$$

U svakom slučaju je $(hr^{-1})v_p \geq v_p(\mathbf{G})$, te je $hr^{-1} \in G$ i $h = (hr^{-1})r \in (G)\varphi$.□

**Korolar 34.5** *Aditivna grupa racionalnih brojeva ima kontinuum mnogo neizomorfnih podgrupa.*

**Dokaz.** Jasno je da $\mathbf{Ra}$ ne može imati više od kontinuum podgrupa (*Ra* je prebrojiv skup). Dovoljno je stoga pokazati da ih ima bar kontinuum. No, već tipova sa vrednostima 0 i $-\infty$ ima kontinuum, svaki od njih, prema prethodnom, definiše jedinstvenu podgrupu i nikoje dve od tih podgrupa nisu izomorfne; jer, ako su $\varphi$ i $\psi$ različiti tipovi s navedenim vrednostima, onda je $\sum_{p \in P} |(p)\varphi - (p)\psi| = \infty$.□

**Lema 34.6** *Neka je $\mathbf{G}$ podgrupa grupe $\mathbf{Ra}$. Podgrupa $\mathbf{H}$ grupe $\mathbf{G}$ je maksimalna akko je $\sum_{p \in P} (v_p(\mathbf{H}) - v_p(\mathbf{G})) = 1$.*

**Dokaz.** Direktno je, po definiciji, $v_p(\mathbf{H}) \geq v_p(\mathbf{G})$ za svaki prost broj $p$, pa je $\sum_{p \in P} (v_p(\mathbf{H}) - v_p(\mathbf{G})) \geq 0$. Prema rečenom je $\mathbf{G} = \mathbf{H}$ akko je $\sum_{p \in P} (v_p(\mathbf{H}) - v_p(\mathbf{G})) = 0$. Stoga, $\mathbf{H}$ je prava podgrupa akko je $\sum_{p \in P} (v_p(\mathbf{H}) - v_p(\mathbf{G})) > 0$. Neka je $\sum_{p \in P} (v_p(\mathbf{H}) - v_p(\mathbf{G})) \geq 2$. Razmotrićemo sledeće slučajeve:

(*I*) $\exists p \in P\ v_p(\mathbf{H}) \geq v_p(\mathbf{G}) + 2$.

No, podgrupa $\mathbf{K}$ grupe $\mathbf{G}$ određena tipom $\varphi_{\mathrm{K}}$, za koji je

$$(q)\varphi_{\mathrm{K}} = \begin{cases} v_q(\mathbf{H}) & q \neq p \\ v_p(\mathbf{G})+1 & q = p, \end{cases}$$

prava je podgrupa i strogo sadrži $\mathbf{H}$;

*(II)* Postoje različiti elementi $p, q$ u $P$ takvi da je $v_p(\mathbf{H}) = v_p(\mathbf{G}) + k_1$, $v_q(\mathbf{H}) = v_q(\mathbf{G}) + k_2$, $k_1, k_2 \geq 1$. Sada je podgrupa $\mathbf{N}$ određena tipom $\varphi_{\mathrm{N}}$, gde je za $r \in P$

$$(r)\varphi_{\mathrm{N}} = \begin{cases} v_r(\mathbf{H}) & r \neq p \\ v_p(\mathbf{G})+1 & r = p, \end{cases}$$

prava podgrupa grupe $\mathbf{G}$ koja strogo sadrži $\mathbf{H}$.□

**Korolar 34.7** *(a) Ako je* $\mathbf{A}$ *maksimalna podgrupa prave podgrupe* $\mathbf{B}$ *grupe* $\mathbf{Ra}$, *onda je* $\mathbf{A} \cong \mathbf{B}$;

*(b) Ako je* $\mathbf{A}$ *prava nenula podgrupa grupe* $\mathbf{Ra}$, *postoji podgrupa* $\mathbf{B}$ *grupe* $\mathbf{Ra}$ *čija je (jedna) maksimalna podgrupa* $\mathbf{A}$.

**Dokaz.** Tačka *(a)* je direktna posledica lema 34.4 i 34.6, a za tačku *(b)* nam treba samo 34.6. Dodajmo samo: ako je, za neki prost broj $p$, $m_p = v_p(\mathbf{A}) \neq -\infty$, za $\mathbf{B}$ uzimamo grupu čiji je tip – $\varphi$ – dat sa:

$$(q)\varphi = \begin{cases} v_q(\mathbf{A}) & q \neq p \\ m_p - 1 & q = p \end{cases} \quad \square.$$

**Korolar 34.8** *Neka je* $\mathbf{G}$ *podgrupa grupe* $\mathbf{Ra}$. *Tada je, za svaki prost broj* $p$, $v_p(\mathbf{Fr}(\mathbf{G})) = v_p(\mathbf{G}) + 1$.

**Dokaz.** Primetimo prvo da svaka prava podgrupa $\mathbf{H}$ grupe $\mathbf{Ra}$ ima bar jednu maksimalnu podgrupu (jer je tada, za bar jedno $p \in P$, $v_p(\mathbf{H}) \neq -\infty$ – grupi $\mathbf{Ra}$ odgovara tip koji svaki prost broj preslikava u $-\infty$); zapravo broj maksimalnih podgrupa jednak je kardinalnosti skupa $\{q \in P \mid v_q(\mathbf{H}) \neq -\infty\}$.

Frattinijeva podgrupa $\mathbf{Fr}(\mathbf{G})$ grupe $\mathbf{G}$ je, podsećamo, presek njenih maksimalnih podgrupa. Za $p \in A = \{q \in P \mid v_q(\mathbf{G}) \neq -\infty\}$ neka je $\mathbf{M}_p$ maksimalna podgrupa grupe $\mathbf{G}$ takva da je

$$v_r(\mathbf{M}_p) = \begin{cases} v_r(\mathbf{G}) & r \neq p \\ v_r(\mathbf{G})+1 & r = p. \end{cases}$$

Očigledno, za Frattinijevu podgrupu $\mathbf{Fr}(\mathbf{G}) = \bigcap_{p\in A} \mathbf{M}_p$ važi: $v_r(\mathbf{Fr}(\mathbf{G})) = v_r(\mathbf{G}) + 1$ za svaki prost broj $r$ (rekli smo da je $-\infty + 1 = -\infty$).□

**Napomena.** Ako su $\mathbf{H}_1, \ldots, \mathbf{H}_n$ nenula podgrupe grupe $\mathbf{Ra}$, onda je

$$v_p(\bigcap_{i=1}^{n} \mathbf{H}_i) = sup\{ v_p(\mathbf{H}_i) \mid i = 1, \ldots, n\}.$$



Ovo se ne može generalisati za beskonačnu familiju podgrupa $\{\mathbf{H}_i \mid i \in I\}$, $|I| \geq \aleph_0$; može se desiti da je npr. $sup\{ v_p(\mathbf{H}_i) \mid i \in I\} = \infty$, tj. da je presek podgrupa nula podgrupa.

**Lema 34.9** *Ako je* $\mathbf{A}$ *lokalno ciklična grupa, onda je Abelova i svaka njena podgrupa i homomorfna slika su lokalno ciklične grupe. Pored toga,* $\mathbf{A}$ *je ili periodična ili torziono slobodna grupa.*

**Dokaz.** Trivijalan.□

**Teorema 34.10** *Grupa je lokalno ciklična akko je izomorfna podgrupi ili grupe* $\mathbf{Ra}$ *ili grupe* $\mathbf{Ra/Z}$ $(\cong \sum_{p\in P} \mathbf{p}^\infty)$.

**Dokaz.** Pravac $(\Longleftarrow)$ je jasan.

$(\Longrightarrow)$ Neka je $\mathbf{A}$ lokalno ciklična grupa, stoga i Abelova. Ako je periodična, svaka njena $p$-komponenta $(\mathbf{A}_p)$ je kociklična grupa. Ovo direktno sledi iz činjenice da $\mathbf{A}_p$ ima za dato $k$ najviše jednu podgrupu reda $p^k$. Ako su $a$ i $b$ elementi reda $p^k$, onda je i ciklična grupa $\langle c\rangle = \langle a, b\rangle$ reda $p^k$; za neke cele brojeve $m$ i $n$ je $c = ma + nb$, te je $p^k c = m(p^k a) + n(p^k b) = 0$. Neka su jedinstvene ciklične podgrupe reda $p^n$ generisane elementima $a_n$. Naravno, $\langle a_k\rangle \leq \langle a_{k+1}\rangle$. Jedino je pitanje da li postoji maksimalna konačna ciklična grupa $\langle a_m\rangle$, u kom slučaju je $\mathbf{A}_p = \langle a_m\rangle$, ili ne, i tada je $\mathbf{A}_p \cong \mathbf{p}^\infty$.

Neka je sada $\mathbf{A}$ torziono slobodna grupa i $b \in A\backslash\{0\}$ jedan njen (proizvoljno odabran) element. Neka je, za pozitivan prirodan broj $n$, $b_n$ jedinstveno rešenje (jer je $\mathbf{A}$ torziono slobodna grupa), ukoliko postoji, jednačine $b = nx$, u suprotnom $b_n = 0$. Skup $\{b_n \mid n \in N = \{1, 2, \ldots\}\}$ generiše celu grupu $\mathbf{A}$. Ako je $c \in A$, onda je $\langle b, c\rangle$ ciklična grupa generisana, recimo, elementom $d$. Stoga je $b = md$ ili $b = m(-d)$ za neko $m \in N$, te je $b_m = d$ ili $b_m = -d$; u svakom slučaju je $c \in \langle b_m\rangle$. Neka je podgrupa $\mathbf{A}_k = \langle b_1, \ldots, b_k\rangle$ ciklična grupa generisana elementom $a_k$. Zbog $\langle a_k\rangle \leq \langle a_{k+1}\rangle$ je $a_k = m_{k+1}a_{k+1}$ za neko $m_{k+1}$. Grupa $\mathbf{A} = \bigcup_{k\in N} \mathbf{A}_k$ preslikava se izomorfno na podgrupu $\mathbf{H}$ grupe $\mathbf{Ra}$ generisanu skupom $\{\prod_{i=1}^{k} \frac{1}{m_i} \mid k \in N\}$. Naime, ako je $\varphi_k$ izomorfno preslikavanje beskonačne ciklične grupe $\langle a_k\rangle = \mathbf{A}_k$ na (beskonačnu cikličnu) grupu $\langle \prod_{i=1}^{k} \frac{1}{m_i}\rangle$ (uzećemo da je $m_1 = 1$), gde je $(a_k)\varphi_k = \prod_{i=1}^{k} \frac{1}{m_i}$, onda je za $r < s$, očigledno, $\varphi_s|_{A_r} = \varphi_r$ $(a_r = (m_{r+1} \ldots m_s)a_s$ i $\prod_{i=1}^{r} \frac{1}{m_i} = (m_{r+1} \ldots m_s)\prod_{i=1}^{s} \frac{1}{m_i})$, a $\bigcup_{k\in N} \varphi_k \in Is(\mathbf{A}, \mathbf{H})$.■

**Korolar 34.11** *Grupa je lokalno ciklična akko je ciklična ili unija rastućeg niza cikličnih grupa.*

**Dokaz.** Pravac $(\Longleftarrow)$ je jasan. S druge strane, već smo videli da su i $\mathbf{Ra}$ i Prüferova $\mathbf{p}^\infty$ grupa unije rastućeg niza cikličnih grupa. No, to je i grupa $\mathbf{Ra/Z} \cong \sum_{p\in P} \mathbf{p}^\infty$ (pa samim tim i svaka njena podgrupa). Očigledno,

$\sum_{p\in P}\mathbf{p}^\infty$ je unija rastućeg niza cikličnih podgrupa, redova, respektivno, $p_0$, $p_0^2p_1$, $p_0^3p_1^2p_2$, ..., $\prod_{i=0}^{n}p_i^{n+1-i}$, ..., gde je $p_i$ $i$-ti po redu prost broj (uzimamo, redom, cikličnu podgrupu reda $p_0$ grupe $\mathbf{p}_0^\infty$, zatim direktnu sumu podgrupe reda $p_0^2$ grupe $\mathbf{p}_0^\infty$ i podgrupe reda $p_1$ grupe $\mathbf{p}_1^\infty$, koja je kao direkta suma cikličnih grupa uzajamno prostih redova i sama ciklična grupa, i tako dalje).□

**Korolar 34.12** *Grupe automorfizama lokalno cikličnih grupa su Abelove.*

**Dokaz.** Direktna posledica lema 4.35 i 8.24.□

**Lema 34.13** *Ako su, za grupu* $\mathbf{G}$, $\mathbf{G}^{(1)}/\mathbf{G}^{(2)}$ *i* $\mathbf{G}^{(2)}/\mathbf{G}^{(3)}$ *lokalno ciklične grupe, onda je* $\mathbf{G}^{(2)}=\mathbf{G}^{(3)}$.

**Dokaz.** Ako je $\mathbf{H}=\mathbf{G}/\mathbf{G}^{(3)}$, onda je, prema 6.22, $(\mathbf{H}'=)\,\mathbf{H}^{(1)}=\mathbf{G}^{(1)}/\mathbf{G}^{(3)}$ i $\mathbf{H}^{(2)}=\mathbf{G}^{(2)}/\mathbf{G}^{(3)}$, pa je $\mathbf{H}^{(1)}/\mathbf{H}^{(2)}$ $(\cong\mathbf{G}^{(1)}/\mathbf{G}^{(2)})$ lokalno ciklična grupa. $\mathbf{H}^{(2)}$ je normalna (šta više, potpuno invarijantna) podgrupa (grupe $\mathbf{H}$), te je i $\mathbf{C}(\mathbf{H}^{(2)})$ normalna podgrupa, a grupa automorfizama podgrupe $\mathbf{H}^{(2)}$ inducirana unutrašnjim automorfizmima grupe $\mathbf{H}$ – $\langle\{u_h|_{H^{(2)}}\mid h\in H\},\circ\rangle$ – izomorfna je, što se lako proverava, grupi $\mathbf{H}/\mathbf{C}(\mathbf{H}^{(2)})$ (dokaz je u potpunosti analogan dokazu da je $\mathbf{Inn}(\mathbf{K})\cong\mathbf{K}/\mathbf{Z}(\mathbf{K})$ za svaku grupu $\mathbf{K}$). Prema prethodnom korolaru ova grupa je Abelova ($\mathbf{H}^{(2)}$ je lokalno ciklična grupa) i stoga je $\mathbf{H}^{(1)}\leq\mathbf{C}(\mathbf{H}^{(2)})$ (6.8), tj. $\mathbf{H}^{(2)}\leq\mathbf{Z}(\mathbf{H}^{(1)})$. Ali tada je $\mathbf{H}^{(1)}/\mathbf{Z}(\mathbf{H}^{(1)})$ $(\cong(\mathbf{H}^{(1)}/\mathbf{H}^{(2)})/(\mathbf{Z}(\mathbf{H}^{(1)}/\mathbf{H}^{(2)}))$ kao faktor grupa lokalno ciklične grupe i sama lokalno ciklična. Prema tome, $\mathbf{H}^{(1)}$ je Abelova grupa (8.19), a $\mathbf{H}^{(2)}$ jedinična grupa; dakle, važi: $\mathbf{G}^{(2)}=\mathbf{G}^{(3)}$.□

Lokalno ciklične grupe imaju interesantnu karakterizaciju i preko mreža svojih podgrupa. O tome u narednoj teoremi. No, prvo jedna definicija i jedna lema.

**Definicija 34.14** *Podgrupe* $\mathbf{A}$ *i* $\mathbf{B}$ *grupe* $\mathbf{G}$ *čine distributivan par akko je za svaku podgrupu* $\mathbf{C}$ *grupe* $\mathbf{G}$ *ispunjeno:*

$$\mathbf{C}\cap(\mathbf{A}\vee\mathbf{B})=(\mathbf{C}\cap\mathbf{A})\vee(\mathbf{C}\cap\mathbf{B}).$$

*Red elementa* $g$ *grupe* $\mathbf{G}$ *s obzirom na podgrupu* $\mathbf{A}$ *je najmanji pozitivan prirodan broj* $n$, *ukoliko takav postoji, za koji je* $g^n\in A$; *u suprotnom kažemo da je* $g$ *beskonačnog reda (ili reda* 0*) s obzirom na podgrupu* $\mathbf{A}$.

Sećamo se, $\mathbf{A}\vee\mathbf{B}$ je podgrupa generisana unijom domena datih podgrupa, tj. najmanja podgrupa grupe $\mathbf{G}$ koja sadrži podgrupe $\mathbf{A}$ i $\mathbf{B}$: $\mathbf{A}\vee\mathbf{B}=\langle A\cup B\rangle$.

Jasno, red elementa (u standardnom smislu) je red (tog) elementa s obzirom na jediničnu podgrupu.

**Lema 34.15** *Podgrupe* $\mathbf{A}$ *i* $\mathbf{B}$ *grupe* $\mathbf{G}$ *čine distributivan par akko su redovi svakog elementa iz* $\langle A\cup B\rangle\setminus(A\cup B)$, *s obzirom na podgrupe* $\mathbf{A}$ *i* $\mathbf{B}$, *uzajamno prosti brojevi.*



**Dokaz.** ($\Longrightarrow$) Neka podgrupe $\mathbf{A}$ i $\mathbf{B}$ čine distributivan par i neka je $c\in\langle A\cup B\rangle\setminus(A\cup B)$. Ako je $\mathbf{C}=\langle c\rangle$, imamo:

$$\mathbf{C}=\mathbf{C}\cap(\mathbf{A}\vee\mathbf{B})=(\mathbf{C}\cap\mathbf{A})\vee(\mathbf{C}\cap\mathbf{B}).$$

Podgrupe $\mathbf{A}\cap\mathbf{C}$ i $\mathbf{B}\cap\mathbf{C}$ ne mogu biti jedinične (inače bi element $c$ "upao" u jednu od podgrupa $\mathbf{A}$, $\mathbf{B}$). Prema tome, indeksi podgrupa $\mathbf{A}\cap\mathbf{C}$ i $\mathbf{B}\cap\mathbf{C}$ u $\mathbf{C}$ su konačni (i veći od 1 – u cikličnoj grupi, konačnoj ili beskonačnoj, sve nejedinične podgrupe su konačnog indeksa), a ti indeksi, opet, nisu ništa drugo do redovi elementa $c$ s obzirom na podgrupe $\mathbf{A}$ i $\mathbf{B}$. Ako su ti redovi (indeksi), redom, $n_A$, $n_B$, onda je, naravno, $\mathbf{A}\cap\mathbf{C}=\langle c^{n_A}\rangle$, $\mathbf{B}\cap\mathbf{C}=\langle c^{n_B}\rangle$, stoga i $\mathbf{C}=\langle c^{n_A},c^{n_B}\rangle$. Dakle, za neke cele brojeve $u$ i $v$ je $(c^{n_A})^u(c^{n_B})^v=c$, tj. $c^{un_A+vn_B}=c$. Proizilazi da su $n_A$ i $n_B$ uzajamno prosti. Ako je element $c$ beskonačnog reda, dobijamo direktno $un_A+vn_B=1$; ako je pak $c$ konačnog reda $n$, s obzirom da su i $n_A$ i $n_B$ delioci broja $n$, kao i da je $un_A+vn_B=1+kn$ za neki ceo broj $k$, odnosno, ako bismo ostali dosledni "našem tretiranju" konačnih cikličnih grupa, $(u-[\frac{u}{n}]n)\cdot_n n_A+_n(v-[\frac{v}{n}]n)\cdot_n n_B=1$, tj. $un_A+vn_B-[\frac{un_A+vn_B}{n}]n=1$, pretpostavka da $n_A$ i $n_B$ imaju zajednički prost faktor $p$ vodi u kontradikciju $(p|1)$.

($\Longleftarrow$) Uočimo prvo da za svaku cikličnu podgrupu $\mathbf{C}=\langle c\rangle$ grupe $\mathbf{A}\vee\mathbf{B}$ važi:

$$\mathbf{C}=\mathbf{C}\cap(\mathbf{A}\vee\mathbf{B})=(\mathbf{C}\cap\mathbf{A})\vee(\mathbf{C}\cap\mathbf{B}).$$

To je trivijalno (i uvek) ispunjeno ako je $\mathbf{C}$ podgrupa jedne od grupa $\mathbf{A}$, $\mathbf{B}$, a ako je $c\in\langle A\cup B\rangle\setminus(A\cup B)$, tada je, sa već uvedenim oznakama iz prvog dela, $(n_A,n_B)=1$, te je, za neke cele brojeve $u$ i $v$, $un_A+vn_B=1$, znači i $c=(c^{n_A})^u(c^{n_B})^v$ $(c^{n_A}\in A\cap C,\ c^{n_B}\in B\cap C)$. Jasno, onda i za svaku podgrupu $\mathbf{D}$ grupe $\mathbf{A}\vee\mathbf{B}$ važi

$$\mathbf{D}=\mathbf{D}\cap(\mathbf{A}\vee\mathbf{B})=(\mathbf{D}\cap\mathbf{A})\vee(\mathbf{D}\cap\mathbf{B});$$

(imamo u vidu da je samo inkluzija $\leq$ u pitanju; obratna nam je uvek na raspolaganju, bez ikakvih ograničenja). No, ako je $\mathbf{H}$ ma koja podgrupa grupe $\mathbf{G}$, onda je, prema konstatovanom:

$$\mathbf{H}\cap(\mathbf{A}\vee\mathbf{B})=((\mathbf{H}\cap(\mathbf{A}\vee\mathbf{B}))\cap\mathbf{A})\vee((\mathbf{H}\cap(\mathbf{A}\vee\mathbf{B}))\cap\mathbf{B})=(\mathbf{H}\cap\mathbf{A})\vee(\mathbf{H}\cap\mathbf{B}).$$□

**Teorema 34.16** *Mreža podgrupa grupe* $\mathbf{G}$ *je distributivna akko je* $\mathbf{G}$ *lokalno ciklična grupa.*

**Dokaz.** ($\Longrightarrow$) Neka je mreža podgrupa grupe $\mathbf{G}$ distributivna. Dovoljno je dokazati, da bismo pokazali da je $\mathbf{G}$ i lokalno ciklična, da je svaka podgrupa generisana sa dva elementa ciklična (ostalo čini indukcija). Neka je $\mathbf{H}$ podgrupa generisana elementima $a$ i $b$; jasno, pretpostavljamo da se nijedna od podgrupa $\mathbf{A}=\langle a\rangle$ i $\mathbf{B}=\langle b\rangle$ ne sadrži u (onoj) drugoj. Pretpostavimo i da

$b^{-1}ab \notin A$ (naravno, $b^{-1}ab \notin B$). Prema prethodnoj lemi, redovi elementa $b^{-1}ab$ s obzirom na podgrupe $\mathbf{A}$ i $\mathbf{B}$, neka su to $n_1$ i $n_2$, uzajamno su prosti brojevi. Stoga je $un_1 + vn_2 = 1$ za neke cele brojeve $u$ i $v$, pa sledi

$$b^{-1}ab = b^{-1}a^{un_1+vn_2}b = b^{-1}a^{un_1}b \cdot b^{-1}a^{vn_2}b =$$

$$((b^{-1}ab)^{n_1})^u((b^{-1}ab)^{n_2})^v = (b^{-1}ab)^{un_1}a^{vn_2} \in A,$$

kontradikcija; koristili smo: $(b^{-1}ab)^{n_2} \in B$, tj. $a^{n_2} \in B$. Proizilazi da su $\mathbf{A}$ i $\mathbf{B}$ normalne podgrupe grupe $\mathbf{H} = \mathbf{A} \vee \mathbf{B}$. Neka je, dalje, $c \in H \setminus (A \cup B)$, $\mathbf{C}$ ciklična grupa generisana sa $c$ i neka su redovi elementa $c$ s obzirom na podgrupe $\mathbf{A}$ i $\mathbf{B}$, respektivno, $n_A$ i $n_B$. Već znamo: $(n_A, n_B) = 1$. Isključeno je npr. $c^{n_A} = e$, zbog $\mathbf{C} = \mathbf{C} \cap (\mathbf{A} \vee \mathbf{B}) = (\mathbf{C} \cap \mathbf{A}) \vee (\mathbf{C} \cap \mathbf{B})$; $\mathbf{C} \cap \mathbf{A} = \mathbf{E}$ bi dalo $\mathbf{C} \leq \mathbf{B}$. No, i indeksi podgrupe $\mathbf{D} = \mathbf{A} \cap \mathbf{B}$ u, redom, $\mathbf{A}$ i $\mathbf{B}$, neka su to $m_1$ i $m_2$, takođe su uzajamno prosti brojevi. Prema 7.3 moguće je izabrati generatorni element $b_1$ u $\mathbf{B}$ takav da je $a^{m_1} = b_1^{m_2}$. Ako bi prost broj $q$ bio zajednički faktor brojeva $m_1$ i $m_2$, recimo, $m_1 = qr_1$, $m_2 = qr_2$, imali bismo: $(a^{r_1})^q = (b_1^{r_2})^q \in D$, element $d = a^{r_1}b_1^{r_2}$ ne pripada nijednoj od podgrupa $\mathbf{A}$ i $\mathbf{B}$, dok je $d^q \in D = A \cap B$, kontradiktorno tvrđenju prethodne leme. Pokažimo samo da je $d^q \in B$ (dokaz za $d^q \in A$ je analogan). Neka je $a' = a^{r_1}$, $b' = b_1^{r_2}$. Tada je

$$d^q = (a'b')^q = \underbrace{(a'b') \cdot \ldots \cdot (a'b')}_{q-puta} =$$

$$a'b'(a')^{-1} \cdot (a')^2b'(a')^{-2} \cdot \ldots \cdot (a')^qb'(a')^{-q} \cdot (a')^q \in B,$$

jer je $\mathbf{B} \lhd \mathbf{A} \vee \mathbf{B}$ i $(a')^q \in D$. Grupa $\mathbf{A} \vee \mathbf{B}$ je i Abelova. Zaista, element $g = a^{-1}b_1^{-1}ab_1$ je u $D$, prema tome je i permutabilan sa svakim od elemenata $a$, $b_1$, pa je:

$$g^{m_1} = (a^{-1}b_1^{-1}ab_1)^{m_1} = a^{-m_1} \cdot b_1^{-1}a^{m_1}b_1 = e;$$

element $b_1^{-1}ab_1$ je, kao element iz $A$ permutabilan sa $a$, a $a^{m_1}$ je, kao element iz $D$ permutabilan sa $b$. Slično: $g^{m_2} = e$, te je, za cele brojeve $u$ i $v$ takve da je $um_1 + vm_2 = 1$, $g = g^{um_1+vm_2} = e$. Konstatujemo na kraju da je, za iste cele brojeve $u$ i $v$, $a^vb_1^u$ generatorni element grupe $\mathbf{A} \vee \mathbf{B}$; jer, $(a^vb_1^u)^{m_2} = a^{vm_2}b_1^{um_2} = a^{vm_2}a^{um_1} = a$ i, slično, $(a^vb_1^u)^{m_1} = b$.

($\Longleftarrow$) Neka je $\mathbf{G}$ lokalno ciklična grupa (znači i Abelova), neka su $\mathbf{A}$ i $\mathbf{B}$ dve njene podgrupe takve da nijedna nije sadržana u drugoj i neka je $c$ element podgrupe $\mathbf{A} \vee \mathbf{B}$ koji nije u $A \cup B$. Onda je, za neko $a \in A$ i neko $b \in B$, $c = ab$, a podgrupa $\langle a, b\rangle$ je ciklična grupa generisana, recimo, elementom $d$; prema tome je, za neke cele brojeve $k$, $m$, $a = d^k$, $b = d^m$. Možemo odmah pretpostaviti da su $k$ i $m$ uzajamno prosti brojevi; stvarno, za $(k, m) = r > 1$ i $k = rk_1$, $m = rm_1$ sledi: $a = (d^r)^{k_1}$, $b = (d^r)^{m_1}$, i $d^r$ je takođe generatorni element grupe $\langle d\rangle$ (što još znači da je $\langle d\rangle$ konačna grupa kao i da je broj $r$ uzajamno prost sa njenim redom). Dalje imamo: $a^m = b^k = d^{km} \in A \cap B$,



pa je $c^k = a^kb^k \in A$, $c^m = a^mb^m \in B$. Neka su $n_1$ i $n_2$ redovi elementa $c$ s obzirom na podgrupe $\mathbf{A}$ i $\mathbf{B}$. Onda $n_1|k$, $n_2|m$, znači i $n_1$ i $n_2$ su uzajmno prosti brojevi. Pozivajući se ponovo na prethodnu lemu, zaključujemo da podgrupe $\mathbf{A}$ i $\mathbf{B}$ obrazuju distributivan par.■

## 35 Direktna suma cikličnih grupa

Već smo videli da su slobodne i konačno generisane Abelove grupe direktne sume cikličnih grupa (u slučaju slobodnih isključivo beskonačnih cikličnih grupa). U ovom paragrafu osvrnućemo se na neke od uslova za dekompozibilnost Abelove grupe u direktnu sumu cikličnih grupa.

**Teorema 35.1** *(Kriterijum Kulikova). Abelova primarna p-grupa* $\mathbf{A}$ *je direktna suma cikličnih grupa akko je unija rastućeg niza podgrupa* $\mathbf{A}_n$, $n \in \omega \setminus \{0\} = N$, *gde su za svako* $n$ *iz* $N$ *visine svih elemenata iz* $\mathbf{A}_n$ *u* $\mathbf{A}$ *konačne i ograničene.*

**Dokaz.** ($\Longrightarrow$) Očigledno. Neka je, za dato $n \in N$, $\mathbf{B}_n$ direktna suma svih cikličnih sumanada reda $p^n$ (ukoliko takvih nema $\mathbf{B}_n$ je nula podgrupa) i neka je $\mathbf{A}_n = \mathbf{B}_1 + \cdots + \mathbf{B}_n$. Tada je $\mathbf{A} = \bigcup_{n\in N} \mathbf{A}_n$ i elementi podgrupe $\mathbf{A}_n$ su visine manje od $n$.

($\Longleftarrow$) Pretpostavimo: $\mathbf{A} = \bigcup_{n\in N} \mathbf{A}_n$, $\mathbf{A}_m \leq \mathbf{A}_n$ za $m < n$, gde za svako $n \in N$ postoji prirodan broj $k_n$ takav da je, za svako $a \in A_n$, $h(a) \leq k_n$ (naravno, $k_1 \leq k_2 \leq \cdots$). Fiksirajmo jedan maksimalan slabo linearno nezavisan sistem podgrupe $\mathbf{A}_1[p] \cap p^{k_1}\mathbf{A}$. Njega proširujemo, u svakom koraku, do maksimalnih slabo linearno nezavisnih sistema podgrupa, redom, $\mathbf{A}_1[p] \cap p^{k_1-1}\mathbf{A}$, ..., $\mathbf{A}_1[p] \cap p\mathbf{A}$, $\mathbf{A}_1[p]$. Konačno dobijeni maksimalan slabo linearno nezavisan sistem – $S_1$ – proširujemo dalje do maksimalnih slabo linearno nezavisnih sistema podgrupa, redom, $\mathbf{A}_2[p] \cap p^{k_2}\mathbf{A}$, $\mathbf{A}_2[p] \cap p^{k_2-1}\mathbf{A}$, ..., $\mathbf{A}_2[p] \cap p\mathbf{A}$, $\mathbf{A}_2[p]$. Finalno dobijeni sistem $S_2$ nastavljamo na analogan način da proširujemo, i tako redom, dobijajući sisteme $S_n$, $n = 3, 4, \ldots$. Skup $\{a_\alpha \mid \alpha < \lambda\} = \bigcup_{n\in N} S_n$ je maksimalan slabo linearno nezavisan sistem (kao unija maksimalnih slabo linearno nezavisnih sistema) podgrupe $\mathbf{A}[p]$, dakle, $\mathbf{A}[p] = \sum_{\alpha<\lambda} \langle a_\alpha\rangle$. Neka je, za $\alpha < \lambda$, $h(a_\alpha) = m_\alpha$ i $a_\alpha = p^{m_\alpha}b_\alpha$. Sistem (skup) $\{b_\alpha \mid \alpha < \lambda\}$ i sam je slabo linearno nezavisan; indukcijom se pokazuje da je za svaki prirodan broj $k$ veći od 1 podskup skupa $\{b_\alpha \mid \alpha < \lambda\}$ kardinalnosti $k$ slabo linearno nezavisan. Za $k = 2$ nenula presek podgrupa $\langle b_\alpha\rangle$ i $\langle b_\beta\rangle$, $\alpha < \beta < \lambda$, sadržavao bi jedinstvene minimalne podgrupe reda $p$ tih grupa – $\langle a_\alpha\rangle$ i $\langle a_\beta\rangle$ (podsetimo se: u cikličnoj $p$-grupi podgrupe su linearno uređene inkluzijom), te bi sledilo $\langle a_\alpha\rangle = \langle a_\beta\rangle$, kontradikcija. Pretpostavimo da je tvrđenje tačno za sve podskupove kardinalnosti $\leq k$, i neka je

$$m_1b_{\alpha_1} + \cdots + m_kb_{\alpha_k} + m_{k+1}b_{\alpha_{k+1}} = 0.$$

Za $m_{k+1}b_{\alpha_{k+1}} \neq 0$ dobili bismo $\langle b_{\alpha_{k+1}}\rangle \cap (\langle b_{\alpha_1}\rangle \oplus \cdots \oplus \langle b_{\alpha_k}\rangle) \neq \mathbf{O}$, pa bi bilo $\langle a_{\alpha_{k+1}}\rangle \leq (\langle a_{\alpha_1}\rangle \oplus \cdots \oplus \langle a_{\alpha_k}\rangle)$, i opet kontradikcija. Stoga je $m_{k+1}b_{\alpha_{k+1}} = 0$, a onda je, po induktivnoj hipotezi, i $m_1 b_{\alpha_1} = \cdots = m_k b_{\alpha_k} = 0$. Pokazujemo konačno da je $\mathbf{A} = \sum_{\alpha<\lambda}\langle b_\alpha\rangle$. Pretpostavimo suprotno i neka je $c$ element najnižeg reda $(p^k)$ iz $A \setminus \sum^d_{\alpha<\lambda}\langle b_\alpha\rangle$. Onda je $p^{k-1}c$, kao element reda $p$, u $A[p] = \sum^d_{\alpha<\lambda}\langle a_\alpha\rangle$. Znači, za neko $\alpha_1, \ldots, \alpha_r$ je $p^{k-1}c = m_1 a_{\alpha_1} + \cdots + m_r a_{\alpha_r}$, $0 < m_j < p$, $j = 1, \ldots, r$. Ako bi neki elementi, recimo baš (uz eventualnu prenumeraciju indeksa) $a_{\alpha_1}, \ldots, a_{\alpha_t}$, bili visine veće od ili jednake $k-1$ $(h(a_{\alpha_i}) = m_{\alpha_i} \geq k-1,\ i = 1, \ldots, t)$, onda bi za $1 \leq i \leq t$ bilo $m_i a_{\alpha_i} = m_i p^{m_{\alpha_i}} b_{\alpha_i} = p^{k-1}(m_i p^{m_{\alpha_i}-(k-1)} b_{\alpha_i})$, dakle i

$$p^{k-1}(c - m_1 p^{m_{\alpha_1}-(k-1)} b_{\alpha_1} - \cdots - m_t p^{m_{\alpha_t}-(k-1)} b_{\alpha_t}) = m_{t+1}a_{\alpha_{t+1}} + \cdots + m_r a_{\alpha_r},$$

i $d = c - (m_1 p^{m_{\alpha_1}-(k-1)} b_{\alpha_1} + \cdots + m_t p^{m_{\alpha_t}-(k-1)} b_{\alpha_t}) \in A \setminus \sum^d_{\alpha<\lambda}\langle b_\alpha\rangle$ (naravno, mora biti $t < r$, u suprotnom $c \in \sum^d_{\alpha<\lambda}\langle b_\alpha\rangle$). Stoga možemo odmah pretpostaviti da je visina svakog elementa $a_{\alpha_i}$, $1 \leq i \leq r$, manja od $k-1$. Neka je $n$ najmanji prirodan broj takav da je $\{a_{\alpha_1}, \ldots, a_{\alpha_r}\} \subseteq S_n$. Prema tome, bar jedan element, uzmimo $a_{\alpha_r}$, nije u $S_{n-1}$ (ako je $n = 1$, $S_{n-1}$ smatramo praznim skupom). No tada je $p^{k-1}c \in A_n[p]$ i $h(p^{k-1}c) \geq p^{k-1} > h(a_{\alpha_r})$, te je, s obzirom kako smo konstruisali skupove $S_m$, $p^{k-1}c$ ili sam u skupu $\{a_\alpha \mid \alpha < \lambda\}$ ili se javlja kao linearna kombinacija konačnog podskupa $\{a_{\beta_1}, \ldots, a_{\beta_s}\}$ koji ne sadrži $a_{\alpha_r}$ (u skupove $S_m$ smo prvo "ubacivali", ukoliko se već ne javljaju kao linearne kombinacije ranije izabranih elemenata, elemente većih visina). Protivrečnost imamo u svakom slučaju, jer dobijamo prezentaciju istog elementa kao različite linearne kombinacije elemenata skupa $\{a_\alpha \mid \alpha < \lambda\}$ koji je slabo linearno nezavisan.■

**Korolar 35.2** *(Prva teorema Prüfera). Ograničena primarna grupa* $\mathbf{A}$ *je direktna suma cikličnih grupa.*

**Dokaz.** Staviti, za $n \in N$ $(= \omega\setminus\{0\})$, $\mathbf{A}_n = \mathbf{A}$ (i pozvati se na prethodnu teoremu – elementi su konačnih i ograničenih redova pa su i konačnih i ograničenih visina).□

**Napomena.** Prüferova prva teorema daje se i u ovoj formulaciji (videti komentar uz definiciju 33.2):

*Primarna grupa* $\mathbf{A}$ *u kojoj su visine elemenata ograničeni direktna je suma cikličnih grupa.*

Uslov ograničenosti, dodajmo, nije i potreban za dekompoziciju primarne grupe u direktnu sumu cikličnih grupa; npr. grupa $\sum_{n\in N}\mathbf{C}_{p^n}$ nije ograničena.

**Primer 35.3** $\mathbf{A}[n]$ *je, za svaku Abelovu grupu* $\mathbf{A}$ *i svaki prirodan broj* $n$*, direktna suma cikličnih grupa.*

**Dokaz.** $\mathbf{A}[n] = \langle\{a \in A \mid na = 0\}, +\rangle$ je podgrupa periodičnog dela grupe $\mathbf{A}$, $t\mathbf{A}$, koji je pak direktna suma primarnih grupa: $t\mathbf{A} = \sum_{p\in P}\mathbf{A}_p$, gde



je $\mathbf{A}_p$ maksimalna $p$-podgrupa grupe $\mathbf{A}$. Ako je $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, onda je $\mathbf{A}[n] = \mathbf{A}_{p_1}[n] + \cdots + \mathbf{A}_{p_k}[n] = \mathbf{A}_{p_1}[p_1^{\alpha_1}] + \cdots + \mathbf{A}_{p_k}[p_k^{\alpha_k}]$, a svaka od grupa $\mathbf{A}_{p_i}[p_i^{\alpha_i}]$ je direktna suma cikličnih grupa kao ograničena primarna grupa.□

**Korolar 35.4** *Nejedinična Abelova nedeljiva grupa* $\mathbf{A}$ *ima (maksimalnu) podgrupu prostog indeksa.*

**Dokaz.** Ako je $n\mathbf{A} = \mathbf{O}$ za neki prirodan broj $n$, onda je, prema 35.2, $\mathbf{A}$ direktna suma cikličnih grupa i kako svaka nejedinična ciklična grupa, konačna ili beskonačna, ima pomenuto svojstvo, sledi tvrđenje (ako je npr. $\mathbf{A} = \sum_{\alpha<\lambda}\mathbf{A}_\alpha$, gde je, za $\alpha < \lambda$, $\mathbf{A}_\alpha$ ciklična grupa i ako je $\mathbf{B}_0$ podgrupa grupe $\mathbf{A}_0$ prostog indeksa $p$, tada je $\mathbf{B}_0 \oplus \sum_{0<\alpha<\lambda}\mathbf{A}_\alpha$ podgrupa grupe $\mathbf{A}$ indeksa $p$). U suprotnom ($n\mathbf{A} \neq \mathbf{O}$ za svako $n \in N$) postoji bar jedan prost broj $q$ za koji je $q\mathbf{A} \neq \mathbf{A}$ (inače bi $\mathbf{A}$ bla deljiva grupa – 33.1). Onda je, za $\overline{\mathbf{A}} = \mathbf{A}/q\mathbf{A}$, $q\overline{\mathbf{A}} = \overline{\mathbf{O}}$, pa je $\overline{\mathbf{A}}$ direktna suma cikličnih grupa reda $q$. Kao takva, očigledno ima podgrupu indeksa $q$, te je, prema 8.7, ima i grupa $\mathbf{A}$.□

**Korolar 35.5** *(Druga teorema Prüfera). Prebrojiva* $p$*-primarna grupa* $\mathbf{A}$ *je direktna suma cikličnih grupa akko nema (nenula) elemenata beskonačne visine.*

**Dokaz.** Pravac $\Longrightarrow$ je jasan.

S druge strane, ako je $A = \{a_n \mid n \in \omega\}$, onda je $\mathbf{A}$ unija rastućeg niza podgrupa $\mathbf{A}_n = \langle a_0, \ldots, a_n\rangle$. No, svaka konačno generisana periodična Abelova grupa je direktna suma konačnog broja konačnih cikličnih grupa (u našem slučaju, jasno, $p$-cikličnih grupa), dakle i konačna (konačnost sledi i iz leme Dicmana). Stoga su visine elemenata svake grupe $\mathbf{A}_n$ konačne i ograničene.□

**Napomena.** Uslov prebrojivosti nije moguće eliminisati iz prethodnog korolara. Sledeći kontraprimer Kuroša to pokazuje:

Neka je $\mathbf{A}$ periodični deo grupe $\sum^c_{n\in N}\mathbf{Z}_{p^n}$. $\mathbf{A}$ je kardinalnosti kontinuum – za svaki podskup $X$ skupa $N = \omega \setminus \{0\}$ element $\mathbf{a}_X = \langle a_k\rangle_{k\in N}$, gde je

$$a_k = \begin{cases} p^{k-1} & k \in X \\ 0 & \text{inače} \end{cases},$$

reda je $p$, pa je $\mathbf{a}_X \in A$. Grupa $\sum^c_{n\in N}\mathbf{Z}_{p^n}$ je bez nenula elemenata beskonačne visine, jer ako je $\mathbf{a} = \langle a_k\rangle$, $\mathbf{b} = \langle b_k\rangle$ i $\mathbf{a} = p^m\mathbf{b}$, sledi $a_1 = \cdots = a_m = 0$. Pretpostavimo da je grupa $\mathbf{A}$ izomorfna direktnoj sumi cikličnih grupa $\mathbf{C} = \sum_{n\in N}\mathbf{C}_n$, gde je $\mathbf{C}_n$ direktna suma cikličnih grupa reda $p^n$. Neka je, za $n \in N$, $\mathbf{D}_n = \sum_{i\geq n}\mathbf{C}_i[p]$. $\mathbf{D}_n$ je, jasno, podgrupa grupe $\mathbf{C}[p]$ sa elementima visine veće od ili jednake $n-1$, pa je $\mathbf{D}_n$ izomorfna podgrupi $\mathbf{B}_n$ grupe $\mathbf{A}$ čiji je domen skup elemenata reda $p$ sa prvih $n-1$ komponenata jednakih nuli. Stoga je $\mathbf{D}_n/\mathbf{D}_{n+1} \cong \mathbf{B}_n/\mathbf{B}_{n+1}$, $n = 1, 2, \ldots$, reda $p$, i kako je $\mathbf{C}_n[p] \cong \mathbf{D}_n/\mathbf{D}_{n+1}$,

proizilazi da je $\mathbf{C}_n$ $(= \mathbf{C}_{p^n})$ konačna grupa. Ali onda je $\mathbf{C}$, pa dakle i $\mathbf{A}$, prebrojiva grupa, kontradikcija.

**Korolar 35.6** *Abelova p-grupa* $\mathbf{A}$ *je direktna suma cikličnih grupa akko je unija rastućeg niza podgrupa* $\mathbf{A}_n$ *takvih da je* $p^n\mathbf{A} \cap \mathbf{A}_n = \mathbf{O}$.

**Dokaz.** $(\Longrightarrow)$ Neka je $\mathbf{A}$ direktna suma cikličnih $p$-grupa i neka je $\mathbf{B}_n$ direktna suma cikličnih sumanada reda $p^n$ ili, ukoliko takvih sumanada nema, nula grupa. Ako je $\mathbf{A}_n = \mathbf{B}_1 + \cdots + \mathbf{B}_n$, onda je, očigledno, $p^n\mathbf{A} \cap \mathbf{A}_n = \mathbf{O}$; $\mathbf{A}_n$ je direktni sumand grupe $\mathbf{A}$, pa ako jednačina $p^n x = a$, $a \in A_n$, ima rešenje u $\mathbf{A}$, mora ga imati i u $\mathbf{A}_n$.

$(\Longleftarrow)$ Ako je $\mathbf{A} = \bigcup_{n\in N} \mathbf{A}_n$, $\mathbf{A}_m \leq \mathbf{A}_n$ za $m < n$, gde je $\mathbf{A}_n \cap p^n\mathbf{A} = \mathbf{O}$, onda su visine elemenata u $\mathbf{A}_n$ konačne i ograničene $(\leq n-1)$ i, prema kriterijumu Kulikova, $\mathbf{A}$ je direktna suma cikličnih grupa.□

**Korolar 35.7** *Ako je primarna grupa* $\mathbf{A}$ *direktna suma cikličnih grupa, onda je to i svaka njena podgrupa* $\mathbf{B}$.

**Dokaz.** Prema kriterijumu Kulikova je $\mathbf{A} = \bigcup_{n\in N} \mathbf{A}_n$, gde je $\mathbf{A}_n \leq \mathbf{A}_{n+1}$, a visine elemenata svake od podgrupa $\mathbf{A}_n$ su konačne i ograničene. No tada je $\mathbf{B} = (\bigcup_{n\in N} \mathbf{A}_n) \cap \mathbf{B} = \bigcup_{n\in N} (\mathbf{A}_n \cap \mathbf{B})$, pa kako su visine elemenata podgrupa $\mathbf{A}_n \cap \mathbf{B}$ konačne i ograničene u $\mathbf{A}$, tim pre su ograničene u $\mathbf{B}$ i $\mathbf{B}$ je (opet prema kriterijumu Kulikova) direktna suma cikličnih grupa.□

**Korolar 35.8** *Ako je grupa* $\mathbf{A}$ *direktna suma cikličnih grupa, onda je i (svaka) njena podgrupa* $\mathbf{B}$ *direktna suma cikličnih grupa.*

**Dokaz.** Neka je $\mathbf{A}$ direktna suma cikličnih grupa. Kao takva ona je i direktna suma svog periodičnog dela i slobodne Abelove (pod)grupe. Jasno, $t\mathbf{B} = \mathbf{B} \cap t\mathbf{A}$, a prema drugoj teoremi o izomorfizmu je: $(\mathbf{B}\,t\mathbf{A})/t\mathbf{A} \cong \mathbf{B}/(\mathbf{B} \cap t\mathbf{A}) = \mathbf{B}/t\mathbf{B}$. Kao grupa izomorfna podgrupi slobodne Abelove grupe $\mathbf{A}/t\mathbf{A}$, $\mathbf{B}/t\mathbf{B}$ je i sama slobodna Abelova grupa. Prema 31.24, $\mathbf{B}$ je direktna suma svog periodičnog dela i slobodne Abelove grupe. Ako su $\mathbf{A}_p$ i $\mathbf{B}_p$ maksimalne $p$-podgrupe grupa, respektivno, $t\mathbf{A}$ i $t\mathbf{B}$, opet je, naravno, $\mathbf{B}_p = t\mathbf{B} \cap \mathbf{A}_p$. S obzirom da je $\mathbf{A}_p$ direktna suma cikličnih $p$-grupa, prema prethodnom korolaru to je i $\mathbf{B}_p$, te je i $\mathbf{B}$ direktna suma cikličnih grupa.□

**Lema 35.9** *Neka je* $\mathbf{G}$ *neabelova grupa bez pravih podgrupa konačnog indeksa i neka je* $\mathbf{A}$ *njena normalna podgrupa izomorfna bilo aditivnoj grupi racionalnih brojeva bilo nekoj Prüferovoj p-grupi. Tada je* $\mathbf{A}$ *podgrupa centra grupe* $\mathbf{G}$.

**Dokaz.** I slučaj: $\mathbf{A}$ je izomorfno grupi $\mathbf{Ra}$.

Prema 30.7 i 2.10$(e)$ je $\mathbf{Aut}(\mathbf{A}) \cong \langle Ra \setminus \{0\}, \cdot\rangle = \prod_{p\in P} \langle p\rangle \times \langle\{1,-1\}, \cdot\rangle$, gde je $P$ skup prostih brojeva. Pošto je i svaka podgrupa grupe $\mathbf{Aut}(\mathbf{A})$



direktni proizvod cikličnih grupa, $\mathbf{Aut}(\mathbf{A})$ je bez deljivih podgrupa. Preslikavanje $\varphi : G \longrightarrow Aut(\mathbf{A})$ dato sa $(g)\varphi = u_g|_A$ homomorfno je preslikavanje grupe $\mathbf{G}$ u grupu $\mathbf{Aut}(\mathbf{A})$. Ako je $\varphi$ trivijalni homomorfizam (svi elementi se preslikavaju u jedinični), direktno sledi da je $\mathbf{A}$ podgrupa centra grupe $\mathbf{G}$. Ali drugačije i ne može biti; ako bi $\mathbf{Ker}(\varphi)$ bilo prava podgrupa grupe $\mathbf{G}$, tada bi $(\mathbf{G})\varphi$ $(\cong \mathbf{G}/\mathbf{Ker}(\varphi))$ bila beskonačna Abelova grupa bez podgrupa konačnog indeksa, znači i deljiva (33.7), kontradikcija.

II slučaj: $\mathbf{A}$ je izomorfno grupi $\mathbf{p}^\infty$.

Neka je $a$ ma koji element podgrupe $\mathbf{A}$ reda, recimo, $p^n$. Podgrupa $\langle a\rangle$ je karakteristična podgrupa grupe $\mathbf{A}$ (u grupi $\mathbf{p}^\infty$ postoji samo jedna podgrupa datog reda $p^n$), zato i normalna podgrupa grupe $\mathbf{G}$. Prema tome, svi konjugati elementa $a$ su u $\langle a\rangle$, što će reći da ih ima konačno mnogo. Zapravo, samo je jedan takav – sam element $a$, u suprotnom bi centralizator elementa $a$ bio prava podgrupa konačnog indeksa. Proizilazi: $a \in Z(\mathbf{G})$.□

**Korolar 35.10** $(a)$ *Abelova grupa* $\mathbf{A}$ *je direktna suma cikličnih grupa akko je, za neki prost* $p$, $p\mathbf{A}$ *direktna suma cikličnih grupa.*

$(b)$ *Abelova grupa* $\mathbf{A}$ *je direktna suma cikličnih grupa akko je, za neki pozitivan prirodan broj* $n$, $n\mathbf{A}$ *direktna suma cikličnih grupa.*

**Dokaz.** Jasno, $(b)$ uključuje $(a)$, ali se dokaz od $(b)$ zasniva na $(a)$.

$(a)$ Neka je $p\mathbf{A} = \sum_{\alpha<\lambda} \langle a_\alpha\rangle$, gde je red od $a_\alpha$ ili beskonačan ili stepen nekog prostog broja (znamo da je svaka konačna ciklična grupa čiji red sadrži više prostih faktora razloživa u direktnu sumu primarnih cikličnih grupa). Izaberimo za svako $\alpha < \lambda$ element $b_\alpha$ takav da je $a_\alpha = pb_\alpha$, s tim da ako je red od $a_\alpha$ uzajamno prost sa $p$, onda je $b_\alpha \in \langle a_\alpha\rangle$; ako je $red(a_\alpha) = q^k$, $k \geq 1$, $q \neq p$, i ako su $u, v$ celi brojevi takvi da je $up + vq^k = 1$, onda je $a_\alpha = (up + vq^k)a_\alpha = p(ua_\alpha)$, pa za $b_\alpha$ možemo uzeti, a i uzećemo, takvo jedno $ua_\alpha$ – konstatujmo odmah i da su u tom slučaju elementi $a_\alpha$ i $b_\alpha$ istog reda. Skup $B = \{b_\alpha \mid \alpha < \lambda\}$ je slabo linearno nezavisan. Jer, pretpostavimo $m_1 b_{\alpha_1} + \cdots + m_k b_{\alpha_k} = 0$ i $m_i b_{\alpha_i} \neq 0$, $i = 1, \ldots, k$ $(\geq 2)$. Sledi ("množenjem" sa $p$) $m_1 a_{\alpha_1} + \cdots + m_k a_{\alpha_k} = 0$, te je $m_i a_{\alpha_i} = 0$ za svako $i$. Ako je $a_{\alpha_i}$ beskonačnog reda, onda je $m_i = 0$, dakle $m_i b_{\alpha_i} = 0$, protivno pretpostavci. Ako je $a_{\alpha_i}$ reda $q^k$, $q \neq p$, onda $q^k | m_i$ i opet $m_i b_{\alpha_i} = 0$. Konačno, ako je red svakog elementa $a_{\alpha_i}$ stepen broja $p$, $p^{s_i}$, $s_i \geq 1$, tada $p^{s_i} | m_i$, recimo, $m_i = p^{s_i} r_i$, pa $m_1 b_{\alpha_1} + \cdots + m_k b_{\alpha_k} = p^{s_1 - 1} r_1 a_{\alpha_1} + \cdots + p^{s_k - 1} r_k a_{\alpha_k} = 0$, a odatle $p^{s_i - 1} r_i a_{\alpha_i} = p^{s_i} r_i b_{\alpha_i} = m_i b_{\alpha_i} = 0$, kontradikcija ponovo. Proširimo skup $B$ elementima iz $A[p]$ do maksimalnog slabo linearno nezavisnog skupa (s obzirom na mogućnost izbora) $C = B \cup \{c_\beta \mid \beta < \mu\}$. Pokazujemo definitivno da je $\mathbf{A}$ direktna suma cikličnih grupa generisanih elementima iz $C$ (drugim rečima da je $C$ baza grupe $\mathbf{A}$). Jasno, samo je pitanje da li je $C$ njen generatorni skup. Neka je $a \in A$. Po uslovu leme $pa$ je linearna kombinacija elemenata iz $\{a_\alpha \mid \alpha < \lambda\}$, npr. $pa = m_1 a_{\alpha_1} + \cdots + m_k a_{\alpha_k} = p(m_1 b_{\alpha_1} + \cdots + m_k b_{\alpha_k})$.

Element $b = a - (m_1 b_{\alpha_1} + \cdots + m_k b_{\alpha_k})$, ukoliko već nije jednak nuli, reda je $p$ i kao takav linearno je zavisan od sistema $C$. Izvodimo: $b \in \langle C \rangle$, a onda i $a \in \langle C \rangle$.

$(b)$ Neka je $n = p_1 \cdot \ldots \cdot p_k$, $k \geq 2$ (dozvoljavamo mogućnost da su neki od prostih faktora jednaki) i neka je $n\mathbf{A} = p_1((p_2 \cdot \ldots \cdot p_k)\mathbf{A})$ direktna suma cikličnih grupa. Prema tački $(a)$ onda je i $(p_2 \cdot \ldots \cdot p_k)\mathbf{A}$ direktna suma cikličnih grupa. Analognim rezonovanjem dokazujemo da je, konačno, i $p_k\mathbf{A}$ direktna suma cikličnih grupa, pa je, ponovo prema $(a)$, i $\mathbf{A}$ direktna suma cikličnih grupa.□

**Lema 35.11** *Ako je* $\mathbf{A}$ *direktna suma cikličnih grupa, tada su svaka dva razlaganja grupe* $\mathbf{A}$ *u direktnu sumu nerazloživih cikličnih grupa izomorfna.*

**Dokaz**. Dokaz se u mnogome svodi na ponavljanje dokaza korolara 32.11; idejno se, zapravo, oni ne razlikuju. Situacija je ovoga puta utoliko komplikovanija što broj sumanada nije nužno konačan. U svakom slučaju broj beskonačnih cikličnih sumanada određuje torziono slobodni rang grupe, te je za bilo koje dve dekompozicije isti. Direktna suma $p$-cikličnih grupa određuje (jedinstvenu) maksimalnu $p$-podgrupu, $\mathbf{A}_p$, grupe $t\mathbf{A}$. Stoga je dovoljno u daljem razmatranju osvrnuti se samo na nju. Dalje rezonujemo kao u slučaju kontraprimera uz korolar 35.5. $\mathbf{A}_p = \sum_{n\in N} \mathbf{B}_n$, gde je $\mathbf{B}_n$ direktna suma cikličnih grupa reda $p^n$ ili, ukoliko takvih sumanada nema, nula grupa. Jasno, $\mathbf{A}_p[p] = \sum_{n\in N} \mathbf{B}_n[p]$. Neka je $\mathbf{C}_n = \sum_{i\geq n} \mathbf{B}_i[p]$. $\mathbf{C}_n$ je podgrupa grupe $\mathbf{A}_p[p]$ sa elementima visine veće od ili jednake $n-1$, dakle nezavisna od izbora dekompozicija, pa je takva i podgrupa $\mathbf{B}_n[p]$ ($\cong \mathbf{C}_n/\mathbf{C}_{n+1}$). No, grupa $\mathbf{B}_n[p]$ u potpunosti određuje grupu $\mathbf{B}_n$, tj. broj cikličnih sumanada reda $p^n$ – ako je $|B_n[p]| = \lambda \geq \aleph_0$, takvih sumanada je $\lambda$; ako je $|B_n[p]| = p^m$, onda $m$.□

**Lema 35.12** *Svaka Abelova grupa* $\mathbf{A}$ *je unija prebrojivog rastućeg niza direktnih suma cikličnih grupa.*

**Dokaz**. Neka je $\mathbf{A}$ podgrupa deljive grupe $\mathbf{D} = \sum_{\alpha<\lambda} \mathbf{R}\mathbf{a}_\alpha \oplus \sum_{p\in P}(\sum_{\beta<\mu_p} \mathbf{p}^\infty_\beta)$; za $\alpha < \lambda$ grupa $\mathbf{R}\mathbf{a}_\alpha$ je kopija aditivne grupe racionalnih brojeva sa domenom $\{a_\alpha \mid a \in Ra\}$, za $\beta < \mu_p$ grupa $\mathbf{p}^\infty_\beta$ je kopija Prüferove $\mathbf{p}^\infty$-grupe sa generatornim elementima $e_\beta^{\frac{2\pi}{p^n}i}$, $n = 1, 2, \ldots$. Znamo da je $\mathbf{R}\mathbf{a}_\alpha = \bigcup_{n\in N} \langle \frac{1}{n\alpha!} \rangle$, $\mathbf{p}^\infty_\beta = \bigcup_{n\in N} \langle e_\beta^{\frac{2\pi}{p^n}i} \rangle$. Ako je, za $n \in N$, $\mathbf{D}_n = \sum_{\alpha<\lambda} \langle \frac{1}{n\alpha!} \rangle \oplus \sum_{p\in P}(\sum_{\beta<\mu_p} \langle e_\beta^{\frac{2\pi}{p^n}i} \rangle)$, jasno, $\mathbf{D}_n \leq \mathbf{D}_{n+1}$ i $\mathbf{A} = \bigcup_{n\in N}(\mathbf{A} \cap \mathbf{D}_n)$, a kao podgrupa direktne sume cikličnih grupa i $\mathbf{A} \cap \mathbf{D}_n$ je (za svako $n$) direktna suma cikličnih grupa.□

Neka je grupa $\mathbf{A}$ direktna suma cikličnih grupa: $\mathbf{A} = \sum_{\alpha<\lambda} \langle a_\alpha \rangle$. Njenu bazu $\mathcal{A} = \{a_\alpha \mid \alpha < \lambda\}$ karakterišu, evidentno, sledeća svojstva:

(1) A je maksimalan slabo linearno nezavisan sistem;

(2) $\mathcal{A}$ je minimalni generatorni skup.



Pitanje da li je neka grupa direktna suma cikličnih grupa ekvivalentno je, dakle, pitanju egzistencije skupa sa uslovima (1) i (2). Sledeći kriterijumi (L. Fuchs, T. Szela) odnose se samo na slučajeve baza sa elementima beskonačnih redova ili redova jednakih stepenima prostih brojeva. U daljim razmatranjima treba nam jedna vrsta poređenja beskonačnih redova elemenata.

**Definicija 35.13** *Neka je* $\mathcal{A} = \{a_\alpha \mid \alpha < \lambda\}$ *slabo linearno nezavisan sistem grupe* $\mathbf{A}$ *sa elementima čiji su redovi ili beskonačni ili stepeni prostih brojeva. Ako su* $a_\alpha \in \mathcal{A}$ *i* $b \in A$ *elementi beskonačnog reda i ako je* $rb = ma_\alpha + m_1 a_{\alpha_1} + \cdots + m_k a_{\alpha_k}$, $r, m \in Z \setminus \{0\}$, *onda je* $b$ *većeg (manjeg) reda od* $a_\alpha$, *s obzirom na* $\mathcal{A}$, *akko je* $|r| > |m|$ $(|r| < |m|)$. *Ako je* $c \in A$ *konačnog reda, on je većeg (manjeg) reda od* $a_\beta \in \mathcal{A}$, *s obzirom na bilo koji slabo linearno nezavisan skup, akko je (u standardnom smislu) njegov red veći (manji) od reda elementa* $a_\beta$.

**Napomena**. U slučaju elemenata beskonačnih redova $b$ i $a_\alpha$ korektnost definicije je zagarantovana slabom linearnom nezavisnošću skupa $\mathcal{A}$. Jer, ako je $rb = ma_\alpha + \cdots$ i $sb = na_\alpha + \cdots$, sledi $0 = (ms - nr)a_\alpha + \cdots$, i dalje, $|m| \cdot |s| = |n| \cdot |r|$; prema tome ako je $|r| > |m|$, mora biti i $|s| > |n|$.

U nastavku, do daljneg, nećemo više posebno naglašavati da su redovi elemenata skupa $\mathcal{A} = \{a_\alpha \mid \alpha < \lambda\}$ ili beskonačni ili stepeni prostih brojeva.

**Teorema 35.14** *Podskup* $\mathcal{A} = \{a_\alpha \mid a_\alpha < \lambda\}$ *domena grupe* $\mathbf{A}$ *je baza grupe akko važi:*

$(i)$ $\mathcal{A}$ *je maksimalan slabo linearno nezavisan sistem*

*i*

$(ii)$ *nijedan skup dobijen od* $\mathcal{A}$ *zamenom bilo kog elementa* $a_\alpha$ *elementom* $b$ *većeg reda, s obzirom na* $\mathcal{A}$ *(u smislu gornje definicije), nije slabo linearno nezavisan.*

**Dokaz**. ($\Longrightarrow$) Neka je $\mathcal{A}$ baza grupe $\mathbf{A}$. $(i)$ već imamo. Neka je $0 \neq b \notin \mathcal{A}$. Kako je $\mathcal{A}$ baza, to je $b = m_1 a_{\alpha_1} + \cdots + m_k a_{\alpha_k}$ za neki skup indeksa $\{\alpha_1, \ldots, \alpha_k\}$ i neke cele nenula brojeve $m_i$, $i = 1, \ldots, k$. Naravno, ako sa $b$ zamenimo bilo koji element $a_\alpha \in \mathcal{A}$ koji se ne javlja u gornjoj linearnoj kombinaciji, gubimo slabu linearnu nezavisnost. Pretpostavimo stoga da je red od $b$ veći od reda elementa $a_{\alpha_1}$. Ako su $a_{\alpha_1}$ i $b$ konačnog reda i ako je $m = red(a_{\alpha_1}) < red(b)$, tada je $0 \neq mb = (mm_2)a_{\alpha_2} + \cdots + (mm_k)a_{\alpha_k}$, pa skup $(\mathcal{A} \setminus \{a_{\alpha_1}\}) \cup \{b\}$ nije slabo linearno nezavisan. Ako su $a_{\alpha_1}$ i $b$ beskonačnih redova, $b$ ne može biti većeg reda od $a_{\alpha_i}$, $i = 1, \ldots, k$, s obzirom na $\mathcal{A}$, jer je $|m_i| \geq 1$.

($\Longleftarrow$) Neka $\mathcal{A}$ ispunjava uslove $(i)$ i $(ii)$. Zbog slabe linearne nezavisnosti je $\langle \mathcal{A} \rangle = \sum_{\alpha<\lambda} \langle a_\alpha \rangle$. Pretpostavimo: $\mathbf{A} \neq \langle \mathcal{A} \rangle$ i $b \in A \setminus \langle \mathcal{A} \rangle$. Kako je skup $\mathcal{A} \cup \{b\}$ linearno zavisan, postoje indeksi $\alpha_1, \ldots, \alpha_k$ $(< \lambda)$ i nenula celi brojevi $p, m_1, \ldots, m_k$ takvi da je

$$pb = m_1 a_{\alpha_1} + \cdots + m_k a_{\alpha_k} \qquad (*).$$

Nema razloga da odmah ne pretpostavimo da je $p$ prost broj (jer ako je $r = p_1 \cdot \ldots \cdot p_k$, $k \geq 2$, najmanji pozitivan prirodan broj takav da je $rb \in \langle \mathcal{A} \rangle$, umesto elementa $b$ uzeli bismo u razmatranje $c = (p_2 \cdot \ldots \cdot p_k)b$; očigledno, $c \notin \langle \mathcal{A} \rangle$ i $p_1 c \in \mathcal{A}$). Isto tako možemo smatrati i da je apsolutna vrednost svakog od brojeva $m_i$ manja od $p$. (Ako je $m_i = pq_i + r_i$, $0 \leq r_i < p$, onda je $p(b - q_1 a_{\alpha_1} - \cdots - q_k a_{\alpha_k}) = r_1 a_{\alpha_1} + \cdots + r_k a_{\alpha_k}$; svi ostaci $r_i$ ne mogu biti 0, jer bismo, za $c = b - (q_1 a_{\alpha_1} + \cdots + q_k a_{\alpha_k}) \notin \mathcal{A}$, imali $pc = 0$ i $\langle c \rangle \cap \langle \mathcal{A} \rangle = \mathbf{O}$, suprotno uslovu o maksimalnosti slabo linearno nezavisnog skupa $\mathcal{A}$, i ostalo bi samo da umesto $b$ odaberemo $c$ i naši zahtevi bi bili ispunjeni.) Ako je bar jedan od elemenata $a_{\alpha_i}$, $i = 1, \ldots, k$, beskonačnog reda, npr. $a_{\alpha_1}$, onda je i $b$ beskonačnog reda, i po usvojenim pretpostavkama, većeg od reda elementa $a_{\alpha_1}$. No, sistem $(\mathcal{A} \setminus \{a_{\alpha_1}\}) \cup \{b\}$ ostao bi slabo linearno nezavisan, suprotnu uslovu $(ii)$; jer, ako je $tb + t_1 a_{\beta_1} + \cdots + t_l a_{\beta_l} = 0$, $tb \neq 0$, $\beta_i \neq \alpha_1$, tada je $t(pb) + t_1 p a_{\beta_1} + \cdots + t_l p a_{\beta_l} = 0$, odnosno $tm_1 a_{\alpha_1} + \cdots + tm_k a_{\alpha_k} + t_1 p a_{\beta_1} + \cdots + t_l p a_{\beta_l} = 0$ i $tm_1 a_{\alpha_1} \neq 0$, dok $a_{\alpha_1} \notin \{a_{\alpha_2}, \ldots, a_{\alpha_k}, a_{\beta_1}, \ldots, a_{\beta_l}\}$. Ako su svi elementi $a_{\alpha_i}$ $(i = 1, \ldots, k)$ u $(*)$ konačnog reda, možemo odmah pretpostaviti da su njihovi redovi stepeni prostog broja $p$ (ako nijedan od elemenata $a_{\alpha_i}$ ne bi imao za red stepen prostog broja $p$, tada bi i red elementa $b$ bio uzajamno prost sa $p$ i stoga $b \in \langle a_{\alpha_1}, \ldots, a_{\alpha_k} \rangle$; ako su pak samo redovi elemenata $a_{\alpha_1}, \ldots, a_{\alpha_t}$, $t < k$, stepeni broja $p$, zamenom elementa $b$ adekvatnim, slučaj bi se sveo na pretpostavljeni). Neka je $p^r = red(a_{\alpha_1}) \geq red(a_{\alpha_i})$, $2 \leq i \leq k$. Tada je $p^r b = p^{r-1} m_1 a_{\alpha_1} + \cdots + p^{r-1} m_k a_{\alpha_k} \neq 0$ (jer $(m_1, p) = 1$), pa je red elementa $b$ veći od reda elementa $a_{\alpha_1}$, i opet je skup $\mathcal{A} \setminus \{a_{\alpha_1}\} \cup \{b\}$ slabo linearno nezavisan. Iz $p^s kb + k_1 a_{\beta_1} + \cdots + k_n a_{\beta_n} = 0$, $s < r + 1$, $(k, p) = 1$, proizilazi, razmatranjem analognim malopređašnjem: $p^r kb + p^{r-s} k_1 a_{\beta_1} + \cdots + p^{r-s} k_n a_{\beta_n} = 0$, tj. $kp^{r-1} m_1 a_{\alpha_1} + \cdots + kp^{r-1} m_k a_{\alpha_k} + p^{r-s} k_1 a_{\beta_1} + \cdots + p^{r-s} k_n a_{\beta_n} = 0$, dok je $kp^{r-1} m_1 a_{\alpha_1} \neq 0$. Zaključujemo (a time i završavamo dokaz): pretpostavka $\mathbf{A} \neq \langle \mathcal{A} \rangle$ vodi u kontradikciju.■

**Teorema 35.15** *Skup $\mathcal{A} = \{a_\alpha \mid \alpha < \lambda\}$ je baza grupe $\mathbf{A}$ akko važi:*

*$(i)$ $\mathcal{A}$ je generatorni skup koji ne sadrži nulu*

*i*

*$(ii)$ nijedan skup dobijen od $\mathcal{A}$ zamenom nekog elementa $a_\alpha$ elementom $b$, manjeg reda u odnosu na slabo linearno nezavisan skup $\{a_\alpha\}$, nije generatorni skup grupe.*

**Dokaz.** $(\Longrightarrow)$ Neka je $\mathcal{A}$ baza. Jasno, $(i)$ važi. Neka je

$$0 \neq b = m_1 a_{\alpha_1} + \cdots + m_k a_{\alpha_k} \qquad (*).$$

Skup $(\mathcal{A} \setminus \{a_\beta\}) \cup \{b\}$, gde $\beta \notin \{\alpha_1, \ldots, \alpha_k\}$, očigledno ne može biti generatorni skup ($b \in \langle a_{\alpha_1}, \ldots, a_{\alpha_k} \rangle$ i $a_\beta \notin (\{a_\gamma \mid \gamma \neq \beta\})$). Neka je npr. $(\mathcal{A} \setminus \{a_{\alpha_1}\}) \cup \{b\}$ generatorni skup. Ako je $b$ konačnog reda, mora biti $(m_1, red(a_{\alpha_1})) = 1$; ako je

$$a_{\alpha_1} = n_1 b + n_2 a_{\alpha_2} + \cdots + n_k a_{\alpha_k} \qquad (**)$$



(jasno, nemamo sabiraka $sa_\gamma$, $\gamma \notin \{\alpha_1, \ldots, \alpha_k\}$, zbog $b \in \langle a_{\alpha_1}, \ldots, a_{\alpha_k} \rangle$), onda iz $(*)$ i $(**)$ sledi (sabiranjem $(**)$ i $n_1 \cdot (*)$) $(m_1 n_1 - 1)a_{\alpha_1} + (m_2 n_1 + n_2)a_{\alpha_2} + \cdots + (m_k n_1 + n_k)a_{\alpha_k} = 0$, a odatle $red(a_{\alpha_1}) | (m_1 n_1 - 1)$ i $(m_1, red(a_{\alpha_1})) = 1$. No tada je $red(b) \geq red(m_1 a_{\alpha_1}) = red(a_{\alpha_1})$. Ako je $b$ beskonačnog i to manjeg reda od reda elementa $a_{\alpha_1}$, s obzirom na $\{a_{\alpha_1}\}$, onda je, za neke nenula cele brojeve $m, n$, $nb = ma_{\alpha_1}$ i $|n| < |m|$. Ali tada su svi elementi $a_{\alpha_i}$, $i = 2, \ldots, k$, konačnog reda ("pomnožiti" $(*)$ sa $n$ i zameniti $nb$ sa $ma_{\alpha_1}$), i prema tome, ako je $q$ najmanji zajednički sadržalac njihovih redova, dobija se iz $(*)$: $qb = qm_1 a_{\alpha_1}$. Znači, $|m_1| > 1$. U $(**)$ je $n_1 \neq 0$ (u suprotnom bi element $a_{\alpha_1}$ bio konačnog reda). Ali iz $(**)$ bismo, analogno, dobili: $qa_{\alpha_1} = qn_1 b$ i $|q| > |q| \cdot |n_1|$, kontradikcija.

$(\Longleftarrow)$ Neka $\mathcal{A}$ ispunjava uslove $(i)$ i $(ii)$. $\mathcal{A}$ je, konstatujmo prvo, minimalni generatorni skup; ako je $a_\alpha \in \langle \{a_\beta \mid \beta \neq \alpha\} \rangle$, mogli bismo $a_\alpha$ jednostavno zameniti nulom, što je u protivurečnosti sa $(ii)$ (novodobijeni skup bi takođe bio generatoran). Preostaje da se pokaže slaba linearna nezavisnost skupa $\mathcal{A}$. Neka je, pretpostavimo: $m_1 a_{\alpha_1} + m_2 a_{\alpha_2} + \cdots + m_k a_{\alpha_k} = 0$, $k \geq 2$, i $m_i a_{\alpha_i} \neq 0$ za svako $i = 1, \ldots, k$. Ako je $a_{\alpha_1}$ beskonačnog reda, onda je $b = (1 + |m_1|)a_{\alpha_1}$ element manjeg reda od $a_{\alpha_1}$, s obzirom na $\{a_{\alpha_1}\}$, ali $(\mathcal{A} \setminus \{a_{\alpha_1}\}) \cup \{b\}$ je generatorni skup ($|m_1| a_{\alpha_1} \in \langle a_{\alpha_2}, \ldots, a_{\alpha_k} \rangle$ i $a_{\alpha_1} = b - |m_1| a_{\alpha_1}$), kontradiktorno sa $(ii)$. Ako su svi elementi $a_{\alpha_i}$, $i = 1, \ldots, k$, konačnog reda, možemo pretpostaviti da su njihovi redovi stepeni istog prostog broja $p$. Neka je $p^t$ najveći stepen od $p$ koji deli sve koeficijente: $m_i = p^t n_i$, $i = 1, \ldots, k$, i neka je npr. $(n_1, p) = 1$. Tada je element $b = n_1 a_{\alpha_1} + \cdots + n_k a_{\alpha_k}$ reda manjeg od ili jednakog $p^t$ $(< red(a_{\alpha_1}))$, ali je $(\mathcal{A} \setminus \{a_{\alpha_1}\}) \cup \{b\}$ generatorni skup ($n_1 a_{\alpha_1} \in \langle b, a_{\alpha_2}, \ldots, a_{\alpha_k} \rangle$, i kako je $(n_1, p) = 1$, to je i $a_{\alpha_1} \in \langle b, a_{\alpha_2}, \ldots, a_{\alpha_k} \rangle$), kontradikcija ponovo.■

## 36 Konačno kogenerisane grupe

U sedmom paragrafu smo opisali kociklične grupe. Ovog puta idemo korak dalje – uporediti narednu definiciju sa 7.13.

**Definicija 36.1** *Sistem kogeneratora grupe $\mathbf{A}$ je familija njenih elemenata $\mathcal{S}$ takva da za svaku grupu $\mathbf{B}$ i svako homomorfno preslikavanje $\varphi \in Hom(\mathbf{A}, \mathbf{B})$ važi: ako je $\mathcal{S} \cap Ker(\varphi) \subseteq \{0\}$, onda je $\varphi$ injektivno.*

*Grupa $\mathbf{A}$ je konačno kogenerisana akko ima konačan sistem kogeneratora.*

**Lema 36.2** *Sistem elemenata $\mathcal{S}$ $(\subseteq \mathcal{A})$ je sistem kogeneratora grupe $\mathbf{A}$ akko svaka nenula podgrupa grupe $\mathbf{A}$ sadrži nenula element iz $\mathcal{S}$.*

**Dokaz.** U osnovi dokaza je očigledna činjenica da je svaka podgrupa $\mathbf{B}$ grupe $\mathbf{A}$, kao normalna, jezgro nekog homomorfizma grupe $\mathbf{A}$ (uvek imamo kanonički homomorfizam $A \longrightarrow A/B$).□

**Teorema 36.3** *Sledeći uslovi su ekvivalentni za grupu* $\mathbf{A}$*:*

(1) $\mathbf{A}$ *je konačno kogenerisana grupa;*

(2) $\mathbf{A}$ *je esencijalna ekstenzija konačne grupe;*

(3) $\mathbf{A}$ *je direktna suma konačnog broja kocikličnih grupa;*

(4) *Podgrupe grupe* $\mathbf{A}$ *ispunjavaju uslov minimalnosti (svaki opadajući lanac podgrupa ima najmanji element).*

**Dokaz.** (1) $\Longrightarrow$ (2) Neka grupa $\mathbf{A}$ ima konačan sistem kogeneratora $\mathcal{S} = \{a_1, \ldots, a_n\}$. $\mathbf{A}$ je onda periodična grupa, jer ako bi element $b$ bio beskonačnog reda, ciklična grupa $\langle b \rangle$ sadržavala bi nenula podgrupu čiji bi domen imao za presek sa $\mathcal{S}$ ili prazan skup ili $\{0\}$. Podgrupa $\langle \mathcal{S} \rangle$ je stoga konačna, a prema prethodnoj lemi $\mathbf{A}$ je njena esencijalna ekstenzija.

(2) $\Longrightarrow$ (3) Neka je $\mathbf{A}$ esencijalna ekstenzija konačne podgrupe $\mathbf{B}$. Opet je, jasno, $\mathbf{A}$ periodična grupa. Isto tako, samo je za konačno mnogo prostih brojeva $p$, $\mathbf{A}_p$ ($p$-komponenta grupe $\mathbf{A}$) nenula podgrupa. Neka je za konačan skup prostih brojeva – $Q$ – $\mathbf{A} = \sum_{p \in Q} \mathbf{A}_p$, $\mathbf{B} = \sum_{p \in Q} \mathbf{B}_p$. Naravno, za dato $p \in Q$, $\mathbf{A}_p$ je esencijalna ekstenzija grupe $\mathbf{B}_p$. Možemo se, stoga, skoncentrisati na $p$-komponente $\mathbf{A}_p$ i $\mathbf{B}_p$. Evidentno, mora biti $\mathbf{A}[p] = \mathbf{B}[p]$ i $|A[p]| = |B[p]| < \infty$; $a \in A[p] \setminus B[p]$ dalo bi: $\langle a \rangle \cap B[p] = \{0\}$, tj. $\langle a \rangle \cap B = \{0\}$. Prema tome, za $a \in A_p$ jednačina $a = px$ može imati samo konačno mnogo rešenja: $\{b_1, \ldots, b_k\}$, $k \geq 0$ ($k = 0$ znači da nemamo nijedno rešenje) – svaka dva različita rešenja jednačine $a = px$ daju element reda $p$. Ako je $h_p(a) = \infty$, mora, za bar jedno $i$, $0 \leq i \leq k$, $b_i$ imati beskonačnu visinu (jer, ako je $a = p^m c$, $m \geq 1$, onda je $p^{m-1} c \in \{b_0, \ldots, b_k\}$). Konsekventno, polazeći od elementa $a$ (beskonačne visine) generišemo Prüferovu grupu $\mathbf{p}^\infty$: $a = a_0$, $a_1 = b_i$ ($h_p(b_i) = \infty$), $a_2$ je rešenje jednačine $a_1 = px$ koje je beskonačne visine i tako dalje. Neka je $\mathbf{D}$ direktna suma svih tako dobijenih Prüferovih grupa. Tada je $\mathbf{A}_p = \mathbf{D} \oplus \mathbf{C}$ za neku podgrupu $\mathbf{C}$. Svi elementi iz $C[p]$ su konačne visine; neka je $m = max\{h_p(c) \mid c \in C[p]\}$. Dakle, $p^{m+1}\mathbf{C} = \mathbf{O}$, te je prema 35.2 $\mathbf{C}$ direktna suma primarnih cikličnih grupa.

(3) $\Longrightarrow$ (4) Neka je $\mathbf{A}$ direktna suma konačnog broja kocikličnih grupa. Indukcijom po rangu grupe $\mathbf{A}$ ($r(\mathbf{A})$) pokazujemo da $\mathbf{A}$ ispunjava uslov minimalnosti podgrupa. Ako je $r(\mathbf{A}) = 1$, tj. ako je $\mathbf{A}$ ili primarna ciklična grupa ili Prüferova grupa, to je očigledno. Pretpostavimo da je tvrđenje tačno za direktne sume kocikličnih grupa ranga $k$ manjeg od $n+1$ i neka je $\mathbf{A} = \mathbf{B} \oplus \mathbf{C}$, gde je $\mathbf{B}$ kociklična grupa i $\mathbf{C}$ direktna suma kocikličnih grupa ranga $n$. Neka je, dalje, $\mathbf{D}_0 \geq \mathbf{D}_1 \geq \cdots \geq \mathbf{D}_m \geq \mathbf{D}_{m+1} \geq \cdots$ opadajući niz podgrupa grupe $\mathbf{A}$. Opadajući niz podgrupa (grupe $\mathbf{C}$) $\mathbf{D}_0 \cap \mathbf{C} \geq \mathbf{D}_1 \cap \mathbf{C} \geq \cdots \geq \mathbf{D}_m \cap \mathbf{C} \geq \mathbf{D}_{m+1} \cap \mathbf{C} \geq \cdots$ ima, po induktivnoj pretpostavci, najmanji element; neka je to $\mathbf{D}_r \cap \mathbf{C}$ (dakle, $\mathbf{D}_r \cap \mathbf{C} = \mathbf{D}_i \cap \mathbf{C}$ za svako $i \geq r$). Prema drugoj teoremi o izomorfizmu je, za svako $i \geq r$:

$$\mathbf{D}_i/(\mathbf{D}_r \cap \mathbf{C}) = \mathbf{D}_i/(\mathbf{D}_i \cap \mathbf{C}) \cong (\mathbf{D}_i + \mathbf{C})/\mathbf{C} \leq \mathbf{A}/\mathbf{C} \cong \mathbf{B}.$$



Znači, za neko $s$ i za svako $i \geq t = max\{r, s\}$ važi:

$$\mathbf{D}_s/(\mathbf{D}_r \cap \mathbf{C}) = \mathbf{D}_i/(\mathbf{D}_r \cap \mathbf{C}) \,(= \mathbf{D}_i/(\mathbf{D}_i \cap \mathbf{C})),$$

te je $\mathbf{D}_t = \mathbf{D}_{t+1} = \cdots$.

(4) $\Longrightarrow$ (1) Neka grupa $\mathbf{A}$ ispunjava uslov minimalnosti podgrupa. Takva grupa je periodična, pošto beskonačna ciklična grupa ne ispunjava uslov minimalnosti podgrupa. Pored toga je, za samo konačno mnogo prostih brojeva $p$, $\mathbf{A}[p]$ nenula podgrupa i, kao direktna suma cikličnih grupa reda $p$, konačna. Ako je, za konačan skup prostih brojeva $Q$, $\mathbf{A} = \sum_{p \in Q} \mathbf{A}_p$, onda je $\bigcup_{p \in Q} A[p]$ konačan sistem kogeneratora grupe $\mathbf{A}$.■

**Korolar 36.4** *Neka je* $\{a_1, \ldots, a_n\}$ *konačan podskup nenula elemenata grupe* $\mathbf{A}$ *i neka je* $\mathbf{B}$ *maksimalna podgrupa grupe* $\mathbf{A}$ *takva da je njen domen disjunktan sa* $\{a_1, \ldots, a_n\}$*. Tada je faktor grupa* $\mathbf{A}/\mathbf{B}$ *konačno kogenerisana. Posebno je, za* $n = 1$, $\mathbf{A}/\mathbf{B}$ *kociklična grupa.*

**Dokaz.** $\{a_i + B \mid i = 1, \ldots, n\}$ je konačan kogenerični sistem grupe $\mathbf{A}/\mathbf{B}$. Jer, ako je $\mathbf{C}/\mathbf{B}$ nenula podgrupa grupe $\mathbf{A}/\mathbf{B}$ (dakle, $B \subset C$), onda je $C \cap \{a_1, \ldots, a_n\} \neq \emptyset$, pa ako je $a_i \in C$, $B \neq a_i + B \in C/B$. Posebno, ako je $n = 1$, element $a_1 + B$ je nenula element koji pripada svakoj nenula podgrupi, pa je $r(\mathbf{A}/\mathbf{B}) = 1$ i $\mathbf{A}/\mathbf{B}$ je kociklična grupa.□

**Korolar 36.5** *Ako je* $\mathbf{A}$ *konačno kogenerisana, onda je i svaka njena podgrupa konačno kogenerisana.*

**Korolar 36.6** *Ako su podgrupa* $\mathbf{B}$ *i faktor grupa* $\mathbf{A}/\mathbf{B}$ *grupe* $\mathbf{A}$ *konačno kogenerisane, onda je i* $\mathbf{A}$ *konačno kogenerisana.*

**Dokaz.** Već dat – 8.15 (koristimo, naravno, ekvivalenciju (1) $\Longleftrightarrow$ (4) iz prethodne teoreme.□

## 37 Potpune podgrupe

Među podgrupama Abelovih grupa pokazuje se da su od posebnog interesa one koje su zatvorene za rešavanje sistema linearnih jednačina sa konačno mnogo nepoznatih. Na prvi pogled traži se manje. Naime, imamo

**Definicija 37.1** *Podgrupa* $\mathbf{A}$ *grupe* $\mathbf{B}$ *je potpuna (izolovana) podgrupa akko važi: za svako* $a \in A$ *i svaki prirodan broj* $n$ *jednačina* $a = nx$ *je rešiva u* $\mathbf{A}$ *akko je rešiva u* $\mathbf{B}$*.*

*Ako za prost broj* $p$ *(ali ne nužno i za ostale proste brojeve) važi: za svaki prirodan broj* $k$ *je* $p^k\mathbf{A} = \mathbf{A} \cap p^k\mathbf{B}$*, onda je podgrupa* $\mathbf{A}$ *p-potpuna.*

Reč dve o samom imenu novouvedenih podgrupa. U engleskoj literaturi u upotrebi su termini: *pure* (u poslednje vreme najčešće), *isolated* ili *serving (subgroup)*. Englesko *pure* mi smo preveli sa potpun. Odgovarao bi i izraz *kompletan*, no on se koji put koristi i za deljive grupe (eng. *divisible* ili *complete groups*).

Uslov da je $\mathbf{A}$ potpuna podgrupa grupe $\mathbf{B}$ može se jednostavno zapisati sa:

$$n\mathbf{A} = \mathbf{A} \cap n\mathbf{B} \quad \textit{za svaki prirodan broj } n.$$

Naravno, inkluzija $\leq$ nam je uvek na raspolaganju. Za potpunost dovoljno je samo proveriti da je $p^k\mathbf{A} = \mathbf{A} \cap p^k\mathbf{B}$ za svaki prost broj $p$ i svaki prirodan broj $k$; jer, $(p_1^{k_1} \dots p_m^{k_m})\mathbf{B} = p_1^{k_1}\mathbf{B} \cap \dots \cap p_m^{k_m}\mathbf{B}$. Relacija $\leq$ je očigledna, a relacija $\geq$ se dokazuje indukcijom po $m$. Slučaj $m = 1$ je trivijalan, a slučaj $m = 2$ objašnjava sve. Neka je $a \in p_1^{k_1}B \cap p_2^{k_2}B$. Onda je $a = p_1^{k_1}b = p_2^{k_2}c$ za neke elemente $b, c$. Neka su $u$ i $v$ celi brojevi takvi da je $up_1^{k_1} + vp_2^{k_2} = 1$. Tada je $c = up_1^{k_1}c + vp_2^{k_2}c = p_1^{k_1}(uc + vb)$, pa je $a = p_1^{k_1}p_2^{k_2}(uc + vb) \in p_1^{k_1}p_2^{k_2}B$. Sada sledi:

$$\mathbf{A} \cap (p_1^{k_1} \dots p_m^{k_m})\mathbf{B} = \mathbf{A} \cap (p_1^{k_1}\mathbf{B} \cap \dots \cap p_m^{k_m}\mathbf{B}) =$$

$$(\mathbf{A} \cap p_1^{k_1}\mathbf{B}) \cap \dots \cap (\mathbf{A} \cap p_m^{k_m}\mathbf{B}) = p_1^{k_1}\mathbf{A} \cap \dots \cap p_m^{k_m}\mathbf{A} = (p_1^{k_1} \dots p_m^{k_m})\mathbf{A}.$$

Neko će možda pomisliti da je dovoljno samo proveriti: za svaki prost broj $p$ je $p\mathbf{A} = \mathbf{A} \cap p\mathbf{B}$. Nažalost, nije; npr. ciklična podgrupa $\mathbf{A}$ grupe $\mathbf{Z}_p \oplus \mathbf{Z}_{p^3}$ generisana elementom $(1, p)$ nije potpuna, dok važi: $p\mathbf{A} = \mathbf{A} \cap p(\mathbf{Z}_p \oplus \mathbf{Z}_{p^3})$. Zaista, za element $(0, p^2)$ $(= p(1, p) \in A)$ je jednačina $(0, p^2) = p^2(x, y)$ rešiva u $\mathbf{Z}_p \oplus \mathbf{Z}_{p^3}$ (rešenja su elementi $(k, sp + 1)$, gde je $k \in p$, $0 \leq s \leq p^2 - 1$) ali nije i u $\mathbf{A}$ (koja je reda $p^2$). Kako je $A = \{(k, rp^2 + kp) \mid 0 \leq r, k \leq p - 1\}$, to je $pA = \{(0, kp^2) \mid , 0 \leq k \leq p - 1\}$. S druge strane, ako je $(k, rp^2 + kp) = p(m, n) = (p \cdot_p m, p \cdot_{p^3} n) \in A \cap p(Z_p + Z_{p^3})$, gde je, jasno, $0 \leq k, r, m \leq p - 1$, $0 \leq n \leq p^3 - 1$, onda, trivijalno, zbog $p \cdot_p m = 0$, sledi $k = 0$, pa su elementi preseka, $(0, rp^2)$, ujedno i elementi podgrupe $p\mathbf{A}$.

U svakom slučaju, pomenuta ideja inspiriše sledeću definiciju.

**Definicija 37.2** *Podgrupa* $\mathbf{A}$ *grupe* $\mathbf{B}$ *je slabo potpuna podgrupa (eng. neat subgroup) grupe* $\mathbf{B}$ *akko je* $p\mathbf{A} = \mathbf{A} \cap p\mathbf{B}$ *za svaki prost broj* $p$.

Jasno, potpuna podgrupa je i slabo potpuna. Takođe, imamo

**Lema 37.3** *Ako je* $\mathbf{A}$ *slabo potpuna podgrupa torziono slobodne grupe* $\mathbf{B}$, *onda je i potpuna podgrupa.*

**Dokaz.** Neka je $0 \neq a \in A$ i neka je $p$ prost broj. Indukcijom po $k \geq 1$ pokazaćemo da je jednačina $a = p^k x$ rešiva u $\mathbf{A}$ akko je rešiva u $\mathbf{B}$. Za $k = 1$ to proizilazi iz uslova leme. Pretpostavimo da je tvrđenje tačno za svako



$m$ manje od ili jednako $k$ i neka je jednačina $a = p^{k+1}x$ rešiva u $\mathbf{B}$. Znači, $a = p^{k+1}b = p^k(pb)$ za neko $b \in B$. Prema induktivnoj hipotezi postoji neko $a_1 \in A$ takvo da je $a = p^k a_1$. Odatle, $p^k(a_1 - pb) = 0$, tj. $a_1 = pb$. Konačno, zbog jedinstvenosti rešenja jednačine $a_1 = px$ sledi $b \in A$.□

Navešćemo još samo sledeći rezultat u vezi sa slabo potpunim podgrupama, uz napomenu da se mnoge osobine potpunih podgrupa prenose i na slabo potpune.

**Lema 37.4** $\mathbf{A}$ *je slabo potpuna podgrupa grupe* $\mathbf{B}$ *akko je* $\mathbf{A} = \mathbf{B} \cap \mathbf{D}$ *za neku deljivu podgrupu* $\mathbf{D}$ *grupe* $\mathbf{I}(\mathbf{B})$.

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{A}$ slabo potpuna podgrupa grupe $\mathbf{B}$ i neka je $\mathbf{I}(\mathbf{A})$ injektivni omotač grupe $\mathbf{A}$ sadržan u (datom) injektivnom omotaču $\mathbf{I}(\mathbf{B})$ grupe $\mathbf{B}$. Tada je $\mathbf{A} = \mathbf{B} \cap \mathbf{I}(\mathbf{A})$. Jer, pretpostavimo: $b \in (B \cap I(\mathbf{A})) \setminus A$, i neka je $n$ najmanji pozitivan ceo broj takav da je $nb \in A$ (znamo da je $\langle b \rangle \cap \mathbf{A} \neq \mathbf{O}$). Ako je, dalje, $n = pn_1$, gde je $p$ prost broj $(n_1 \geq 1)$, tada $n_1 b \notin A$ i $p(n_1 b) \in A$. Stoga je, za neko $a \in A$, $p(n_1 b) = pa$, tj. $p(n_1 b - a) = 0$. Znači, $n_1 b - a$ je element podgrupe $\mathbf{B} \cap \mathbf{I}(\mathbf{A})$ reda $p$, i kako je $\langle n_1 b - a \rangle \cap \mathbf{A} \neq \mathbf{O}$, proizilazi $n_1 b - a \in A$, odnosno $n_1 b \in A$, kontradikcija.

($\Longleftarrow$) Neka je $\mathbf{D}$ deljiva podgrupa grupe $\mathbf{I}(\mathbf{B})$ za koju je $\mathbf{A} = \mathbf{B} \cap \mathbf{D}$ i neka je, za $a \in A = B \cap D$, $a = pb$ $(b \in B)$. No, jednačina $a = px$ je rešiva i u $\mathbf{D}$. Neka je $a = pc$ za neko $c \in D$. Ali onda je ili odmah $b = c$ ili je, za $b \neq c$, $b - c \in I(\mathbf{B})[p] = B[p]$ (33.26); u svakom slučaju je $c \in B \cap D$.□

**Lema 37.5** *Podgrupa* $\mathbf{A}$ *grupe* $\mathbf{B}$ *je potpuna akko postoji transverzala* $\{b_\alpha \mid \alpha < \lambda\}$ *podgrupe* $\mathbf{A}$ *takva da je* $red(b_\alpha) = red(b_\alpha + A)$.

**Dokaz.** ($\Longrightarrow$) Ako je element $c_\alpha + A$ $(\in B/A)$ beskonačnog reda, za $b_\alpha$ možemo uzeti bilo koji element tog koseta. Ako je $c_\alpha + A$ reda $n$, onda je $nc_\alpha \in A$, pa zbog potpunosti podgrupe $\mathbf{A}$ postoji $a_\alpha \in A$ takvo da je $nc_\alpha = na_\alpha$. Element $b_\alpha = c_\alpha - a_\alpha$ je reda $n$ (jer je $n$ najmanji "umnožak" elementa $c_\alpha$ koji "upada" u $A$) i $b_\alpha + A = c_\alpha + A$.

($\Longleftarrow$) Neka je $a = nc$, $a \in A$, i neka je $b \in c + A$ predstavnik koseta čiji je red (u grupi $\mathbf{B}$) jednak redu koseta. Tada je $c - b \in A$ i $n(c - b) = nc - nb = nc = a$.□

**Lema 37.6** *Neka je* $\mathbf{A}$ *podgrupa p-grupe* $\mathbf{B}$. $\mathbf{A}$ *je potpuna akko svaki element njenog najnižeg sloja* $(\mathbf{A}[p])$ *ima istu visinu u* $\mathbf{A}$ *i* $\mathbf{B}$.

**Dokaz.** Pravac ($\Longrightarrow$) je deo definicije.

($\Longleftarrow$) Indukcijom po $n$ pokazujemo da svi elementi podgrupe $\mathbf{A}$ reda $p^n$ imaju istu visinu u $\mathbf{A}$ i $\mathbf{B}$. Slučaj $n = 1$ je upravo dati uslov. Pretpostavimo da je tvrđenje tačno za elemente reda $p^r$, $r \leq n$ $(\geq 1)$ i neka je element $a$

iz $A$ reda $p^{n+1}$ i visine $k$ u $\mathbf{B}$. Neka je $a = p^k b$. Tada je $pa = p^{k+1}b$ i za neko $a_1$ iz $A$ je $pa = p^{k+1}a_1$. Odatle je $p(a - p^k a_1) = 0$, tj. $a - p^k a_1 \in A[p]$ i $a - p^k a_1 = p^k(b - a_1)$. Po uslovu leme postoji neko $a_2 \in A$ takvo da je $a - p^k a_1 = p^k a_2$, odnosno $a = p^k(a_1 + a_2)$.□

**Lema 37.7** *Ako je* $\mathbf{A}$ *potpuna podgrupa p-grupe* $\mathbf{B}$ *i ako je* $\mathrm{B}[p] \leq \mathbf{A}$, *tada je* $\mathbf{A} = \mathbf{B}$.

**Dokaz.** Indukcijom po $n$ pokazujemo da su svi elementi reda $p^n$ u $\mathbf{A}$. Slučaj $n = 1$ je upravo uslov leme. Pretpostavimo da je tvrđenje tačno za sve elemente reda $p^r$, $r \leq n$ $(\geq 1)$ i neka je $b$ reda $p^{n+1}$. Po induktivnoj hipotezi je $pb \in A$, a zbog potpunosti podgrupe $\mathbf{A}$ je $pb = pa$ za neko $a$ iz $A$. Stoga je $b - a \in B[p] \subseteq A$, pa je i $b \in A$.□

**Lema 37.8** (*a*) *Svojstvo potpunosti je tranzitivno.*

(*b*) *Unija rastućeg lanca potpunih podgrupa je potpuna podgrupa.*

(*c*) *Presek proizvoljne familije potpunih podgrupa torziono slobodne grupe je potpuna podgrupa.*

(*d*) *Ako je* $\mathbf{A}$ *podgrupa grupe* $\mathbf{B}$ *i ako je faktor grupa* $\mathbf{B}/\mathbf{A}$ *torziono slobodna, onda je* $\mathbf{A}$ *potpuna podgrupa.*

*Ako je* $\mathbf{B}$ *torziono slobodna važi i obrat: ako je* $\mathbf{A}$ *prava potpuna podgrupa grupe* $\mathbf{B}$, *onda je* $\mathbf{B}/\mathbf{A}$ *torziono slobodna.*

**Dokaz.** (*a*) Neka je $\mathbf{A}$ potpuna podgrupa grupe $\mathbf{B}$, a $\mathbf{B}$ potpuna podgrupa grupe $\mathbf{C}$. Tada je za svaki prirodan broj $n$:

$$n\mathbf{A} = \mathbf{A} \cap n\mathbf{B} = \mathbf{A} \cap (\mathbf{B} \cap n\mathbf{C}) = \mathbf{A} \cap n\mathbf{C}.$$

(*b*) Neka je $\gamma$ granični ordinal i neka su, za $\alpha < \beta < \gamma$, $\mathbf{A}_\alpha$, $\mathbf{A}_\beta$ potpune podgrupe grupe $\mathbf{B}$ i $\mathbf{A}_\alpha \leq \mathbf{A}_\beta$. Tada je $\mathbf{A} = \bigcup_{\alpha<\gamma} \mathbf{A}_\alpha$ takođe potpuna podgrupa jer:

$$\mathbf{A} \cap n\mathbf{B} = (\bigcup_{\alpha<\gamma} \mathbf{A}_\alpha) \cap n\mathbf{B} = \bigcup_{\alpha<\gamma} (\mathbf{A}_\alpha \cap n\mathbf{B}) = \bigcup_{\alpha<\gamma} n\mathbf{A}_\alpha = n(\bigcup_{\alpha<\gamma} \mathbf{A}_\alpha) = n\mathbf{A}.$$

(*c*) Neka je $\mathbf{B}$ torziono slobodna grupa i neka je, za $\alpha < \lambda$, $\mathbf{A}_\alpha$ njena potpuna podgrupa. Ako je za $a \in \bigcap_{\alpha<\lambda} A_\alpha$ jednačina $a = nx$ rešiva u $\mathbf{B}$, rešenje je, neka to bude $b$, jedinstveno (jer nema nenula elemenata konačnog reda). Kako je (za svako $\alpha < \lambda$) $\mathbf{A}_\alpha$ potpuna podgrupa, to je $b \in A_\alpha$, te je $b$ i u $\bigcap_{\alpha<\lambda} A_\alpha$.

(*d*) Direktna posledica leme 37.5. Dajemo i direktni dokaz.

Neka je $a \in A$ i $a = kb$. Tada je $A = k(b + A)$, pa je $b + A = A$, tj. $b \in A$.

Neka je, sada, $\mathbf{B}$ torziono slobodna i neka je $\mathbf{A}$ njena prava potpuna podgrupa. Pretpostavimo: $n(b + A) = A$, tj. $nb \in A$. No onda je $nb = na$ za neko $a \in A$, odnosno, $n(b - a) = 0$, pa je $b - a = 0$; dakle, $b \in A$.□



**Korolar 37.9** *Neka je* $\mathbf{B}$ *torziono slobodna grupa i* $X \subseteq B$. *Tada postoji minimalna potpuna podgrupa* $\mathbf{A}$ *grupe* $\mathbf{B}$ *čiji domen sadrži* $X$. *Ako je* $X \neq \emptyset$, *domen podgrupe* $\mathbf{A}$ *je* $\{a \in B \mid ka \in \langle X \rangle$ *za neki nenula ceo broj* $k$ *(koji zavisi od* $a)\}$ *(ako je* $X$ *prazan skup, trivijalno* $\mathbf{A} = \mathbf{O}$*).*

**Dokaz.** Jasno, $\mathbf{A} = \bigcap \{\mathbf{C} \mid \mathbf{C}$ je potpuna podgrupa grupe $\mathbf{B}$ i $X \subseteq C\}$.

Skup $A_1 = \{a \in B \mid ka \in \langle X \rangle,\ k \in Z \setminus \{0\}\}$ domen je podgrupe: ako $ka, lb \in \langle X \rangle$, $k, l \in Z \setminus \{0\}$, onda $(-k)(-a), kl(a + b) \in \langle X \rangle$. Ta podgrupa $(\mathbf{A}_1)$ je i potpuna: ako je $ka \in \langle X \rangle$ i $a = nc$, onda je $(kn)c \in \langle X \rangle$. Prema tome, $\mathbf{A} \leq \mathbf{A}_1$. S druge strane, ako je $\mathbf{C}$ potpuna podgrupa čiji domen sadrži $X$ i $0 \neq ka \in \langle X \rangle \subseteq C$, recimo $ka = c \in C$, sledi da $a$, kao jedinstveno rešenje jednačine $c = kx$, mora biti u $C$. Stoga je i $\mathbf{A}_1 \leq \mathbf{A}$.□

**Lema 37.10** *Neka je* $\mathbf{A}$ *podgrupa kardinalnosti* $\lambda \geq \aleph_0$ *grupe* $\mathbf{C}$ *kardinalnosti* $\mu > \lambda$. *Tada postoji potpuna podgrupa* $\mathbf{B}$ *grupe* $\mathbf{C}$ *kardinalnosti* $\lambda$ *koja sadrži* $\mathbf{A}$.

**Dokaz.** Ako je $\mathbf{C}$ torziono slobodna grupa, dokaz je već dat u prethodnom korolaru. U izvesnom smislu taj dokaz je sadržan i u opštem slučaju. Neka je $C = \{c_\alpha \mid \alpha < \mu\}$. Formirajmo rastući niz podgrupa $\mathbf{A}_n$, $n \in \omega$, na sledeći način: $\mathbf{A}_0 = \mathbf{A}$, $\mathbf{A}_{n+1} = \langle A_n \cup \{c \mid c$ je "prvo" rešenje, s obzirom na dato uređenje skupa $C$, jednačine $a = kx$, $a \in A_n$, $k \in N$, rešive u $\mathbf{C}\}\rangle$ (kad je grupa $\mathbf{C}$ torziono slobodna jedinstvenost rešenja isključuje potrebu za dobrim uređenjem skupa $C$). Očigledno, svaka od grupa $\mathbf{A}_n$ je, prema datoj konstrukciji, kardinalnosti $\lambda$ (podsetimo se: grupa generisana skupom beskonačne kardinalnosti $\lambda$ i sama je kardinalnosti $\lambda$). Stoga je i $\mathbf{B} = \bigcup_{n\in\omega} \mathbf{A}_n$ kardinalnosti $\lambda$. No, $\mathbf{B}$ je i potpuna podgrupa. Jer, ako je za $b \in B$ i $m \in N$ jednačina $b = mx$ rešiva u $\mathbf{C}$, rešiva je i u $\mathbf{B}$; za neko $n \in \omega$ je $b \in A_n$ i jedno rešenje jednačine $b = mx$ je, po definiciji grupe $\mathbf{A}_{n+1}$, sadržano u $\mathbf{A}_{n+1}$.□

**Napomena.** Prethodna konstrukcija je opšteg karaktera. Naime, njeni se analogoni (kadkad su nam potrebni i "dvojni lanci") koriste u konstrukciji egzistencijalno zatvorenih struktura induktivnih klasa (klasa zatvorenih za unije lanaca) algebarskih struktura ili, još šire gledano, modela.

Primetimo još da, generalno, u gornjoj konstrukciji jednačina $a = mx$ može da ima i više od $\lambda$ rešenja (tj. svih $\mu$ rešenja). Jedan primer nam daje ciklična grupa reda $p$, $\langle a \rangle$, koja se javlja kao adekvatni amalgam $\mu$ Prüferovih grupa $\mathrm{p}^\infty_\alpha$, $\alpha < \mu$.

**Primer 37.11** (*a*) *Nula podgrupa i cela grupa su trivijalne potpune podgrupe. Direktni sumand je potpuna podgrupa.*

(*b*) *Deljiva podgrupa je potpuna podgrupa.*

(*c*) *Periodični deo je potpuna podgrupa.*

(*d*) *Maksimalna p-primarna podgrupa grupe je potpuna podgrupa.*

**Dokaz.** Uočimo da je maksimalna $p$-primarna podgrupa direktni sumand, dakle i potpuna podgrupa periodičnog dela.

(*e*) *p-potpuna p-podgrupa je potpuna podgrupa.*

**Dokaz.** Koristimo već više puta ponavljani stav: u cikličnoj $p$-grupi svaki element je deljiv svim celim brojevima uzajamno prostim sa $p$.

(*f*) *Ako su zbir i presek podgrupa* $\mathbf{A}$ *i* $\mathbf{B}$ *grupe* $\mathbf{C}$ *potpune podgrupe, onda su i* $\mathbf{A}$ *i* $\mathbf{B}$ *potpune.*

**Dokaz.** Neka je, za $a \in A$, $a = kc$. Kako je $a \in A + B$, to je, za neko $a_1 \in A$, $b_1 \in B$, $a = k(a_1 + b_1)$. Element $a - ka_1 = kb_1$ u preseku je podgrupa i deljiv je sa $k$, pa je $a - ka_1 = kd$ za neko $d \in A \cap B$. Stoga je $a = k(a_1 + d)$.

(*g*) *Neka je dat rastući lanac podgrupa* $\mathbf{B}_\alpha$, $\alpha < \lambda$. *Ako je* $\mathbf{A}$ *potpuna podgrupa svake grupe iz lanca, onda je potpuna podgrupa i grupe* $\bigcup_{\alpha<\lambda} \mathbf{B}_\alpha$.
**Dokaz.**

$$\mathbf{A} \cap n(\bigcup_{\alpha<\lambda} \mathbf{B}_\alpha) = \mathbf{A} \cap \bigcup_{\alpha<\lambda} n\mathbf{B}_\alpha = \bigcup_{\alpha<\lambda} (\mathbf{A} \cap n\mathbf{B}_\alpha) = \bigcup_{\alpha<\lambda} n\mathbf{A} = n\mathbf{A}.$$

(*h*) *Ako je* $\mathbf{A}$ *potpuna podgrupa grupe* $\mathbf{B}$, *onda je i* $n\mathbf{A}$ *potpuna podgrupa grupe* $n\mathbf{B}$.

**Dokaz.** Ako je $a \in A$ i $na = k(nb)$ $(= (kn)b \in A)$, tada je, za neko $a_1 \in A$, $na = (kn)a_1$, tj. $na = k(na_1)$.

(*i*) *Zbir periodičnog dela* $(t\mathbf{B})$ *i potpune podgrupe* $\mathbf{A}$ *grupe* $\mathbf{B}$ *je potpuna podgrupa.*

**Dokaz.** Neka je $a$ iz $A$ beskonačnog reda, $b$ iz $tB$ reda $n$ i neka je $a + b = kc$. Onda je $na = (kn)c$, i kako je $\mathbf{A}$ potpuna podgrupa, za neko $a_1$ iz $A$ je $na = (kn)a_1$. Odatle je $n(kc - ka_1) = 0$. Ako je $kc = ka_1$, gotovi smo odmah. U suprotnom je, zbog $kc - ka_1 = k(c - a_1) \in tB$, za neko $b_1 \in tB$, $k(c - a_1) = kb_1$, dakle i $a + b = kc = k(a_1 + b_1)$.□

**Lema 37.12** *Neka su* $\mathbf{B}$ *i* $\mathbf{C}$ *podgrupe grupe* $\mathbf{A}$ *i neka je* $\mathbf{C} \leq \mathbf{B}$. *Tada važi:*

(*a*) *Ako je* $\mathbf{B}$ *potpuna podgrupa grupe* $\mathbf{A}$, *onda je i* $\mathbf{B}/\mathbf{C}$ *potpuna podgrupa grupe* $\mathbf{A}/\mathbf{C}$;

(*b*) *Ako je* $\mathbf{C}$ *potpuna podgrupa grupe* $\mathbf{A}$ *i ako je* $\mathbf{B}/\mathbf{C}$ *potpuna podgrupa grupe* $\mathbf{A}/\mathbf{C}$, *onda je* $\mathbf{B}$ *potpuna podgrupa grupe* $\mathbf{A}$.

**Dokaz.** (*a*) Neka je $\mathbf{B}$ potpuna podgrupa grupe $\mathbf{A}$ i neka je, za $b \in B$ i $a \in A$, $b + C = k(a + C)$. Odatle je, za neko $c \in C$, $b - ka = c$, tj. $b - c = ka$. S obzirom na potpunost grupe $\mathbf{B}$ je $b - c = kb_1$ za neko $b_1 \in B$, pa je $b + C = k(b_1 + C)$ (i $b_1 + C \in B/C$).



(*b*) Pretpostavimo da važe navedeni uslovi i neka je $b = ka$ za $b \in B$. Onda je $b + C = k(a + C)$, te je i $b + C = k(b_1 + C)$ za neko $b_1 + C \in B/C$. Stoga je $b - kb_1 = k(a - b_1) = c$ za neko $c \in C$, a zbog potpunosti grupe $\mathbf{C}$ je $c = kc_1$ za neko $c_1 \in C$. Sledi $k(a - b_1) = kc_1$, tj. $b = k(b_1 + c_1)$.□

Već smo videli da periodični deo ne mora biti direktni sumand (30.4). Jedan opštiji primer potpunih podgrupa koje nisu direktni sumandi daje sledeća

**Lema 37.13** *Svaka direktna suma* $\mathbf{A}$ *cikličnih p-grupa čiji redovi nisu ograničeni ima potpunu podgrupu koja nije direktni sumand.*

**Dokaz.** Možemo odmah pretpostaviti da je $\mathbf{A} = \sum_{i\in N} \mathbf{Z}_{p^{k_i}}$, gde je $k_1 < k_2 < \cdots < k_n < \cdots$ (u suprotnom bismo izabrali odgovarajući direktni sumand polazne grupe) – $\mathbf{Z}_{p^{k_i}}$ je ciklična grupa generisana elementom $1_i$. Neka je $\mathbf{B}$ podgrupa grupe $\mathbf{A}$ generisana skupom $\{b_n \mid n \in N\}$, gde je $b_n = 1_n - p^{k_{n+1}-k_n} 1_{n+1}$ element reda $p^{k_n}$. Visina elementa

$$\begin{aligned} b &= \sum_{n=1}^{m} l_n b_n = \sum_{n=1}^{m} l_n (1_n - p^{k_{n+1}-k_n} 1_{n+1}) \\ &= l_1 1_1 + \sum_{n=2}^{m} (l_n - l_{n-1} p^{k_n - k_{n-1}}) 1_n - l_m p^{k_{m+1}-k_m} 1_{m+1} \end{aligned}$$

(jasno, uzimamo da je $l_n < p^{k_n}$) je
$min\{h(l_1 1_1), h((l_2 - l_1 p^{k_2-k_1})1_2), \ldots,$
$\ldots h((l_m - l_{m-1} p^{k_m-k_{m-1}})1_m), h(l_m p^{k_{m+1}-k_m} 1_{m+1})\}$,
dakle, najveći stepen broja $p$, neka je to $p^r$, koji deli sve koeficijente: $l_1$, $l_2 - l_1 p^{k_2-k_1}$, …, $l_m - l_{m-1} p^{k_m-k_{m-1}}$, $l_m p^{k_{m+1}-k_m}$. No tada $p^r$ deli i sve koeficijente $l_1, l_2, \ldots, l_m$, te je $h(b) \leq h_{\mathbf{B}}(b)$; znači: za svako $b$ iz $B$ je $h_{\mathbf{B}}(b) = h(b)$, i $\mathbf{B}$ je potpuna podgrupa. $\mathbf{B} \cap \langle 1_1 \rangle = \mathbf{O}$, jer iz $k1_1 = l_1 1_1 + (l_2 - l_1 p^{k_2-k_1})1_2 + \cdots + (l_m - l_{m-1} p^{k_m-k_{m-1}})1_m - l_m p^{k_{m+1}-k_m} 1_{m+1}$ sledi $l_m = 0$ (pretpostavili smo: $l_m < p^{k_m}$), a onda redom i $l_{m-1} = 0, \ldots, l_2 = 0, l_1 = 0$. Naravno, nijedan od elemenata $1_i$ nije u $\mathbf{B}$ ($1_2 \in B$ bi implicirało $1_1 \in B$, $1_3 \in B$ bi implicirało $1_2 \in B$ itd.). Faktor grupa $\mathbf{A}/\mathbf{B}$ je Prüferova $\mathbf{p}^\infty$ grupa – generisana je elementima $1_n + B$, $n \geq 1$, i zbog $1_n - p^{k_{n+1}-k_n} 1_{n+1} \in B$, važi (za svako $n$) $1_n + B = p^{k_{n+1}-k_n}(1_{n+1} + B)$ (ranije smo pokazali da svaka grupa reda $p^n$ ima podgrupu reda $p^{n-1}$). Iz navedenog proizilazi da $\mathbf{B}$ ne može biti direktni sumand grupe $\mathbf{A}$; jer, $\mathbf{A} = \mathbf{B} \oplus \mathbf{C}$, $\mathbf{C} \neq \mathbf{O}$, dalo bi, s jedne strane, da je $\mathbf{C}$ direktna suma cikličnih grupa (35.8), a s druge, da je $\mathbf{C}$ $(\cong \mathbf{A}/\mathbf{B})$ Prüferova grupa, kontradikcija.□

U par narednih rezultata dajemo nekoliko dovoljnih uslova da bi potpuna podgrupa bila i direktni sumand.

**Lema 37.14** (*a*) *Ako je* $\mathbf{A}$ *potpuna podgrupa grupe* $\mathbf{B}$ *i ako je faktor grupa* $\mathbf{B}/\mathbf{A}$ *direktna suma cikličnih grupa, tada je* $\mathbf{A}$ *i direktni sumand grupe* $\mathbf{B}$.

(*b*) *Ako je* **A** *p-potpuna podgrupa grupe* **B** *i ako je faktor grupa* **B**/**A** *direktna suma cikličnih grupa sa p-primarnim periodičnim delom, onda je* **A** *direktni sumand grupe* **B**.

**Dokaz.** (*a*) Neka je $\mathbf{B}/\mathbf{A} = \sum_{\alpha<\lambda} \langle c_\alpha + A\rangle$, pri čemu je $red(c_\alpha) = red(c_\alpha + A)$ (videti 37.5). No, onda je $\mathbf{B} = \mathbf{A} \oplus \mathbf{C}$, gde je **C** podgrupa generisana transverzalom (podgrupe **A**) $\{c_\alpha \mid \alpha < \lambda\}$. Očigledno, samo treba dokazati da je $\mathbf{A} \cap \mathbf{C} = \mathbf{O}$. Pretpostavimo: $a = m_1 c_{\alpha_1} + \cdots + m_k c_{\alpha_k} \in A \cap C$. Tada je $A = m_1(c_{\alpha_1} + A) + \cdots + m_k(c_{\alpha_k} + A)$, pa kako se radi (na desnoj strani) o zbiru komponenata u direktnoj sumi to za svako $j$, $1 \leq j \leq k$, $m_j$ mora biti ili nula ili deljivo sa redom elementa $c_{\alpha_j} + A$. U svakom slučaju je i $m_j c_{\alpha_j} = 0$.

(*b*) Dokaz je u osnovi isti kao u tački (*a*). Ako je element $c_\alpha + A$ konačnog reda, taj red mora biti, po pretpostavci, stepen prostog broja $p$, recimo $p^{n_\alpha}$, a s obzirom da je **A** $p$-potpuna podgrupa, postoji element $a_\alpha \in A$ takav da je $p^{n_\alpha} c_\alpha = p^{n_\alpha} a_\alpha$.□

**Korolar 37.15** *Ako je* **A** *potpuna podgrupa grupe* **B** *i ako je faktor grupa* **B**/**A** *konačno generisana, onda je* **A** *direktni sumand grupe* **B**.

**Korolar 37.16** *Neka je* **A** *potpuna podgrupa grupe* **G** *i neka sistem linearnih jednačina* (∗) (33.15) *nad* **A** *ima samo konačno mnogo nepoznatih* ($\lambda \in \omega$). *Ako je taj sistem rešiv u* **G**, *rešiv je i u* **A**.

**Dokaz.** Neka su $b_0, \ldots, b_{\lambda-1}$ rešenja sistema (∗) u **G**. Prema prethodnom korolaru, **A** je direktni sumand grupe $\mathbf{B} = \langle A, b_0, \ldots, b_{\lambda-1}\rangle$, dakle za neku podgrupu **C** grupe **B** je $\mathbf{B} = \mathbf{A} \oplus \mathbf{C}$. Ako je $b_i = a_i + c_i$, $0 \leq i < \lambda$, jasno je da će $a_0, \ldots, a_{\lambda-1}$ biti rešenja sistema (∗) u **A**.□

**Korolar 37.17** **A** *je potpuna podgrupa grupe* **C** *akko je direktni sumand svake podgrupe* **B** *grupe* **C** *takve da je* $\mathbf{A} \leq \mathbf{B}$ *i* **B**/**A** *je konačno generisana grupa.*

**Dokaz.** Pravac ($\Longrightarrow$) smo upravo dokazali.

($\Longleftarrow$) Neka grupa **A** ispunjava dati uslov. Pokazaćemo da postoji transverzala $\{c_\alpha \mid \alpha < \lambda\}$ podgrupe **A** takva da je $red(c_\alpha) = red(c_\alpha + A)$ za svako $\alpha < \lambda$. Neka je $c + A$ konačnog reda $m$. Po pretpostavci je **A** direktni sumand grupe $\mathbf{B} = \langle A, c\rangle$, dakle, za neku podgrupu **D** je $\mathbf{B} = \mathbf{A} \oplus \mathbf{D}$. **D** ($\cong$ **B**/**A**) je ciklična grupa reda $m$ generisana, recimo, elementom $d$. Ako je $c = a + kd$, onda mora biti $(k, m) = 1$; u suprotnom bismo, za $k = k_1 p$, $m = m_1 p$, $p > 1$, imali: $m_1 c = m_1 a + k_1(md) = m_1 a$ i $m_1(c + A) = A$, kontradikcija. Možemo, stoga, za predstavnika koseta $c + A - c_\alpha$ - uzeti $kd$. Jasno, $c + A = c_\alpha + A$ i $red(c_\alpha) = red(d) = red(c_\alpha + A) = m$. Ako je $c + A$ beskonačnog reda, već znamo da je svaki element koseta jednako dobar predstavnik.□

**Lema 37.18** *Ako je* **A** *potpuna i ograničena podgrupa grupe* **B**, *onda je* **A** *i direktni sumand grupe* **B**.



**Dokaz.** Neka red svakog elementa $a \in A$ deli $n$. Jasno, $\mathbf{A} \cap n\mathbf{B} = \mathbf{O}$ (iz $a = nb$ sledi, zbog potpunosti podgrupe **A**, da je $nb = na_1 = 0$ za neko $a_1 \in A$). Neka je $\mathbf{C} = \mathbf{A} \oplus n\mathbf{B}$. Grupa $\overline{\mathbf{B}} = \mathbf{B}/n\mathbf{B}$ je ograničena, a $\overline{\mathbf{C}} = \mathbf{C}/n\mathbf{B}$ je njena potpuna podgrupa. Zaista, ako je $a + nB = m(b + nB)$, gde $m|n$, $n = mk$, onda je $a = mb + nb_1 = m(b + kb_1)$ za neko $b_1 \in B$. Zbog potpunosti podgrupe **A** je $a = ma_1$ za neko $a_1 \in A$, pa je $a + nB = m(a_1 + nB)$. Ali ograničenje $m|n$ nije restrikcija uopšte: ako je $(n, l) = 1$, onda je i $(red(a), l) = 1$ i jednačina $a = lx$ ima rešenje u $\langle a\rangle$, a ako je $(n, l) = r$, $l = l_1 r$ i $a + nB = l(b + nB) = r(l_1 b + nB)$, prema dokazanom postoji element $a_1 + nB$ takav da je $a + nB = r(a_1 + nB)$, dok jednačina $a_1 = l_1 x$ ima rešenje, recimo $a_2$, u **A** (štaviše u $\langle a\rangle$), te je, konačno, $a + nB = r(a_1 + nB) = r(l_1 a_2 + nB) = l(a_2 + nB)$. Faktor grupa $\overline{\mathbf{B}}/\overline{\mathbf{C}}$ ($\cong$ **B**/**C**) je, kao ograničena grupa, direktna suma cikličnih grupa. Stoga je, prema prethodnoj lemi, $\overline{\mathbf{C}}$ direktni sumand grupe $\overline{\mathbf{B}}$; stavimo: $\overline{\mathbf{B}} = \overline{\mathbf{C}} \oplus \overline{\mathbf{D}}$. Ako je $\overline{\mathbf{D}} = \mathbf{D}/n\mathbf{B}$, onda je $\mathbf{B} = \langle C, D\rangle$ i $\overline{C} \cap \overline{D} = \{nB\}$. Ali kako je $\mathbf{C} = \mathbf{A} \oplus n\mathbf{B}$ i $\mathbf{A} \cap n\mathbf{B} = \mathbf{O}$, to je $\mathbf{B} = \mathbf{A} \oplus \mathbf{D}$.□

**Korolar 37.19** *Ako je konačna grupa* **A** *potpuna podgrupa grupe* **B**, *onda je ona i direktni sumand grupe* **B**.

**Korolar 37.20** *Za grupu* **B** *i njenu podgrupu* **A** *sledeći uslovi su ekvivalentni:*

(1) **A** *je potpuna podgrupa grupe* **B**;

(2) *Za svaki prirodan broj n je* **A**/$n$**A** *direktni sumand grupe* **B**/$n$**A**;

(3) *Ako je* **C** *podgrupa grupe* **A** *takva da je faktor grupa* **A**/**C** *konačno kogenerisana, onda je* **A**/**C** *direktni sumand grupe* **B**/**C**.

**Dokaz.** (1) $\Longrightarrow$ (2) Neka je **A** potpuna podgrupa grupe **B**. Prema 37.12, **A**/$n$**A** je potpuna podgrupa grupe **B**/$n$**A**, a prema prethodnoj lemi i njen direktni sumand.

(2) $\Longrightarrow$ (3) Neka važi (2) i neka je, za $\mathbf{C} \leq \mathbf{A}$, **A**/**C** konačno kogenerisana grupa. S obzirom da je deljiva grupa uvek direktni sumand, možemo odmah pretpostaviti da je **A**/**C** reducirana grupa (sećamo se: svaka Abelova grupa je direktna suma deljive i reducirane grupe). Prema lemi 36.3, **A**/**C** je onda konačna grupa, pa je $n(A/C) = \{C\}$ za neki pozitivan prirodan broj $n$, i odatle, $nA \subseteq C$. Dakle, $\mathbf{C}/n\mathbf{A} \leq \mathbf{A}/n\mathbf{A}$, i kako je, za neku podgrupu **D**, $n\mathbf{A} \leq \mathbf{D} \leq \mathbf{B}$, $\mathbf{B}/n\mathbf{A} = \mathbf{A}/n\mathbf{A} \oplus \mathbf{D}/n\mathbf{A}$, sledi:

$$\mathbf{B}/\mathbf{C} \cong (\mathbf{B}/n\mathbf{A})/(\mathbf{C}/n\mathbf{A}) = (\mathbf{A}/n\mathbf{A} \oplus \mathbf{D}/n\mathbf{A})/(\mathbf{C}/n\mathbf{A}) \cong \mathbf{A}/\mathbf{C} \oplus \mathbf{D}/n\mathbf{A};$$

(koristimo: ako je $\mathbf{G} = \mathbf{H} \oplus \mathbf{K}$ i $\mathbf{M} \leq \mathbf{H}$, onda je $\mathbf{G}/\mathbf{M} \cong (\mathbf{H}/\mathbf{M}) \oplus \mathbf{K}$; jedno izomorfno preslikavanje - $\varphi$ - je dato sa: $((h + k) + M)\varphi = (h + M) + k$).

(3) $\Longrightarrow$ (1) Neka je ispunjen uslov (3) i neka za $a \in A$ i $n$ veće od 1 jednačina $a = nx$ ima rešenje u **B** ali ne i u **A**. Onda $a \notin nA$. Neka je **C**

maksimalna podgrupa grupe $\mathbf{A}$ koja sadrži $n\mathbf{A}$ i ne sadrži $a$. Prema korolaru 36.4, $\mathbf{A/C}$ je kociklična grupa, stoga, prema (3), i direktni sumand grupe $\mathbf{B/C}$. Ali tada je element $(C \neq)\ a + C \in A/C$ deljiv sa $n$ u grupi $\mathbf{B/C}$, dok je $n(\mathbf{A/C}) = \mathbf{O}$, kontradikcija ($\mathbf{A/C}$ je kao direktni sumand i potpuna podgrupa).□

**Korolar 37.21** *Podgrupa* $\mathbf{A}$ *grupe* $\mathbf{B}$ *je potpuna akko za svako homomorfno preslikavanje* $\varphi$ *grupe* $\mathbf{A}$ *u kocikličnu grupu* $\mathbf{G}$ *postoji homomorfno preslikavanje* $\psi$ *grupe* $\mathbf{B}$ *u* $\mathbf{G}$ *koje je ekstenzija homomorfizma* $\varphi$ $(\psi|_A = \varphi)$.

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{A}$ potpuna podgrupa grupe $\mathbf{B}$ i $\varphi \in Hom(\mathbf{A}, \mathbf{G})$. Možemo pretpostaviti da je $\mathbf{G}$ konačna direktna suma kocikličnih grupa, tj. prema lemi 36.3, konačno kogenerisana grupa. Kako su podgrupe konačno kogenerisanih podgrupa konačno kogenerisane, nema razloga da ne pretpostavimo i da je $\varphi$ surjektivi homomorfizam. Pošto je $\mathbf{A/Ker}(\varphi) \cong \mathbf{G}$, prema prethodnom korolaru je $\mathbf{A/Ker}(\varphi)$ direktni sumand grupe $\mathbf{B/Ker}(\varphi)$. Neka je

$$\mathbf{B/Ker}(\varphi) = \mathbf{A/Ker}(\varphi) \oplus \mathbf{C/Ker}(\varphi).$$

Jasno, $B = A + C$. Preslikavanje $\psi : B \longrightarrow G$ definisano sa $(a + c)\psi = (a)\varphi$ homomorfno je preslikavanje grupe $\mathbf{B}$ na $\mathbf{G}$ i važi: $\psi|_A = \varphi$. Zaista, $\psi$ je dobro definisano, jer ako je $a_1 + c_1 = a_2 + c_2$, $a_1, a_2 \in A$, $c_1, c_2 \in C$, onda je $a_1 - a_2 = c_2 - c_1 \in Ker(\varphi)$, pa je $(a_1 - a_2)\varphi = (a_1)\varphi - (a_2)\varphi = 0$, tj. $(a_1)\varphi = (a_2)\varphi$. Ostalo je još očiglednije.

($\Longleftarrow$) Neka su ispunjeni uslovi (pravca $\Longleftarrow$) i neka je $\mathbf{D}$ podgrupa grupe $\mathbf{A}$ takva da je $\mathbf{A/D}$ konačno kogenerisana. Neka je za kanonički homomorfizam $\varphi \in Hom(\mathbf{A}, \mathbf{A/D})$ homomorfizam $\psi \in Hom(\mathbf{B}, \mathbf{A/D})$ takav da je $\psi|_A = \varphi$. Onda je $\mathbf{B/D} = \mathbf{A/D} \oplus \mathbf{Ker}(\psi)/\mathbf{D}$. Jasno, $\mathbf{D} \leq \mathbf{A} \cap \mathbf{Ker}(\psi)$, a s druge strane, ako je $a \in A \cap Ker(\psi)$, tada je $(a)\psi = (a)\varphi = a + D = D$ i $a \in D$. Dalje, iz $(b)\psi = a + D = (a)\varphi = (a)\psi$ sledi: $(b - a)\psi = D$, odnosno $b - a \in Ker(\psi)$, pa je $b \in A + Ker(\psi)$. Ponovo prema prethodnom korolaru, $\mathbf{A}$ je potpuna podgrupa grupe $\mathbf{B}$.□

**Korolar 37.22** *Ako je* $\mathbf{A}$ *maksimalna podgrupa među podgrupama grupe* $\mathbf{B}$ *čiji je presek sa* $p^n\mathbf{B}$ *nula podgrupa (*$p$ *- prost broj), onda je ona i direktni sumand grupe* $\mathbf{B}$.

**Dokaz.** Kako je $p^n\mathbf{A} \leq \mathbf{A} \cap p^n\mathbf{B} = \mathbf{O}$, $\mathbf{A}$ je ograničena podgrupa. Pokazaćemo da je i potpuna. S obzirom da je $p$-(pod)grupa treba samo dokazati: $\mathbf{A} \cap p^k\mathbf{B} \leq p^k\mathbf{A}$ (ne zaboravimo da je element čiji je red stepen prostog broja $p$ deljiv svim prostim brojevima različitim od $p$). Dokaz je, standardno, indukcijom. Slučaj $k = 0$ je trivijalan. Pretpostavimo da je tvrđenje tačno za svako $m$ manje od ili jednako $k$ ($> 0$) i neka je $a = p^{k+1}b = p(p^kb) \neq 0$. Onda je, zbog $\mathbf{A} \cap p^n\mathbf{B} = \mathbf{O}$, $k + 1 < n$, i prema 30.15, $p^kb \in A + p^nB$. Stoga je, za neko



$a_1 \in A$ i neko $b_1$ $(\in B)$, $p^kb = a_1 + p^nb_1$ i dalje $a_1 = p^kb - p^nb_1 \in A \cap p^kB =$ (po induktivnoj pretpostavci) $p^kA$. Odatle, $a = p^{k+1}b = p(p^kb) = pa_1 + p^{n+1}b_1$, tj. $a - pa_1 = p^{n+1}b \in A \cap p^nB = \{0\}$, pa je $a = pa_1 \in p^{k+1}A$.□

**Korolar 37.23** *p-podgrupa* $\mathbf{A}$ *grupe* $\mathbf{B}$ *sadržana je u ograničenom direktnom sumandu grupe* $\mathbf{B}$ *akko je visina njenih nenula elemenata (u* $\mathbf{B}$*) ograničena.*

**Dokaz.** Naravno, kad govorimo o visinama elemenata grupe $\mathbf{A}$, mislimo na visine s obzirom na $p$. Pravac ($\Longrightarrow$) je (jako) očigledan. Što se tiče suprotnog pravca, neka je $n$ gornja granica visine elemenata iz $\mathbf{A}$ (to će reći, postoji element $a \in A \setminus \{0\}$ takav da je jednačina $a = p^nx$ rešiva u $\mathbf{B}$, ali ni za jedno $a_1 \in A \setminus \{0\}$ jednačina $a_1 = p^{n+1}x$ nema rešenje u $\mathbf{B}$, tj. drugim rečima, $\mathbf{A} \cap p^{n+1}\mathbf{B} = \mathbf{O}$) i neka je $\mathbf{A}_1$ maksimalna podgrupa grupe $\mathbf{B}$ koja sadrži $\mathbf{A}$ i čiji je presek sa $p^{n+1}\mathbf{B}$ nula podgrupa. Prema prethodnom korolaru $\mathbf{A}_1$ je direktni sumand i $p^{n+1}\mathbf{A}_1 = \mathbf{O}$.□

**Korolar 37.24** *Element* $a$ *grupe* $\mathbf{A}$ *čiji je red stepen prostog broja sadržan je u konačnom direktnom sumandu akko je ciklična grupa* $\langle a \rangle$ *bez elemenata beskonačne visine.*

**Dokaz.** Pravac ($\Longrightarrow$) je trivijalan, a pravac ($\Longleftarrow$) je direktna posledica prethodnog korolara.□

Elementi prethodne leme (37.18) sadržani su u narednoj, koja opet može poslužiti za njen novi dokaz.

**Lema 37.25** *Neka je podgrupa* $\mathbf{A}$ *grupe* $\mathbf{B}$ *direktna suma cikličnih grupa istog (konačnog) reda* $n$*. Tada su sledeći uslovi ekvivalentni:*

($a$) $\mathbf{A}$ *je direktni sumand grupe* $\mathbf{B}$*;*

($b$) $\mathbf{A}$ *je potpuna podgrupa grupe* $\mathbf{B}$*;*

($c$) $\mathbf{A} \cap n\mathbf{B} = \mathbf{O}$.

**Dokaz.** Implikaciju $(a) \Longrightarrow (b)$ smo već konstatovali (ali ne i dokazali, zbog trivijalnosti dokaza) - 37.11($a$).

$(b) \Longrightarrow (c)$ Neka je $a = nb$. Zbog potpunosti podgrupe $\mathbf{A}$ je $a = na_1 = 0$ za neko $a_1 \in A$.

$(c) \Longrightarrow (a)$ Neka je $\mathbf{C}$ maksimalna podgrupa grupe $\mathbf{B}$ koja sadrži $n\mathbf{B}$ i ima trivijalan presek sa $\mathbf{A}$ ($\mathbf{A} \cap \mathbf{C} = \mathbf{O}$) i neka je $\mathbf{B}_1 = \mathbf{A} \oplus \mathbf{C}$. Tvrdimo: $\mathbf{B} = \mathbf{B}_1$. Pretpostavimo suprotno. Neka je $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ $(\alpha_i \geq 1)$ i $g \in B \setminus B_1$. Posmatrajmo element $b = p_{i_1}^{\beta_1 - 1} \cdots p_{i_m}^{\beta_m} g$, gde je $p_{i_1}^{\beta_1} \cdots p_{i_m}^{\beta_m}$, $i_j \in \{1, \ldots, k\}$, $1 \leq \beta_j \leq \alpha_{i_j}$, $1 \leq j \leq m$, najmanji delilac broja $n$ za koji "umnožak" elementa $g$ "upada" u $\mathbf{B}_1$ (takav sigurno postoji jer je $ng \in nB \subseteq C \subseteq B_1$). Važi: $b \notin B_1$ i $p_{i_1}b \in B_1$. Stoga je, za neko $a \in A$ i neko $c \in C$, $p_{i_1}b = a + c$, pa

je $nb = \frac{n}{p_{i_1}}(a+c)$, odnosno $nb - \frac{n}{p_{i_1}}c = \frac{n}{p_{i_1}}a \in A \cap C$. Sledi: $\frac{n}{p_{i_1}}a = 0$, iz čega proizilazi da je $a$ deljivo sa $p_{i_1}$ (ako je $a = a'_1 + \cdots + a'_r$, gde su $a'_j$, $1 \leq j \leq r$, elementi direktnih cikličnih sumanada grupe $\mathbf{A}$ generisanih elementima $a_j$, $1 \leq j \leq r$, onda je za svako $j$, $1 \leq j \leq r$, $\frac{n}{p_{i_1}}a'_j = 0$, i ako je $a'_j = k_j a_j$, onda $p_{i_j} | k_j$). Neka je $a = p_{i_1}a'$ i $d = b - a'$. Onda $d \notin B_1$, $p_{i_1}d = c \in C$ $(\subseteq B_1)$ i, prema pretpostavci o podgrupi $\mathbf{C}$, $\langle C, d\rangle \cap \mathbf{A} \neq \mathbf{O}$. Stoga je, za neko $k$, $0 < k < p_{i_1}$, i neko $c_1 \in C$, $0 \neq kd + c_1 \in A$, te je i $kd \in B_1$, a tada je i $d \in B_1$, kontradikcija (imamo u vidu: $(k, p_{i_1}) = 1$ i, jasno, Euklidovu teoremu).□

**Korolar 37.26** *Neka je $a$ element grupe $\mathbf{A}$ reda $p$ i konačne visine (po $p$, jasno). Tada postoji konačan direktni sumand grupe $\mathbf{A}$ koji sadrži $a$.*

**Dokaz.** Neka je $h_p(a) = n$ i neka je $a = p^n b$. Tada je $\langle b\rangle$ potpuna podgrupa, pa prema prethodnoj lemi, ili korolaru 37.19, i direktni sumand grupe $\mathbf{A}$. Svi elementi podgrupe $\langle b\rangle$ deljivi su svim prostim brojevima različitim od $p$ (kao elementi $p$ grupe), a $kb$ je deljivo sa $p^m$ akko je $p^m$ faktor broja $k$. Jer, pretpostavimo: $0 \neq kb = p^m c$, $c \in A$ i $k = p^r s$, gde je $r < m$ (jasno, $r \leq n$) i $(s, p) = 1$. Onda iz $p^r sb = p^m c$ sledi $sa = p^{n-r}(p^r sb) = p^{n-r}p^m c = p^{n+(m-r)}c$, pa je $h_p(sa) > n$, kontradikcija ($a$ i $sa$ imaju istu visinu; za nedovoljno ubeđene: ako su $u$ i $v$ celi brojevi takvi da je $us + vp = 1$, imamo $a = usa + vpa = usa = p^{n+(m-r)}(uc)$).□

**Korolar 37.27** *Ako grupa $\mathbf{A}$ sadrži element konačnog reda sadrži i kocikličnu podgrupu kao direktni sumand (u ovom, kao uostalom i u prethodnom korolaru, dozvoljavamo mogućnost da je "drugi" direktni sumand nula grupa).*

**Dokaz.** Neka grupa $\mathbf{A}$ ima elemenata reda $p$. Posmatrajmo podgrupu $\mathbf{A}_p$ (generisanu svim elementima čiji su redovi stepeni od $p$). Ako $\mathbf{A}_p$ sadrži Prüferovu grupu $\mathbf{p}^\infty$, ova je, kao deljiva, direktni sumand grupe $\mathbf{A}$. U suprotnom je bar jedan element reda $p$ konačne visine (videti 33.3) i stoga, prema prethodnom korolaru, sadržan u cikličnoj $p$-grupi, koja je i direktni sumand.□

**Korolar 37.28** *Među Abelovim grupama koje nisu torziono slobodne nerazložive su jedino kocikличne.*

**Korolar 37.29** *Prüferove grupe su jedine beskonačne Abelove grupe čije su sve prave podgrupe konačne.*

**Definicija 37.30** *Abelova grupa $\mathbf{A}$ je potpuno prosta akko nema netrivijalnih potpunih podgrupa (trivijalne su, jasno, $\mathbf{O}$ i $\mathbf{A}$).*

**Lema 37.31** *Grupa $\mathbf{A}$ je potpuno prosta akko je izomorfna ili podgrupi grupe $\mathbf{Ra}$ ili podgrupi neke Prüferove grupe.*



**Dokaz.** ($\Longleftarrow$) Grupe $\mathbf{Ra}$ i $\mathbf{p}^\infty$ su potpuno proste, jer bi svaka njihova nenula prava potpuna podgrupa bila i sama deljiva, prema tome i direktni sumand.

Neka je, dakle, $\mathbf{B}$ prava nenula podgrupa grupe $\mathbf{Ra}$ i neka je $\mathbf{A}$ nenula prava podgrupa grupe $\mathbf{B}$. Ako bi $\mathbf{A}$ bila potpuna u $\mathbf{B}$, bila bi potpuna i u podgrupi $\mathbf{C}$ grupe $\mathbf{B}$, koja sadrži $\mathbf{A}$ kao maksimalnu podgrupu (videti 34.7($b$)). Možemo stoga odmah pretpostaviti da je $\mathbf{A}$ maksimalna podgrupa grupe $\mathbf{B}$. Neka je, za neki prost broj $p$, $m_p = v_p(\mathbf{A}) = v_p(\mathbf{B}) + 1$; jasno, onda je, za sve ostale proste brojeve $q$, $v_q(\mathbf{A}) = v_q(\mathbf{B})$. Ako je $0 \neq a = p^{m_p}a' \in A$, tada je $b = p^{m_p - 1}a' \in B$ (34.1), pa jednačina $a = px$ ima rešenje u $\mathbf{B}$, ali ne i u $\mathbf{A}$ (za svaki element $a_1 \in A$ je $(a_1)v_p \geq v_p(\mathbf{A}) = m_p$). Znači, $\mathbf{B}$ je potpuno prosta podgrupa.

Prave podgrupe grupe $\mathbf{p}^\infty$ su $p$-primarne ciklične grupe. No, ako je $\mathbf{H} = \langle p^k\rangle$ prava podgrupa grupe $\mathbf{Z}_{p^m}$, $0 < k < m$ (videti 7.2), onda je $p^k = p \cdot_{p^m} p^{k-1}$, dakle, jednačina $p^k = px$ je rešiva u $\mathbf{Z}_{p^m}$, ali ne i u $\mathbf{H}$, što se lako proverava; za $0 < t < p^{m-k}$, $p^k = p \cdot_{p^m} p^k t$ bi dalo: $p^k = p^{k+1}t - [\frac{p^{k+1}t}{p^m}]p^m$, i odatle, $p$ deli 1, kontradikcija. Zaključujemo da su i primarne ciklične grupe potpuno proste.

($\Longrightarrow$) Već smo rekli da je svaka mešovita grupa razloživa (37.28), a da od periodičnih nisu razložive jedino kocikличne grupe; rekli smo već i: svaki direktni sumand je potpuna podgrupa. Pretpostavimo da je $\mathbf{A}$ torziono slobodna i potpuno prosta grupa. Kako je svaka Abelova grupa direktna suma deljive i reducirane grupe, to je $\mathbf{A} = \mathbf{A}_1 \oplus \mathbf{A}_2$, gde je $\mathbf{A}_1$ (maksimalna) deljiva podgrupa grupe $\mathbf{A}$ i $\mathbf{A}_2$ reducirana podgrupa. Ako je $\mathbf{A}_2 = \mathbf{O}$, $\mathbf{A}$ je deljiva grupa, pa mora biti $\mathbf{A} \cong \mathbf{Ra}$ (svaka deljiva torziono slobodna grupa je direktna suma "kopija" aditivne grupe racionalnih brojeva). Ako je $\mathbf{A}_1 = \mathbf{O}$, onda je $\mathbf{A}$ $(= \mathbf{A}_2)$ reducirana grupa. Posmatrajmo injektivni omotač, $\mathbf{I}(\mathbf{A})$, grupe $\mathbf{A}$. Zbog $\mathbf{O} = \mathbf{A}[p] = \mathbf{I}(\mathbf{A})[p]$ za svaki prost broj $p$ (33.26), $\mathbf{I}(\mathbf{A})$ je izomorfna direktnoj sumi kopija grupe $\mathbf{Ra}$. Ako je $\mathbf{A}$ beskonačna ciklična grupa, onda je $\mathbf{I}(\mathbf{A}) \cong \mathbf{Ra}$. Pretpostavimo da $\mathbf{A}$ nije beskonačna ciklična grupa i neka je $0 \neq a \in A$. Ako bismo pretpostavili da je $\mathbf{I}(\mathbf{A})$ izomorfna direktnoj sumi dve ili više kopija grupe $\mathbf{Ra}$, onda bismo za $\mathbf{I}(\langle a\rangle) \leq \mathbf{I}(\mathbf{A})$ imali da je $\mathbf{O} \neq \mathbf{I}(\langle a\rangle) \cap \mathbf{A}$ potpuna podgrupa grupe $\mathbf{A}$ (videti 37.3 i 37.4), te bi sledilo, dalje, $\mathbf{I}(\langle a\rangle) \cap \mathbf{A} = \mathbf{A}$, tj. $\mathbf{A} \leq \mathbf{I}(\langle a\rangle) \cong \mathbf{Ra}$, kontradikcija.□

**Lema 37.32** ($a$) *Svaka grupa $\mathbf{A}$ je homomorfna slika direktne sume cikličnih grupa, pri čemu je jezgro homomorfizma potpuna podgrupa.*

($b$) *Svaka grupa $\mathbf{A}$ je potpuna podgrupa direktne sume kartezijanske sume konačnih cikličnih grupa i deljive grupe.*

**Dokaz.** ($a$) Neka je $A = \{a_i \mid i \in I\}$. Formirajmo direktnu sumu cikličnih grupa $\mathbf{B} = \sum_{i \in I}\langle b_i\rangle$, gde je $red(b_i) = red(a_i)$. Preslikavanje $\varphi : B \longrightarrow A$ dato sa $(b_i)\varphi = a_i$ surjektivni je homomorfizam (videti npr. 21.9). Neka je $nb \in Ker(\varphi)$. Onda je, za neko $a_i \in A$, $(b)\varphi = a_i$ i $na_i = n(b)\varphi = (nb)\varphi = 0$.

Ako je $c = b - b_i$, tada je, očigledno, $c \in Ker(\varphi)$ i $nc = n(b - b_i) = nb$ ($nb_i = 0$ jer je $na_i = 0$).

($b$) Neka je $\mathbf{A}_1 = \bigcap_{n\in N} n\mathbf{A}$ i $\mathbf{D} = \mathbf{I}(\mathbf{A}_1)$. S obzirom da je $\mathbf{D}$ injektivna grupa, za utapanja $\imath_{A_1} : A_1 \longrightarrow A$ i $\imath_{A_1} : A_1 \longrightarrow D$ postoji homomorfizam $\phi : A \longrightarrow D$ takav da je $\phi|_{A_1} = \imath_{A_1}$. Neka je $\psi : A \longrightarrow \sum_{n\in N} A/nA$ definisano sa $(a)\psi = \langle a + nA\rangle_{n\in N}$ ($\psi$ je, evidentno, homomorfizam) i neka je $\theta$ homomorfno preslikavanje grupe $\mathbf{A}$ u direktnu sumu $\mathbf{D} \oplus \sum^c_{n\in N} \mathbf{A}/n\mathbf{A}$ dato sa $(a)\theta = (a)\phi + (a)\psi$. $\theta$ je injektivno, jer ako je $(a)\theta = (a)\phi + (a)\psi = 0$, onda je $(a)\phi = (a)\psi = 0$, iz $(a)\psi = \langle a + nA\rangle_{n\in N} = \langle nA\rangle_{n\in N}$ sledi $a \in \bigcap_{n\in N} nA = A_1$, pa $0 = (a)\phi = (a)\imath_{A_1} = a$. Dakle, $\mathbf{A} \cong (\mathbf{A})\theta$. $(\mathbf{A})\theta$ je pak potpuna podgrupa. Ako je $(a)\theta = (a)\phi + (a)\psi$ deljivo sa $n$, tada je svaka pojedina komponenta deljiva sa $n$. Prema tome je $\langle a + kA\rangle_{k\in N} = n\langle b_k + kA\rangle_{k\in N}$, $b_k \in A$, te je posebno, za $k = n$, $a + nA = nb_n + nA = nA$ i $a \in nA$. Stoga je, za neko $a_1$, $a = na_1$ i $(a)\theta = n\,(a_1)\theta$.

Preostaje nam još da konstatujemo da je svaka grupa $\mathbf{A}/n\mathbf{A}$ direktna suma cikličnih grupa jer je $red(a + nA) \leq n$ za svako $a \in A$ (videti 35.2 i setiti se da je periodična grupa direktna suma primarnih grupa).□

Tačka ($b$) prethodne leme daje se često u formi

**Korolar 37.33** *Svaka grupa je potpuna podgrupa kartezijanske sume Prüferovih i primarnih cikličnih grupa.*

**Dokaz**. Kao što je i za očekivati ideja dokaza je ista. Neka je data grupa $\mathbf{A}$ i neka je element $a \in A \setminus \{0\}$ deljiv sa $p^n$ ali ne i sa $p^{n+1}$ – $h_p(a) = n$. Za maksimalnu podgrupu $\mathbf{A}^p_a$ grupe $\mathbf{A}$ koja kao podgrupu sadrži $p^{n+1}\mathbf{A}$ (takva, po Zornovoj lemi, postoji jer po pretpostavci $a \notin p^{n+1}A$) faktor grupa $\mathbf{A}/\mathbf{A}^p_a$ je ciklična grupa reda $p^{n+1}$. Visina elementa $a + A^p_a$ je veća od ili jednaka $n$ (kao slika elementa visine $n$), ali manja od $n + 1$ (zbog $p^{n+1}\mathbf{A} \leq \mathbf{A}^p_a$). Konačno, za svaki nenula element $b$ iz $A$ i svaki prost broj $p$ za koje je $h_p(b) = k < \infty$ fiksirajmo jednu maksimalnu podgrupu $\mathbf{A}^p_b$ sa svojstvom da je faktor grupa $\mathbf{A}/\mathbf{A}^p_b$ ciklična grupa reda $p^{k+1}$.

Ako je pak $a$ beskonačne visine za svaki prost broj, tj. ako je deljivo sa svim pozitivnim prirodnim brojevima (jer, ako je $a$ deljivo i sa $p^m$ i sa $q^n$, onda je deljivo i sa $p^mq^n$; zaista, ako je $a = p^mb = q^nc$ i ako je $1 = up^m + vq^n$ za neke cele brojeve $u$ i $v$, sledi: $b = up^mb + vq^nb = uq^nc + vq^nb = q^n(uc + vb)$, pa je $a = p^mq^n(uc + vb)$), fiksiramo jednu proizvoljnu maksimalnu podgrupu $\mathbf{A}_a$ grupe $\mathbf{A}$ koja ne sadrži $a$. (Jasno, podgrupa svih elemenata deljivih svim pozitivnim prirodnim brojevima je $\bigcap_{n\in N} n\mathbf{A}$.) Svaka nenula podgrupa faktor grupé $\mathbf{A}/\mathbf{A}_a$ sadrži element $a + A_a$, stoga i podgrupu $\langle a + A_a\rangle$. Zaključujemo da je $\langle a + A_a\rangle$ jedinstvena minimalna podgrupa (sadržana u svakoj drugoj), pa je $\mathbf{A}/\mathbf{A}_a$ ili primarna ciklična grupa ili Prüferova grupa – to su jedine Abelove grupe koje imaju jedinstvenu minimalnu podgrupu sadržanu u svakoj drugoj



(beskonačna ciklična grupa nema minimalnih podgrupa, a ciklična grupa čiji red sadrži više prostih faktora direktna je suma primarnih cikličnih grupa).

Neka je $\mathbf{B} = \sum^c_{a\in\bigcap_{n\in N} nA} \mathbf{A}_a \oplus \sum^c_{p\in P}(\sum^c_{h_p(a)<\infty} \mathbf{A}^p_a)$ i neka je $\varphi : A \longrightarrow B$ preslikavanje, gde je za $b$ iz $A$ komponenta elementa $(b)\varphi$ u $\mathbf{A}/\mathbf{A}_a$ ($\mathbf{A}/\mathbf{A}^p_a$) $b + A_a$ ($b + A^p_a$). Evidentno, $\varphi$ je homomorfno preslikavanje. No, ono je i injektivno, jer ako je $b \in A \setminus \{0\}$ i $b \in \bigcap_{n\in N} nA$, onda je $b + A_b \neq A_b$, a ako je npr. $h_p(b) < \infty$, tada je $b + A^p_b \neq A^p_b$. Preostaje još da se pokaže da je $(\mathbf{A})\varphi$ potpuna podgrupa grupe $\mathbf{B}$. Neka je za $a$ iz $A$ jednačina $(a)\varphi = p^kx$ rešiva u $\mathbf{B}$. Ako je $h_p(a) = \infty$, jednačina $a = p^kx$ ima rešenje u $\mathbf{A}$, recimo $b$, te je $(a)\varphi = p^k(b)\varphi$. Ako je $h_p(a) = n < \infty$, onda je, prema izboru podgrupe $\mathbf{A}^p_a$, element $a + A^p_a$ reda $p$ i visine $n$, pa mora biti, s obzirom na rešivost jednačine $(a)\varphi = p^kx$ (u $\mathbf{B}$), $k \leq n$ i ponovo imamo rešenje jednačine $a = p^kx$ u $\mathbf{A}$.□

**Definicija 37.34** *Abelova grupa $\mathbf{A}$ je potpuno projektivna akko za svako surjektivno homomorfno preslikavanje $\phi$ Abelove grupe $\mathbf{B}$ na grupu $\mathbf{C}$ čije je jezgro potpuna podgrupa (ukoliko takvo postoji) i svaki homomorfizam $\psi \in Hom(\mathbf{A}, \mathbf{C})$ postoji homomorfizam $\theta \in Hom(\mathbf{A}, \mathbf{B})$ takav da je $\theta \circ \phi = \psi$ ($\mathbf{B}$ i $\mathbf{C}$ su ma kakve Abelove grupe).*

**Lema 37.35** *Abelova grupa $\mathbf{A}$ je potpuno projektivna akko je direktna suma cikličnih grupa.*

**Dokaz**. ($\Longrightarrow$) Prema prethodnoj lemi grupa $\mathbf{A}$ sa domenom $\{a_i \mid i \in I\}$ homomorfna je slika grupe $\mathbf{B} = \sum_{i\in I} \langle b_i\rangle$ za preslikavanje $\varphi$, gde je $red(b_i) = red(a_i)$ i $(b_i)\varphi = a_i$. Videli smo takođe da je $\mathbf{Ker}(\varphi)$ potpuna podgrupa. Za $\varphi$ i $\imath_A : A \longrightarrow A$ postoji homomorfizam $\theta \in Hom(\mathbf{A}, \mathbf{B})$ takav da je $\theta \circ \varphi = \imath_A$. $\theta$ je injektivno (jer je i $\imath_A$ injektivno), a kao i u slučaju teoreme 33.7 ($(b) \Longrightarrow (c)$) imamo: $\mathbf{B} = \mathbf{Ker}(\varphi) \oplus (\mathbf{A})\theta$. Ponavljamo: ako je $(b)\varphi = a = (a)(\theta \circ \varphi)$ $(= (a)\imath_A)$, sledi $(b - (a)\theta)\varphi = 0$, pa je $b - (a)\theta \in Ker(\varphi)$, tj. $b \in Ker(\varphi) + (A)\theta$. Trivijalno, $\mathbf{Ker}(\varphi) \cap (\mathbf{A})\theta = \mathbf{O}$ ($b \in Ker(\varphi) \cap (A)\theta$ implicira: za neko $a$ iz $A$ je $b = (a)\theta$ i $0 = (b)\varphi = ((a)\theta)\varphi = (a)\imath_A = a$, znači i $b = 0$). Prema 35.8, $\mathbf{A}$ ($\cong (\mathbf{A})\theta$) je direktna suma cikličnih grupa.

($\Longleftarrow$) Neka je $\mathbf{A}$ direktna suma cikličnih grupa, $\psi$ surjektivno homomorfno preslikavanje Abelove grupe $\mathbf{B}$ na grupu $\mathbf{C}$ čije je jezgro potpuna podgrupa i $\varphi \in Hom(\mathbf{A}, \mathbf{C})$. Neka je, dalje, $\mathbf{D}$ povratna grupa (povratnog) dijagrama $(\mathbf{A}, \mathbf{B}, \mathbf{C}, \varphi, \psi)$. Podsećamo se: $D = \{(a, b) \in A \times B \mid (a)\varphi = (b)\psi\}$, $\varphi_1 : D \longrightarrow A$ je projekcija: $(a, b)\varphi_1 = a$, $\psi_1 : D \longrightarrow B$ je projekcija $(a, b)\psi_1 = b$. Uočimo prvo da je $Ker(\varphi_1) = \{(0, b) \mid b \in Ker(\psi)\}$ (jer $(0, b) \in D$ povlači $0 = (0)\varphi = (b)\psi$, tj. $b \in Ker(\psi)$). Kako je $\mathbf{Ker}(\psi)$ potpuna podgrupa grupe $\mathbf{B}$, to je i $\mathbf{Ker}(\varphi_1)$ potpuna podgrupa grupe $\mathbf{D}$. S obzirom da je $\mathbf{D}/\mathbf{Ker}(\varphi_1) \cong \mathbf{A}$, prema 37.14($a$) $\mathbf{Ker}(\varphi_1)$ je direktni sumand grupe $\mathbf{D}$: $\mathbf{D} = \mathbf{Ker}(\varphi_1) \oplus \mathbf{G}$. Kompozicija $\theta$ izomorfnih preslikavanja $G \longrightarrow D/Ker(\varphi_1) \longrightarrow A$ je izomorfno preslikavanje grupe $\mathbf{G}$ na grupu $\mathbf{A}$. Primetimo da za $(a, b) \in G$

imamo: $(a,b) \longrightarrow (a,b) + Ker(\varphi_1) \longrightarrow (a,b)\varphi_1 = a$, dakle, $(a,b)\theta = a$. Za inverzno preslikavanje $\theta^{-1} : A \longrightarrow G \leq D$ je $\theta^{-1} \circ \varphi_1 = \imath_A$. Traženo homomorfno preslikavanje grupe $\mathbf{A}$ u grupu $\mathbf{B}$ je $\theta^{-1} \circ \psi_1$. Zaista, $((a)(\theta^{-1} \circ \psi_1))\psi = ((a)\theta^{-1})(\psi_1 \circ \psi) = ((a)\theta^{-1})(\varphi_1 \circ \varphi) = ((a)(\theta^{-1} \circ \varphi_1))\varphi = (a)\varphi$.□

## 38 Algebarski kompaktne grupe

Videli smo da potpuna podgrupa ne mora biti direktni sumand (npr. 30.4, 37.13). S pojačanom verzijom tog uslova dobija se interesantna klasa Abelovih grupa o kojoj će ovde biti reči.

**Definicija 38.1** *Grupa* $\mathbf{A}$ *je algebarski kompaktna akko je direktni sumand svake grupe* $\mathbf{B}$ *koja je sadrži kao potpunu podgrupu.*

Kao prve primere algebarski kompaktnih grupa navodimo deljive i ograničene grupe (37.18).

**Definicija 38.2** *Grupa* $\mathbf{A}$ *je potpuno injektivna akko za svako injektivno homomorfno preslikavanje* $\phi$ *grupe* $\mathbf{B}$ *u* $\mathbf{C}$, *pri čemu je* $(\mathbf{B})\phi$ *potpuna podgrupa grupe* $\mathbf{C}$, *i svaki homomorfizam* $\psi \in Hom(\mathbf{B},\mathbf{A})$ *postoji homomorfno preslikavanje* $\theta$ *grupe* $\mathbf{C}$ *u grupu* $\mathbf{A}$ *takvo da je* $\psi = \phi \circ \theta$.

**Lema 38.3** *Kartezijanska (direktna) suma* $\sum_{i\in I}^{c} \mathbf{A}_i$ $(\sum_{i\in I} \mathbf{A}_i)$ *je potpuno injektivna grupa akko je* $\mathbf{A}_i$ *potpuno injektivna grupa za svako* $i \in I$.

**Dokaz**. Trivijalan. Dajemo ga samo vežbe radi.

($\Longrightarrow$) Neka je $\mathbf{A} = \sum_{i\in I}^{c} \mathbf{A}_i$ potpuno injektivna grupa, $\mathbf{B}$ potpuna podgrupa grupe $\mathbf{C}$ i neka je $\psi$ homomorfno preslikavanje grupe $\mathbf{B}$ u $\mathbf{A}_i$, $i \in I$. Onda za neko $\theta \in Hom(\mathbf{C},\mathbf{A})$ važi: $\psi \circ \phi_i = \imath_B \circ \theta = \theta|_B$, gde je $\phi_i$ prirodno utapanje grupe $\mathbf{A}_i$ u $\mathbf{A}$ (jasno, za $a_i \in A_i$ je $(a_i)\phi_i = f_{a_i}$, gde je opet, za $j \neq i$, $(j)f_{a_i} \stackrel{\text{def}}{=} 0_j$ – neutralni element grupe $\mathbf{A}_j$, i $(i)f_{a_i} \stackrel{\text{def}}{=} a_i$), pa je za $\theta \circ \pi_i \in Hom(\mathbf{C},\mathbf{A}_i)$, gde je $\pi_i$ projekcija grupe $\mathbf{A}$ na $\mathbf{A}_i$, $\psi = \psi \circ \imath_{A_i} = \psi \circ (\phi_i \circ \pi_i) = \imath_B \circ (\theta \circ \pi_i) = (\theta \circ \pi_i)|_B$.

($\Longleftarrow$) Neka je, ponovo, $\mathbf{B}$ potpuna podgrupa grupe $\mathbf{C}$, $\mathbf{A} = \sum_{i\in I}^{c} \mathbf{A}_i$ i neka je $\mathbf{A}_i$ potpuno injektivna grupa za svako $i \in I$. Ako je $\psi \in Hom(\mathbf{B},\mathbf{A})$, onda za svako $i$ iz $I$ postoji homomorfno preslikavanje $\theta_i$ grupe $\mathbf{C}$ u $\mathbf{A}_i$ takvo da je $\psi \circ \pi_i = \imath_B \circ \theta_i = \theta_i|_B$ (naravno, $\pi_i$ ostaje projekcija grupe $\mathbf{A}$ na $\mathbf{A}_i$). Neka je $\theta : C \longrightarrow A$, dato sa $(i)((c)\theta) = (c)\theta_i$. $\theta$ je, evidentno, dobro definisano i homomorfno preslikavanje. Konačno, za $b \in B$ i svako $i \in I$ je: $(i)((b)\theta) = (b)\theta_i = (b)(\psi \circ \pi_i) = (i)((b)\psi)$, dakle $\theta|_B = \psi$.□

Korolar **38.4** (*a*) *Svaka kociklična grupa je potpuno injektivna;*

(*b*) *Kartezijanska suma kocikličnih grupa je potpuno injektivna.*



**Dokaz**. (*a*) Direktna posledica korolara 37.21.□

**Teorema 38.5** *Sledeći uslovi su ekvivalentni:*

(*a*) $\mathbf{A}$ *je potpuno injektivna grupa;*

(*b*) $\mathbf{A}$ *je algebarski kompaktna grupa;*

(*c*) $\mathbf{A}$ *je direktni sumand kartezijanske sume kocikličnih grupa;*

(*d*) *Sistem linearnih jednačina nad* $\mathbf{A}$ *ima rešenje u* $\mathbf{A}$ *akko svaki konačan podsistem ima rešenje.*

**Dokaz**. (*a*) $\Longrightarrow$ (*b*) Neka je potpuno injektivna grupa $\mathbf{A}$ potpuna podgrupa grupe $\mathbf{B}$. No, onda postoji homomorfno preslikavanje $\theta$ grupe $\mathbf{B}$ na grupu $\mathbf{A}$ takvo da je $\imath_A = \imath_A \circ \theta$. Sledi $\mathbf{B} = \mathbf{A} \oplus \mathbf{Ker}(\theta)$ (videti dokaz implikacije (*b*) $\Longrightarrow$ (*c*) u 33.7).

(*b*) $\Longrightarrow$ (*c*) Prema 37.33 svaka grupa je potpuna podgrupa kartezijanske sume kocikličnih, pa ako je uz to i algebarski kompaktna, onda je i direktni sumand te sume.

(*c*) $\Longrightarrow$ (*a*) Direktna posledica prethodnog korolara i prethodne leme.

(*b*) $\Longrightarrow$ (*d*) Neka je $\mathbf{A}$ algebarski kompaktna grupa i neka je

$$k_{\alpha_1}x_{\beta_1} + \cdots + k_{\alpha_m}x_{\beta_m} = a_\alpha, \quad \alpha < \mu \qquad (*)$$

(već poznat) sistem linearnih jednačina ($\mathcal{S}$) nad $\mathbf{A}$ sa $\lambda$ nepoznatih takav da je svaki njegov konačan podsistem rešiv u $\mathbf{A}$; jednačinu ($*$) pisaćemo kraće: $\sum k_{\alpha_j}x_{\beta_j} = a_\alpha$. Posmatrajmo kanoničkog predstavnika grupa sa prezentacijom $(A \cup \{x_\beta \mid \beta < \lambda\}; P_A \cup \{\sum k_{\alpha_j}x_{\beta_j} = a_\alpha \mid \alpha < \mu\}) \cup \{x_\beta + x_\gamma = x_\gamma + x_\beta \mid \beta,\gamma < \lambda\} \cup \{x_\beta + a = a + x_\beta \mid \beta < \lambda, a \in A\})$, gde je $P_A$ "aditivna" tablica grupe $\mathbf{A}$ (videti 21.6(*b*)). Skup izvodnih simbola obeležićemo sa $B$, skup navedenih relacija sa $Q$ (prezentacija je, dakle, $(B;Q)$). Preslikavanje $\psi : a \longrightarrow [a]_Q$ je utapanje grupe $\mathbf{A}$ u $\mathbf{G}_{(B;Q)}$. Zaista, neka je $[a]_Q = [b]_Q$, tj. $a \sim_Q b$. Onda postoji konačan niz:

$$a \equiv a_0, a_1, \ldots, a_n \equiv b$$

takav da je svako $a_i$ $(1 \leq i \leq n)$ dobijeno od $a_{i-1}$ "umetanjem" ili "brisanjem" neke od reči iz $Q$ ili neke trivijalne odrednice; jasno, relaciji $\sum k_{\alpha_j}x_{\beta_j} = a_\alpha$ odgovara reč $\sum k_{\alpha_j}x_{\beta_j} - a_\alpha$ itd. S obzirom da je u pitanju niz konačne dužine, to se i samo konačno mnogo reči koje odgovaraju jednačinama sistema mogu u njemu javiti. Konačan sistem svih tih jednačina – $\mathcal{S}_1$ ($\subseteq \mathcal{S}$) – sa konačno mnogo nepoznatih, recimo $\{x_{\beta_1}, \ldots, x_{\beta_m}\}$, ima rešenje u $\mathbf{A}$, recimo: $a_{\beta_1}, \ldots, a_{\beta_m}$. Stoga je $\mathbf{A}$ homomorfna slika kanoničkog predstavnika grupa sa prezentacijom $(A \cup \{x_{\beta_1}, \ldots, x_{\beta_m}\}\ (= B_1 = A \cup A'); P_A \cup \{\sum k_{\alpha_j}x_{\beta_j} - a_\alpha \mid \sum k_{\alpha_j}x_{\beta_j} = a_\alpha \in \mathcal{S}_1\} \cup \{x_\alpha + x_\beta = x_\beta + x_\alpha \mid x_\alpha, x_\beta \in A'\} \cup \{x_\alpha + a = a + x_\alpha \mid a \in A, x_\alpha \in A'\}\ (= Q_1))$; homomorfno preslikavanje, $\theta$, određeno je

sa: $([a]_{Q_1})\theta = a$, $([x_{\beta_j}]_{Q_1})\theta = a_{\beta_j}$, $1 \leq j \leq m$. No kako je i $a \sim_{Q_1} b$, sledi $a = b$. Ostalo je, što se tiče preslikavanja $\psi$ još očiglednije. Izomorfna slika $(\mathbf{A})\psi$ grupe $\mathbf{A}$ je i potpuna podgrupa grupe $\mathbf{G}_{(B;Q)}$. Jer, neka je $[m_1x_{\gamma_1} + \cdots + m_nx_{\gamma_n} + b]_Q$ rešenje jednačine $[a]_Q = ky$, $a \in A$, u grupi $\mathbf{G}_{(B;Q)}$. Znači, $km_1x_{\gamma_1} + \cdots + km_nx_{\gamma_n} \sim_Q a - kb$. Ponovo bismo, rezonujući kao maločas, dobili da je $\mathbf{A}$ homomorfna slika neke grupe $\mathbf{G}_{(B_2;Q_2)}$, gde je još $k(m_1x_{\gamma_1} + \cdots + m_nx_{\gamma_n}) \sim_{Q_2} a - kb$, pa bismo za rešenja $a_{\gamma_1}, \ldots, a_{\gamma_n}$ konačnog sistema jednačina u kojima se javljaju $x_{\gamma_1}, \ldots, x_{\gamma_n}$ imali: $[km_1a_{\gamma_1} + \cdots + km_na_{\gamma_n}]_Q = [a - kb]_Q$. I tako je, prema već konstatovanom: $a = k(b + m_1a_{\gamma_1} + \cdots + m_na_{\gamma_n})$. Proizilazi da je $(\mathbf{A})\psi$ direktni sumand grupe $\mathbf{G}_{(B;Q)}$ u kojoj je sistem $\mathcal{S}$ evidentno rešiv, pa je $\mathcal{S}$ rešiv i u $(\mathbf{A})\psi$ (a onda i u $\mathbf{A}$).

$(d) \Longrightarrow (a)$ Pretpostavimo da važi $(d)$ i neka je, da uprostimo stvar (što ne umanjuje opštost razmatranja), $\mathbf{B}$ potpuna podgrupa grupe $\mathbf{C}$, a $\psi \in Hom(\mathbf{B}, \mathbf{A})$. Neka je, dalje, $C_1 = \{c_\beta \mid \beta < \lambda\}$ generatorni skup grupe $\mathbf{C}$ modulo podgrupa $\mathbf{B}$, tj. $\mathbf{C} = \langle B \cup C_1 \rangle$. Uzećemo da je $C_1 \cap B = \emptyset$. Posmatrajmo sve jednakosti oblika

$$k_{\alpha_1}c_{\beta_1} + \cdots + k_{\alpha_m}c_{\beta_m} = b_\alpha, \quad \alpha < \mu \qquad (*)$$

koje važe u grupi $\mathbf{C}$. Onda svaki konačan podsistem sistema linearnih jednačina

$$k_{\alpha_1}x_{\beta_1} + \cdots + k_{\alpha_m}x_{\beta_m} = (b_\alpha)\psi, \quad \alpha < \mu \qquad (**)$$

ima rešenje u $\mathbf{A}$. Zaista, jedan dati odgovarajući sistem relacija uključuje samo konačno mnogo elemenata iz $C_1$, neka su to, recimo, $c_{\beta_0}, \ldots, c_{\beta_k}$, pa je prema 37.15 $\mathbf{B}$ direktni sumand grupe $\mathbf{D} = \langle B \cup \{c_{\beta_0}, \ldots, c_{\beta_k}\}\rangle$; za neku podgrupu $\mathbf{B}_1$ grupe $\mathbf{D}$ je $\mathbf{D} = \mathbf{B} \oplus \mathbf{B}_1$. Ako je $c_{\beta_i} = c'_{\beta_i} + c''_{\beta_i}$, $i = 0, \ldots, k$, gde je $c'_{\beta_i} \in B$, $c''_{\beta_i} \in B_1$, tada su $(c'_{\beta_i})\psi$, $i = 0, \ldots, k$, rešenja tog podsistema. S obzirom na $(d)$ ceo sistem $(**)$ ima rešenje u $\mathbf{A}$. Ako je skup rešenja $\{a_\beta \mid \beta < \lambda\}$, preslikavanje $\theta : C \longrightarrow A$ dato sa $(b + k_1c_{\beta_1} + \cdots + k_rc_{\beta_r})\theta = (b)\psi + k_1a_{\beta_1} + \cdots + k_ra_{\beta_r}$ homomorfno je preslikavanje grupe $\mathbf{C}$ u grupu $\mathbf{A}$ i, jasno, $\theta|_B = \psi$. Proverićemo samo da je $\theta$ dobro definisano (ostalo je još lakše). Neka je $b_1 + k_1c_{\beta_1} + \cdots + k_rc_{\beta_r} = b_2 + l_1c_{\gamma_1} + \cdots + l_sc_{\gamma_s}$, $b_1, b_2 \in B$, $c_{\beta_i}, c_{\gamma_j} \in C_1$ (ne isključujemo mogućnost da su, eventualno, $b_1$, $b_2$ jednaki, ili da su neki od elemenata $c_{\beta_i}$, $c_{\gamma_j}$ jednaki). Onda je

$$b_1 - b_2 = (-k_1)c_{\beta_1} + \cdots + (-k_r)c_{\beta_r} + l_1c_{\gamma_1} + \cdots + l_sc_{\gamma_s},$$

te je prema rečenom

$$(b_1 - b_2)\psi = (b_1)\psi - (b_2)\psi = (-k_1)a_{\beta_1} + \cdots + (-k_r)a_{\beta_r} + l_1a_{\gamma_1} + \cdots + l_sa_{\gamma_s},$$

odnosno

$$(b_1 + k_1c_{\beta_1} + \cdots + k_rc_{\beta_r})\theta = (b_2 + l_1c_{\gamma_1} + \cdots + l_sc_{\gamma_s})\theta.\blacksquare$$



**Korolar 38.6** *Kartezijanska suma* $\mathbf{A} = \sum^c_{\alpha<\kappa} \mathbf{A}_\alpha$ *je algebarski kompaktna akko je svaka grupa* $\mathbf{A}_\alpha$, $\alpha < \kappa$, *algebarski kompaktna.*

**Dokaz.** Prema prethodnoj i lemi 38.3.□

**Korolar 38.7** *Svaka grupa je potpuna podgrupa algebarski kompaktne grupe.*

**Dokaz.** Prema 37.32$(b)$ i prethodnom korolaru.□

**Korolar 38.8** *Direktni sumand algebarski kompaktne grupe je algebarski kompaktna grupa.*

**Korolar 38.9** *Reducirana algebarski kompaktna grupa* $\mathbf{A}$ *direktni je sumand kartezijanske sume primarnih cikličnih grupa.*

**Dokaz.** Prema tački $(c)$ prethodne teoreme važi za neku grupu $\mathbf{B}$:

$$\mathbf{A} \oplus \mathbf{B} = \mathbf{C}_1 \oplus \mathbf{C}_2 \ (= \mathbf{C}),$$

gde je $\mathbf{C}_1$ kartezijanska suma Prüferovih grupa, a $\mathbf{C}_2$ primarnih cikličnih grupa. Ako je, opet, $\mathbf{B} = \mathbf{B}_1 \oplus \mathbf{B}_2$, gde je $\mathbf{B}_1$ maksimalna deljiva podgrupa a $\mathbf{B}_2$ reducirani deo grupe $\mathbf{B}$, onda je, prema 33.33, 33.34, $\mathbf{B}_1$ ujedno i maksimalna deljiva podgrupa grupe $\mathbf{C}$. Stoga je $\mathbf{C}_1 \leq \mathbf{B}_1$, pa je $\mathbf{B}_1 = \mathbf{C}_1 \oplus (\mathbf{B}_1 \cap \mathbf{C}_2)$ (videti 10.17). Prema tome, imamo:

$$\mathbf{A} \oplus \mathbf{C}_1 \oplus (\mathbf{B}_1 \cap \mathbf{C}_2) \oplus \mathbf{B}_2 = \mathbf{C}_1 \oplus \mathbf{C}_2,$$

i odatle:

$$\mathbf{A} \oplus (\mathbf{B}_1 \cap \mathbf{C}_2) \oplus \mathbf{B}_2 \cong \mathbf{C}_2 \cong \mathbf{C}/\mathbf{C}_1.\square$$

**Lema 38.10** *Grupa je algebarski kompaktna akko je njen reducirani deo algebarski kompaktan.*

**Dokaz.** Neka je $\mathbf{A} = \mathbf{D} \oplus \mathbf{B}$, gde je $\mathbf{D}$ njena maksimalna deljiva podgrupa, a $\mathbf{B}$ reducirani deo koji je i algebarski kompaktan, potpuna podgrupa grupe $\mathbf{G}$. Onda je, za neku podgrupu $\mathbf{H}$ grupe $\mathbf{G}$ koja sadrži $\mathbf{B}$, $\mathbf{G} = \mathbf{D} \oplus \mathbf{H}$ (33.8). Jasno, $\mathbf{B}$ je potpuna podgrupa grupe $\mathbf{H}$ (jednačina $b = nx$, $n \in N$, koja ima rešenje u $\mathbf{H}$, dakle i u $\mathbf{G}$, ima ga i u $\mathbf{A}$, a onda i u $\mathbf{B}$), pa je $\mathbf{H} = \mathbf{B} \oplus \mathbf{C}$ za neku podgrupu $\mathbf{C}$ grupe $\mathbf{H}$. Sledi: $\mathbf{G} = \mathbf{A} \oplus \mathbf{C}$.□

**Korolar 38.11** *Grupa* $\mathbf{A}$ *je potpuno injektivna akko je direktna suma deljive grupe i direktnog sumanda kartezijanske sume konačnih cikličnih grupa.*

**Dokaz.** Direktna posledica prethodna dva tvrđenja i tačke $(c)$ teoreme 38.5.□

**Primer 38.12** (*a*) *Grupa* $\mathbf{Z}$ *nije algebarski kompaktna.*

**Dokaz.** Posmatrajmo sistem linearnih jednačina (sa beskonačno mnogo nepoznatih):

$$x_1 - 2x_2 = 1$$
$$x_2 - 2^2x_3 = 1$$
$$\vdots$$
$$x_n - 2^nx_{n+1} = 1$$
$$\vdots$$

Evidentno, svaki konačan podsistem ima rešenje u $\mathbf{Z}$. Prvih $n$ jednačina (za svako $n \in N$) obrazuje jednostruko neodređen sistem (i rešenja u $\mathbf{Z}$ ima beskonačno mnogo). S druge strane, sam sistem nema rešenje. Naime, ako bismo pretpostavili da je $\{b_n \mid n \in N\}$ jedan skup rešenja, onda bismo za $b_1 > 0$ ($b_1 < 0$) imali, uopšte, $b_k > 0$ ($b_k < 0$) za svako $k$ (isključena je mogućnost da je bilo koje $b_i$ jednako nuli zbog $b_i = 1 + 2^ib_{i+1}$). No, lako se pokazuje da bi $b_1$ bilo veće (manje) od svakog unapred zadanog celog pozitivnog (negativnog) broja.

(*b*) *Slobodne Abelove grupe nisu algebarski kompaktne.*

**Dokaz.** Direktna posledica korolara 38.8 i prethodne tačke.

(*c*) *Ako je grupa* $\mathbf{A}$ *algebarski kompaktna, onda je i* $n\mathbf{A}$ *algebarski kompaktna grupa.*

**Dokaz.** Prema 38.5, $\mathbf{A}$ je direktni sumand kartezijanske sume kockičnih grupa $\sum^c \mathbf{C}_{p_\alpha^{k_\alpha}} \oplus \sum^c \mathbf{p}_\beta^\infty$; ne stavljamo (da ne komplikujemo notaciju) skup indeksa; jasno $p_\alpha$, $p_\beta$ su prosti brojevi (ne moraju svi biti prisutni) i moguće je da je $p_{\alpha_1} = p_{\alpha_2}$ za $\alpha_i \neq \alpha_2$, a isto tako i $k_{\alpha_1} = k_{\alpha_2}$ (za svaku eventualnost naglasimo da je $\mathbf{C}_{p_\alpha^{k_\alpha}}$ ciklična grupa reda $p_\alpha^{k_\alpha}$). Dakle, $\mathbf{A} \oplus \mathbf{B} = \sum^c \mathbf{C}_{p_\alpha^{k_\alpha}} \oplus \sum^c \mathbf{p}_\beta^\infty$, pa je $n(\mathbf{A} \oplus \mathbf{B}) = n(\sum^c \mathbf{C}_{p_\alpha^{k_\alpha}} \oplus \sum^c \mathbf{p}_\beta^\infty)$, odnosno $n\mathbf{A} \oplus n\mathbf{B} = \sum^c n\mathbf{C}_{p_\alpha^{k_\alpha}} \oplus \sum^c n\mathbf{p}_\beta^\infty$. No, ako je $n = q_1^{m_1} \cdots q_r^{m_r}$, $q_i$ prost broj, $m_i \geq 1$, $i = 1, \ldots, r$, i $p_\alpha \notin \{q_1, \ldots, q_r\}$, onda je $n\mathbf{C}_{p_\alpha^{k_\alpha}} = \mathbf{C}_{p_\alpha^{k_\alpha}}$, $n\mathbf{p}_\alpha^\infty = \mathbf{p}_\alpha^\infty$. Ako je npr. $p_\alpha = q_1$, tada je, za $k_\alpha \leq m_1$, $n\mathbf{C}_{p_\alpha^{k_\alpha}} = \mathbf{O}$, za $k_\alpha > m_1$, $n\mathbf{C}_{p_\alpha^{k_\alpha}} \cong \mathbf{C}_{p_\alpha^{k_\alpha - m_1}}$; slično je za $p_\beta \in \{q_1, \ldots, q_r\}$: za $p_\beta = q_1$ je $n\mathbf{q}_1^\infty = (q_2^{m_2} \cdots q_r^{m_r})q_1^{m_1}\mathbf{q}_1^\infty \cong \mathbf{q}_1^\infty$. Znači, i $n\mathbf{A}$ je direktni sumand kartezijanske sume kockičnih grupa, prema tome i algebarski kompaktna grupa.□

**Teorema 38.13** *Grupa* $\mathbf{A}$ *je algebarski kompaktna akko je direktni sumand svake grupe* $\mathbf{B}$ *koja je sadrži kao potpunu podgrupu i za koju je* $\mathbf{B/A}$ *izomorfna ili sa* $\mathbf{Ra}$ *ili sa nekom Prüferovom grupom* $\mathbf{p}^\infty$.

**Dokaz.** Pravac ($\Longrightarrow$) je deo definicije.

($\Longleftarrow$) Pretpostavimo da $\mathbf{A}$ ispunjava uslov (pravca ($\Longleftarrow$)). Neka je $\mathbf{A}$ potpuna podgrupa grupe $\mathbf{B}$ i neka je grupa $\mathbf{B/A}$ ranga 1. Ako je $\mathbf{B/A}$ ciklična grupa reda $p^k$ za neki prost broj $p$, onda je, prema 37.14, $\mathbf{A}$ i direktni sumand



grupe $\mathbf{B}$. Ako je $\mathbf{B/A}$ izomorfna bilo sa $\mathbf{Ra}$ bilo sa $\mathbf{p}^\infty$ (za neki prost broj $p$), $\mathbf{A}$ je prema datom uslovu direktni sumand. Ako je $\mathbf{B/A}$ izomorfna pravoj podgrupi grupe $\mathbf{Ra}$, onda prema 33.30 postoji podgrupa $\mathbf{C}$ takva da je $\mathbf{B} \leq \mathbf{C}$ i $\mathbf{C/A} \cong \mathbf{Ra}$. Proizilazi da je $\mathbf{A}$ potpuna podgrupa i grupe $\mathbf{C}$ (iz $a = nc$ za $a \in A$, $c \in C$ i $n > 0$, sledi: $A = n(c + A)$, pa je $c \in A$ – $\mathbf{C/A}$ je torziono slobodna grupa). Stoga je, opet prema uslovu, $\mathbf{A}$ direktni sumand grupe $\mathbf{C}$, a tada i grupe $\mathbf{B}$; ako je $\mathbf{C} = \mathbf{A} \oplus \mathbf{D}$, onda je $\mathbf{B} = \mathbf{A} \oplus (\mathbf{B} \cap \mathbf{D})$.

Neka je sada $\mathbf{B/A} = \overline{\mathbf{B}}$ proizvoljna grupa. Konstruisaćemo niz $\overline{\mathbf{B}}_0 \leq \overline{\mathbf{B}}_1 \leq \cdots \leq \overline{\mathbf{B}}_\alpha \leq \overline{\mathbf{B}}_{\alpha+1} \leq \cdots \leq \overline{\mathbf{B}}_\lambda = \overline{\mathbf{B}}$, gde je svaka podgrupa $\overline{\mathbf{B}}_\alpha$ potpuna podgrupa u $\overline{\mathbf{B}}$, $\overline{\mathbf{B}}_{\alpha+1}/\overline{\mathbf{B}}_\alpha$ je ranga 1 i za granični ordinal $\alpha$ je $\overline{\mathbf{B}}_\alpha = \bigcup_{\beta<\alpha} \overline{\mathbf{B}}_\beta$. Neka je $t(\overline{\mathbf{B}})$ periodični deo grupe $\overline{\mathbf{B}}$. Prema korolaru 37.27, $t(\overline{\mathbf{B}})$ sadrži kockičnu podgrupu kao direktni sumand; izaberimo jednu takvu i neka je to $\overline{\mathbf{B}}_1$. Ako je $\overline{\mathbf{B}}_1 \neq t(\overline{\mathbf{B}})$, faktor grupa $t(\overline{\mathbf{B}})/\overline{\mathbf{B}}_1$ je periodična nenula grupa i kao takva sadrži kockičnu grupu $\overline{\mathbf{B}}_2/\overline{\mathbf{B}}_1$ kao direktni sumand. Prema 37.12(*b*), $\overline{\mathbf{B}}_2$ je potpuna podgrupa grupe $t(\overline{\mathbf{B}})$, stoga i grupe $\overline{\mathbf{B}}$ (zbog tranzitivnosti svojstva "biti potpuna podgrupa"). Postupak nastavljamo dok ne dostignemo grupu $t(\overline{\mathbf{B}})$, s tim što za granične ordinale ($\gamma$) uzimamo: $\overline{\mathbf{B}}_\gamma = \bigcup_{\delta<\gamma} \overline{\mathbf{B}}_\delta$. Neka je $t(\overline{\mathbf{B}}) = \overline{\mathbf{B}}_\mu$. Ako je $\overline{\mathbf{B}}_\mu \neq \overline{\mathbf{B}}$, faktor grupa $\overline{\mathbf{B}}/\overline{\mathbf{B}}_\mu$ je torziono slobodna grupa. Ako je $\overline{B}_\mu \neq b + \overline{B}_\mu \in \overline{B}/\overline{B}_\mu$, onda prema korolaru 37.9 postoji minimalna potpuna podgrupa $\overline{\mathbf{B}}_{\mu+1}/\overline{\mathbf{B}}_\mu$ grupe $\overline{\mathbf{B}}/\overline{\mathbf{B}}_\mu$ koja sadrži cikličnu grupu $\langle b + \overline{B}_\mu \rangle$. Prema istom korolaru, $\overline{\mathbf{B}}_{\mu+1}/\overline{\mathbf{B}}_\mu$ je ranga 1 (za svaki element $c + \overline{B}_\mu \in \overline{B}_{\mu+1}/\overline{B}_\mu$ postoji nenula ceo broj $k$ takav da je $k(c + \overline{B}_\mu) \in \langle b + \overline{B}_\mu \rangle$). $\overline{\mathbf{B}}_{\mu+1}$ je, ponovo prema 37.12(*b*), potpuna podgrupa grupe $\overline{\mathbf{B}}$. Ukoliko je $\overline{\mathbf{B}}_{\mu+1} \neq \overline{\mathbf{B}}$, postupak ponavljamo (primetimo da je $\overline{\mathbf{B}}/\overline{\mathbf{B}}_{\mu+1}$ torziono slobodna grupa ali to, u opštem, nije bitno za ovo razmatranje, jer imamo na raspolaganju 37.27). U slučajevima graničnih ordinala ($\gamma$) uzimamo, kao i ranije, $\overline{\mathbf{B}}_\gamma = \bigcup_{\delta<\gamma} \overline{\mathbf{B}}_\delta$. Za odgovarajući niz $\mathbf{A} = \mathbf{B}_0 \leq \mathbf{B}_1 \leq \cdots \leq \mathbf{B}_\alpha \leq \mathbf{B}_{\alpha+1} \leq \cdots \leq \mathbf{B}_\lambda = \mathbf{B}$ takođe važi: za svako $\alpha$ je $\mathbf{B}_\alpha$ potpuna podgrupe grupe $\mathbf{B}$ (37.14) i $\mathbf{B}_{\alpha+1}/\mathbf{B}_\alpha$ je ranga 1 ($\mathbf{B}_{\alpha+1}/\mathbf{B}_\alpha \cong \overline{\mathbf{B}}_{\alpha+1}/\overline{\mathbf{B}}_\alpha$). Prema prvom delu dokaza je $\mathbf{B}_1 = \mathbf{A} \oplus \mathbf{C}_0$ (= $\mathbf{B}_0 \oplus \mathbf{C}_0$) za neku podgrupu $\mathbf{C}_0$ grupe $\mathbf{B}_1$. Indukcijom pokazujemo da je $\mathbf{A}$ direktni sumand svake grupe $\mathbf{B}_\alpha$. Pretpostavimo da je tvrđenje tačno za svako $\beta < \gamma$: $\mathbf{B}_\beta = \mathbf{A} \oplus \mathbf{C}_\beta$. Ako je $\gamma = \delta + 1$, onda je $\mathbf{B}_\delta = \mathbf{A} \oplus \mathbf{C}_\delta$ potpuna podgrupa grupe $\mathbf{B}_\gamma$, pa je prema 37.12(a) ($\mathbf{A} \cong$) $\mathbf{B}_\delta/\mathbf{C}_\delta$ potpuna podgrupa grupe $\mathbf{B}_\gamma/\mathbf{C}_\delta$. Grupa $(\mathbf{B}_\gamma/\mathbf{C}_\delta)/(\mathbf{B}_\delta/\mathbf{C}_\delta) \cong \mathbf{B}_\gamma/\mathbf{B}_\delta$ je ranga 1 i stoga je, prema pokazanom, $\mathbf{B}_\delta/\mathbf{C}_\delta$ direktni sumand grupe $\mathbf{B}_\gamma/\mathbf{C}_\delta$. Neka je $\mathbf{B}_\gamma/\mathbf{C}_\delta = \mathbf{B}_\delta/\mathbf{C}_\delta \oplus \mathbf{C}_\gamma/\mathbf{C}_\delta$. Kako je $\langle A, C_\gamma \rangle = \langle A, C_\delta, C_\gamma \rangle = \langle B_\delta, C_\gamma \rangle = \mathbf{B}_\gamma$ i $\mathbf{A} \cap \mathbf{C}_\gamma = \mathbf{A} \cap \mathbf{B}_\delta \cap \mathbf{C}_\gamma = \mathbf{A} \cap \mathbf{C}_\delta = \mathbf{O}$, to je $\mathbf{B}_\gamma = \mathbf{A} \oplus \mathbf{C}_\gamma$, gde je $\mathbf{C}_\delta \leq \mathbf{C}_\gamma$. Ako je $\gamma$ granični ordinal, neka je $\mathbf{C}_\gamma = \bigcup_{\beta<\gamma} \mathbf{C}_\beta$ ($\langle \{\mathbf{C}_\beta \mid \beta < \gamma\}, \leq \rangle$ je, prema upravo datoj napomeni, lanac). Tada je $\mathbf{B}_\gamma = \bigcup_{\beta<\gamma} \mathbf{B}_\beta = \bigcup_{\beta<\gamma} (\mathbf{A} \oplus \mathbf{C}_\beta) = \mathbf{A} \oplus \bigcup_{\beta<\gamma} \mathbf{C}_\beta = \mathbf{A} \oplus \mathbf{C}_\gamma$.■

## 39 Bazične podgrupe $p$-grupa

Primarne Abelove grupe koje su direktne sume cikličnih grupa, jasno, bez elemenata su beskonačne visine. Za prebrojive primarne Abelove grupe važi i obrat ovog trvđenja (druga teorema Prüfera – 35.5). Kontraprimer dat uz ovu teoremu pokazuje da generalno uzev implikaciju u tom, suprotnom, pravcu, nemamo. Dalje razmatranje primarnih Abelovih grupa bez elemenata beskonačne visine započinjemo upoznavanjem sa bazičnim podgrupama.

**Definicija 39.1** *Sistem elemanata $\{a_i \mid i \in I\}$ grupe $\mathbf{A}$ je potpuno slabo linearno nezavisan akko je slabo linearno nezavisan i grupa $\sum_{i\in I}\langle a_i\rangle$ je potpuna podgrupa grupe $\mathbf{A}$.*

Prema lemi Zorna uvek postoji maksimalan potpuno slabo linearno nezavisan sistem; jer, ako je $\{\mathcal{S}_\alpha \mid \alpha < \lambda\}$ lanac potpunih slabo linearno nezavisnih sistema, onda je to, evidentno, i $\bigcup_{\alpha<\lambda}\mathcal{S}_\alpha$ (primetimo da je prazan skup potpuno slabo linearno nezavisan). Analognim rezonovanjem zaključujemo i da je svaki potpuno slabo linearno nezavisan sistem sadržan u nekom maksimalnom takvom. Za maksimalnost potpuno linearno nezavisnog sistema $p$-grupe postoji sledeći kriterijum:

**Lema 39.2** *Potpuni slabo linearno nezavisan sistem $\mathcal{S} = \{a_i \mid i \in I\}$ $p$-grupe $\mathbf{A}$ je maksimalan (potpuno linearno nezavisan) akko je faktor grupa $\mathbf{A}/\langle\mathcal{S}\rangle$ deljiva.*

**Dokaz.** ($\Longrightarrow$) Pretpostavimo da je $\mathcal{S}$ potpuni maksimalan slabo linearno nezavisan sistem $p$-grupe $\mathbf{A}$, ali da faktor grupa $\overline{\mathbf{A}} = \mathbf{A}/\langle\mathcal{S}\rangle$ nije deljiva, dakle, ni nula grupa. Onda, prema 33.3, postoji neki njen element reda $p$ konačne visine, pa prema 37.26 postoji i njen direktni sumand koji je ujedno i ciklična grupa. Neka je to $\overline{\mathbf{B}} = \langle b + \langle\mathcal{S}\rangle\rangle$. Sledi dalje, prema 37.14, da je $\langle\mathcal{S}\rangle$ direktni sumand (pod)grupe $\langle\{b\}\cup\mathcal{S}\rangle$ $(= \mathbf{B})$, te je $\mathbf{B} = \langle\mathcal{S}\rangle \oplus \langle b^*\rangle$, gde je $b^* \in b+\langle\mathcal{S}\rangle$; jasno, $\mathbf{B}/\langle\mathcal{S}\rangle = \overline{\mathbf{B}}$. Kako je $\overline{\mathbf{B}}$ potpuna podgrupa grupe $\overline{\mathbf{A}}$, to je i $\mathbf{B}$ potpuna podgrupa grupe $\mathbf{A}$ (37.12($b$)). No, onda je $\mathcal{S}\cup\{b^*\}$ takođe potpuno linearno nezavisan sistem, protivno pretpostavci o maksimalnosti sistema $\mathcal{S}$.

($\Longleftarrow$) Neka je $\overline{\mathbf{A}} = \mathbf{A}/\langle\mathcal{S}\rangle$ deljiva grupa i neka je $\mathcal{S}\cup\{a\}$, $a \notin \mathcal{S}$, slabo linearno nezavisan sistem. Ali tada podgrupa $\langle\mathcal{S}\cup\{a\}\rangle$ nije potpuna. Zaista, jednačina ($\langle\mathcal{S}\rangle \neq$) $a+\langle\mathcal{S}\rangle = p(x+\langle\mathcal{S}\rangle) = px+\langle\mathcal{S}\rangle$ je rešiva u $\overline{\mathbf{A}}$, znači, za neko $b \in A$ i neko $c \in \langle\mathcal{S}\rangle$ je $a - c = pb$, dok jednačina $a - c = px$ nema rešenje u $\langle\mathcal{S}\cup\{a\}\rangle = \langle\mathcal{S}\rangle \oplus \langle a\rangle$ (jednačina $a = px$ nema rešenja u $p$-cikličnoj grupi $\langle a\rangle$ – pretpostavljeno rešenje bi takođe bilo generatorni element; videti 7.2($f$)).□

**Definicija 39.3** *Podgrupa $\mathbf{B}$ primarne grupe $\mathbf{A}$ je bazična akko važi:* (1) $\mathbf{B}$ *je potpuna podgrupa,* (2) $\mathbf{B}$ *je direktna suma cikličnih grupa i* (3) $\mathbf{A}/\mathbf{B}$ *je deljiva grupa.*



**Korolar 39.4** *Svaka $p$-grupa sadrži (bar jednu) bazičnu podgrupu.*

**Dokaz.** Direktna posledica prethodne leme – egzistenciju maksimalnog potpunog slabo linearno nezavisnog sistema garantuje, rekli smo, lema Zorna.□

**Primer 39.5** ($a$) *Jedina bazična podgrupa $p$-deljive grupe je nula grupa.*

**Dokaz.** Potpuna podgrupa deljive grupe je i sama deljiva, u deljivoj $p$-grupi su svi elementi beskonačne visine, dok, kako smo već naglasili, direktna suma $p$-cikličnih grupa je bez elemenata beskonačne visine.

($b$) *Ako je $\mathbf{A}$ direktna suma $p$-cikličnih grupa, onda je i svoja bazična podgrupa, i to jedina u slučaju da su visine elemenata ograničene.*

**Dokaz.** Pretpostavimo da je $p^n\mathbf{A} = \mathbf{O}$ za neko $n \in N$ i da je $\mathbf{B}$ prava bazična podgrupa grupe $\mathbf{A}$. No tada je $\mathbf{A}/\mathbf{B}$ deljiva ograničena nenula podgrupa, kontradikcija (ponavljamo: u deljivoj grupi su svi elementi beskonačne visine).

($c$) *Ako je $\mathbf{A} = \sum_{k\in N}\mathbf{Z}_{p^{n_k}}$, $n_1 < n_2 < \cdots$, onda grupa $\mathbf{A}$ ima pravu bazičnu podgrupu.*

**Dokaz.** Videti dokaz leme 37.13. Jedna prava bazična podgrupa je, prema notaciji iz te leme, baš data potpuna podgrupa $\mathbf{B}$. Već smo videli da je $\mathbf{A}/\mathbf{B}$ Prüferova grupa, a provera da je generatorni sistem elemenata grupe $\mathbf{B}$ – $\{b_n \mid n \in N\}$ (gde je, podsećamo, $b_n = 1_n - p^{k_{n+1}-k_n}1_{n+1}$) – slabo linearno nezavisan analogna je proveri da svaki element iz $\mathbf{B}$ ima istu visinu i u $\mathbf{A}$ i u $\mathbf{B}$.□

Generalno se definicija 39.3 daje sa:

*Podgrupa $\mathbf{B}$ grupe $\mathbf{A}$ je, za dati prost broj $p$, $p$-bazična akko je ispunjeno:* (1) $\mathbf{B}$ *je potpuna podgrupa,* (2) $\mathbf{B}$ *je direktna suma beskonačnih i $p$-cikličnih grupa i* (3) $\mathbf{A}/\mathbf{B}$ *je $p$-deljiva grupa.*

Ali, ako je $\mathbf{A}$ $p$-grupa, onda je njena jedina $q$-bazična podgrupa, za $q \neq p$ ($q$ – prost broj), nula podgrupa. Prema tome, jedine od interesa $q$-bazične podgrupe $p$-grupe su baš $p$-bazične podgrupe, te smo, u tom smislu, tako odmah i definisali bazičnu podgrupu ($p$-grupe).

**Teorema 39.6** *Neka je podgrupa $\mathbf{B}$ $p$-grupe $\mathbf{A}$ direktna suma cikličnih grupa: $\mathbf{B} = \sum_{n\in N}\mathbf{B}_n$, gde je $\mathbf{B}_n$ direktna suma cikličnih grupa reda $p^n$. Tada je $\mathbf{B}$ bazična podgrupa grupe $\mathbf{A}$ akko je, za svako $n \in N$, $\mathbf{A} = \mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n \oplus \langle B_n^* \cup p^n A\rangle$, gde je $\mathbf{B}_n^* = \sum_{k>n}\mathbf{B}_k$.*

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{B}$ bazična podgrupa. Fiksirajmo prirodan (nenula) broj $n$. Pošto je $\mathbf{A}/\mathbf{B}$ deljiva grupa, za svako $a$ iz $A$ postoji rešenje jednačine $a + B = p^n(x + B)$. Ako je jedno rešenje $c + B$, tada je, za neko $b \in B$, $a = p^n c + b$, pa je $B\cup p^n A$ generatorni skup grupe $\mathbf{A}$. Pretpostavimo dalje da

je $c$ u preseku podgrupa $\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n$ i $\langle B_n^* \cup p^n A\rangle$. Ako bismo pretpostavili da je $c \neq 0$, imali bismo: $c = b_1 + \cdots + b_n = b + p^n d$, gde je $b_i \in B_i$, $b \in B_n^*$, $d \in A$, i gde je, za bar jedno $i$, $1 \leq i \leq n$, $b_i$ različito od nule. Sada je $0 \neq p^n d = (b_1 + \cdots + b_n) - b \in B$ (inače, direktno sledi $c = 0$) i kako je $\mathbf{B}$ potpuna podgrupa, to je, za neko $b' \in B$, $0 \neq p^n b' = (b_1 + \cdots + b_n) - b$. Prema tome, $b' \in B_n^*$ i $0 \neq b_1 + \cdots + b_n = b + p^n b' \in (B_1 + \cdots + B_n) \cap B_n^*$, kontradikcija.

($\Longleftarrow$) Neka je ispunjen uslov pravca ($\Longleftarrow$). Već nam je dato da je $\mathbf{B}$ direktna suma cikličnih grupa. Podgrupe $\mathbf{G}_n = \mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n$, $n \in N$, su potpune podgrupe grupe $\mathbf{A}$ (kao direktni sumandi) te je i $\mathbf{B} = \bigcup_{n\in N} \mathbf{G}_n$ potpuna podgrupa. Posmatrajmo, konačno, jednačinu $a + B = p^n(x + B)$, $n \geq 1$. Kako je $\mathbf{A} = (\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n) \oplus (\mathbf{B}_n^* + p^n\mathbf{A})$ $(= \mathbf{G}_n \oplus (\mathbf{B}_n^* + p^n\mathbf{A}))$, to je $a = b' + b'' + p^n c$ za neko $b' \in G_n$, $b'' \in B_n^*$, $c \in A$. Sledi: $a + B = p^n c + B = p^n(c + B)$.■

**Korolar 39.7** *Ako je* $\mathbf{B}$ *bazična podgrupa p-grupe* $\mathbf{A}$, *tada je* $\mathbf{A} = \mathbf{B} + p^n\mathbf{A}$ *za svaki prirodan broj* $n$.

**Korolar 39.8** *Neka je, kao u prethodnoj teoremi,* $\mathbf{B} = \sum_{n\in N} \mathbf{B}_n$ *podgrupa p-grupe* $\mathbf{A}$. $\mathbf{B}$ *je bazična akko je* $(p^n\mathbf{A})[p] = \mathbf{B}_{n+1}[p] \oplus (p^{n+1}\mathbf{A})[p]$ *za svako* $n \in \omega$.

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{B}$ bazična podgrupa. Onda je $p^n(B_n^* + p^n A) = p^n A$. Slučaj $n = 0$ je trivijalan. Neka je zato $n > 0$. Naravno, samo je relacija $\geq$ u pitanju. Pretpostavimo da $p^n a \notin p^n(B_n^* + p^n A)$ za neko $a \in A$. Tada $p^n a \notin B$, jer je $\mathbf{B}$ potpuna podgrupa ($p^n a \in B$ bi dalo $p^n a = p^n b$ za neko $b \in B$ i, jasno, $b \in B_n^*$). No, $\mathbf{A}/\mathbf{B}$ je deljiva grupa, pa je jednačina $(B \neq )$ $p^n a + B = p^{2n}(x + B)$ rešiva u njoj. Neka je $p^n a + B = p^{2n}(a' + B)$ za $a' \in A$. Odatle je $p^n a = p^{2n} a' + b'$ za neko $b' \in B$, pa je, s obzirom na potpunost podgrupe $\mathbf{B}$, $b' = p^n b''$ za neko $b'' \in B$. Stoga je $p^n a = p^n(b'' + p^n a') \in p^n(B_n^* + p^n A)$ (za svako $b \in B$ je $p^n b \in B_n^*$), kontradikcija. Sledi: $(p^n A)[p] = (p^n(B_n^* + p^n A))[p] \subseteq (B_n^* + p^n A)[p]$. Zapravo, važi jednakost. Jer, neka je $a = b^* + p^n a'$, $b^* \in B_n^*$, $a' \in A$, element reda $p$ i visine $k < n$. Tada je i $h(b^*) = k$. Ali, zbog $pa = pb^* + p^{n+1}a' = 0$, $h(pb^*) \geq n + 1$, kontradikcija; imamo u vidu da je $b^*$ element direktne sume cikličnih grupa reda većeg od ili jednakog $p^{n+1}$ i da je $\mathbf{B}$ potpuna podgrupa. Preostaje još da se pozovemo na: $\mathbf{B}_n^* + p^n\mathbf{A} = \mathbf{B}_{n+1} \oplus (\mathbf{B}_{n+1}^* + p^{n+1}\mathbf{A})$ (inkluzija $\geq$ je očigledna, a $\leq$ je posledica prethodne teoreme), kao i na to da je $(\mathbf{B}_{n+1}^* + p^{n+1}\mathbf{A})[p] = (p^{n+1}\mathbf{A})[p]$; jer, ako je, za $b \in B_{n+1}^*$ i $a \in A$, $p(b + p^{n+1}a) = 0$, tj. $pb = p^{n+2}(-a)$, onda je, zbog potpunosti grupe $\mathbf{B}_{n+1}^*$, za neko $b' \in B_{n+1}^*$, $pb = p^{n+2}b'$, te je $p(b - p^{n+1}b') = 0$, $b - p^{n+1}b' \in B_{n+1}^*[p] \subseteq (p^{n+1}A)[p]$ i $b + p^{n+1}a \in p^{n+1}A$.

($\Longleftarrow$) Neka je $(p^n A)[p] = B_{n+1}[p] \oplus (p^{n+1}A)[p]$ za svako $n \in \omega$ i neka je $\mathbf{B}_{n+1} = \sum_{\alpha<\lambda_{n+1}} \langle a_\alpha\rangle$. Tada je $\mathbf{B}_{n+1}[p] = \sum_{\alpha<\lambda_{n+1}} \langle p^n a_\alpha\rangle$. Jasno, za svako



$a \in B_{n+1}[p] \setminus \{0\}$, $a = p^n r_1 a_{\alpha_1} + \cdots + p^n r_k a_{\alpha_k}$, $(p_i, r_i) = 1$, $\alpha_i \in \lambda_{n+1}$, važi: $h_{\mathbf{B}}(a) = n = h_{\mathbf{B}}(p^n r_i a_{\alpha_i})$ za svako $i = 1, \ldots, k$. Pretpostavka da je $a = p^{n+1}c$ za neko $c \in A$ dala bi $a \in B_{n+1}[p] \cap (p^{n+1}A)[p] = \{0\}$, kontradikcija. Sledi da je, uopšte, za $b' \in B[p] \setminus \{0\}$, $b' = b_{n_1} + \cdots + b_{n_t}$, $b_{n_i} \in B_{n_i}[p]$, $n_1 < \cdots < n_t$, $h_{\mathbf{B}}(b') = n_1 = h_{\mathbf{B}}(b_{n_1})$ $(= h(b_{n_1}))$. Iz $b' = p^{n_1+1}c'$ za neko $c' \in A$ proizašlo bi: $b_{n_1} = p^{n_1+1}c' - (b_{n_2} + \cdots + b_{n_t})$, odnosno $h(b_{n_1}) \geq n_1 + 1$, protivurečnost ponovo. Dakle, svaki element iz $B[p]$ ima istu visinu i u $\mathbf{A}$ i u $\mathbf{B}$, pa je $\mathbf{B}$ potpuna podgrupa grupe $\mathbf{A}$ (37.6). Pokažimo, konačno, da je $\mathbf{A}/\mathbf{B}$ deljiva grupa. Ako je $\mathbf{B} = \mathbf{A}$ gotovi smo. Uzmimo zato da je $\mathbf{A}/\mathbf{B}$ nenula grupa. Prema 33.3 dovoljno je pokazati da su elementi najnižeg sloja beskonačne visine. Neka je $B \neq a + B \in (A/B)[p]$. Zbog potpunosti podgrupe $\mathbf{B}$ možemo pretpostaviti da je $a$ reda $p$. Posmatrajmo jednačinu $a + B = p^n(x + B)$, $n \geq 1$. No, $a \in A[p] = B_1[p] \oplus (pA)[p] = B_1[p] \oplus B_2[p] \oplus (p^2A)[p] = \cdots = B_1[p] \oplus \cdots \oplus B_n[p] \oplus (p^nA)[p]$ implicira: za neko $b \in B_1[p] \oplus \cdots \oplus B_n[p]$ i neko $a' \in (p^nA)[p]$ je $a = b + a'$ ($a' \neq 0$ jer $a \notin B$), i kako je $a' = p^n a''$ za neko $a'' \in A$, imamo $a + B = (b + p^n a'') + B = p^n a'' + B = p^n(a'' + B)$.□

**Korolar 39.9** *Neka je opet kao u prethodnoj teoremi,* $\mathbf{B} = \sum_{n\in N} \mathbf{B}_n$ *podgrupa grupe* $\mathbf{A}$. $\mathbf{B}$ *je bazična akko je, za svako* $n \in N$, $\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n$ *maksimalni* $p^n$*-ograničeni direktni sumand grupe* $\mathbf{A}$.

**Dokaz.** Naravno, pod $p^n$-ograničenom podgrupom $\mathbf{C}$ grupe $\mathbf{A}$ podrazumevamo podgrupu $\mathbf{C}$ za koju je $p^n\mathbf{C} = \mathbf{O}$.

($\Longrightarrow$) Neka je $\mathbf{B}$ bazična podgrupa i pretpostavimo da je, za neko $n \in N$, $\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n$ strogo sadržano u nekom $p^n$-ograničenom direktnom sumandu $\mathbf{C}$ grupe $\mathbf{A}$; $\mathbf{A} = \mathbf{C} \oplus \mathbf{D}$. Onda je, zbog $\mathbf{A} = (\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n) \oplus (\mathbf{B}_n^* + p^n\mathbf{A})$, $\mathbf{C} = (\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n) \oplus (\mathbf{C} \cap (\mathbf{B}_n^* + p^n\mathbf{A}))$, pa je $\mathbf{A} = (\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n) \oplus (\mathbf{C} \cap (\mathbf{B}_n^* + p^n\mathbf{A})) \oplus \mathbf{D}$. Kako je $\mathbf{B}_n^* + p^n\mathbf{A} \cong (\mathbf{C} \cap (\mathbf{B}_n^* + p^n\mathbf{A})) \oplus \mathbf{D}$ $(\cong \mathbf{A}/(\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n))$, proizilazi da $\mathbf{B}_n^* + p^n\mathbf{A}$ ima nenula $p^n$-ograničeni direktni sumand. No, svaki nenula element reda $p$ tog sumanda bio bi, s jedne strane, visine veće od ili jednake $n$, a s druge, visine manje od $n$ (zbog $p^n$ ograničenosti sumanda), kontradikcija.

($\Longleftarrow$) Neka su ispunjeni uslovi pravca ($\Longleftarrow$). Tačke (1) i (2) definicije (bazične podgrupe) trivijalno su ispunjeni (grupe $\mathbf{G}_n = \mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n$, $n \in N$, su potpune, pa je to i njihova unija: $\mathbf{B} = \bigcup_{n\in N} \mathbf{G}_n$). Pretpostavimo da grupa $\overline{\mathbf{A}} = \mathbf{A}/\mathbf{B}$ nije deljiva. Rezonujući kao u 39.2 zaključujemo da $\overline{\mathbf{A}}$ sadrži kao direktni sumand cikličnu podgrupu reda, recimo, $p^m$. Neka je to $\langle a + B\rangle$ $(= \langle\{a\} \cup B\rangle/\mathbf{B})$ i neka je $\mathbf{C} = \langle\{a\} \cup B\rangle = \mathbf{B} \oplus \langle a^*\rangle$, gde je $a^* \in a + B$ (37.14). $a^*$ je reda $p^m$, jer je $\mathbf{C}/\mathbf{B} = (\mathbf{B} \oplus \langle a^*\rangle)/\mathbf{B} \cong \langle a^*\rangle$. $\mathbf{C}$ je potpuna podgrupa grupe $\mathbf{A}$ (37.12($b$)), te je to i $\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_m \oplus \langle a^*\rangle$ (kao direktni sumand podgrupe $\mathbf{C}$). Prema 37.18 sledi da je $\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_m \oplus \langle a^*\rangle$ $p^m$-ograničnI direktni sumand grupe $\mathbf{A}$, protivno pretpostavci o $\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_m$ kao maksimalnom takvom.□

**Korolar 39.10** *Neka je* $\mathbf{A}$ *periodični deo kartezijanske sume p-grupa* $\mathbf{A}_i$, $i \in I$ $(\mathbf{A} = t(\sum_{i\in I}^{c} \mathbf{A}_i))$ *i neka je, za svako* $i \in I$, $\mathbf{B}_i = \sum_{n\in N} \mathbf{B}_{in}$, *gde je* $\mathbf{B}_{in} \cong \sum \mathbf{C}_{p^n}$ *(direktna suma cikličnih grupa reda* $p^n$*), bazična podgrupa grupe* $\mathbf{A}_i$. *Tada je* $\sum_{n\in N}(\sum_{i\in I}^{c} \mathbf{B}_{in})$ *bazična podgrupa grupe* $\mathbf{A}$.

**Dokaz.** Prema 39.6 je, za svako $i \in I$ i svako $n \in N$, $\mathbf{A}_i = \mathbf{B}_{i1} \oplus \cdots \oplus \mathbf{B}_{in} \oplus (\mathbf{B}_{in}^{*} + p^n\mathbf{A}_i)$, a prema prethodnom korolaru $\mathbf{B}_{in}^{*} + p^n\mathbf{A}_i$ nema direktnih cikličnih sumanada reda manjeg od ili jednakog $p^n$. Očigledno, $\mathbf{A} = \sum_{i\in I}^{c} \mathbf{B}_{i1} \oplus \cdots \oplus \sum_{i\in I}^{c} \mathbf{B}_{in} \oplus t(\sum_{i\in I}^{c}(\mathbf{B}_{in}^{*} + p^n\mathbf{A}_i))$ (koristimo, što se lako proverava: ako je skup redova familija grupa $\mathbf{H}_i$, $i \in I$, ograničen, onda je $t(\sum_{i\in I}^{c}(\mathbf{H}_i \oplus \mathbf{K}_i)) = \sum_{i\in I}^{c} \mathbf{H}_i \oplus t(\sum_{i\in I}^{c} \mathbf{K}_i)$), i isto tako očigledno, $t(\sum_{i\in I}^{c}(\mathbf{B}_{in}^{*} + p^n\mathbf{A}_i))$ nema cikličnih sumanada reda manjeg od ili jednakog $p^n$ (dakle, ni direktnih $p^n$-ograničenih sumanada); jer, pretpostavimo: $t(\sum_{i\in I}^{c}(\mathbf{B}_{in}^{*} + p^n\mathbf{A}_i)) = \mathbf{G} \oplus \mathbf{H}$, gde je $\mathbf{G} = \langle g\rangle \cong \mathbf{C}_{p^m}$, $m \leq n$. Jasno, $\mathbf{G}$ je onda potpuna podgrupa grupe $\mathbf{A}$, a $p^{m-1}g = \langle b_i^{*} + p^n a_i\rangle_{i\in I}$, $b_i \in B_{in}^{*}$, $a_i \in A_i$, njen element reda $p$, bio bi, s jedne strane, visine veće od ili jednake $n$ (svaka njegova komponenta je deljiva sa $p^n$; ovo tvrđenje se bazira na činjenicama da je u direktnoj sumi visina elemenata jednaka minimalnoj visini komponenata i da je u cikličnoj grupi $\mathbf{Z}_{p^k} = \langle p^k, +_{p^k}\rangle$ element $r$ visine $m$ $(< k)$ akko $p^m | r)$, a s druge strane (u grupi $\mathbf{G}$, dakle i u $\mathbf{A}$) visine manje od $m$, kontradikcija.□

**Korolar 39.11** *Podgrupa* $\mathbf{G}$ *p-grupe* $\mathbf{A}$ *je sadržana u nekoj bazičnoj podgrupi* $\mathbf{B}$ *akko je* $\mathbf{G}$ *unija lanca podgrupa,* $\mathbf{G}_n$, $n \in N$, *gde su visine elemenata (u* $\mathbf{A}$*) svake od podgrupe lanca ograničene.*

**Dokaz.** $(\Longrightarrow)$ Neka je $\mathbf{G} \leq \mathbf{B}$, gde je $\mathbf{B} = \sum_{n\in N} \mathbf{B}_n$ bazična podgrupa grupe $\mathbf{A}$ ($\mathbf{B}_n$ je, kao i ranije, direktna suma cikličnih grupa reda $p^n$). Ako je, za $n \in N$, $\mathbf{G}_n = \mathbf{G} \cap (\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n)$, jasno, $\mathbf{G} = \mathbf{G} \cap \mathbf{B} = \bigcup_{n\in N} \mathbf{G}_n$ i visine elemenata svake podgrupe $\mathbf{G}_n$ su ograničene $(< n)$, jer je $\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n$ potpuna podgrupa grupe $\mathbf{A}$ (kao direktni sumand potpune podgrupe $\mathbf{B}$ grupe $\mathbf{A}$) i stoga je, za $g \in G_n$, $h_{\mathbf{A}}(g) = h_{\mathbf{B}_1\oplus\cdots\oplus\mathbf{B}_n}(g)$.

$(\Longleftarrow)$ Neka je za lanac podgrupa $\mathbf{G}_n$, $n \in N$, gde su visine elemenata (u $\mathbf{A}$) svake od podgrupa $\mathbf{G}_n$ ograničene, $\mathbf{G} = \bigcup_{n\in N} \mathbf{G}_n$. Zapravo, možemo odmah pretpostaviti da je, za $n \in N$, $max\{h(g) \mid g \in G_n \setminus \{0\}\} < n$, tj. da je $\mathbf{G}_n \cap p^n\mathbf{A} = \mathbf{O}$. (U suprotnom, ukoliko taj uslov ne bi bio odmah ispunjen, formirali bismo novi lanac podgrupa – $\mathbf{H}_n$, $n \in N$, adekvatnim "ubacivanjem" nule podgrupe ili ponavljanjem članova niza.) Posmatrajmo sve lance podgrupa $(\mathbf{D}_n)_{n\in N}$ koji ispunjavaju uslov: za svako $n \in N$ je $\mathbf{G}_n \leq \mathbf{D}_n$ i $\mathbf{D}_n \cap p^n\mathbf{A} = \mathbf{O}$ (jedan takav je sam lanac $(\mathbf{G}_n)_{n\in N}$). Familiju svih takvih lanaca uredimo relacijom $\preceq$ na sledeći način: $(\mathbf{D}_n)_{n\in N} \preceq (\mathbf{H}_n)_{n\in N}$ akko je $\mathbf{D}_n \leq \mathbf{H}_n$ za svako $n \in N$. Evidentno, ispunjen je uslov leme Zorna, pa postoji (bar) jedan maksimalan lanac (s obzirom na dato uređenje) – neka je to $(\mathbf{B}_n)_{n\in N}$. Tvrdimo da je $\mathbf{B} = \bigcup_{n\in N} \mathbf{B}_n$ bazična podgrupa grupe $\mathbf{A}$.



Pokazaćemo prvo da je $\mathbf{B}_n$ $p^n\mathbf{A}$-visoka podgrupa za svako $n \in N$ (30.15). Pretpostavimo suprotno. Neka je $k$ najmanji pozitivan prirodan broj takav da postoji $a$ u $A \setminus B_k$ za koje je $pa \in B_k$ i $\langle B_k \cup \{a\}\rangle \cap p^k\mathbf{A} = \mathbf{O}$ (na umu nam je: ako $a' \notin B_k$, $\langle B_k \cup \{a'\}\rangle \cap p^k\mathbf{A} = \mathbf{O}$ i $p^r$, $r > 1$, je najmanji stepen broja $p$ za koji je $p^r a' \in B_k$ – $\mathbf{A}/\mathbf{B}_k$ je $p$-grupa, onda za $a$ možemo uzeti $p^{r-1}a'$). S obzirom na maksimalnost lanca $(\mathbf{B}_n)_{n\in N}$ mora biti $\langle B_n \cup \{a\}\rangle \cap p^n\mathbf{A} \neq \mathbf{O}$ za neko $n \geq k+1$. Neka je $m$ $(\geq k+1)$ najmanji prirodan broj za koji to važi. Prema tome je, za neko $b_m \in B_m$ i neko $c \in A$, $b_m + a = p^m c \neq 0$ (ako bismo krenuli od $b'_m + sa = p^m c' \neq 0$, gde je $b'_m \in B_m$, $c' \in A$ i $0 < s < p$, onda bismo za cele brojeve $u$ i $v$ takve da je $us + vp = 1$ izveli: $ub'_m + (us)a = p^m(uc')$, tj. $ub'_m + a - (vp)a = p^m(uc')$, pa stavili: $b_m = ub'_m - v(pa) \in B_m$, $c = uc' \in A$; naravno, zbog $p^m c' \neq 0$ i $(u,p) = 1$, i $p^m uc' \neq 0$). Odatle, $pb_m + pa = p^{m+1}c \in B_m \cap p^m A = \{0\}$, odnosno $pb_m = -pa \in B_k$. Jasno, $b_m \notin B_k$ – u suprotnom bismo imali: $0 \neq b_m + a = p^m c \in \langle B_k \cup \{a\}\rangle \cap p^k A = \{0\}$, kontradikcija. Neka je $t$, $1 < t \leq m - k$, najmanji broj za koji je $b_m \in B_{k+t} \setminus B_{k+t-1}$. Opet zbog maksimalnosti lanca $(\mathbf{B}_n)_{n\in N}$, $\mathbf{B}_{k+t-1}$ je maksimalna podgrupa grupe $\mathbf{B}_{k+t}$ sa svojstvom: $\mathbf{B}_{k+t-1} \cap p^{k+t-1}\mathbf{A} = \mathbf{O}$, pa je $\langle B_{k+t-1} \cup \{b_m\}\rangle \cap p^{k+t-1}\mathbf{A} \neq \mathbf{O}$. Rezonujući kao maločas zaključujemo: za neko $b_{k+t-1} \in B_{k+t-1}$ i neko $d \in A$ je $b_{k+t-1} + b_m = p^{k+t-1}d$, što sa $b_m + a = p^m c$ daje $a - b_{k+t-1} = p^m c - p^{k+t-1}d \in \langle B_{k+t-1} \cup \{a\}\rangle \cap p^{k+t-1}A = \{0\}$ (zbog $k + t - 1 < m$ i pretpostavke o $m$). Stoga je $a \in B_{k+t-1} \subseteq B_m$, te je $\langle B_m \cup \{a\}\rangle = \mathbf{B}_m$ i $\mathbf{B}_m \cap p^m\mathbf{A} = \mathbf{O}$, kontradikcija. Dalje, prema 37.22, svaka podgrupa $\mathbf{B}_n$, $n \in N$, je direktni sumand grupe $\mathbf{A}$; prema tome je $\mathbf{B}_{n+1} = \mathbf{B}_n \oplus \mathbf{H}_n$ za neke podgrupe $\mathbf{H}_n$, $n \in N$. Prema 35.1 je $\mathbf{B} = \bigcup_{n\in N} \mathbf{B}_n$ direktna suma cikličnih grupa, pa je prema 35.7 i svaka podgrupa $\mathbf{B}_n$ direktna suma cikličnih grupa. Sve to (uz 39.9) dokazuje našu tvrdnju da je $\mathbf{B}$ bazična grupa.□

**Lema 39.12** *Neka je* $\mathbf{B}_n$ *direktna suma cikličnih grupa reda* $p^n$ *za svako* $n \in N$. *Tada je* $\mathbf{B} = \sum_{n\in N} \mathbf{B}_n$ *bazična podgrupa grupe* $t(\sum_{n\in N}^{c} \mathbf{B}_n)$, *tzv. zatvorenja grupe* $\mathbf{B}$.

**Dokaz.** Obeležimo, kraće, grupu $t(\sum_{n\in N}^{c} \mathbf{B}_n)$ sa $\overline{\mathbf{B}}$. Jasno, ako pišemo elemente grupe $\sum_{n\in N}^{c} \mathbf{B}_n$ kao nizove, tada je, za svako $n \in N$, $\overline{\mathbf{B}} = \mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n \oplus \overline{\mathbf{B}}_n$, gde je $\overline{B}_n = \{\langle b_k\rangle_{k\in N} \mid b_k \in B_k,\ b_1 = \cdots = b_n = 0$ i, za neko $r \in N$, $p^r\langle b_k\rangle = \langle 0\rangle\}$. Ako bi podgrupa $\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n$ bila strogo sadržana u nekom $p^n$ ograničenom direktnom sumandu $\mathbf{D}$ (grupe $\overline{\mathbf{B}}$), imali bismo $\mathbf{D} = \mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n \oplus (\mathbf{D} \cap \overline{\mathbf{B}}_n)$ i $\mathbf{D} \cap \overline{\mathbf{B}}_n \neq \mathbf{O}$. No, svaki element reda $p$ grupe $\mathbf{D} \cap \overline{\mathbf{B}}_n$ bio bi s jedne strane visine veće od ili jednake $n$, a s druge, kao element $p^n$-ograničene grupe $\mathbf{D}$, visine manje od $n$, kontradikcija. Znači, $\mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n$ je za svako $n \in N$ maksimalni $p^n$-ograničeni direktni sumand grupe $\overline{\mathbf{B}}$, pa je $\mathbf{B}$ bazična podgrupa.□

**Lema 39.13** *Neka je* $\mathbf{B}$ *bazična podgrupa p-grupe* $\mathbf{A}$. *Tada je za sve prirodne brojeve* $n, k$:

(1) $\mathbf{B}/p^n\mathbf{B} \cong \mathbf{A}/p^n\mathbf{A}$;

(2) $p^n\mathbf{A}/p^n\mathbf{B} \cong \mathbf{A}/\mathbf{B}$;

(3) $p^n\mathbf{A} = p^n\mathbf{B} + p^{n+k}\mathbf{A}$;

(4) $p^n\mathbf{B}/p^{n+1}\mathbf{B} \cong p^n\mathbf{A}/p^{n+1}\mathbf{A}$;

(5) $r(\mathbf{B}) = r(\mathbf{A}/p\mathbf{A})$.

**Dokaz**. (1) Prema 39.7 je $\mathbf{A} = \mathbf{B} + p^n\mathbf{A}$, pa je prema drugoj teoremi o izomorfizmu:

$$\mathbf{A}/p^n\mathbf{A} \cong \mathbf{B}/(\mathbf{B} \cap p^n\mathbf{A}) = \mathbf{B}/p^n\mathbf{B};$$

zbog potpunosti podgrupe $\mathbf{B}$ je $\mathbf{B} \cap p^n\mathbf{A} = p^n\mathbf{B}$.

(2) Slično kao u prethodnoj tački; polazimo od $\mathbf{A} = \mathbf{B} + p^n\mathbf{A}$ i primenjujemo drugu teoremu o izomorfizmu (samo sada u formi):

$$\mathbf{A}/\mathbf{B} \cong p^n\mathbf{A}/(\mathbf{B} \cap p^n\mathbf{A}) = p^n\mathbf{A}/p^n\mathbf{B}.$$

(3) Jasno, u pitanju je samo inkluzija $p^nA \subseteq p^nB + p^{n+k}A$. No, kako je $A = B + p^{n+k}A$, to za svako $a \in A$ postoji $b \in B$ i $a' \in A$ tako da je $p^na = b + p^{n+k}a'$. Sledi da je $b$ deljivo sa $p^n$ u $\mathbf{A}$, dakle i u $\mathbf{B}$, te je $b = p^nb'$ za neko $b' \in B$. Prema tome, $p^na = p^nb' + p^{n+k}a'$.

(4) Prema prethodnoj tački imamo, kao poseban slučaj: $p^nA = p^nB + p^{n+1}A$, a odatle, prema drugoj teoremi o izomorfizmu i potpunosti podgrupe $\mathbf{B}$:

$$p^n\mathbf{A}/p^{n+1}\mathbf{A} \cong p^n\mathbf{B}/(p^n\mathbf{B} \cap p^{n+1}\mathbf{A}) = p^n\mathbf{B}/p^{n+1}\mathbf{B}.$$

(5) Kako je $\mathbf{B} = \mathbf{B}_1 \oplus \sum_{n\geq 2}\mathbf{B}_n$, gde je, kao i obično, $\mathbf{B}_n$ direktna suma cikličnih grupa reda $p^n$, to je $r(\mathbf{B}) = r(\mathbf{B}_1) + \sum_{n\geq 2} r(\mathbf{B}_n)$. Evidentno, za $n \geq 2$ je $r(\mathbf{B}_n) = r(\mathbf{B}_n/p\mathbf{B}_n)$ (ako je $\mathbf{B}_n \cong \sum_{\alpha<\lambda}\mathbf{Z}_{p^n}^{\alpha}$, onda je $p\mathbf{B}_n \cong \sum_{\alpha<\lambda}\mathbf{Z}_{p^{n-1}}^{\alpha}$ i, prema 10.3, $\mathbf{B}_n/p\mathbf{B}_n \cong \sum_{\alpha<\lambda}\mathbf{Z}_p$; dakle, $r(\mathbf{B}_n) = r(\mathbf{B}_n/p\mathbf{B}_n) = |\lambda|$). Stoga je:

$$r(\mathbf{B}) = r(\mathbf{B}_1) + \sum\nolimits_{n\geq 2} r(\mathbf{B}_n/p\mathbf{B}_n) = r(\mathbf{B}_1 \oplus \sum\nolimits_{n\geq 2}\mathbf{B}_n/p\mathbf{B}_n).$$

No, kao maločas, pozivajući se još na 10.17, izvodimo:

$$\mathbf{B}/p\mathbf{B} = (\mathbf{B}_1 \oplus \sum\nolimits_{n\geq 2}\mathbf{B}_n)/(p\mathbf{B}_1 \oplus p\sum\nolimits_{n\geq 2}\mathbf{B}_n) =$$

$$(\mathbf{B}_1 \oplus \sum\nolimits_{n\geq 2}\mathbf{B}_n)/\sum\nolimits_{n\geq 2} p\mathbf{B}_n \cong \mathbf{B}_1 \oplus \sum\nolimits_{n\geq 2}\mathbf{B}_n/p\mathbf{B}_n.$$

Prema tome je $r(\mathbf{B}) = r(\mathbf{B}/p\mathbf{B}) = r(\mathbf{A}/p\mathbf{A})$.□

**Korolar 39.14** *Ako je* $\mathbf{B}$ *bazična podgrupa p-grupe* $\mathbf{A}$, *onda je* $p^n\mathbf{B}$ *bazična podgrupa grupe* $p^n\mathbf{A}$ *za svaki prirodan broj* $n$.



**Dokaz**. Direktna posledica korolara 35.7, tačke $(h)$ primera 37.11 i tačke (2) prethodne leme.□

Neka je $\mathbf{B} = \sum_{\alpha<\kappa}\langle b_\alpha\rangle$, gde su $\langle b_\alpha\rangle$ $(\alpha < \kappa)$ ciklične $p$-grupe, bazična podgrupa $p$-grupe $\mathbf{A}$ i neka je $\mathbf{A}/\mathbf{B} = \sum_{\beta<\lambda}\mathbf{G}_\beta$, gde je, za svako $\beta < \lambda$, $\mathbf{G}_\beta$ Prüferova $p$-grupa generisana skupom elemenata $\{g_n^\beta + B \mid n \in N\}$ za koje važi: $red(g_n^\beta) = red(g_n^\beta + B) = p^n$ (videti 37.5) i $p(g_{n+1}^\beta + B) = g_n^\beta + B$. Sistem elemenata $\{b_\alpha \mid \alpha < \kappa\} \cup \{g_n^\beta \mid n \in N, \beta < \lambda\}$ je tzv. *kvazibaza* grupe $\mathbf{A}$. Za nju važi

**Lema 39.15** *Ako je, s notacijom iz prethodnog pasusa,* $\mathcal{S} = \{b_\alpha \mid \alpha < \kappa\} \cup \{g_n^\beta \mid n \in N, \beta < \lambda\}$ *kvazibaza grupe* $\mathbf{A}$ *(za bazičnu podgrupu* $\mathbf{B}$*), tada se svaki nenula element* $(a)$ *grupe* $\mathbf{A}$ *može zapisati na jedinstven način u obliku:*

$$a = s_1b_{\alpha_1} + \cdots + s_kb_{\alpha_k} + t_1g_{n_1}^{\beta_1} + \cdots + t_lg_{n_l}^{\beta_l},$$

*gde je* $k, l \geq 0$, *svi indeksi* $\alpha_1, \ldots, \alpha_k$, *kao i* $\beta_1, \ldots, \beta_l$, *su različiti i za* $1 \leq i \leq k$ *i* $1 \leq j \leq l$ *je* $0 < s_i < red(b_{\alpha_i})$ *i* $0 < t_j < p$.

**Dokaz**. Jasno, ako je npr. $k = 0$, smatramo da nemamo sabiraka "tipa" $sb_\alpha$; analogno tretiramo slučaj $l = 0$.

Očigledno je $\mathcal{S}$ generatorni skup grupe $\mathbf{A}$; $\{b_\alpha \mid \alpha < \kappa\}$ je generatorni sistem (pod)grupe $\mathbf{B}$, a $\{g_n^\beta + B \mid n \in N, \beta < \lambda\}$ faktor grupe $\mathbf{A}/\mathbf{B}$. Uslov da nijedno $t_j$ nije deljivo sa $p$ lako je ostvarljiv zbog relacija $p(g_{n+1}^\beta + B) = g_n^\beta + B$. Pretpostavimo da je za neko $a \in A$:

$$a = s_1b_{\alpha_1} + \cdots + s_kb_{\alpha_k} + t_1g_{n_1}^{\beta_1} + \cdots + t_lg_{n_l}^{\beta_l} = s_1'b_{\gamma_1} + \cdots + s_q'b_{\gamma_q} + t_1'g_{m_1}^{\delta_1} + \cdots + t_r'g_{m_r}^{\delta_r},$$

kao i da u tim prezentacijama elementa $a$ važe sve pretpostavke leme o celim brojevima $s_i, s_j', t_u, t_v'$. Onda je $a + B = t_1(g_{n_1}^{\beta_1} + B) + \cdots + t_l(g_{n_l}^{\beta_l} + B) = t_1'(g_{m_1}^{\delta_1} + B) + \cdots + t_r'(g_{m_r}^{\delta_r} + B)$, pa s obzirom na jedinstvenost prezentacija elementa u direktnoj sumi i uslova da nijedno $t_u, t_v'$ nije deljivo sa $p$ sledi: $l = r$, $\{\beta_1, \ldots, \beta_l\} = \{\delta_1, \ldots, \delta_l\}$; možemo uzeti, bez uticanja na opštost razmatranja, da je $\beta_i = \delta_i$, $1 \leq i \leq l$, a onda je $t_i = t_i'$. Posle "potiranja", opet zbog jedinstvenosti prezentacije u direktnoj sumi, iz $s_1b_{\alpha_1} + \cdots + s_kb_{\alpha_k} = s_1'b_{\gamma_1} + \cdots + s_q'b_{\gamma_q}$ sledi direktno: $k = q$, $\{\alpha_1, \ldots, \alpha_k\} = \{\gamma_1, \ldots, \gamma_k\}$ i, opet uz pretpostavku $\alpha_i = \gamma_i$, $s_i = s_i'$, $1 \leq i \leq k$.□

**Korolar 39.16** *Ako je* $\mathbf{A}$ *p-reducirana grupa i* $\mathbf{B}$ *njena bazična podgrupa, tada je* $|A| \leq |B|^{\aleph_0}$.

**Dokaz**. Neka je $\mathcal{S} = \{b_\alpha \mid \alpha < \kappa\} \cup \{g_n^\beta \mid n \in N, \beta < \lambda\}$ (jedna) kvazibaza grupe $\mathbf{A}$ (s obzirom na bazičnu podgrupu $\mathbf{B}$). Nema razloga da ne pretpostavimo da je $\lambda$ baš kardinal, pa ćemo to i učiniti. Prema prethodnoj lemi dovoljno je pokazati da je $|\{g_n^\beta \mid n \in N, \beta < \lambda\}| = \aleph_0 \cdot \lambda \leq |B|^{\aleph_0}$. Iz

$p(g^\beta_{n+1}+B)=g^\beta_n+B$ sledi da za svako (dato) $\beta<\lambda$ i svako $n\in N$ postoji jedinstven element $b^\beta_n\in B$ takav da je $pg^\beta_{n+1}=g^\beta_n+b^\beta_n$. Znači, svakom ordinalu $\beta<\lambda$ pridružujemo na ovaj način jednoznačno određeni niz (elemenata grupe $\mathbf{B}$) $\langle b^\beta_n\rangle_{n\in N}$. Pokazaćemo, a time i završiti dokaz, da su za $\beta<\gamma\ (<\lambda)$ nizovi $\langle b^\beta_n\rangle$ i $\langle b^\gamma_n\rangle$ različiti, tj. da je preslikavanje $\varphi:\lambda\longrightarrow B^\omega$ dato sa $(\beta)\varphi=\langle b^\beta_n\rangle$ injektivno (onda je, naravno, $\lambda\leq|B^\omega|=|B|^{\aleph_0}$ i, jasno, $\aleph_0<|B|^{\aleph_0}$ – $\mathbf{B}$ je, s obzirom na reduciranost grupe $\mathbf{A}$, nenula grupa). Pretpostavimo suprotno. Neka je, dakle, $\langle b^\beta_n\rangle=\langle b^\gamma_n\rangle$ za neke ordinale $\beta<\gamma\ (<\lambda)$. Ali tada je $b^\beta_n=b^\gamma_n$ za svako $n\in N$, pa je $pg^\beta_{n+1}=g^\beta_n+b^\beta_n$, $pg^\gamma_{n+1}=g^\gamma_n+b^\beta_n$ i odatle $p(g^\gamma_1-g^\beta_1)=0,\ldots,p(g^\gamma_{n+1}-g^\beta_{n+1})=g^\gamma_n-g^\beta_n,\ldots$. Proizilazi, s obzirom na date relacije, da sistem (nenula) elemenata $\{g^\gamma_n-g^\beta_n\mid n\in N\}$ generiše deljivu podgrupu grupe $\mathbf{A}$, suprotno pretpostavci da je $\mathbf{A}$ reducirana grupa.□

**Lema 39.17** *Neka je* $\mathbf{C}$ *potpuna podgrupa p-grupe* $\mathbf{A}$. *Faktor grupa* $\mathbf{A/C}$ *je deljiva akko* $\mathbf{C}$ *sadrži neku bazičnu podgrupu grupe* $\mathbf{A}$.

**Dokaz.** Pravac ($\Longleftarrow$) je trivijalan. Ako je $\mathbf{B}\leq\mathbf{C}$ i $\mathbf{B}$ bazična podgrupa grupe $\mathbf{A}$, onda je $\mathbf{A/B}$ deljiva grupa, te je i $\mathbf{A/C}$, kao njena homomorfna slika, deljiva (videti dokaz treće teoreme o izomorfizmu – $\mathbf{A/C}\cong(\mathbf{A/B})/(\mathbf{C/B})$).

($\Longrightarrow$) Neka je $\mathbf{A/C}$ deljiva grupa i neka je $\mathbf{B}$ (jedna) bazična podgrupa grupe $\mathbf{C}$; $\mathbf{B}$ je, dakle, direktna suma cikličnih grupa i (zbog tranzitivnosti svojstva potpunosti) potpuna podgrupa grupe $\mathbf{A}$. Kao deljiva grupa $\mathbf{C/B}$ je direktni sumand grupe $\mathbf{A/B}$. Neka je $\mathbf{A/B}=\mathbf{C/B}\oplus\mathbf{D/B}$. Prema drugoj teoremi o izomorfizmu imamo:

$$\mathbf{A/C}=(\mathbf{C}+\mathbf{D})/\mathbf{C}\cong\mathbf{D}/(\mathbf{C}\cap\mathbf{D})=\mathbf{D/B}.$$

Proizilazi da je $\mathbf{A/B}$, kao direktna suma deljivih grupa, i sama deljiva, pa je $\mathbf{B}$ bazična podgrupa i grupe $\mathbf{A}$.□

**Korolar 39.18** *Ako je* $\mathbf{C}$ *bazična podgrupa bazične podgrupe* $\mathbf{B}$ *p-grupe* $\mathbf{A}$, *tada je* $\mathbf{C}$ *bazična podgrupa i grupe* $\mathbf{A}$; *drugim rečima, svojstvo "biti bazična podgrupa" je tranzitivno.*

**Lema 39.19** *Neka je* $\mathbf{A}^1$ *podgrupa p-grupe* $\mathbf{A}$ *sa domenom* $A^1\stackrel{\text{def}}{=}\{a\in A\mid a$ *je beskonačne visine*$\}$. *Ako je* $\varphi:A\longrightarrow A/A^1=\overline{A}$ *kanonički homomorfizam, onda je, za svaku bazičnu podgrupu* $\mathbf{B}$ *grupe* $\mathbf{A}$, $(\mathbf{B})\varphi=\overline{\mathbf{B}}$ *bazična podgrupa grupe* $\overline{\mathbf{A}}$ *i* $\mathbf{B}\cong\overline{\mathbf{B}}$.

**Dokaz.** Primetimo, pre nego što pređemo na sam dokaz, da je $A^1$ stvarno domen podgrupe; jer, jasno, $0\in A^1$ i ako $a,b\in A^1$, onda i $-a,a+b\in A^1$.

Neka je $\mathbf{B}$ bazična podgrupa grupe $\mathbf{A}$. Kao direktna suma $p$-cikličnih grupa $\mathbf{B}$ je bez nenula elemenata beskonačne visine. Stoga je $\mathbf{B}\cap\mathbf{A}^1=\mathbf{O}$, pa je



prema 10.16 $(\mathbf{B})\varphi=(\mathbf{B}\oplus\mathbf{A}^1)/\mathbf{A}^1\cong\mathbf{B}$. Pošto je, za svako $n\in N$, $\mathbf{A}=\mathbf{B}_1\oplus\cdots\oplus\mathbf{B}_n\oplus(\mathbf{B}^*_n+p^n\mathbf{A})$ i $A^1\subseteq p^nA$, sledi, ponovo prema 10.16 i očiglednoj činjenici da je $p^n\mathbf{A}/\mathbf{A}^1=p^n\overline{\mathbf{A}}$: $\overline{\mathbf{A}}=((\mathbf{B}_1\oplus\cdots\oplus\mathbf{B}_n)\oplus(\mathbf{B}^*_n+p^n\mathbf{A}))/\mathbf{A}^1\cong(\mathbf{B}_1\oplus\cdots\oplus\mathbf{B}_n)\oplus((\mathbf{B}^*_n\oplus p^n\mathbf{A})/\mathbf{A}^1)$ (ovde imamo spoljašnju direktnu sumu grupa $\mathbf{B}_1\oplus\cdots\oplus\mathbf{B}_n$ i $(\mathbf{B}^*_n+p^n\mathbf{A})/\mathbf{A}^1)=(\mathbf{B}_1\oplus\cdots\oplus\mathbf{B}_n)\oplus((\mathbf{B}^*_n+\mathbf{A}^1)/\mathbf{A}^1+p^n\mathbf{A}/\mathbf{A}^1)=(\mathbf{B}_1\oplus\cdots\oplus\mathbf{B}_n)\oplus(\overline{\mathbf{B}^*_n}+p^n\overline{\mathbf{A}})\cong(\overline{\mathbf{B}_1}\oplus\cdots\oplus\overline{\mathbf{B}_n})\oplus(\overline{\mathbf{B}^*_n}+p^n\overline{\mathbf{A}})$. Prema tome, i $\overline{\mathbf{B}}$ je bazična podgrupa grupe $\overline{\mathbf{A}}$.□

**Korolar 39.20** *Ako je* $\mathbf{A}$ *p-reducirana grupa, onda je* $|A|\leq|A/A^1|^{\aleph_0}$.

**Dokaz.** Direktna posledica korolara 39.16 i prethodne leme (za svaku bazičnu podgrupu $\mathbf{B}$ grupe $\mathbf{A}$ je, s notacijom iz prethodne leme: $|B|=|\overline{B}|\leq|\overline{A}|$).□

**Teorema 39.21** *Sve bazične podgrupe p-grupe* $\mathbf{A}$ *su međusobno izomorfne.*

**Dokaz.** Neka je $\mathbf{B}=\sum_{n\in N}\mathbf{B}_n$ bazična podgrupa grupe $\mathbf{A}$, gde je, kao i dosad, $\mathbf{B}_n$ direktna suma cikličnih grupa reda $p^n$. Prema 35.11, svaka dva razlaganja grupe $\mathbf{B}$ u direktnu sumu nerazloživih cikličnih grupa su izomorfna, dakle, broj cikličnih sumanada reda $p^n$, neka je to $\lambda_n$, nezavisan je od razlaganja (znamo: $\lambda_n=\mu\geq\aleph_0$ ako je $|B_n|=\mu$, $\lambda_n=m\in\omega$ ako je $|B_n|=p^{mn}$ – podrazumevamo, naravno, da je $\mathbf{B}_n$ nula podgrupa ako nema cikličnih sumanada reda $p^n$). S druge strane, broj cikličnih sumanada reda $p^n$ isti je u grupama $\mathbf{B}$ i $\mathbf{B}/p^k\mathbf{B}$ za svako $k>n$. Jer, $p^k\mathbf{B}=p^k\mathbf{B}^*_k=p^{k+1}\mathbf{B}_{k+1}\oplus p^k\mathbf{B}_{k+2}\oplus\cdots$, pa je, kao i ranije:

$$\mathbf{B}/p^k\mathbf{B}=(\mathbf{B}_1\oplus\cdots\oplus\mathbf{B}_k\oplus\mathbf{B}^*_k)/p^k\mathbf{B}\cong$$

$$(\mathbf{B}_1\oplus\cdots\oplus\mathbf{B}_k)\oplus\mathbf{B}^*_k/p^k\mathbf{B}\cong(\mathbf{B}_1\oplus\cdots\oplus\mathbf{B}_k)\oplus\sum\nolimits_{r\in N}(\mathbf{B}_{k+r}/p^k\mathbf{B}_{k+r}).$$

No, ako je za dato $r$ $\mathbf{B}_{k+r}\cong\sum_{\alpha<\kappa_r}\mathbf{Z}^\alpha_{p^{k+r}}$, gde su, jasno, $\mathbf{Z}^\alpha_{p^{k+r}}$ "standardne" ciklične grupe reda $p^{k+r}$ sa elementima $m_\alpha$, $m=0,1,\ldots,p^{k+r}-1$, onda je:

$$\mathbf{B}_{k+r}/p^k\mathbf{B}_{k+r}\cong\sum\nolimits_{\alpha<\kappa_r}\mathbf{Z}^\alpha_{p^{k+r}}/p^k\mathbf{Z}^\alpha_{p^{k+r}}\cong\sum\nolimits_{\alpha<\kappa_r}\mathbf{C}^\alpha_{p^k},$$

(jer: $|p^kZ_{p^{k+r}}|=|\{0,p^k,2\cdot p^k,\ldots,p^{r-1}\cdot p^k\}|=p^r$). S obzirom da je prema 39.13(1) $\mathbf{B}/p^k\mathbf{B}\cong\mathbf{A}/p^k\mathbf{A}$, zaključujemo konačno da je broj cikličnih sumanada reda $p^n$ isti u svim bazičnim podgrupama grupe $\mathbf{A}$.■

**Teorema 39.22** *p-grupa* $\mathbf{A}$ *ima jedinstvenu bazičnu podgrupu akko je ili deljiva ili ograničena.*

**Dokaz.** ($\Longleftarrow$) Već smo videli da deljive i ograničene $p$-grupe imaju jedinstvene bazične podgrupe – 39.5($a$),($b$).

($\Longrightarrow$) Neka je $\mathbf{B}$ bazična podgrupa $p$-grupe $\mathbf{A}$. Ako $\mathbf{B}$ nije ograničena grupa, onda sadrži direktni sumand – $\mathbf{B}_1$ – oblika (izomorfan sa) $\sum_{n\in N}\mathbf{C}_{p^{n_k}}$,

gde je $n_1 < n_2 < \cdots$; recimo da je $\mathbf{B} = \mathbf{B}_1 \oplus \mathbf{B}_2$. Prema 39.5(c) $\mathbf{B}_1$ sadrži pravu bazičnu podgrupu, neka je to $\mathbf{H}$. Ali onda je $\mathbf{H} \oplus \mathbf{B}_2$ prava bazična podgrupa grupe $\mathbf{B}$ (ne zaboravimo: $(\mathbf{B}_1 \oplus \mathbf{B}_2)/(\mathbf{H} \oplus \mathbf{B}_2) \cong (\mathbf{B}_1/\mathbf{H}) \oplus (\mathbf{B}_2/\mathbf{B}_2) \cong \mathbf{B}_1/\mathbf{H}$), dakle i grupe $\mathbf{A}$ (39.18). Zaključujemo: ako je $\mathbf{B}$ jedinstvena bazična podgrupa grupe $\mathbf{A}$, onda mora biti i ograničena, stoga i direktni sumand grupe $\mathbf{A}$ (37.18). Neka je $\mathbf{A} = \mathbf{B} \oplus \mathbf{C}$, gde je $\mathbf{C}$ ($\cong \mathbf{A}/\mathbf{B}$) deljiva grupa i kao takva apsolutni direktni sumand grupe $\mathbf{A}$. Ako bi i $\mathbf{B}$ i $\mathbf{C}$ bile nenula podgrupe, onda bismo ponovo imali i drugih bazičnih podgrupa. Zaista, za nenula elemente $b \in B$, $c \in C$, i maksimalnu podgrupu $\mathbf{D}$ grupe $\mathbf{A}$ koja sadrži element $b + c$ i čiji je presek sa $\mathbf{C}$ nula podgrupa sledilo bi: $\mathbf{A} = \mathbf{D} \oplus \mathbf{C}$, i $\mathbf{D}$ bi bila bazična podgrupa grupe $\mathbf{A}$; primetimo da bi $p^n\mathbf{B} = \mathbf{O}$ impliciralo $p^n\mathbf{D} = \mathbf{O}$, te bi grupa $\mathbf{D}$ bila direktni sumand $p$-cikličnih grupa (za $d \in D$, $d = b_1 + c_1$, $b_1 \in B$, $c_1 \in C$, bilo bi: $p^n d = p^n b_1 + p^n c_1 = p^n c_1 \in D \cap C = \{0\}$). Prema tome, zbog uslova o jedinstvenosti bazične podgrupe je ili $\mathbf{B} = \mathbf{O}$ ili $\mathbf{C} = \mathbf{O}$. U prvom slučaju je $\mathbf{A}$ ($= \mathbf{C}$) deljiva, u drugom, $\mathbf{A}$ ($= \mathbf{B}$), ograničena grupa.■

Ako je $\mathbf{B}$ bazična podgrupa $p$-grupe $\mathbf{A}$, onda je $r(\mathbf{A}/\mathbf{B}) \leq r(\mathbf{A})$. Zaista, neka je $\mathbf{A}/\mathbf{B} = \sum_{\alpha<\lambda} \mathbf{P}_\alpha$, gde su $\mathbf{P}_\alpha$, $\alpha < \lambda$, Prüferove $p$-grupe, i neka su, za svako $\alpha < \lambda$, $a_\alpha + B \in P_\alpha$ i $a_\alpha \in A$ elementi reda $p$ (37.5). No, tada je $\{a_\alpha \mid \alpha < \lambda\}$ slabo linearno nezavisan sistem elemenata grupe $\mathbf{A}$; iz $m_1 a_{\alpha_1} + \cdots + m_k a_{\alpha_k} = 0$ izvodimo: $m_1(a_{\alpha_1} + B) + \cdots + m_k(a_{\alpha_k} + B) = B$, pa $p$ deli $m_i$ za svako $i$, $1 \leq i \leq k$.

**Definicija 39.23** *Finalni rang p-grupe* $\mathbf{A}$, *u oznaci* $fin\ r(\mathbf{A})$, *definišemo sa:*

$$fin\ r(\mathbf{A}) = min\{r(p^n\mathbf{A}) \mid n \in \omega\}.$$

*Bazična podgrupa* $\mathbf{B}$ *p-grupe* $\mathbf{A}$ *je niža bazična podgrupa akko je* $r(\mathbf{A}/\mathbf{B}) = fin\ r(\mathbf{A})$.

Očigledno, finalni rang je dobro definisan, tj. uvek postoji, jer svaki nenula skup kardinala ima najmanji element. Inače, s obzirom da je u pitanju opadajući lanac podgrupa $\mathbf{A} \geq p\mathbf{A} \geq p^2\mathbf{A} \geq \cdots$, imamo: $r(\mathbf{A}) \geq r(p\mathbf{A}) \geq r(p^2\mathbf{A}) \geq \cdots$. Stoga, ako je $m$ najmanji prirodan broj za koji je $fin\ r(\mathbf{A}) = r(p^m\mathbf{A})$, onda je $r(p^{m+k}\mathbf{A}) = r(p^m\mathbf{A})$ za svako $k \in N$.

**Lema 39.24** *Za svaku bazičnu podgrupu* $\mathbf{B}$ *p-grupe* $\mathbf{A}$ *važi:*

$$r(\mathbf{A}/\mathbf{B}) \leq fin\ r(\mathbf{A}).$$

**Dokaz.** Prema 39.13(2) i 39.14 je za svaki prirodan broj $n$:

$$r(\mathbf{A}/\mathbf{B}) = r(p^n\mathbf{A}/p^n\mathbf{B}) \leq r(p^n\mathbf{A}).\square$$

Svaka $p$-grupa ima nižu bazičnu podgrupu; još konkretnije, važi



**Lema 39.25** *Svaka bazična podgrupa p-grupe* $\mathbf{A}$ *sadrži nižu bazičnu podgrupu.*

**Dokaz.** Ako je $fin\ r(\mathbf{A})$ konačan broj, onda je i $fin\ r(\mathbf{B})$ konačan broj ($r(p^k\mathbf{B}) \leq r(p^k\mathbf{A})$). Neka je $fin\ r(\mathbf{B}) = r(p^m\mathbf{B})$. Kako je $\mathbf{B} = \mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_m \oplus \mathbf{B}_m^*$, iz $r(p^m\mathbf{B}) = r(p^{m+1}\mathbf{B})$, tj. $r(p^m\mathbf{B}_m^*) = r(p^{m+1}\mathbf{B}_{m+1}^*)$, $r(p^m\mathbf{B}_m^*) = r(p^m\mathbf{B}_{m+1}) + r(p^m\mathbf{B}_{m+1}^*) = r(\mathbf{B}_{m+1}) + r(\mathbf{B}_{m+1}^*)$ i $r(p^{m+1}\mathbf{B}_{m+1}^*) = r(\mathbf{B}_{m+1}^*)$ sledi $r(\mathbf{B}_{m+1}) = 0$. Analogno je $r(\mathbf{B}_{m+k}) = 0$ za svako $k \in N$, pa je $p^m\mathbf{B} = \mathbf{O}$; dakle, $\mathbf{B}$ je ograničena grupa i $fin\ r(\mathbf{B}) = 0$. $\mathbf{B}$ je onda, prema 39.13(2), niža bazična podgrupa grupe $\mathbf{A}$. Kao što vidimo, u ovom slučaju su sve bazične podgrupe niže bazične.

Neka je sada $fin\ r(\mathbf{A})$ beskonačni kardinal i neka bazična podgrupa $\mathbf{B}$ grupe $\mathbf{A}$ nije niža bazična podgrupa. Znači, $r(\mathbf{A}/\mathbf{B}) < fin\ r(\mathbf{A})$. Ponovo je prema 39.13(2), za prirodan broj $n$, $r(\mathbf{A}/\mathbf{B}) = r(p^n\mathbf{A}/p^n\mathbf{B}) < r(p^n\mathbf{A})$, te je $r(p^n\mathbf{B}) = r(p^n\mathbf{A})$. Zaista, ako je grupa beskonačnog ranga, onda joj je red jednak rangu; $p^n\mathbf{B}$ je direktna suma cikličnih grupa, pa bi u slučaju da je konačnog ranga i sama bila konačna, i na kraju, ako bi $p^n\mathbf{B}$ bila ranga $\mu \geq \aleph_0$ (stoga i reda $\mu$), a $p^n\mathbf{A}$ ranga $\lambda > \mu$, faktor grupa $p^n\mathbf{A}/p^n\mathbf{B}$ bi bila reda $\lambda$, dakle i ranga $\lambda$. Proizilazi da je broj cikličnih direktnih sumanada reda većeg od $p^n$ u grupi $\mathbf{B}$ veći ili jednak od $fin\ r(\mathbf{A})$. Prema tome, grupa $\mathbf{B}$ se može predstaviti kao direktna suma $\sum_{\alpha<fin\ r(\mathbf{A})} \mathbf{C}_\alpha$, gde je (za svako $\alpha < fin\ r(\mathbf{A})$) $\mathbf{C}_\alpha$ neograničena direktna suma cikličnih grupa. Prema 39.5(c), svaki sumand $\mathbf{C}_\alpha$ sadrži pravu bazičnu podgrupu – $\mathbf{D}_\alpha$. Naravno, $\mathbf{D} = \sum_{\alpha<fin\ r(\mathbf{A})} \mathbf{D}_\alpha$ je prava bazična podgrupa grupe $\mathbf{B}$, znači i grupe $\mathbf{A}$. Štaviše, ona je niža bazična podgrupa grupe $\mathbf{A}$:

$$r(\mathbf{A}/\mathbf{D}) \geq r(\mathbf{B}/\mathbf{D}) = \sum\nolimits_{\alpha<fin\ r(\mathbf{A})} r(\mathbf{C}_\alpha/\mathbf{D}_\alpha) \geq fin\ r(\mathbf{A}),$$

a rekli smo, uvek je $r(\mathbf{A}/\mathbf{D}) \leq fin\ r(\mathbf{A})$.□

**Teorema 39.26** *Ako je* $\mathbf{B}$ *bazična podgrupa p-grupe* $\mathbf{A}$, *onda postoji endomorfizam grupe* $\mathbf{A}$ *koji je preslikava na* $\mathbf{B}$.

**Dokaz.** Ako je $\mathbf{B}$ ograničena grupa tada je, već smo konstatovali, i direktni sumand grupe $\mathbf{A}$ i taj slučaj je trivijalan (rešenje je projekcija grupe $\mathbf{A}$ na $\mathbf{B}$). Pretpostavimo zato da $\mathbf{B} = \sum_{n\in N} \mathbf{B}_n$ nije ograničena grupa (stalno ponavljamo: $\mathbf{B}_n$ je direktna suma cikličnih grupa reda $p^n$). Neka je $fin\ r(\mathbf{B}) = r(p^m\mathbf{B}) = r(\mathbf{B}_m^*) = \lambda$, $r(\mathbf{B}_i) = \lambda_i$ (za $i \in N$) i, za $k > m$, $\mathbf{B}_k = \sum_{\alpha<\lambda_k} \langle b_\alpha^k \rangle$, gde je, jasno, $\langle b_\alpha^k \rangle$ ciklična grupa reda $p^k$ generisana elementom $b_\alpha^k$. Dalje, neka je $\varphi$ injektivno preslikavanje skupa $\{\langle b_\alpha^k \rangle \mid \alpha < \lambda_k, k > m\}$ u sebe, koje ispunjava uslov: ako je $(\langle b_\alpha^r \rangle)\varphi = \langle b_\beta^s \rangle$, onda je $s \geq 2r$. Egzistencija (bar jednog) ovakvog preslikavanja zagarantovana je činjenicom da je, za $l > k > m$, $\lambda_k \leq r(\mathbf{B}_{l-1}^*) = \lambda = \sum_{i=m+1}^{\infty} \lambda_i$) (videti komentar uz definiciju 39.23). Koristeći dato preslikavanje $\varphi$ definišemo preslikavanje ($\psi$) podskupa skupa $B$ u $B$ sa:

(1) $(b)\psi = b$ za svako $b \in B_1 \oplus \cdots \oplus B_m$;

(2) $(b^s_\beta)\psi = b^r_\alpha$ akko je $((\langle b^r_\alpha\rangle))\varphi = \langle b^s_\beta\rangle$;

i

(3) $(b^t_\gamma)\psi = 0$ ako $\langle b^t_\gamma\rangle \not\leq ran(\varphi)$.

Preslikavanje $\psi$ se na prirodan način proširuje do surjektivnog endomorfizma grupe $\mathbf{B}$ – $\overline{\psi}$; surjektivnost je posledica činjenice da je domen preslikavanja $\varphi$ skup svih cikličnih sumanada grupe $\mathbf{B}^*_m$ i tačke $(h)$ teoreme 7.2. Konačno, $\overline{\psi}$ proširujemo do endomorfizma $(\theta)$ grupe $\mathbf{A}$ na sledeći način.

Neka je $a \in A$ reda $p^r$ i neka je $n \geq max\{m, 2r\}$. Pošto je $\mathbf{A} = \mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n \oplus (\mathbf{B}^*_n + p^n\mathbf{A})$, to je $a = b + c$ za neko $b \in B_1 \oplus \cdots \oplus B_n$ i neko $c \in B^*_n + p^nA$. Definišemo: $(a)\theta = (b)\overline{\psi}$. Preslikavanje $\theta$ ne zavisi od izbora broja $n\ (\geq max\{m, 2r\})$, jer $\overline{\psi}$ "prevodi" za svako $t \geq m, 2r$ komponentu elementa $b$ u $B_t$, neka je to $b_t$, u nulu. Razlog pak tome je ili, direktno, tačka (3) definicije preslikavanja $\psi$ (zbog koje je, između ostalog, $(\mathbf{B}_{m+1} \oplus \cdots \oplus \mathbf{B}_{2m+1})\overline{\psi} = \mathbf{O}$) ili činjenica da je $b_t$ deljivo sa $p^{t-r}$; znamo, naime, da se pri preslikavanju ciklične grupe $\langle b^t_\alpha\rangle$ u (cikličnu grupu) $\langle b^r_\beta\rangle$, gde je $b^r_\beta$ slika od $b^t_\alpha$ i $t \geq 2r$, svaki element deljiv sa $p^{t-r}$ preslikava u nulu (videti još jedanput tačku $(h)$ teoreme 7.2). Kako je (u Abelovoj grupi) $red(a_1 + a_2) \leq NZS(red(a_1), red(a_2))$ (2.7$(d)$) i $\overline{\psi}$ homomorfizam, proizilazi, zbog upravo rečenog, da je i $\theta$ homomorfno preslikavanje.■

**Korolar 39.27** *Ako je direktna suma cikličnih grupa* $\mathbf{C}$ *potpuna podgrupa p-grupe* $\mathbf{A}$, *onda postoji endomorfizam grupe* $\mathbf{A}$ *koji je preslikava na* $\mathbf{C}$.

**Dokaz.** Neka je $\mathbf{C} = \sum_{\alpha<\lambda}\langle c_\alpha\rangle$. Proširimo potpuni slabo linearno nezavisan sistem $\{c_\alpha \mid \alpha < \lambda\}$ do (jednog) maksimalnog takvog (videti komentar uz definiciju 39.1): $\{c_\alpha \mid \alpha < \lambda\} \cup \{b_\beta \mid \beta < \mu\}$; moguće je da je $\mu = 0$, ali u tom slučaju je $\mathbf{C}$ i bazična podgrupa grupe $\mathbf{A}$ (39.2), pa se onda direktno pozivamo na prethodnu teoremu. Grupa $\mathbf{B} = \mathbf{C} \oplus \sum_{\beta<\mu}\langle b_\beta\rangle$ je bazična podgrupa grupe $\mathbf{A}$, te postoji endomorfizam $\varphi \in End(\mathbf{A})$ za koji je $(\mathbf{A})\varphi = \mathbf{B}$. Ako je, dalje, $\pi_C$ projekcija grupe $\mathbf{B}$ na $\mathbf{C}$, tada je traženi endomorfizam (grupe $\mathbf{A}$) $\varphi \circ \pi_C$.□

**Korolar 39.28** *Neka je* $\mathbf{C}$ *homomorfna slika p-grupe* $\mathbf{A}$ *i neka je* $\mathbf{D}$ *bazična podgrupa grupe* $\mathbf{C}$. *Tada je* $\mathbf{D}$ *homomorfna slika svake bazične podgrupe grupe* $\mathbf{A}$.

**Dokaz.** Pošto su sve bazične podgrupe grupe $\mathbf{A}$ međusobno izomorfne, dovoljno je da tvrđenje dokažemo za bilo koju od njih. Neka je, dakle, $\mathbf{B}$ (jedna) bazična podgrupa grupe $\mathbf{A}$. S druge strane, kako su i $\mathbf{B}$ i $\mathbf{D}$ direktne sume $p$-cikličnih grupa, dovoljno je da pokažemo da je broj cikličnih sumanada reda $p^k$, $k \in N$, u grupi $\mathbf{D}$ manji ili jednak od broja istih takvih u $\mathbf{B}$. Prema prethodnoj teoremi je $\mathbf{D}$ homomorfna slika grupe $\mathbf{C}$, prema tome i grupe $\mathbf{A}$. Analogno, za $n \in \omega$ je $p^n\mathbf{D}$ homomorfna slika grupe $p^n\mathbf{C}$, koja je, opet, homomorfna slika



grupe $p^n\mathbf{A}$. Proizilazi da je grupa $p^n\mathbf{D}$ homomorfna slika grupe $p^n\mathbf{A}$, pa je to (i njena homomorfna slika) $p^n\mathbf{D}/p^{n+1}\mathbf{D}$. Ako je $\varphi : p^nA \longrightarrow p^nD/p^{n+1}D$ surjektivni homomorfizam, onda je, očigledno, $p^{n+1}A \subseteq Ker(\varphi)$, pa je, zbog

$$(p^n\mathbf{A}/p^{n+1}\mathbf{A})/(\mathbf{Ker}(\varphi)/p^{n+1}\mathbf{A}) \cong p^n\mathbf{A}/\mathbf{Ker}(\varphi) \cong p^n\mathbf{D}/p^{n+1}\mathbf{D},$$

$p^n\mathbf{D}/p^{n+1}\mathbf{D}$ homomorfna slika i grupe $p^n\mathbf{A}/p^{n+1}\mathbf{A}$, izomorfne sa $p^n\mathbf{B}/p^{n+1}\mathbf{B}$ (39.13(4)). Znači, postoji homomorfno preslikavanje grupe $p^n\mathbf{B}/p^{n+1}\mathbf{B}$ na grupu $p^n\mathbf{D}/p^{n+1}\mathbf{D}$. Obe ove grupe su direktne sume cikličnih grupa reda $p$, a broj sumanada u svakoj od njih jednak je broju sumanada reda većeg od ili jednakog $p^{n+1}$ grupa, respektivno, $\mathbf{B}$ i $\mathbf{D}$; ponavljamo (za grupu $\mathbf{B}$):

$$(\textstyle\sum_{k\geq n+1} p^n\mathbf{B}_k)/(\sum_{k\geq n+2} p^{n+1}\mathbf{B}_k) \cong p^n\mathbf{B}_{n+1} \oplus \sum_{k\geq n+2} p^n\mathbf{B}_k/p^{n+1}\mathbf{B}_k,$$

i, ako je (za dato $k$) $\mathbf{B}_k = \sum_{\alpha<\lambda_k}\langle b_\alpha\rangle$, onda je:

$$p^n\mathbf{B}_k/p^{n+1}\mathbf{B}_k \cong \textstyle\sum_{\alpha<\lambda_k} p^n\langle b_\alpha\rangle/p^{n+1}\langle b_\alpha\rangle \cong \sum_{\alpha<\lambda_k} \mathbf{C}^\alpha_p.$$

Zaključujemo: za svako $n \in \omega$ broj sumanada reda $p^{n+1}$ u grupi $\mathbf{B}$ veći je ili jednak od broja istih takvih u grupi $\mathbf{D}$.□

**Primer 39.29** $(a)$ *Neka je* $\mathbf{C}$ *bazična podgrupa potpune podgrupe* $\mathbf{B}$ *grupe* $\mathbf{A}$. *Tada je* $\mathbf{C}$ *podgrupa i neke bazične podgrupe grupe* $\mathbf{A}$.

**Dokaz.** Tvrđenje je direktna posledica korolara 39.11 i tranzitivnosti svojstva potpunosti.

$(b)$ *Ako je prebrojiva podgrupa* $\mathbf{C}$ *p-grupe* $\mathbf{A}$ *bez elemenata beskonačne visine, onda je sadržana u nekoj bazičnoj podgrupi grupe* $\mathbf{A}$.

**Dokaz.** Podgrupa $\mathbf{C}$ je unija rastućeg niza konačnih grupa (videti dokaz druge teoreme Prüfera – 35.5), dakle, s obzirom na uslov, i ograničenih visina. Preostaje da se pozovemo, još jedanput, na 39.11.

$(c)$ *Neka je* $\mathbf{A}$ *p-grupa bez elemenata beskonačne visine i neka je* $\tau$ *topologija na* $A$ *data sa: sistem okolina tačke* 0 *je* $\{p^nA \mid n \in \omega\}$ *(podrazumeva se da je onda sistem okolina proizvoljne "tačke"* $a$ *–* $\{a + p^nA \mid n \in \omega\}$*). Podgrupa* $\mathbf{B}$ *je, po definiciji, svuda gusta u* $\mathbf{A}$ *s obzirom na topologiju* $\tau$ *akko je, za svako* $a \in A$ *i svako* $n \in \omega$, *presek njenog domena* $B$ *i koseta* $a + p^nA$ *neprazan* $(B \cap (a + p^nA) \neq \emptyset)$. *Važi:*

$(i)$ *Podgrupa* $\mathbf{B}$ *je svuda gusta u* $\mathbf{A}$ *akko je faktor grupa* $\mathbf{A}/\mathbf{B}$ *deljiva;*

$(ii)$ *Podgrupa* $\mathbf{B}$ *grupe* $\mathbf{A}$ *je bazična akko ispunjava uslove* (1) *i* (2) *definicije* 39.3 *i svuda je gusta u* $\mathbf{A}$ *(s obzirom na topologiju* $\tau$*).*

**Dokaz.** $(i)$ Neka je podgrupa $\mathbf{B}$ svuda gusta u $\mathbf{A}$. Onda za dato $a \in A$ i $n \in \omega$ postoji neko $b$ iz $B$ koje je i element koseta $a + p^nA$. Ako je $a = b + p^na_1$, sledi $a + B = p^na_1 + B = p^n(a_1 + B)$ i $\mathbf{A}/\mathbf{B}$ je deljiva grupa.

Obrat je još lakši. Za dato $a \in A$ i $n \in \omega$ rešivost jednačine $a+B \doteq p^n(x+B)$ (u faktor grupi $\mathbf{A/B}$) implicira: za neko $a_1 \in A$ je $a+B = p^n a_1 + B$, pa je dalje, za neko $b \in B$, $p^n a_1 = a+b$, odnosno $b = a+p^n(-a_1) \in B \cap (a+p^n A)$.□

## 40 $p$-grupe bez elemenata beskonačne visine

Neka je $\mathbf{A}$ $p$-grupa, $a$ jedan njen element i $\mathbf{B}$ jedna njena bazična podgrupa. Prema 39.6 je za svako $n \in N$:

$$\mathbf{A} = \mathbf{B}_1 \oplus \cdots \oplus \mathbf{B}_n \oplus (\mathbf{B}_n^* + p^n\mathbf{A}),$$

gde je, podsećamo, $\mathbf{B}_k$ suma cikličnih sumanada grupe $\mathbf{B}$ reda $p^k$. Stoga za dato $n \in N$ postoje jedinstveni elementi $b_i \in B_i$, $i = 1, \ldots, n$, i $a_n \in B_n^* + p^n A$ takvi da je:

$$a = b_1 + \cdots + b_n + a_n.$$

Ako je $k > n$ i $a \doteq b_1' + \cdots + b_k' + a_k'$, onda je $0 = (b_1' - b_1) + \cdots + (b_n' - b_n) + (b_{n+1}' + \cdots + b_k' + a_k' - a_n) \in B_1 \oplus \cdots \oplus B_n \oplus (B_n^* + p^n A)$, pa je $b_1 = b_1', \ldots, b_n = b_n'$. Stoga je preslikavanje $\varphi : A \longrightarrow t(\sum_{n\in N} B_n)$ dato sa $(a)\varphi = \langle b_n \rangle_{n\in N}$, gde je, za svako $n \in N$, $b_n \in B_n$ i gde za dato $k \in N$ postoji (jedinstven) element $a_k \in B_k^* + p^k A$ takav da je $a = b_1 + \cdots + b_k + a_k$, homomorfno preslikavanje grupe $\mathbf{A}$ u zatvorenje grupe $\mathbf{B}$ – $t(\sum^c_{n\in N} \mathbf{B}_n)$, obično u oznaci $\overline{\mathbf{B}}$ – videti 39.12 (u 39.19 koristili smo oznaku $\overline{\mathbf{B}}$ u sasvim drugom kontekstu); jasno, ako je $(a_1)\varphi = \langle b_n^1 \rangle$ i $(a_2)\varphi = \langle b_n^2 \rangle$, onda je $(a_1 + a_2)\varphi = \langle b_n^1 + b_n^2 \rangle$. Uočimo dalje: ako je $a$ element beskonačne visine, tada je $(a)\varphi = \langle 0 \rangle$ (nula element grupe $\overline{\mathbf{B}}$). Jer, ako je $a = b_1 + \cdots + b_n + a_n$, $b_i \in B_i$, $a_n \in B_n^* + p^n A$, onda je $h(a) = min\{h(b_1), \ldots, h(b_n), h(a_n)\} = \infty$, te je svaka komponenta $b_i$, $i = 1, \ldots, n$, jednaka nuli ($\mathbf{B}_i$ je ograničena potpuna podgrupa grupe $\mathbf{A}$, dakle, jedini element beskonačne visine u njoj je nula element). S druge strane, ako je $(a)\varphi = \langle 0 \rangle$, tada je $a$ element beskonačne visine. Zaista, pretpostavka da je za element $a$ konačne visine $(a)\varphi = \langle 0 \rangle$, vodi u kontradikciju. Pokazaćemo to indukcijom po redu elementa. Neka je $red(a) = p$, $h(a) = m$ i $a = b_1 + \cdots + b_m + b_{m+1} + a_{m+1}$. Zbog potpunosti podgrupa $\mathbf{B}_i$ (u grupi $\mathbf{A}$) važi: $b_1 = \cdots = b_m = 0$. Ako bi bilo i $b_{m+1} = 0$, onda bi nenula element $a_{m+1} \in B_{m+1}^* + p^{m+1}A$ bio (reda $p$ i) visine veće od ili jednake $m+1$; svaki element u grupi $\mathbf{B}_{m+1}^*$ reda $p$ je visine veće od ili jednake $m+1$, a elementi grupe $p^{m+1}\mathbf{A}$ su i "vidljivo" deljivi sa $p^{m+1}$. Pretpostavimo u nastavku da se nijedan element konačne visine i reda manjeg od ili jednakog $p^k$ ne preslikava u nulu i neka je $a$ reda $p^{k+1}$ i visine $r$. $(a)\varphi = \langle 0 \rangle$ impliciralo bi $(pa)\varphi = 0$, i stoga bi, po induktivnoj hipotezi, element $pa$ bio beskonačne visine. Za $pa = p^{r+2}c$, element $a - p^{r+1}c$ je reda $p$ i visine $r$. Prema tome, videli smo, ako je $(a - p^{r+1}c)\varphi = \langle b_n' \rangle$, onda je $b_1' = \cdots = b_r' = 0$ i $b_{r+1}' \neq 0$. Opet,



ako je $(p^{r+1}c)\varphi = \langle b_n'' \rangle$, tada je $b_1'' = \cdots = b_r'' = b_{r+1}'' = 0$, pa dobijamo $(a - p^{r+1}c)\varphi \neq (a)\varphi + (p^{r+1}(-c))\varphi$, kontradikcija.

Iz svega navedenog (gotovo) direktno sledi

**Teorema 40.1** *Ako je* $\mathbf{A}$ *p-grupa,* $\mathbf{A}^1$ *njena podgrupa čiji je domen skup elemenata grupe* $\mathbf{A}$ *beskonačne visine,* $\mathbf{B}$ *bazična podgrupa i* $\overline{\mathbf{B}}$ *zatvorenje grupe* $\mathbf{B}$, *onda je faktor grupa* $\mathbf{A/A}^1$ *izomorfna nekoj potpunoj podgrupi grupe* $\overline{\mathbf{B}}$ *koja sadrži (izomorfnu sliku grupe)* $\mathbf{B}$.

**Dokaz.** Prema korišćenoj notaciji sve je već dokazano osim potpunosti grupe $(\mathbf{A})\varphi$ u $\overline{\mathbf{B}}$; inače, u $\overline{\mathbf{B}}$ grupu $\mathbf{B}$ identifikujemo sa njenom izomorfnom slikom $(\mathbf{B})\varphi$; gore smo pokazali da je $\mathbf{Ker}(\varphi) = \mathbf{A}^1$, a jasno, $\mathbf{B} \cap \mathbf{A}^1 = \mathbf{O}$.

Prema 39.19, $(\mathbf{B} \oplus \mathbf{A}^1)/\mathbf{A}^1$ ($\cong \mathbf{B}$) bazična je podgrupa grupe $\mathbf{A/A}^1$ ($\cong (\mathbf{A})\varphi$), pa je $(\mathbf{A})\varphi/\mathbf{B}$ deljiva podgrupa deljive grupe $\overline{\mathbf{B}}/\mathbf{B}$ (39.12). Ako je, za $a \in A$, $(a)\varphi = p^n\bar{b} \in \overline{B}$, dakle i $(a)\varphi + B = p^n(\bar{b} + B)$, onda je, za neko $a' \in A$, $(a)\varphi + B = p^n((a')\varphi + B)$. Sledi: $(a - p^n a')\varphi = p^n\bar{b} - p^n(a')\varphi \in B$, te je, za neko $b \in B$ (zbog potpunosti grupe $\mathbf{B}$ u $\overline{\mathbf{B}}$), $(a)\varphi = p^n((a')\varphi + b) \in p^n(A)\varphi$.■

**Korolar 40.2** *Ako je* $\mathbf{A}$ *p-grupa bez elemenata beskonačne visine i* $\mathbf{B}$ *(jedna) njena bazična podgrupa, onda je* $\mathbf{A}$ *izomorfna potpunoj podgrupi zatvorenja grupe* $\mathbf{B}$ ($\overline{\mathbf{B}}$) *koja sadrži* $\mathbf{B}$.

**Definicija 40.3** *Niz elemenata* $\langle a_n \rangle_{n\in N}$ *p-grupe* $\mathbf{A}$ *bez elemenata beskonačne visine konvergira ka* $a$ ($\in A$) *akko je* $a - a_n \in p^n A$ *za svako* $n \in N$.

*Niz elemenata* $\langle a_n \rangle_{n\in N}$ *p-grupe* $\mathbf{A}$ *bez elemenata beskonačne visine je Cauchyev akko je* $a_n - a_{n+1} \in p^n A$ *za svako* $n \in N$.

*p-grupa* $\mathbf{A}$ *bez elemenata beskonačne visine je zatvorena akko svaki njen Cauchyev niz konvergira.*

Činjenica da je $p$-grupa $\mathbf{A}$ bez elemenata beskonačne visine garantuje da ako neki njen niz $\langle a_n \rangle_{n\in N}$ ima graničnu vrednost, onda je ova i jedinstvena. Zaista, ako su i $a$ i $b$ granične vrednosti niza $\langle a_n \rangle_{n\in N}$, tada iz $a - a_n$, $b - a_n \in p^n A$ za svako $n \in N$ sledi: za svako $n \in N$ je $a - b \in p^n A$, tj. $a - b$ je element beskonačne visine, odnosno 0; dakle, $a = b$.

Lako se proverava da su suma i razlika dva konvergentna niza $\langle a_n \rangle_{n\in N}$ i $\langle a_n' \rangle_{n\in N}$, gde je, naravno, $\langle a_n \rangle_{n\in N} \pm \langle a_n' \rangle_{n\in N} \stackrel{\text{def}}{=} \langle a_n \pm a_n' \rangle_{n\in N}$, takođe konvergentni nizovi. Preciznije, mogli bismo rečnikom analize da kažemo: limes sume (razlike) jednak je sumi (razlici) limesa (pod uslovom da ovi postoje). Isto tako je očigledno da je podniz konvergentnog niza konvergentan niz.

Analogna tvrđenja važe za Cauchyeve nizove. Zbir i razlika Cauchyevih nizova su Cauchyevi nizovi, podniz Cauchyevog niza je Cauchyev niz.

**Teorema 40.4** *p-grupa* $\mathbf{A}$ *bez elemenata beskonačne visine je zatvorena akko je jednaka (izomorfna) zatvorenju neke svoje bazične podgrupe.*

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{A}$ zatvorena $p$-grupa i neka je $\mathbf{B} = \sum_{n\in N}\mathbf{B}_n$ jedna njena bazična podgrupa. Prema 40.2, grupa $\mathbf{A}$ je izomorfna (nekoj) podgrupi zatvorenja grupe $\mathbf{B}$ - $\overline{\mathbf{B}} = t(\sum^c_{n\in N}\mathbf{B}_n)$, koja sadrži $\mathbf{B}$, preciznije, izomorfnu sliku grupe $\mathbf{B}$. Pokazaćemo da je, u stvari, $\overline{\mathbf{B}} = (\mathbf{A})\varphi$, gde je $\varphi$ izomorfizam iz 40.2. Neka je $\langle b_n\rangle_{n\in N} \in t(\sum_{n\in N}B_n)$ i neka je $p^m\langle b_n\rangle_{n\in N} = \langle p^m b_n\rangle_{n\in N} = \langle 0\rangle$. Onda važi:

$$\forall n\,\exists k \geq n\,\forall l > k\;\; b_l \in p^n A.$$

Jer, pretpostavimo suprotno i neka za prirodan broj $n_0$ i svako $k \geq n_0$ postoji $l > k$ takvo da $b_l \notin p^{n_0}A$. Posebno, za (proizvoljno izabrano) $k_0 > m + n_0$ imamo neko $l_0 > k_0$ za koje $b_{l_0} \notin p^{n_0}A$. Neka je $\mathbf{B}_{l_0} = \sum_{\alpha<\lambda_0}\langle b^{l_0}_\alpha\rangle$ i $b_{l_0} = p^{r_1}s_1 b^{l_0}_{\alpha_1} + \cdots + p^{r_t}s_t b^{l_0}_{\alpha_t}$, gde je $(p, s_i) = 1$ za svako $i = 1,\ldots,t$. Onda je $r_i < n_0$ za bar jedno $i$. Ali, iz $p^m b_{l_0} = 0$ sledi: $p^{r_i+m}s_i b^{l_0}_{\alpha_i} = 0$, pa $p^{l_0}$ deli $p^{r_i+m}$, tj. $r_i + m \geq l_0 > k_0 > m + n_0$, kontradikcija.

Definišimo sada u $\mathbf{A}$ (faktički u $\mathbf{B}$) niz $\langle a_n\rangle_{n\in N}$ sa: $a_n = b_1 + \cdots + b_{k_n}$, gde je $k_n$ najmanji među prirodnim brojevima $k \geq n$ takvim da je $b_l \in p^n A$ za svako $l > k$. Niz $\langle a_n\rangle_{n\in N}$ je, evidentno, bez elemenata beskonačne visine (jer je i niz $\langle b_n\rangle_{n\in N}$ bez njih), a za svako $n \in N$ je $a_n - a_{n+1} = (b_1 + \cdots + b_{k_n}) - (b_1 + \cdots + b_{k_n} + \cdots + b_{k_{n+1}}) = (-b_{k_n+1}) + \cdots + (-b_{k_{n+1}}) \in p^n A$. Radi se, znači, o Cauchyevom, dakle i konvergentnom nizu. Neka je $a$ njegova granična vrednost i $(a)\varphi = \langle b'_n\rangle_{n\in N}$. Jasno, $(a_n)\varphi = \langle b_1,\ldots,b_{k_n},0,\ldots,0,\ldots\rangle$; ovde, naglasimo, imamo izvesnu nedoslednost u pisanju nizova, no verujemo da to, s obzirom na ceo kontekst, ne unosi zabunu. Sledi: $(a-a_n)\varphi = \langle b'_1 - b_1,\ldots,b_{k_n} - b'_{k_n}, b'_{k_n+1},\ldots\rangle \in (p^n A)\varphi = p^n(A)\varphi$, te je $b'_i - b_i = 0$ za $i = 1,\ldots,n$. Prema tome: $(a)\varphi = \langle b'_n\rangle_{n\in N} = \langle b_n\rangle_{n\in N}$.

($\Longleftarrow$) Neka je $(\mathbf{A})\varphi = \overline{\mathbf{B}}$ za bazičnu podgrupu $\mathbf{B}$ grupe $\mathbf{A}$ i neka je $\langle a_n\rangle_{n\in N}$ Cauchyev niz u $\mathbf{A}$, a $(a_n)\varphi = \langle b^n_k\rangle_{k\in N} \in \overline{B}$. Kako je $a_n - a_{n+1} \in p^n A$, to je $(a_n - a_{n+1})\varphi = \langle b^n_k - b^{n+1}_k\rangle_{k\in N} \in p^n(A)\varphi = p^n\overline{B}$, pa je $b^n_i = b^{n+1}_i$ za $i = 1,\ldots,n$, i generalno, za svako $r \in N$ je $b^n_r - b^{n+1}_r \in p^n\overline{B}$. Zapravo, lako se pokazuje indukcijom da je $b^k_i - b^n_i \in p^n\overline{B}$ za svako $k > n$. No onda je element-niz $\overline{b} = \langle b^n_n\rangle_{n\in N}$ grupe $\sum^c_{n\in N}\mathbf{B}_n$ u podgrupi $\overline{\mathbf{B}}$, jer je (za ma koje $n \in N$):

$$\overline{b} - (a_n)\varphi = \langle 0,\ldots,0,b^{n+1}_{n+1} - b^n_{n+1}, b^{n+2}_{n+2} - b^n_{n+2},\ldots\rangle \in p^n\overline{B},$$

pa ako je, za neko $\overline{b}' \in \overline{B}$, $\overline{b} - (a_n)\varphi = p^n\overline{b}'$ i $p^m a_n = 0$, $p^k\overline{b}' = 0$, onda $p^{m+k}(\overline{b} - (a_n)\varphi) = p^{m+k+n}\overline{b}'$ daje $p^{m+k}\overline{b} = \langle 0\rangle$. Ujedno smo pokazali da je $\overline{b}$ i granična vrednost (limit) niza $\langle(a_n)\varphi\rangle_{n\in N}$.■

**Korolar 40.5** *Dve zatvorene p-grupe su izomorfne akko imaju izomorfne bazične podgrupe.*

**Dokaz.** Pravac ($\Longrightarrow$) važi uvek (tj. uslov zatvorenosti nije za njega potreban). Ako je $\psi$ izomorfno preslikavanje $p$-grupe $\mathbf{A}_1$ na grupu $\mathbf{A}_2$ i ako je $\mathbf{B}$ bazična podgrupa grupe $\mathbf{A}_1$, onda je $(\mathbf{B})\psi$ bazična podgrupa grupe $\mathbf{A}_2$.



S druge strane, neka su izomorfne grupe $\mathbf{B}_1$ i $\mathbf{B}_2$ bazične podgrupe zatvorenih $p$-grupa, respektivno, $\mathbf{A}_1$ i $\mathbf{A}_2$. Prema prethodnoj teoremi je (videti dokaz): $\mathbf{A}_1 \cong \overline{\mathbf{B}}_1$ i $\mathbf{A}_2 \cong \overline{\mathbf{B}}_2$, a jasno, imamo i $\overline{\mathbf{B}}_1 \cong \overline{\mathbf{B}}_2$.

Primetimo još samo (iako nam to nije trebalo u dokazu) da prema 39.21 važi: ako su neke dve bazične podgrupe grupa, respektivno, $\mathbf{A}_1$ i $\mathbf{A}_2$, izomorfne, onda je i svaka bazična podgrupa grupe $\mathbf{A}_1$ izomorfna sa svakom bazičnom podgrupom grupe $\mathbf{A}_2$.□

**Lema 40.6** *Ako je $\mathbf{A} = \sum_{\alpha<\lambda}\mathbf{A}_\alpha$ zatvorena p-grupa, onda za neki dovoljno velik prirodan broj $m$ važi: $p^m\mathbf{A}_\alpha = \mathbf{O}$ za skoro svako $\alpha < \lambda$.*

**Dokaz.** Pokazaćemo prvo da je direktni sumand zatvorene $p$-grupe takođe zatvorena grupa. Neka je $\mathbf{A} = \mathbf{C}\oplus\mathbf{D}$ i neka je $\langle c_n\rangle_{n\in N}$ Cauchyev niz u $\mathbf{C}$ sa limesom $a = c + d$ u $\mathbf{A}$. Onda je, za svako $n \in N$, $a - c_n = (c - c_n) + d \in p^n A = p^n C\oplus p^n D$, pa je $d$, kao element konačne visine, jednak 0, i $a = c \in C$.

Pretpostavimo dalje da postoji niz $\mathbf{A}_{\alpha_1},\ldots,\mathbf{A}_{\alpha_k},\ldots$ podgrupa (direktnih sumanada date dekompozicije) za koje je $p^n\mathbf{A}_{\alpha_n} \neq \mathbf{O}$. Neka je, za $n \in N$, $0 \neq a_n \in p^n A_{\alpha_n}$ element reda $p$ i $g_n = a_1 + \cdots + a_n$. Kako je $g_n - g_{n+1} = -a_{n+1} \in p^{n+1}A_{\alpha_{n+1}} \subseteq p^n\sum^d_{k\in N}A_{\alpha_k}$, niz $\langle g_n\rangle_{n\in N}$ je Cauchyev niz u direktnom sumandu grupe $\mathbf{A}$ - $\sum_{k\in N}\mathbf{A}_{\alpha_k}$. Prema gore konstatovanom, limes niza $\langle g_n\rangle_{n\in N}$ je u $\sum_{k\in N}\mathbf{A}_{\alpha_k}$; neka je to $g \in A_{\alpha_1} + \cdots + A_{\alpha_l}$. Onda je, zbog $g - g_n = (g - g_l) + (-a_{l+1}) + \cdots + (-a_n) \in p^n\sum^d_{k\in N}A_{\alpha_k}$ za svako $n > l$, $n \leq h(g - g_n) \leq h(a_{l+1})$ (jer je $-a_{l+1}$ komponenta elementa $g - g_n$ u direktnoj sumi). Proizilazi da je $h(a_{l+1}) = \infty$, tj. da je $a_{l+1} = 0$, kontradikcija. Znači, za dovoljno veliko $m$ je $p^m A_\alpha = O$ za skoro svako $\alpha$; u protivnom bismo dobili niz kao gore: $\mathbf{A}_{\alpha_1}$ je "prvi" sumand, s obzirom na uređenje ordinala $\lambda$, takav da je $p\mathbf{A}_{\alpha_1} \neq \mathbf{O}$, $\mathbf{A}_{\alpha_2}$ "prvi" od preostalih sumanada (posmatramo ordinale iz $\lambda \setminus \{\alpha_1\}$) takav da je $p^2\mathbf{A}_{\alpha_2} \neq \mathbf{O}$ (primetimo da ne mora biti $\alpha_1 < \alpha_2$) itd.□

**Korolar 40.7** *Zatvorena p-grupa je direktna suma cikličnih grupa akko je ograničena.*

**Dokaz.** Pravac ($\Longleftarrow$) je dat (35.2), a pravac ($\Longrightarrow$) je direktna posledica prethodne leme. Ako je $\mathbf{A} = \sum_{\alpha<\lambda}\langle a_\alpha\rangle$, prema prethodnoj lemi je za neko dovoljno $m$ $p^m\langle a_\alpha\rangle = \mathbf{O}$ za skoro svako $\alpha < \lambda$. Ostaje, dakle, samo konačno mnogo cikličnih sumanada (eventualno nijedan) $\langle a_{\alpha_1}\rangle,\ldots,\langle a_{\alpha_k}\rangle$, redova, respektivno, $p^{m_1},\ldots,p^{m_k}$, većih od $p^m$. Ako je $n = max\{m_1,\ldots,m_k\}$, onda je $p^n\mathbf{A} = \mathbf{O}$.□

**Teorema 40.8** *Reducirana p-grupa je algebarski kompaktna akko je zatvorena.*

**Dokaz.** Ako je $p$-grupa $\mathbf{A}$ podgrupa grupe $\mathbf{B}$, onda je podgrupa i podgrupe $\mathbf{B}_p$ grupe $\mathbf{B}$, gde je, podsećamo, $B_p \overset{\text{def}}{=} \{b \in B \mid red(b)$ je stepen (prostog) broja $p\}$. Takođe, ako je, recimo, $\mathbf{C}$ potpuna podgrupa grupe $\mathbf{B}_p$, onda

je $\mathbf{C}$ potpuna podgrupa i grupe $\mathbf{B}$ (imamo u vidu "tranzitivnost" svojstva potpunosti). Stoga ćemo se u nastavku ograničiti na razmatranje $p$-grupa.

($\Longrightarrow$) Neka je $\mathbf{A}$ $p$-reducirana algebarski kompaktna grupa. Pokazaćemo prvo da je bez elemenata beskonačne visine. Zaista, neka je $a$ jedan njen element reda $p$ i beskonačne visine. Posmatrajmo Abelovu grupu $\mathbf{C}$ sa prezentacijom $(A \cup \{c_n \mid n \in N\};\ P_{\mathbf{A}} \cup \{pc_1 \sim a\} \cup \{pc_{n+1} \sim c_n\} \cup \{a' + c_k \sim c_k + a' \mid a' \in A, k \in N\}$, gde je $P_{\mathbf{A}}$ tablica "sabiranja" grupe $\mathbf{A}$, a $A \cap \{c_n \mid \in n \in N\} = \emptyset$. Uzajamna permutabilnost elemenata $c_i, c_j$, $i < j$, sledi iz izvedenih veza $p^{j-i}c_j \sim c_i$. Zbog tih veza je i svaki element grupe $\mathbf{C}$ oblika $a' + rc_k$ (za neko $a' \in A$, neko $k \in N$ i neko $r \in Z$ uzajamno prosto sa $p$). $\mathbf{A}$ je potpuna podgrupa grupe $\mathbf{C}$. Jer, neka je $a' + rc_k$ rešenje jednačine $p^m x = a'' \in A$. Onda je $p^m a' + p^m rc_k = a''$, tj. $p^m rc_k = a'' - p^m a' \in A$, i prema relacijama koje određuju grupu $\mathbf{A}$ mora biti $m \geq k$; inače je $p^m rc_k = rc_{k-m} \in A$, a tada i $c_{k-m} \in A$, kontradikcija (za cele brojeve $u$ i $v$ takve da je $ur + vp^{k-m} = 1$ imali bismo $c_{k-m} = (ur + vp^{k-m})c_{k-m} = u(rc_{k-m}) + vp^{k-m}c_{k-m} = u(rc_{k-m}) + va \in A$). Dakle, $p^m rc_k \in \langle a \rangle$ i pošto je $a$ beskonačne visine, to je $p^m rc_k = p^m a'''$ za neko $a''' \in A$, pa je i $a'' + a'''$ rešenje jednačine $p^m x = a'$. Prema uslovu je $\mathbf{A}$ direktni sumand grupe $\mathbf{C}$; neka je $\mathbf{C} = \mathbf{A} \oplus \mathbf{D}$. Ali, ako je, za $n \in N$, $c_n = a_n + d_n$, sistem elemenata $\{a\} \cup \{a_n \mid n \in N\}$ generiše Prüferovu (znači deljivu) grupu $(pa_1 = a, \ldots, pa_{n+1} = a_n, \ldots)$, kontradikcija. Ako $\mathbf{A}$ ne bi bila zatvorena grupa, onda bi prema 40.2 i 40.4 bila izomorfna nekoj pravoj potpunoj podgrupi zatvorenja $\overline{\mathbf{B}}$ neke svoje bazične podgrupe $\mathbf{B}$. Identifikujući $\mathbf{A}$ i $\mathbf{B}$ sa slikama u $\overline{\mathbf{B}}$, imali bismo $\mathbf{B} \leq \mathbf{A}$, a, prema uslovu leme grupa $\mathbf{A}$ bi bila i direktni sumand grupe $\overline{\mathbf{B}}$. No, to je nemoguće. Prema 39.12 je $\overline{\mathbf{B}}/\mathbf{B}$ deljiva grupa, pa je i $\overline{\mathbf{B}}/\mathbf{A}$ ($\cong (\overline{\mathbf{B}}/\mathbf{B})/(\mathbf{A}/\mathbf{B})$) deljiva grupa, te bi $\overline{\mathbf{B}}$ sadržavala deljivu grupu, prema tome i elemente beskonačne visine. Opet, očigledno je da $\overline{\mathbf{B}}$ nema elemenata beskonačne visine; uostalom, tako nešto smo već pokazali u kontraprimeru Kuroša datom nakon 35.5.

($\Longleftarrow$) Neka je $p$-zatvorena grupa $\mathbf{A}$ potpuna podgrupa grupe $\mathbf{C}$ i neka je $\mathbf{B}_1 = \sum_{\alpha<\lambda} \langle b_\alpha \rangle$ bazična podgrupa grupe $\mathbf{A}$. Sistem $\{b_\alpha \mid \alpha < \lambda\}$ je maksimalan slabo linearno nezavisni potpuni sistem grupe $\mathbf{A}$ (39.2). Proširimo ga do maksimalnog takvog grupe $\mathbf{C}$: $\{b_\alpha \mid \alpha < \lambda\} \cup \{c_\gamma \mid \gamma < \mu\}$. Onda je $\mathbf{B}_1 \oplus \mathbf{B}_2 = \sum_{\alpha<\lambda} \langle b_\alpha \rangle \oplus \sum_{\gamma<\mu} \langle c_\gamma \rangle$ bazična podgrupa grupe $\mathbf{C}$ i prema uvodu u teoremu 40.1 postoji homomorfno preslikavanje ($\varphi$) grupe $\mathbf{C}$ u zatvorenje grupe $\mathbf{B}_1 \oplus \mathbf{B}_2$ – $\overline{\mathbf{B}_1} \oplus \overline{\mathbf{B}_2}$. Kompozicija preslikavanja $\varphi \circ \pi_{\overline{B_1}}$, gde je $\pi_{\overline{B_1}}$ projekcija grupe $\overline{\mathbf{B}_1} \oplus \overline{\mathbf{B}_2}$ na grupu $\overline{\mathbf{B}_1}$, homomorfno je preslikavanje grupe $\mathbf{C}$ u $\overline{\mathbf{B}_1}$. $\varphi|_{B_1}$ je injektivno preslikavanje ($\mathbf{Ker}(\varphi)$ je, podsećamo, $\mathbf{C}^1$ ili, jednostavnije, videti kako je $\varphi$ definisano). $\varphi|_A$ je isto tako izomorfno preslikavanje grupe $\mathbf{A}$ na $\overline{\mathbf{B}_1}$ (imamo u vidu da je $\mathbf{A} \cap \mathbf{B}_2 = \mathbf{O}$ – videti i 39.6). Stoga je $(\varphi|_A)^{-1}$ izomorfno preslikavanje grupe $\overline{\mathbf{B}_1}$ na $\mathbf{A}$, a $\varphi \circ \pi_{\overline{B_1}} \circ (\varphi|_A)^{-1}$ idempotentni endomorfizam grupe $\mathbf{C}$ koji je preslikava na $\mathbf{A}$. Prema korolaru 30.12 $\mathbf{A}$ je direktni sumand grupe $\mathbf{C}$.■



**Primer 40.9** (*a*) *Niz $\langle a_n \rangle_{n\in N}$ $p$-grupe $\mathbf{A}$ bez elemenata beskonačne visine konvergentan je akko je presek familije koseta $\{a_n + p^n A \mid n \in N\}$ neprazan ($\bigcap_{n\in N}(a_n + p^n A) \neq \emptyset$).*

(*b*) *Ako su $\langle a_n \rangle_{n\in N}$ i $\langle b_n \rangle_{n\in N}$ konvergentni nizovi sa istim limesom $p$-grupe $\mathbf{A}$ bez elemenata beskonačne visine, niz $a_1, b_1, a_2, b_2, \ldots, a_n, b_n, \ldots$ ne mora biti konvergentan.*

**Dokaz.** Neka je $\mathbf{A} = t(\sum^c_{n\in N} \mathbf{Z}_{p^n})$, gde je $\mathbf{Z}_{p^n} = \langle p^n, +_{p^n} \rangle$ "standardna" ciklična grupa reda $p^n$. $\mathbf{A}$ je, već smo pokazali, bez elemenata beskonačne visine. Neka je, za $n \in N$, $a_n = \langle 1, p, \ldots, p^{n-1}, 0, \ldots, 0, \ldots \rangle$, a $b_n = a_{n+1}$. Oba niza imaju isti limes – $c = \langle 1, p, p^2, \ldots, p^n, \ldots \rangle$:

$c - a_n = \langle 0, \ldots, 0, p^n, p^{n+1}, p^{n+2}, \ldots \rangle \in p^n A$,

$c - b_n = c - a_{n+1} = \langle 0, \ldots, 0, p^{n+1}, p^{n+2}, \ldots \rangle \in p^{n+1} A \subseteq p^n A$.

S druge strane, niz $\langle c_n \rangle_{n\in N}$, gde je $c_n = \begin{cases} a_{\frac{n+1}{2}} & \text{za neparno } n \\ b_{\frac{n}{2}} = a_{\frac{n}{2}+1} & \text{za parno } n \end{cases}$ (dakle niz: $a_1, a_2, a_2, a_3, a_3, \ldots, a_n, a_n, \ldots$), nije konvergentan. Jer, pretpostavimo da je $d = \langle d_1, d_2, \ldots, d_n, \ldots \rangle$ njegov limes. Iz $d - c_2 = d - b_1 = d - a_2 = \langle d_1 - 1, d_2 - p, d_3, d_4, \ldots \rangle \in p^2 A$ sledi: $d_1 = 1$, $d_2 = p$ i $d_i$ je deljivo sa $p^2$ za $i > 2$. Iz $d - c_3 = d - a_2 = \langle 0, 0, d_2, d_3, \ldots \rangle \in p^3 A$ sledi: $d_3 = 0$ i $d_i$ je deljivo sa $p^3$ za $i > 3$. No, sada $d - c_4 = d - b_2 = d - a_3 = \langle 0, 0, -p^2, d_4, d_5, \ldots \rangle \notin p^4 A$.

(*c*) *Homomorfna slika zatvorene $p$-grupe ne mora biti zatvorena.*

**Dokaz.** Prema 39.12 $\mathbf{B} = \sum_{n\in N} \mathbf{B}_n$, gde je $\mathbf{B}_n$, kao i obično, direktna suma cikličnih grupa reda $p^n$, bazična je podgrupa svog zatvorenja $\overline{\mathbf{B}} = t(\sum^c_{n\in N} \mathbf{B}_n)$, pa je prema 40.4 $\overline{\mathbf{B}}$ zatvorena $p$-grupa. Prema 39.26 postoji endomorfizam grupe $\overline{\mathbf{B}}$ koji je preslikava na $\mathbf{B}$. Ponovo prema lemi 40.4 $\mathbf{B}$ nije zatvorena $p$-grupa.□

## 41 Nizovi Ulma $p$-grupa

S nizovima Ulma započinjemo ispitivanje $p$-grupa sa elementima beskonačne visine. Pre same definicije podsetimo se da je za $p$-grupu $\mathbf{A}$ sa $\mathbf{A}^1$ obeležena njena podgrupa čiji je domen skup svih elemenata beskonačne visine (grupe $\mathbf{A}$).

**Definicija 41.1** *Za datu $p$-grupu $\mathbf{A}$ definišemo rekurzivno (koristimo transfinitnu rekurziju po klasi ordinala):*

$\mathbf{A}^0 = \mathbf{A}$;

$\mathbf{A}^{\alpha+1} = (\mathbf{A}^\alpha)^1$;

*i za granični ordinal $\alpha$*

$\mathbf{A}^\alpha = \bigcap_{\beta<\alpha} \mathbf{A}^\beta$.

S obzirom da je $\mathbf{A}^\alpha \geq \mathbf{A}^\beta$ za $\alpha < \beta$, postoji najmanji ordinal $\tau$, kardinalnosti manje od ili jednake $|A|$, za koji je ispunjeno: $\mathbf{A}^\tau = \mathbf{A}^{\tau+1} = \cdots$. Ordinal $\tau$ naziva se *tipom Ulma* grupe $\mathbf{A}$, ili kraće, kada se ne pominju i neki drugi tipovi, *tipom* grupe $\mathbf{A}$. Piše se i $\tau = \tau(\mathbf{A})$.

**Definicija 41.2** *Neka je $\tau$ tip grupe $\mathbf{A}$ i neka je, za $\alpha < \tau$, $\mathbf{A}_\alpha = \mathbf{A}^\alpha/\mathbf{A}^{\alpha+1}$. Niz:*

$$\mathbf{A}_0, \ldots, \mathbf{A}_\alpha, \ldots, \quad \alpha < \tau,$$

*je niz Ulma grupe $\mathbf{A}$, a grupe $\mathbf{A}_\alpha$, $\alpha < \tau$, su faktori Ulma (grupe $\mathbf{A}$).*

*Nizovi Ulma p-grupa $\mathbf{A}$ i $\mathbf{B}$ su izomorfni akko je $\tau(\mathbf{A}) = \tau(\mathbf{B})$ i $\mathbf{A}_\alpha \cong \mathbf{B}_\alpha$ za svako $\alpha < \tau(\mathbf{A})$.*

Pre nego što pređemo na dalja razmatranja uočimo da je $\mathbf{A}^\tau$, gde je $\tau$ tip grupe $\mathbf{A}$, deljiva podgrupa (jer $\mathbf{A}^\tau = \mathbf{A}^{\tau+1}$ upravo znači da su svi elementi grupe $\mathbf{A}^\tau$ beskonačne visine) i kao takva direktni sumand grupe $\mathbf{A}$. Kako je karakterizacija deljivih grupa poznata, od interesa su jedino $p$-reducirane grupe. Ako je $\mathbf{A}$ jedna takva, onda je, jasno, $\mathbf{A}^\tau$ nula podgrupa.

**Lema 41.3** *Neka je $\varphi$ surjektivno homomorfno preslikavanje p-grupe $\mathbf{A}$ na grupu $\mathbf{B}$ i neka je $\mathbf{Ker}(\varphi) \leq \mathbf{A}^1$. Tada (za svako $a \in A$) $a$ i $(a)\varphi$ imaju iste visine.*

**Dokaz.** Uvek imamo, zbog svojstva homomorfnosti preslikavanja $\varphi$: $h(a) \leq h((a)\varphi)$. Stoga je samo relacija $h((a)\varphi) \leq h(a)$ u pitanju. Neka je $(a)\varphi = p^m b$. Onda je, zbog surjektivnosti preslikavanja $\varphi$, $b = (a_1)\varphi$ za neko $a_1 \in A$, pa je $a - p^m a_1 \in Ker(\varphi)$. Neka je $a - p^m a_1 = a_2 \in Ker(\varphi)$. Po uslovu leme je $a_2$ beskonačne visine, te je $a = p^m a_1 + a_2$ deljivo sa $p^m$.□

**Korolar 41.4** *Svi faktori Ulma reducirane p-grupe $\mathbf{A}$ tipa $\tau$ su bez elemenata beskonačne visine i, osim možda faktora $\mathbf{A}_{\tau-1} = \mathbf{A}^{\tau-1}/\mathbf{A}^\tau \cong \mathbf{A}^{\tau-1}$, ukoliko ovaj uopšte postoji, neograničeni.*

**Dokaz.** Pre samog dokaza recimo, ukoliko je to uopšte potrebno, da sa $\tau - 1$ obeležavamo prethodnika ordinala $\tau$ ($\tau = (\tau-1)^+$) ako ovaj postoji, tj. ako je $\tau$ nasledni ordinal.

Prvi deo tvrđenja je direktna posledica prethodne leme.

Pretpostavimo da je $p^m\mathbf{A}_\alpha = p^m(\mathbf{A}^\alpha/\mathbf{A}^{\alpha+1}) = \mathbf{O}$ za neko $\alpha < \tau$ i neki prirodan broj $m$. Znači, za svako $a \in A^\alpha$ je $p^m(a + A^{\alpha+1}) = A^{\alpha+1}$, odnosno $p^m a \in A^{\alpha+1}$. Prema tome, $p^m A^\alpha \subseteq A^{\alpha+1}$. Pokazaćemo da je $p\mathbf{A}^{\alpha+1} = \mathbf{A}^{\alpha+1}$, drugim rečima da je $\mathbf{A}^{\alpha+1}$ deljiva podgrupa (33.1), dakle nula grupa. Neka je $b \in A^{\alpha+1} = (A^\alpha)^1$. Onda je, za neko $c \in A^\alpha$, $b = p^{m+1}c = p(p^m c) \in p(p^m A) \subseteq pA^{\alpha+1}$. Zaključujemo da je $\tau = \alpha + 1$ (ili, po volji, $\alpha = \tau - 1$); dakle, samo faktor $\mathbf{A}_{\tau-1}$ može biti ograničen.□



**Lema 41.5** *Neka je $\mathbf{A}$ reducirana p-grupa tipa $\tau$. Tada važi:*

*(a) niz Ulma podgrupe $\mathbf{A}^\gamma$ je $\mathbf{A}_\gamma, \mathbf{A}_{\gamma+1}, \ldots$;*

*(b) niz Ulma faktor grupe $\mathbf{A}/\mathbf{A}^\gamma = \overline{\mathbf{A}}$ je, do na izomorfizam:*

$$\mathbf{A}_0, \ldots, \mathbf{A}_\alpha, \ldots, \quad \alpha < \gamma.$$

**Dokaz.** (*b*) Prema 41.3, za kanonički homomorfizam $\varphi : A \longrightarrow A/A^\gamma = \overline{A}$ važi: $(\overline{\mathbf{A}}^1)\varphi^{-1} = \mathbf{A}^1$, dakle, $(\mathbf{A}^1)\varphi = \mathbf{A}^1/\mathbf{A}^\gamma = \overline{\mathbf{A}}^1$. Transfinitnom indukcijom dokazujemo da je, generalno, $\overline{\mathbf{A}}^\alpha = \mathbf{A}^\alpha/\mathbf{A}^\gamma = (\mathbf{A}^\alpha)\varphi$ za $\alpha < \gamma$. Ako je $\alpha$ ($= \beta + 1$) nasledni ordinal, onda je, kao i maločas, za kanonički homomorfizam $\varphi_\beta : A^\beta \longrightarrow A^\beta/A^\gamma = \overline{A}^\beta$ (po induktivnoj pretpostavci):

$$(\overline{\mathbf{A}}^\alpha)\varphi_\beta^{-1} = (\overline{\mathbf{A}}^{\beta+1})\varphi_\beta^{-1} = ((\overline{\mathbf{A}}^\beta)^1)\varphi_\beta^{-1} = (\mathbf{A}^\beta)^1 = \mathbf{A}^{\beta+1} = \mathbf{A}^\alpha.$$

Za granični ordinal $\alpha$ je $\overline{\mathbf{A}}^\alpha = \bigcap_{\beta<\alpha} \overline{\mathbf{A}}^\beta$, pa je $(\overline{\mathbf{A}}^\alpha)\varphi^{-1} = (\bigcap_{\beta<\alpha} \overline{\mathbf{A}}^\beta)\varphi^{-1} = \bigcap_{\beta<\alpha}(\overline{\mathbf{A}}^\beta)\varphi^{-1} = \bigcap_{\beta<\alpha} \mathbf{A}^\beta$ (po induktivnoj pretpostavci) $= \mathbf{A}^\alpha$ i opet važi $(\mathbf{A}^\alpha)\varphi = \mathbf{A}^\alpha/\mathbf{A}^\gamma = \overline{\mathbf{A}}^\alpha$. Prema trećoj teoremi o izomorfizmu i upravo dokazanom je, konačno, za svako $\alpha < \gamma$:

$$\overline{\mathbf{A}}_\alpha = \overline{\mathbf{A}}^\alpha/\overline{\mathbf{A}}^{\alpha+1} = (\mathbf{A}^\alpha/\mathbf{A}^\gamma)/(\mathbf{A}^{\alpha+1}/\mathbf{A}^\gamma) \cong \mathbf{A}^\alpha/\mathbf{A}^{\alpha+1} = \mathbf{A}_\alpha.\square$$

**Lema 41.6** *Neka je reducirana p-grupa $\mathbf{A}$ direktna suma: $\mathbf{A} = \sum_{\gamma<\lambda} \mathbf{B}_\gamma$. Tada važi:*

*(a) $\mathbf{A}^\alpha = \sum_{\gamma<\lambda} \mathbf{B}_\gamma^\alpha$ za svako $\alpha < \tau(\mathbf{A})$;*

*(b) niz Ulma grupe $\mathbf{A}$ je, do na izomorfizam:*

$$\sum_{\gamma<\lambda}(\mathbf{B}_\gamma)_0, \ldots, \sum_{\gamma<\lambda}(\mathbf{B}_\gamma)_\alpha, \ldots, \quad \alpha < \tau(\mathbf{A}),$$

*gde je, za $\gamma < \lambda$ i $\alpha \geq \tau(\mathbf{B}_\gamma)$, $(\mathbf{B}_\gamma)_\alpha$ nula grupa.*

**Dokaz.** (*a*) Jasno, $\mathbf{A}^1 = \sum_{\gamma<\lambda}(\mathbf{B}_\gamma)^1$. Rekli smo, u direktnoj sumi visina elementa jednaka je minimalnoj visini njegovih komponenata; matematički zapisano: ako je $a = b_{\gamma_1} + \cdots + b_{\gamma_k}$, onda je $h(a) = min\{h(b_{\gamma_1}), \ldots, h(b_{\gamma_k})\}$. Transfinitnom indukcijom pokazujemo da važi (*a*). Ako je $\alpha$ ($= \beta+1$) nasledni ordinal, onda je $\mathbf{A}^\alpha = (\mathbf{A}^\beta)^1 = (\sum_{\gamma<\lambda}(\mathbf{B}_\gamma)^\beta)^1$ (prema induktivnoj hipotezi) $= \sum_{\gamma<\lambda}((\mathbf{B}_\gamma)^\beta)^1$ (prema gornjoj diskusiji) $= \sum_{\gamma<\lambda}(\mathbf{B}_\gamma)^{\beta+1} = \sum_{\gamma<\lambda}(\mathbf{B}_\gamma)^\alpha$. Ako je $\alpha$ granični ordinal, imamo: $\mathbf{A}^\alpha = \bigcap_{\beta<\alpha} \mathbf{A}^\beta = \bigcap_{\beta<\alpha}(\sum_{\gamma<\lambda}(\mathbf{B}_\gamma)^\beta)$ (prema induktivnoj hipotezi) $= \sum_{\gamma<\lambda}(\bigcap_{\beta<\alpha}(\mathbf{B}_\gamma)^\beta) = \sum_{\gamma<\lambda}(\mathbf{B}_\gamma)^\alpha$. Što se tiče jednakosti $\bigcap_{\beta<\alpha}(\sum_{\gamma<\lambda}(\mathbf{B}_\gamma)^\beta) = \sum_{\gamma<\lambda}(\bigcap_{\beta<\alpha}(\mathbf{B}_\gamma)^\beta)$, inkluzija $\geq$ je očigledna, a ako je $a = b_{\gamma_1} + \cdots + b_{\gamma_k} \in \bigcap_{\beta<\alpha}(\sum_{\gamma<\lambda}(B_\gamma)^\beta)$, onda je, za svako $\beta < \alpha$, $b_{\gamma_1} + \cdots + b_{\gamma_k} \in \sum_{\gamma<\lambda}(B_\gamma)^\beta$, pa je $b_{\gamma_i} \in (B_{\gamma_i})^\beta$ za $i = 1, \ldots, k$. Znači, $b_{\gamma_i} \in \bigcap_{\beta<\alpha}(B_{\gamma_i})^\beta$ i $a \in \sum_{\gamma<\lambda}(\bigcap_{\beta<\alpha}(B_\gamma)^\beta)$.

($b$) Direktna posledica prethodne tačke i toliko puta ponavljane tačke ($c$) leme 10.3:

$$\mathbf{A}_\alpha = \mathbf{A}^\alpha/\mathbf{A}^{\alpha+1} = (\sum_{\gamma<\lambda}(\mathbf{B}_\gamma)^\alpha)/(\sum_{\gamma<\lambda}(\mathbf{B}_\gamma)^{\alpha+1}) \cong$$

$$\sum_{\gamma<\lambda}(\mathbf{B}_\gamma)^\alpha/(\mathbf{B}_\gamma)^{\alpha+1} = \sum_{\gamma<\lambda}(\mathbf{B}_\gamma)_\alpha.$$

**Teorema 41.7** *Neka je* $\mathbf{A}$ *reducirana p-grupa tipa* $\tau\,(=\tau(\mathbf{A}))$ *i neka je* $\mathbf{A}_0$, $\mathbf{A}_1, \ldots, \mathbf{A}_\alpha, \ldots, \alpha < \tau$, *njen niz Ulma. Tada važi:*

($a$) $\sum_{\alpha<\tau}|A_\alpha| \leq |A| \leq \prod_{\alpha<min\{\omega,\tau\}}|A_\alpha|$;

($b$) *za svako* $\beta < \tau$ *je* $\sum_{\beta\leq\alpha<\tau}|A_\alpha| \leq |A_\beta|^{\aleph_0}$;

($c$) *ako je* $\mathbf{B}_{\alpha+1}$ *bazična podgrupa grupe* $\mathbf{A}_{\alpha+1}$ *i ako je* $\alpha+1<\tau$, *onda je* $r(\mathbf{B}_{\alpha+1}) \leq fin\ r(\mathbf{A}_\alpha)$.

**Dokaz.** ($a$) Pretpostavićemo, naravno, da je grupa $\mathbf{A}$ beskonačna; slučaj je inače trivijalan.

Kako je $A = \bigcup_{\alpha<\tau}(A^\alpha - A^{\alpha+1}) \cup \{0\}$ i $|A^\alpha - A^{\alpha+1}| \geq |A^\alpha/A^{\alpha+1}| = |A_\alpha|$ za svako $\alpha < \tau$ (osim možda za $\alpha = \tau - 1$, što podrazumeva i da je $\tau$ nasledni ordinal), imamo:

$$|A| = \sum_{\alpha<\tau}|A^\alpha - A^{\alpha+1}| \geq \sum_{\alpha<\tau}|A^\alpha/A^{\alpha+1}| = \sum_{\alpha<\tau}|A_\alpha|.$$

U slučaju druge nejednakosti – $|A| \leq \prod_{\alpha<min\{\omega,\tau\}}|A_\alpha|$ – razlikovaćemo slučajeve: $\tau$ je prirodan broj i $\tau$ je beskonačni kardinal. Ako je $\tau = n \in N$, onda je prema 3.9:

$$|A| = [\mathbf{A}:\mathbf{A}^1]\cdot|A^1| = \cdots = |A/A^1|\cdot|A^1/A^2|\cdot\ldots\cdot|A^{n-1}/A^n| =$$

$$|A_0|\cdot\ldots\cdot|A_{n-1}| = \prod_{k<n}|A_k|.$$

Ako je $\tau$ beskonačni kardinal i $|A_m| = min\{|A_k| \mid k \in \omega\}$, onda je (s obzirom na 39.20):

$$|A| = |A/A^m|\cdot|A^m| = |A_0|\cdot\ldots\cdot|A_{m-1}|\cdot|A^m| \leq |A_0|\cdot\ldots\cdot|A_{m-1}|\cdot|A_m|^{\aleph_0} \leq$$

$$|A_0|\cdot\ldots\cdot|A_{m-1}|\cdot\prod_{m\leq\alpha<min\{\omega,\tau\}}|A_\alpha| = \prod_{\beta<min\{\omega,\tau\}}|A_\beta|.$$

($b$) Prema prethodnoj tački i korolaru 39.20 izvodimo direktno:

$$\sum_{\beta\leq\alpha<\tau}|A_\alpha| \leq |A^\beta| \leq |A_\beta|^{\aleph_0}.$$

($c$) Neka je $B_{\alpha+1} = \sum_{\beta<\lambda}\langle b_\beta + A^{\alpha+2}\rangle$ bazična podgrupa grupe $\mathbf{A}_{\alpha+1} = A^{\alpha+1}/\mathbf{A}^{\alpha+2}$; dakle, $r(\mathbf{B}_{\alpha+1}) = \lambda$. Onda za svako $\beta < \lambda$ i svaki prirodan broj $n$ jednačina $b_\beta + A^{\alpha+2} = p^n(x + A^{\alpha+2})$ ima rešenje u $\mathbf{A}^\alpha/\mathbf{A}^{\alpha+2}$ (svi elementi grupe $\mathbf{A}^{\alpha+1}$ su beskonačne visine u $\mathbf{A}^\alpha$). Neka su rešenja, za dato $\beta < \lambda$ i $n \in N$, $a^n_\beta + A^{\alpha+2} \in A^\alpha/A^{\alpha+2}$. Za $\beta \neq \gamma$ $(\beta,\gamma<\lambda)$ elementi $a^m_\beta$ i $a^n_\gamma$ ne pripadaju istom kosetu podgrupe $\mathbf{A}^{\alpha+1}$. Zaista, u suprotnom bismo, za $a^n_\gamma - a^m_\beta \in A^{\alpha+1}$ i, recimo, $m \leq n$, dobili: $p^n((a^n_\gamma - a^n_\beta) + A^{\alpha+2}) = p^n(a_\gamma + A^{\alpha+2}) - p^{n-m}p^m(a^m_\beta + A^{\alpha+2}) = (b_\gamma + A^{\alpha+2}) - p^{n-m}(b_\beta + A^{\alpha+2}) \in A_{\alpha+1}$, i zbog potpunosti podgrupe $\mathbf{B}_{\alpha+1}$ postojalo bi rešenje jednačine $p^n(x + A^{\alpha+2}) = (b_\gamma - p^{n-m}b_\beta) + A^{\alpha+2}$ u $\mathbf{B}_{\alpha+1}$. No, ako je to $(m_1 b_{\beta_1} + A^{\alpha+2}) + \cdots + (m_k b_{\beta_k} + A^{\alpha+2})$, onda bi za neko $i$, $1 \leq i \leq k$, bilo $\beta_i = \gamma$ i $p^n(m_i b_\gamma + A^{\alpha+2}) = b_\gamma + A^{\alpha+2}$, prema tome i $(1 - p^n m_i)b_\gamma \in A^{\alpha+2}$, odnosno $b_\gamma \in A^{\alpha+2}$ (zbog $(1 - p^n m_i, p) = 1$), kontradikcija. Element $a^n_\gamma$, $\gamma < \lambda$, $n \in N$, reda je $n$ s obzirom na podgrupu $\mathbf{A}^{\alpha+1}$ (videti definiciju 34.14). Jer, iz $p^k a^n_\gamma \in A^{\alpha+1}$ sledi za $k < n$:

$$b_\gamma + A^{\alpha+2} = p^n(a^n_\gamma + A^{\alpha+2}) = p^{n-k}(p^k a^n_\gamma + A^{\alpha+2}) \in A^{\alpha+1}/A^{\alpha+2} = A_{\alpha+1},$$

i element $b_\gamma + A^{\alpha+2}$ bi, opet bi zbog potpunosti podgrupe $\mathbf{B}_{\alpha+1}$, bio deljiv sa $p^{n-k}$ u $\mathbf{B}_{\alpha+1}$, kontradikcija. Znači, sistem elemenata reda $p$ – $\{p^n(a^{n+1}_\beta + A^{\alpha+1}) \mid \beta < \lambda\}$ – podskup je skupa $p^n A_\alpha = p^n(A^\alpha/A^{\alpha+1})$, i uz to je linearno nezavisan. Ponavljamo se: $m_1(p^n a^{n+1}_{\beta_1} + A^{\alpha+1}) + \cdots + m_k(p^n a^{n+1}_{\beta_k} + A^{\alpha+1}) = A^{\alpha+1}$, gde je $\beta_i \neq \beta_j$ za $i \neq j$ i $0 \leq m_i < p$, daje redom:

$$m_1 p^n a^{n+1}_{\beta_1} + \cdots + m_k p^n a^{n+1}_{\beta_k} = a \in A^{\alpha+1},$$

$$m_1 p^n(a^{n+1}_{\beta_1} + A^{\alpha+2}) + \cdots + m_k p^n(a^{n+1}_{\beta_k} + A^{\alpha+2}) = a + A^{\alpha+2},$$

$$m_1(b_{\beta_1} + A^{\alpha+2}) + \cdots + m_k(b_{\beta_k} + A^{\alpha+2}) = p(a + A^{\alpha+2}) \in A_{\alpha+1},$$

a po treći put potpunost podgrupe $\mathbf{B}_{\alpha+1}$ implicira $m_1 = \cdots = m_k = 0$. Zaključujemo: $r(\mathbf{B}_{\alpha+1}) \leq r(p^n\mathbf{A}_\alpha)$ za svako $n \in N$, pa je $r(\mathbf{B}_{\alpha+1}) \leq fin\ r(\mathbf{A}_\alpha)$.■



## 42 Reducirane prebrojive $p$-grupe

U vezi sa nizovima Ulma dva pitanja se prirodno nameću. Prvo, da li je svaki niz grupa

$$\mathbf{A}_0, \ldots, \mathbf{A}_\alpha, \ldots, \quad \alpha < \tau,$$

gde je $\tau$ proizvoljan ordinal i $\mathbf{A}_\alpha$ $p$-grupa bez elemenata beskonačne visine za svako $\alpha < \tau$, takođe i neograničena za $\alpha < \tau - 1$ (ukoliko je $\tau$ nasledni ordinal), niz Ulma neke $p$-grupe? Drugo, da li su $p$-grupe sa izomorfnim nizovima Ulma izomorfne?

U nastavku ograničićemo se na razmatranje prebrojivih reduciranih $p$-grupa, u kom slučaju se, jasno, gornja pitanja postavljaju sa dodatnim ograničenjima: $\tau$ je prirodan broj ili beskonačni prebrojivi ordinal, a $\mathbf{A}_\alpha$, $\alpha < \tau$, prebrojiva grupa bez elemenata beskonačne visine, dakle i direktna suma cikličnih grupa (videti 35.5). Odgovor na oba pitanja je, odmah da kažemo, potvrdan. Na pitanja su odgovorili L. Zippin i H. Ulm.

**Teorema 42.1** *(Teorema L. Zippina). Neka je $\tau$ konačan ili beskonačan prebrojiv ordinal i neka je, za svako $\alpha < \tau$, $\mathbf{A}_\alpha$ prebrojiva p-grupa bez elemenata beskonačne visine i za $\alpha < \tau - 1$ (ukoliko je $\tau$ nasledni ordinal) neograničena. Tada postoji prebrojiva reducirana p-grupa $\mathbf{A}$ čiji je niz Ulma: $\mathbf{A}_0, \ldots, \mathbf{A}_\alpha, \ldots$, $\alpha < \tau$.*

**Dokaz.** Već smo konstatovali, svaka od grupa $\mathbf{A}_\alpha$, $\alpha < \tau$, direktna je suma cikličnih grupa; neka je $\mathbf{A}_\alpha = \sum_{k\in N} \langle a_{\alpha k}\rangle$, gde je $\langle a_{\alpha k}\rangle$ ciklična grupa reda $p^{n_{\alpha k}}$. Tražena grupa $\mathbf{A}$ biće data prezentacijom $(B; R)$, gde je $B = \{b_{\alpha k} \mid \alpha < \tau, k \in N\}$, a $R$ pored relacija komutativnosti $(b_{\alpha k} + b_{\beta m} \sim b_{\beta m} + b_{\alpha k})$ uključuje i relacije oblika $p^{n_{\alpha k}} b_{\alpha k} \sim b_{\beta m}$, gde je $\alpha < \beta$, ili $p^{n_{\alpha k}} b_{\alpha k} \sim 0$ (pisaćemo 0 i + radije nego 1 i ·, kao što smo to činili u drugoj glavi; konačno, mogli smo koristiti samo $p^{n_{\alpha k}} b_{\alpha k}$) – 0 će biti znak i za "pravi" neutralni element, ali iz konteksta će biti jasno o kojoj od njenih uloga je reč. Pri svemu tome su ispunjeni sledeći uslovi:

(1) ako je $p^{n_{\alpha k}} b_{\alpha k} \sim b_{\alpha_1 k_1}$, $p^{n_{\alpha_1 k_1}} b_{\alpha_1 k_1} \sim b_{\alpha_2 k_2}$ i tako dalje, onda će se posle konačno mnogo koraka taj niz "zaustaviti", tj. stići ćemo do nekog elementa $b_{\alpha_m k_m}$ (pre toga smo imali: $p^{n_{\alpha_{m-1} k_{m-1}}} b_{\alpha_{m-1} k_{m-1}} \sim b_{\alpha_m k_m}$) za koji je $p^{n_{\alpha_m k_m}} b_{\alpha_m k_m} \sim 0$;

(2) za dati element $b_{\beta m}$, $0 < \beta < \tau$, prirodan broj $n$ i ordinal $\gamma < \beta$ postoji element $b_{\alpha i}$ takav da je $\gamma \leq \alpha < \beta$, $n_{\alpha i} > n$ i $p^{n_{\alpha i}} b_{\alpha i} \sim b_{\beta m}$
i

(3) ako je $\tau$ granični ordinal, onda za svaki ordinal $\gamma < \tau$ i svaki prirodan broj $n$ postoji element $b_{\alpha i}$ takav da je $\gamma < \alpha\ (< \tau)$, $n_{\alpha i} > n$ i $p^{n_{\alpha i}} b_{\alpha i} \sim 0$.

Dokaz je transfinitnom indukcijom. Ako je $\tau = 1$, stavljamo: $p^{n_{0k}} b_{0k} \sim 0$ (uslovi (1), (2) i (3) su trivijalno ispunjeni) i grupa sa prezentacijom $(\{b_{0k} \mid k \in N\}\ (= B); \{b_{0k} + b_{0m} \sim b_{0m} + b_{0k} \mid k, m \in N\} \cup \{p^{n_{0k}} b_{0k} \sim 0 \mid k \in N\}\ (= R))$ izomorfna je grupi $\mathbf{A}_0$, dakle, bez elemenata je beskonačne visine i njen niz Ulma je dužine 1: – $\mathbf{A}_0$. Odista, prema tačkama $(c)$ i $(i)$ primera 21.10, grupa $\mathbf{G}_{(B;R)}$ je direktna suma cikličnih grupa $\mathbf{G}_{(\{b_{\alpha k}\};\{p^{n_{\alpha k}} b_{\alpha k}\})}$ reda $p^{n_{\alpha k}}$.

Neka je u nastavku $\tau \geq 2$. Pretpostavimo prvo da je $\tau$ nasledni ordinal $(\tau = (\tau - 1)^+)$. Prema induktivnoj hipotezi postoji prebrojiva reducirana $p$-grupa $\mathbf{C}$ sa nizom Ulma: $\mathbf{A}_0, \ldots, \mathbf{A}_\alpha, \ldots$, $\alpha < \tau - 1$, i prezentacijom u predočenoj formi: $(\{b_{\alpha k} \mid \alpha < \tau - 1, k \in N\}; R)$, gde je $R$, ponavljamo, skup relacija komutativnosti i relacija oblika $p^{n_{\alpha k}} b_{\alpha k} \sim 0$ ili $p^{n_{\alpha k}} b_{\alpha k} \sim b_{\beta m}$ (za neko $\beta > \alpha$ i neko $m \in N$) za koje su ispunjeni uslovi (1), (2) i (3). Neka je, dalje, $B_1 = B \cup \{b_{\tau-1,k} \mid k \in N\}$, a $R_1$ skup relacija koja uključuje sve (potrebne) relacije komutativnosti, zadržava iz $R$ relacije oblika $p^{n_{\alpha k}} b_{\alpha k} \sim b_{\beta m}$, uključuje relacije $p^{n_{\tau-1,k}} b_{\tau-1,k} \sim 0$ i "transformiše" relacije $p^{n_{\alpha k}} b_{\alpha k} \sim 0$ iz $R$ u $p^{n_{\alpha k}} b_{\alpha k} \sim b_{\tau-1,m}$ za neko $m \in N$. Pri tome se sve učini tako da uslovi (1), (2) i (3) i dalje važe (sada za $R_1$). Naravno, samo je ispunjenje uslova (2)



u pitanju (uslov (3) uopšte nije "u igri", a uslov (1) je očigledno ispunjen). No, elemenata $b_{\tau-1,k}$ je najviše prebrojivo mnogo, pa ako je $\tau - 1$ granični ordinal, onda iz činjenice da uslov (3) važi za $R$ proizilazi da imamo dovoljno elemenata na raspolaganju da bismo ispunili "novi" uslov (2). Ako je pak $\tau - 1$ nasledni ordinal, grupa $\mathbf{A}_{\tau-2}$ je neograničena direktna suma cikličnih $p$-grupa i za svaki element $b_{\tau-2,k}$ je $p^{n_{\tau-2,k}} b_{\tau-2,k} \sim 0$ (grupa $\mathbf{G}_{(B;R)}$ je tipa $\tau - 1$, a znamo kako relacije u $R$ izgledaju); dakle, za svako $n \in N$ postoji $n_{\tau-2,i} > n$ i opet ne oskudevamo u izboru elemenata za ispunjenje uslova (2). Grupa $\mathbf{G}_{(B_1;R_1)}$ je, evidentno, $p$-grupa. Pokazaćemo sada da su svi njeni elementi $[b_{\alpha k}]$ različiti od nule. Zaista, datom elementu $b_{\alpha k}$ odgovara konačan niz relacija:

$p^{n_{\alpha k}} b_{\alpha k} \sim b_{\alpha_1 k_1}$, $p^{n_{\alpha_1 k_1}} b_{\alpha_1 k_1} \sim b_{\alpha_2 k_2}$, $\ldots$,
$p^{n_{\alpha_m k_m}} b_{\alpha_m k_m} \sim b_{\tau-1,k}$, $p^{n_{\tau-1,k}} b_{\tau-1,k} \sim 0$.

Obeležimo sumu $n_{\alpha k} + n_{\alpha_1 k_1} + \cdots + n_{\alpha_m k_m} + n_{\tau-1,k}$ sa $l(\alpha, k)$. Neka je, dalje, $\mathbf{p}^\infty$ "standardna" Prüferova grupa sa domenom $P = \{z \in C \mid z^{p^n} = 1, n \in \omega\}$, i neka je $\psi : B_1 \longrightarrow P$ preslikavanje dato sa $(b_{\alpha k})\psi = e^{\frac{2\pi}{p^{l(\alpha,k)}} i}$. Očigledno je $(u)\overline{\psi} = 1$ za svako $u \in R_1$, pa se prema 21.9 grupa $\mathbf{G}_{(B_1;R_1)}$ homomorfno preslikava u $\mathbf{p}^\infty$. Homomorfizam $\theta$ je dat sa, sećamo se, $([u])\theta = (u)\overline{\psi}$. Posebno sledi da je $[b_{\alpha k}]$ reda $p^{l(\alpha,k)}$; tog reda je element $e^{\frac{2\pi}{p^{l(\alpha,k)}} i}$ u grupi $\mathbf{p}^\infty$, prema relacijama iz datog niza je $p^{l(\alpha,k)} b_{\alpha k} \sim 0$.

S obzirom na uslov (2) lako se pokazuje transfinitnom indukcijom da je $[b_{\alpha m}] \in G^\alpha_{(B_1;R_1)}$ za svako $\alpha < \tau$ i svaki prirodan broj $m$, pa je, posebno, $[b_{\tau-1,k}] \in G^{\tau-1}_{(B_1;R_1)}$. Ako je $\alpha$ nasledni ordinal – $\alpha = \beta + 1$, onda prema uslovu (2) za svaki prirodan broj $n$ postoji element $b_{\beta k}$ takav da je $n_{\beta k} > n$ i $p^{n_{\beta k}} b_{\beta k} \sim b_{\alpha m}$, dakle, $p^{n_{\beta k}}[b_{\beta k}] = [b_{\alpha m}]$ i $[b_{\beta k}] \in G^\beta_{(B_1;R_1)}$. Zaključujemo: $[b_{\alpha m}] \in (G^\beta_{(B_1;R_1)})^1 = G^{\beta+1}_{(B_1;R_1)} = G^\alpha_{(B_1;R_1)}$. Analogno rezonujemo i u slučaju da je $\alpha$ granični ordinal. Za svako $\beta < \alpha$ i svaki prirodan broj $n$ postoji element $b_{\gamma k}$ takav da je $\beta < \gamma < \alpha$, $n_{\gamma k} > n$ i $p^{n_{\gamma k}} b_{\gamma k} \sim b_{\alpha m}$; znači, $p^{n_{\gamma k}}[b_{\gamma k}] = [b_{\alpha m}] \in G^\gamma_{(B_1;R_1)}$ $(\leq G^\beta_{(B_1;R_1)})$ i opet je $[b_{\alpha m}] \in (G^\beta_{(B_1;R_1)})^1 = G^{\beta+1}_{(B_1;R_1)}$ (a odatle je $[b_{\alpha m}] \in \bigcap_{\beta<\alpha} G^{\beta+1}_{(B_1;R_1)} = G^\alpha_{(B_1;R_1)}$).

Neka je $\mathbf{F}$ podgrupa grupe $\mathbf{G}_{(B_1;R_1)}$ generisana skupom $\{[b_{\tau-1,k}] \mid k \in N\}$ (dakle, $\mathbf{F} \leq \mathbf{G}^{\tau-1}_{(B_1;R_1)}$). Prezentacija faktor grupe $\mathbf{G}_{(B_1;R_1)}/\mathbf{F}$ je $(B_1; R_1 \cup \{b_{\tau-1,k} \sim 0 \mid k \in N\})$ (21.11), a ova se Tietzeovim transformacijama $T_2$ i $T_4$ (videti 22.1) "svodi" na $(B; R)$. Prema tome: $\mathbf{G}_{(B_1;R_1)}/\mathbf{F} \cong \mathbf{G}_{(B;R)}$. S obzirom da je $\mathbf{G}_{(B;R)}$, znači i $\mathbf{G}_{(B_1;R_1)}/\mathbf{F}$, tipa $\tau - 1$, u grupi $\mathbf{G}_{(B_1;R_1)}$ nema elemenata u $\mathbf{G}^{\tau-1}_{(B_1;R_1)}$ koji nisu u $\mathbf{F}$. Direktno se proverava transfinitnom indukcijom da je $(\mathbf{G}_{(B_1;R_1)}/\mathbf{F})^\alpha = \mathbf{G}^\alpha_{(B_1;R_1)}/\mathbf{F}$ za $\alpha < \tau$. Pretpostavimo da je tvrđenje tačno za svako $\beta < \alpha$ i neka je $\alpha = \gamma + 1$ (nasledni ordinal). Onda je:

$$(\mathbf{G}_{(B_1;R_1)}/\mathbf{F})^\alpha = ((\mathbf{G}_{(B_1;R_1)}/\mathbf{F})^\gamma)^1 = (\mathbf{G}^\gamma_{(B_1;R_1)}/\mathbf{F})^1 =$$
$$\mathbf{G}^{\gamma+1}_{(B_1;R_1)}/\mathbf{F} = \mathbf{G}^\alpha_{(B_1;R_1)}/\mathbf{F};$$

$(\mathbf{G}^{\gamma}_{(B_1;R_1)}/\mathbf{F})^1 \leq \mathbf{G}^{\gamma+1}_{(B_1;R_1)}/\mathbf{F}$ sledi iz $\mathbf{F} \leq \mathbf{G}^{\tau-1}_{(B_1;R_1)} \leq (\mathbf{G}^{\gamma}_{(B_1;R_1)})^1$ - 41.3. Za granični ordinal $\alpha$ imamo:

$$(\mathbf{G}_{(B_1;R_1)}/\mathbf{F})^{\alpha} = \bigcap_{\beta<\alpha}(\mathbf{G}_{(B_1;R_1)}/\mathbf{F})^{\beta} = (\bigcap_{\beta<\alpha}\mathbf{G}^{\beta}_{(B_1;R_1)})/\mathbf{F} = \mathbf{G}^{\alpha}_{(B_1;R_1)}/\mathbf{F}.$$

Stoga je za $\alpha < \tau - 1$ (što smo i inače znali):

$$(\mathbf{G}_{(B_1;R_1)})_{\alpha} = \mathbf{G}^{\alpha}_{(B_1;R_1)}/\mathbf{G}^{\alpha+1}_{(B_1;R_1)} \cong (\mathbf{G}^{\alpha}_{(B_1;R_1)}/\mathbf{G}^{\tau-1}_{(B_1;R_1)})/(\mathbf{G}^{\alpha+1}_{(B_1;R_1)}/\mathbf{G}^{\tau-1}_{(B_1;R_1)})$$

$$= (\mathbf{G}_{(B_1;R_1)}/\mathbf{G}^{\tau-1}_{(B_1:R_1)})^{\alpha}/(\mathbf{G}_{(B_1;R_1)}/\mathbf{G}^{\tau-1}_{(B_1;R_1)})^{\alpha+1} \cong \mathbf{G}^{\alpha}_{(B;R)}/\mathbf{G}^{\alpha+1}_{(B;R)} =$$

$$(\mathbf{G}_{(B;R)})_{\alpha} \cong \mathbf{A}_{\alpha}.$$

Grupa $\mathbf{G}^{\tau-1}_{(B_1;R_1)}$ je, jasno, izomorfna grupi $\mathbf{A}_{\tau-1}$. U pitanju je direktna suma cikličnih grupa $\sum_{k\in N}\langle[b_{\tau-1,k}]\rangle$, gde je $\langle[b_{\tau-1,k}]\rangle$ ciklična grupa reda $p^{n_{\tau-1,k}}$; jer, i $\mathbf{G}_{(B_1;R_1)}$ je direktna suma podgrupa, gde je svaki direktni sumand generisan svim onim elementima $[b_{\alpha m}]$ čije ciklične grupe ($\langle[b_{\alpha m}]\rangle$) sadrže (jedan) fiksni element $[b_{\tau-1,k}]$ - 21.10($i$). Proizilazi da je niz Ulma grupe $\mathbf{G}_{(B_1;R_1)}$, do na izomorfizam, dati niz: $\mathbf{A}_0, \ldots, \mathbf{A}_{\alpha}, \ldots$, $\alpha < \tau$.

Neka je sada $\tau$ granični ordinal. Sve grupe $\mathbf{A}_{\alpha}$, $\alpha < \tau$, neograničene su direktne sume cikličnih $p$-grupa. S obzirom da je $\tau$ prebrojivi ordinal, ovo omogućuje da se svaka od grupa $\mathbf{A}_{\alpha}$ predstavi u obliku direktne sume $\sum_{\alpha\leq\beta<\tau}\mathbf{A}_{\alpha,\beta}$, gde je svaka grupa $\mathbf{A}_{\alpha,\beta}$ neograničena suma cikličnih grupa. Prema induktivnoj hipotezi za svako $\alpha < \tau$ postoji grupa $\mathbf{H}_{\alpha}$ tipa $\alpha+1$, čiji je niz Ulma $\mathbf{A}_{0,\alpha}, \mathbf{A}_{1,\alpha}, \ldots, \mathbf{A}_{\alpha,\alpha}$, a koja je zadana prezentacijom $(B_{\alpha}; R_{\alpha})$ pri čemu su ispunjeni uslovi (1), (2) i (3). Prema 41.6($b$) za $\sum_{\beta<\tau}\mathbf{H}_{\beta}$ važi:

$$(\sum_{\beta<\tau}\mathbf{H}_{\beta})_{\alpha} = \sum_{\beta<\tau}(\mathbf{H}_{\beta})_{\alpha} = \sum_{\alpha\leq\beta<\tau}(\mathbf{H}_{\beta})_{\alpha} = \mathbf{A}_{\alpha,\alpha} + \mathbf{A}_{\alpha,\alpha+1} + \cdots = \mathbf{A}_{\alpha}.$$

Prezentacija grupe $\sum_{\beta<\tau}\mathbf{H}_{\beta}$ je sa skupom izvodnih simbola $B = \bigcup_{\alpha<\tau}B_{\alpha}$ i skupom odrednica koja je unija skupova odrednica $R_{\alpha}$ i skupom "dodatnih" relacija komutativnosti; pod "dodatnim" relacijama podrazumevamo, jasno: za svako $x \in B_{\alpha}$, $y \in B_{\beta}$, $\alpha < \tau$, imamo $x + y \sim y + x$. Koristili smo, da bismo pojednostavili notaciju, $x$ i $y$; ako bismo se držali dosledno uvođenja notacije prema prethodnom slučaju, jedno od mogućih rešenja bi bilo: $B_{\alpha} = \{b^{\alpha}_{\gamma,k} \mid \gamma \leq \alpha, k \in N\}$ i u tom slučaju podrazumevamo da je, za $\alpha \leq \delta < \tau$, $\mathbf{A}_{\alpha,\delta} = \sum_{k\in N}\langle a^{\alpha}_{\delta,k}\rangle$ i $\mathbf{A}_{\alpha} = \sum_{\alpha\leq\delta<\tau}\mathbf{A}_{\alpha,\delta} = \sum_{\alpha\leq\delta<\tau}(\sum_{k\in N}\langle a^{\alpha}_{\delta,k}\rangle)$. Ova prezentacija ispunjava, evidentno, uslove (1) i (2). Recimo, uslov (2) sada formulišemo sa: ako je dato $b^{\alpha}_{\gamma,k}$, $\gamma \geq \alpha$, prirodan broj $n$ i ordinal $\beta < \alpha$, onda postoji neko $b^{\delta}_{\epsilon,m}$ takvo da je $\beta \leq \delta < \alpha$, $n^{\delta}_{\epsilon,m} > n$ i $p^{n^{\delta}_{\epsilon,m}}b^{\delta}_{\epsilon,m} \sim b^{\alpha}_{\gamma,k}$. Dovoljno je uzeti da je $\epsilon = \gamma$, a egzistencija traženog $b^{\delta}_{\gamma,m}$, koji ispunjava date zahteve, sledi iz induktivne pretpostavke o prezentaciji grupe $\mathbf{H}_{\gamma}$. Uslov (3) je pak ispunjen jer je svaka grupa $\mathbf{A}_{\alpha,\alpha}$ neograničena.■



**Definicija 42.2** *Neka je* $\mathbf{A}$ *reducirana p-grupa tipa* $\tau$.

*Element* $a \in A$ *je tipa* $\alpha$ *akko je* $a \in A^{\alpha} \setminus A^{\alpha+1}$.

*Podgrupa* $\mathbf{B}$ *grupe* $\mathbf{A}$ *je savršena akko je za svako* $\alpha < \tau$ *slika podgrupe* $\mathbf{B} \cap \mathbf{A}^{\alpha}$ *(grupe* $\mathbf{A}^{\alpha}$*) pri prirodnom homomorfizmu* $\varphi_{\alpha} : A^{\alpha} \longrightarrow A^{\alpha}/A^{\alpha+1} = A_{\alpha}$, *obeležimo je sa* $(\mathbf{A_B})_{\alpha}$, *potpuna podgrupa grupe* $\mathbf{A}_{\alpha}$.

*Neka je* $\mathbf{D}$ *podgrupa reducirane p-grupe* $\mathbf{C}$ *i neka je* $\varphi$ *izomorfno preslikavanje podgrupe* $\mathbf{B}$ *grupe* $\mathbf{A}$ *na* $\mathbf{D}$. $\varphi$ *očuvava tip akko su* $b$ *i* $(b)\varphi$ *istog tipa (u grupama, respektivno,* $\mathbf{A}$ *i* $\mathbf{C}$*) za svako* $b \in B$.

Naravno, svaki element je izvesnog tipa; jer, ako je $\beta$ granični ordinal i $a \in A^{\alpha}$ za svako $\alpha < \beta$, onda je i $a \in \bigcap_{\alpha<\beta}A^{\alpha} = A^{\beta}$.

**Lema 42.3** *Neka su* $\mathbf{A}$ *i* $\mathbf{C}$ *prebrojive reducirane p-grupe istog tipa* $\tau$ $(= \tau(\mathbf{A}) = \tau(\mathbf{C}))$, *neka je* $\mathbf{A}_{\alpha} \cong \mathbf{C}_{\alpha}$ *za svako* $\alpha < \tau$ *i neka je* $\varphi$ *izomorfno preslikavanje koje očuvava tip konačne savršene podgrupe* $\mathbf{B}$ *grupe* $\mathbf{A}$ *na savršenu podgrupu* $\mathbf{D}$ *grupe* $\mathbf{C}$. *Ako je* $a$ *element grupe* $\mathbf{A}$ *koji nije u* $\mathbf{B}$, *tada postoje konačne savršene podgrupe* $\overline{\mathbf{B}}$ *i* $\overline{\mathbf{D}}$ *grupa, respektivno,* $\mathbf{A}$ *i* $\mathbf{C}$ *i izomorfizam* $\overline{\varphi} \in Is(\overline{\mathbf{B}}, \overline{\mathbf{D}})$ *za koje važi:* $B \cup \{a\} \subseteq \overline{B}$, $D \subseteq \overline{D}$, $\overline{\varphi}$ *očuvava tip i ekstenzija je izomorfizma* $\varphi - \overline{\varphi}|_B = \varphi$.

**Dokaz.** Možemo odmah pretpostaviti da je $pa \in B$; u suprotnom, ako je $p^n a \in B$ i $p^{n-1}a \notin B$, $n > 1$, krenuli bismo od elementa $p^{n-1}a$ i sukcesivno "ubacivali" jedan po jedan elemente $p^{n-1}a, p^{n-2}a, \ldots, pa, a$.

Neka je $\alpha$ maksimalni ordinal među tipovima elemenata koseta $a+B$ (radi se o konačno mnogo ordinala - tipova elemenata, pa, dakle, imamo najveći među njima). Među elementima koseta $a + B$ tipa $\alpha$ neka je $a' = a + b_0$ najveće visine u $A^{\alpha}$ (elementi tipa $\alpha$ su konačne visine u $A^{\alpha}$, s obzirom da po definiciji nisu u $A^{\alpha+1}$). Neka je $h(a') = n - 1$, $n \geq 1$, $a' = p^{n-1}\overline{a}$, $\overline{a} \in A^{\alpha}$ ($\setminus A^{\alpha+1}$) i $\overline{\mathbf{B}} = \mathbf{B} + \langle\overline{a}\rangle$. $\overline{\mathbf{B}}$ je, jasno, konačna grupa, a imamo i $a = a' - b_0 = p^{n-1}\overline{a} - b_0 \in \overline{B}$. No, $\overline{\mathbf{B}}$ je i savršena podgrupa grupe $\mathbf{A}$. Pokažimo to. Kako je $p^n\overline{a} = pa' = pa + pb_0 \in B$, elementi podgrupe $\overline{\mathbf{B}}$ su oblika $\overline{b} = b + k\overline{a}$, gde je $b \in B$ i $0 \leq k < p^n$. Neka je $\overline{b} = b + k\overline{a} \in \overline{B}$ tipa $\beta$ i visine $m$ u $A^{\beta}$, recimo, $\overline{b} = b + k\overline{a} = p^m x$ za neko $x \in A^{\beta}$. Element $\overline{b} + A^{\beta+1}$ faktor grupe $\mathbf{A}^{\beta}/\mathbf{A}^{\beta+1} = \mathbf{A}_{\beta}$, u stvari podgrupe $((\overline{\mathbf{B}} \cap \mathbf{A}^{\beta}) + \mathbf{A}^{\beta+1})/\mathbf{A}^{\beta+1}$, takođe je visine $m$; pri homomorfnom preslikavanju visina slike veća je od ili jednaka visini originala, a kako su elementi podgrupe $\mathbf{A}^{\beta+1}$ beskonačne visine u $\mathbf{A}^{\beta}$, baš je jednakost u pitanju. Tražimo, dakle, element $\overline{b}' \in \overline{B}$ tipa $\beta$ takav da je $\overline{b} + A^{\beta+1} = p^m(\overline{b}' + A^{\beta+1})$. Za $k = 0$ ili $\beta < \alpha$ je $k\overline{a} \in A^{\beta+1}$, pa je $\overline{b} + A^{\beta+1} = b + A^{\beta+1}$ i egzistencija elementa $\overline{b}'$ proizilazi iz činjenice da je $\mathbf{B}$ savršena podgrupa (element $\overline{b}'$ ćemo naći u samoj grupi $\mathbf{B}$). Ako je $\beta = \alpha$ i $k$ deljivo sa $p^m$ - $k = p^m r$, iz $\overline{b} = b + k\overline{a} = p^m x$ sledi $b = p^m(x - r\overline{a})$ i zbog $x - r\overline{a} \in A^{\alpha}$ i savršenosti podgrupe $\mathbf{B}$ postoji element $b' \in B \cap A^{\alpha}$ takav da je $b + A^{\alpha+1} = p^m(b' + A^{\alpha+1})$. Odatle izvodimo direktno: $\overline{b} + A^{\alpha+1} =$

$p^m((b'+r\overline{a})+A^{\alpha+1})$; jasno, $b'+r\overline{a}\in\overline{B}\cap A^\alpha$. Drugi slučajevi, međutim, i nisu mogući, preciznije, protivureče izboru elementa $a'$. Proverimo. Neka je $p^j$ najveći stepen broja $p$ koji deli $k$: $k=p^jk'$, $(k',p)=1$. Naravno, $j\leq n-1$ (jer je $0<k<p^n$). Iz teorije Diofantovih jednačina poznato je da postoje celi brojevi $l$ i $q$ takvi da je $0<l<p$ i $k'l=1+qp$. "Množenjem" jednačine $b+k\overline{a}=p^mx$ sa $lp^{n-j-1}$ dobijamo $lp^{n-j-1}b+lp^{n-j-1}p^jk'\overline{a}=lp^{n-j-1}p^mx$, to jest, posle malo sređivanja, $lp^{n-j-1}b+p^{n-1}\overline{a}+qp^n\overline{a}=lp^{n+m-j-1}x$. $p^n\overline{a}\in B$, stoga je i $lp^{n-j-1}b+qp^n\overline{a}=b'\in B$; $p^{n-1}\overline{a}=a'$, $lx=x'\in A^\beta$ i $b'+a'=p^{n+m-j-1}x'$. Ako je $\beta>\alpha$, onda je $b'+a'\in A^\beta$, pa koset $a'+B=a+B$ ima elemente tipa većeg od $\alpha$, suprotno pretpostavci. Ako je pak $\beta=\alpha$, ali $k$ nije deljivo sa $p^m$ $(j\leq m-1)$, onda je $n+m-j-1\geq n$ i među elementima koseta $a+B$ tipa $\alpha$ imamo elemente visine veće od $n-1$, ponovo suprotno pretpostavci o izboru elementa $a'$. Zaključujemo: $\overline{\mathbf{B}}$ je savršena podgrupa.

Ako se krene od relacije $p^n\overline{a}\in B\cap A^\alpha$, tada je zbog savršenosti podgrupe $\mathbf{B}$ za neki element $b_1\in B\cap A^\alpha$, koji je tipa $\alpha$ ili je eventualno nula, $p^n\overline{a}+A^{\alpha+1}=p^n(b_1+A^{\alpha+1})$. Stoga je, za neko $b_2\in B\cap A^{\alpha+1}$, $p^n\overline{a}=p^nb_1+b_2$, odnosno $b_2=p^n(\overline{a}-b_1)$. Ako je $\overline{\overline{a}}=\overline{a}-b_1$, onda je $\overline{\overline{a}}$ tipa $\alpha$, $\overline{\mathbf{B}}=\mathbf{B}+\langle\overline{a}\rangle=\mathbf{B}+\langle\overline{\overline{a}}\rangle$ i za svako $k$, $0<k<p^n$, $k\overline{\overline{a}}\notin B$ (znamo da $p^{n-1}\overline{a}\notin B$ i $p^n\overline{a}\in B$, a $k\overline{\overline{a}}\in B$ akko $k\overline{a}\in B$; no, ako bi za neko $mp^r$, $0<mp^r<p^n$, gde je $(m,p)=1$, bilo $mp^r\overline{a}\in B$, onda bismo, kao i obično u takvim slučajevima, pošli od celih brojeva $u$ i $v$ za koje je $um=1+vp^{n-r}$ i izvodili redom, sve do kontradikcije: $ump^r\overline{a}\in B$, $(1+vp^{n-r})p^r\overline{a}\in B$, $p^r\overline{a}\in B$). Tipovi elemenata iz $\overline{\mathbf{B}}$ koji nisu u $\mathbf{B}$, već je pokazano u dokazu savršenosti podgrupe $\overline{\mathbf{B}}$, manji su od ili jednaki $\alpha$, a iz gornje diskusije sledi da je grupa $(\mathbf{A}_{\overline{\mathbf{B}}})_\alpha=((\mathbf{A}^\alpha\cap\overline{\mathbf{B}})+\mathbf{A}^{\alpha+1})/\mathbf{A}^{\alpha+1}$ direktna suma grupe $(\mathbf{A}_\mathbf{B})_\alpha$ i ciklične grupe reda $p^n$ - $\langle\overline{\overline{a}}+A^{\alpha+1}\rangle$: za element $\overline{b}=b+k\overline{\overline{a}}$, $b\in B$, $0\leq k<p^n$, tipa $\alpha$ imamo $\overline{b}+A^{\alpha+1}=(b+A^{\alpha+1})+(k\overline{\overline{a}}+A^{\alpha+1})$ i, očigledno, $(\mathbf{A}_\mathbf{B})_\alpha\cap\langle\overline{\overline{a}}+A^{\alpha+1}\rangle=\mathbf{O}$; $k\overline{\overline{a}}+A^{\alpha+1}=b+A^{\alpha+1}$ daje $k\overline{\overline{a}}-b\in A^{\alpha+1}\cap\overline{B}$, dakle, $k\overline{\overline{a}}-b\in B$, $\overline{\overline{a}}\in B$, te je $k=0$ i $b\in B\cap A^{\alpha+1}$. S druge strane, kao potpuna i ograničena podgrupa $(\mathbf{A}_{\overline{\mathbf{B}}})_\alpha$ je direktni sumand grupe $\mathbf{A}_\alpha$ (37.18), pa su i $(\mathbf{A}_\mathbf{B})_\alpha$ i $\langle\overline{\overline{a}}+A^{\alpha+1}\rangle$ njeni direktni sumandi. Grupe $(\mathbf{A}_\mathbf{B})_\alpha$ i $(\mathbf{C}_\mathbf{D})_\alpha$ su izomorfne jer $\varphi\in Is(\mathbf{B},\mathbf{D})$ očuvava tip. Preslikavanje $\psi:(A_\mathbf{B})_\alpha\longrightarrow(C_\mathbf{D})_\alpha$ dato sa $(b+A^{\alpha+1})\psi=(b)\varphi+C^{\alpha+1}$ je izomorfizam; pošto je $b\in B\cap A^\alpha$ akko je $(b)\varphi\in D\cap C^\alpha$, $\psi$ je odista preslikavanje grupe $(\mathbf{A}_\mathbf{B})_\alpha$ u grupu $(\mathbf{C}_\mathbf{D})_\alpha$, zapravo "na" preslikavanje, homomorfnost preslikavanja $\psi$ je očigledna, a dobra definisanost i injektivnost se simultano proveravaju: $b'+A^{\alpha+1}=b''+A^{\alpha+1}$ akko $b'-b''\in A^{\alpha+1}$ $(\cap B)$ akko $(b'-b'')\varphi\in C^{\alpha+1}$ $(\cap D)$ akko $(b')\varphi+C^{\alpha+1}=(b'')\varphi+C^{\alpha+1}$. Iz već navedenih razloga podgrupa $(\mathbf{C}_\mathbf{D})_\alpha$ je direktni sumand grupe $\mathbf{C}_\alpha$, koja je, opet prema 35.5, direktna suma cikličnih grupa. Zbog izomorfnosti grupa $\mathbf{A}_\alpha$ i $\mathbf{C}_\alpha$ kao i njihovih podgrupa $(\mathbf{A}_\mathbf{B})_\alpha$, $(\mathbf{C}_\mathbf{D})_\alpha$, u grupi $\mathbf{C}_\alpha$ postoji kao direktni sumand ciklična grupa reda $p^n$ koja sa $(\mathbf{C}_\mathbf{D})_\alpha$ ima nula presek (koristimo se i činjenicom da se izomorfizam $\psi\in Is((\mathbf{A}_\mathbf{B})_\alpha,(\mathbf{C}_\mathbf{D})_\alpha)$ može proširiti do



izomorfizma $\overline{\psi}\in Is(\mathbf{A}_\alpha,\mathbf{C}_\alpha)$ - videti 35.11). Neka je to $\langle c+C^{\alpha+1}\rangle$. Element $c$ je, jasno, tipa $\alpha$ i $p^nc\in C^{\alpha+1}$, ali $p^{n-1}c\notin C^{\alpha+1}$. Slika elementa $b_2$ $(\in A^{\alpha+1}\cap B)$ za izomorfizam $\varphi$ - $(b_2)\varphi=d_2$ - element je grupe $\mathbf{C}^{\alpha+1}\cap\mathbf{D}$, te je $d_2-p^nc\in C^{\alpha+1}$ (kao element beskonačne visine u $\mathbf{C}^\alpha$) deljiv sa $p^{n+1}$. Neka je, za $c_0\in C^\alpha$, $d_2-p^nc=p^{n+1}c_0$, odnosno $d_2=p^n(c+pc_0)=p^n\overline{c}$ (stavili smo $c+pc_0=\overline{c}$) i neka je $\overline{\mathbf{D}}=\mathbf{D}+\langle\overline{c}\rangle$. Element $p^{n-1}\overline{c}$ nije u $\mathbf{D}$, u suprotnom bi $p^{n-1}\overline{c}=d_0\in D$, tj. $d_0-p^{n-1}c=p^nc_0$, dalo: $(d_0+C^{\alpha+1})+(-p^{n-1}c+C^{\alpha+1})=p^n(c_0+C^{\alpha+1})\in(C_\mathbf{D})_\alpha\oplus\langle c+C^{\alpha+1}\rangle$, kontradikcija (u direktnoj sumi $(\mathbf{C}_\mathbf{D})_\alpha\oplus\langle c+C^{\alpha+1}\rangle$ imamo element visine veće od visine njegove komponente u $\langle c+C^{\alpha+1}\rangle$). Iz navedenog proizilazi da u grupi $\mathbf{C}_\alpha$ podgrupe $(\mathbf{C}_\mathbf{D})_\alpha$ i $\langle\overline{c}+C^{\alpha+1}\rangle$ obrazuju direktnu sumu. Dalje, iz $p^n\overline{\overline{a}}=b_2$, $p^n\overline{c}=d_2=(b_2)\varphi$ i $p^{n-1}\overline{\overline{a}}\notin B$, $p^{n-1}\overline{c}\notin D$ sledi da je preslikavanje $\overline{\varphi}:\overline{B}\longrightarrow\overline{D}$, gde je $(b+k\overline{\overline{a}})\overline{\varphi}=(b)\varphi+k\overline{c}$, $0\leq k<p^n$, izomorfizam grupa $\overline{\mathbf{B}}$ i $\overline{\mathbf{D}}$ (i očigledno ekstenzija izomorfizma $\varphi$). Proverimo samo homomorfnost:

$$((b+k\overline{\overline{a}})+(b'+k'\overline{\overline{a}}))\overline{\varphi}=((b+b')+((k+_{p^n}k')+[\frac{k+k'}{p^n}]p^n)\overline{\overline{a}})\overline{\varphi}=$$

$$(b+b'+[\frac{k+k'}{p^n}]b_2+(k+_{p^n}k')\overline{\overline{a}})\overline{\varphi}=(b+b'+[\frac{k+k'}{p^n}]b_2)\varphi+(k+_{p^n}k')\overline{c}=$$

$$(b)\varphi+(b')\varphi+[\frac{k+k'}{p^n}]d_2+(k+_{p^n}k')\overline{c}=(b)\varphi+(b')\varphi+[\frac{k+k'}{p^n}]p^n\overline{c}+(k+_{p^n}k')\overline{c}=$$

$$(b)\varphi+(b')\varphi+(k+k')\overline{c}=(b)\varphi+k\overline{c}+(b')\varphi+k'\overline{c}=(b+k\overline{\overline{a}})\overline{\varphi}+(b'+k'\overline{\overline{a}})\overline{\varphi}.$$

$\overline{\varphi}$ takođe očuvava tip. Jer, korespondentni elementi $b+k\overline{\overline{a}}$ i $(b)\varphi+k\overline{c}$ su, jasno, za $k=0$ istog tipa; ako je $0<k<p^n$ i $b$ i $(b)\varphi$ su tipa $\beta\neq\alpha$, onda, s obzirom da su $\overline{\overline{a}}$ i $\overline{c}$ tipa $\alpha$, elementi $b+k\overline{\overline{a}}$ i $(b)\varphi+k\overline{c}$ su tipa $min\{\alpha,\beta\}$ (naravno, tip sume dva elementa različitih tipova jednak je manjem od tipova sumanada); ako su $b$ i $(b)\varphi$ tipa $\alpha$ i $0<k<p^n$, opet su $b+k\overline{\overline{a}}$ i $(b)\varphi+k\overline{c}$ tipa $\alpha$ (pošto $(\mathbf{A}_\mathbf{B})_\alpha$ i $\langle\overline{\overline{a}}+A^{\alpha+1}\rangle$, kao i $(\mathbf{C}_\mathbf{D})_\alpha$ i $\langle\overline{c}+C^{\alpha+1}\rangle$, obrazuju direktnu sumu u grupama, respektivno, $\mathbf{A}_\alpha$ i $\mathbf{C}_\alpha$, a recimo, visina elementa u direktnoj sumi jednaka je minimalnoj od visina njegovih komponenti).

Preostalo je još da se dokaže da je $\overline{\mathbf{D}}=\mathbf{D}+\langle\overline{c}\rangle$ savršena podgrupa grupe $\mathbf{C}$. No to se svodi na ponavljanje dokaza da je $\overline{\mathbf{B}}$ savršena podgrupa grupe $\mathbf{A}$, dodeljujući elmentima $\overline{c}$ i $p^{n-1}\overline{c}$ uloge koju su imali $\overline{a}$ i $a'$ $(=p^{n-1}\overline{a})$. Imamo u vidu da je $\overline{c}$ nula visine u $\mathbf{C}^\alpha$, kao što je $\overline{a}$ nula visine u $\mathbf{A}^\alpha$ (grupa $\langle\overline{c}+C^{\alpha+1}\rangle$ je direktni sumand grupe $\mathbf{C}_\alpha$, i element $\overline{c}+C^{\alpha+1}$, kao njen generatorni element, ima nula visinu u njoj, dakle i u $\mathbf{C}_\alpha$, a visina slike je, podsećamo, veća od ili jednaka visini originala). Dalje, tipovi elemenata koseta $p^{n-1}\overline{c}+D$ nisu veći od tipa elementa $p^{n-1}\overline{c}$, tj. $\alpha$. Konačno, pretpostavka da je neki element koseta $p^{n-1}\overline{c}+D$ visine veće od $n-1$ u $\mathbf{C}^\alpha$, npr. da je $p^{n-1}\overline{c}+d=p^mc_0$ za neko $m>n-1$ i neko $c_0\in C^\alpha$, vodi u kontradikciju: $(p^{n-1}\overline{c}+C^{\alpha+1})+(d+C^{\alpha+1})=p^m(c_0+C^{\alpha+1})$; ispada da je $p^m(c_0+C^{\alpha+1})$

element veće visine u $(\mathbf{C_D})_\alpha \oplus \langle \overline{c} + C^{\alpha+1} \rangle$ od visine svoje komponente u $\langle \overline{c} + C^{\alpha+1} \rangle$.□

**Teorema 42.4** *(Teorema H. Ulma). Neka su* $\mathbf{A}$ *i* $\mathbf{C}$ *prebrojive reducirane p-grupe istog tipa* $\tau$ *i neka je* $\mathbf{A}_\alpha \cong \mathbf{C}_\alpha$ *za svako* $\alpha < \tau$. *Tada je i* $\mathbf{A} \cong \mathbf{C}$.

**Dokaz.** Koristimo se prethodnom lemom i poznatom "back and forth" metodom. Neka je $A = \{a_n \mid n \in \omega\}$, $C = \{c_n \mid n \in \omega\}$ i $\mathbf{B}_0 = \mathbf{O}$, $\mathbf{D}_0 = \mathbf{O}$. Jasno, $\mathbf{B}_0$ i $\mathbf{D}_0$ su savršene podgrupe i jedini izomorfizam među njima – $\varphi_0$ – očuvava tip (nula je tipa $\tau$). Pretpostavimo da su za dato $n$ $(> 0)$ formirani rastući nizovi savršenih podgrupa $\mathbf{B}_0, \ldots, \mathbf{B}_{n-1}$ i $\mathbf{D}_0, \ldots, \mathbf{D}_{n-1}$ grupa, respektivno, $\mathbf{A}$ i $\mathbf{C}$, gde svaki par podgrupa $\mathbf{B}_k, \mathbf{D}_k$, $0 \leq k \leq n-1$, ispunjava uslove prethodne leme, a izomorfizam $\varphi_k \in Is(\mathbf{B}_k, \mathbf{D}_k)$ koji očuvava tip je za $k > 0$ ekstenzija izomorfizma $\varphi_{k-1}$. Ako je $n$ neparno, uzimamo prvi element iz $A$, s obzirom na uvedeno uređenje, koji nije u $\mathbf{B}_{n-1}$ i kao u prethodnoj lemi konstruišemo savršene izomorfne podgrupe $\mathbf{B}_n$ i $\mathbf{D}_n$, gde je $\mathbf{B}_{n-1} + \langle a \rangle \leq \mathbf{B}_n$ i $\mathbf{D}_{n-1} \leq \mathbf{D}_n$, a izomorfizam $\varphi_n$ ekstenzija izomorfizma $\varphi_{n-1}$. Ako je $n$ parno, polazimo od $\mathbf{D}_{n-1}$ i prvog elementa iz $\mathbf{C}$ koji nije u $\mathbf{D}_{n-1}$. Naravno, sada zahtevamo da je izomorfizam koji preslikava $\mathbf{D}_n$ na $\mathbf{B}_n$ i očuvava tip, neka to bude $\psi_n$, ekstenzija izomorfizma $\varphi_{n-1}^{-1} \in Is(\mathbf{D}_{n-1}, \mathbf{B}_{n-1})$, a mi za $\varphi_n$ uzimamo $\psi_n^{-1}$. Očigledno je $A = \bigcup_{n\in\omega} B_n$ i $C = \bigcup_{n\in\omega} D_n$, a $\varphi = \bigcup_{n\in\omega} \varphi_n$ je izomorfno preslikavanje grupe $\mathbf{A}$ na grupu $\mathbf{C}$.■

Teoreme Prüfera, Zippina i Ulma omogućuju potpunu karakterizaciju prebrojivih reduciranih $p$-grupa. Jer, videli smo da je svaki prebrojivi $\tau$-niz ($\tau < \aleph_1$ – prvi neprebrojivi kardinal; hipoteza kontinuuma kaže da je to baš kontinuum – $c = 2^{\aleph_0}$) prebrojivih $p$-grupa bez elemenata beskonačne visine koje su i neograničene, osim možda poslednje u nizu, kada je $\tau$ nasledni ordinal, niz Ulma neke prebrojive reducirane $p$-grupe, kao i da su prebrojive reducirane $p$-grupe sa izomorfnim nizovima Ulma i same izomorfne. Kako je prebrojiva $p$-grupa bez elemenata beskonačne visine direktna suma cikličnih ($p$-)grupa, to svakoj klasi izomorfnih prebrojivih reduciranih $p$-grupa sa (do na izomorfizam) nizom Ulma: $\mathbf{A}_0, \ldots, \mathbf{A}_\alpha, \ldots$, $\alpha < \tau$, odgovara matrica, tj. preslikavanje: $M : \tau \times N \longrightarrow \omega^+ = \omega \cup \{\omega\}$ definisano sa (za $\alpha < \tau$ i $k \in N := \{1, 2, \ldots\}$) $(\alpha, k)M = n_{\alpha,k}$, gde je $n_{\alpha,k}$ $(\in \omega^+)$ broj cikličnih sumanada reda $p^k$ u grupi $\mathbf{A}_\alpha$ (uobičajenim jezikom matrica: u $\alpha$-toj vrsti matrice $M$ na $k$-tom mestu je $n_{\alpha,k}$); uslov da je $\mathbf{A}_\alpha$ neograničena grupa za $\alpha < \tau - 1$ ogleda se u tome da je u $\alpha$-toj vrsti, $\alpha < \tau - 1$, broj elemenata različit od nule beskonačan. S druge strane, svaka matrica, kao upravo opisana, određuje, do na izomorfizam, prebrojivu reduciranu $p$-grupu tipa $\tau$ čiji je $\alpha$-ti faktor Ulma grupa (izomorfna grupi) $\sum_{k\in N}(\sum_{\beta<n_{\alpha,k}} \mathbf{Z}^{\beta}_{p^k})$. Iz navedenog sledi da se opisane matrice mogu smatrati kao kompletan sistem invarijanata prebrojivih reduciranih $p$-grupa.



Teorema Ulma ne važi generalno. Sledeći kontraprimer Kulikova to ilustruje.

**Primer 42.5** *Neka je* $\mathbf{A}$ *zatvorenje grupe* $\sum^c_{n\in N} \mathbf{Z}_{p^n}$ $(\mathbf{A} = t(\sum^c_{n\in N} \mathbf{Z}_{p^n}))$ *i neka su* $\mathbf{B}$ *i* $\mathbf{C}$ *njene podgrupe sa domenima, respektivno:*

$B = \{(b_n)_{n\in N} \mid b_n \in Z_{p^n},\ p(b_n)_{n\in N} = (0)$ *i samo konačno mnogo komponenti* $b_n$ *je različito od nule* $\}$;

$C = \{(c_n)_{n\in N} \mid c_n \in Z_{p^n},\ p(c_n)_{n\in N} = (0)$ *i samo konačno mnogo komponenti sa neparnim indeksom je različito od nule* $\}$.

*Tada su faktor grupe* $\mathbf{G} = \mathbf{A}/\mathbf{B}$ *i* $\mathbf{H} = \mathbf{A}/\mathbf{C}$ *neizomorfne reducirane p-grupe tipa 2 sa izomorfnim faktorima Ulma.*

**Dokaz.** Koristićemo očiglednu činjenicu: $\mathbf{B} \leq \mathbf{C} \leq \mathbf{A}_1$, gde je $\mathbf{A}_1$ najniži sloj grupe $\mathbf{A} - \mathbf{A}[p]$.

Konstatujemo prvo: $\mathbf{G}^1 = \mathbf{A}_1/\mathbf{B}$. Zaista, neka je $\overline{a} = \langle p^{k-1} r_k \rangle_{k\in N}$, $(p, r_k) = 1$, $0 \leq r_k < p$, (jedan) element podgrupe $\mathbf{A}_1$. Onda je za $\overline{a}' = \langle a'_k \rangle_{k\in N} \in A$, gde je $a'_k = \begin{cases} 0 & k \leq n \\ p^{k-n-1} r_k & k > n \end{cases}$, $\overline{a} - p^n \overline{a}' \in B$ i $\overline{a} + B = p^n(\overline{a}' + B)$; dakle, $\overline{a} + B$ je deljivo sa $p^n$ za svako $n \in N$, pa je $\mathbf{A}_1/\mathbf{B} \leq (\mathbf{A}/\mathbf{B})^1 = \mathbf{G}^1$. S druge strane je

$$(\mathbf{A}/\mathbf{B})/(\mathbf{A}_1/\mathbf{B}) \cong \mathbf{A}/\mathbf{A}_1 \cong p\mathbf{A};$$

(preslikavanje $\varphi : A \longrightarrow pA$ dato sa $(\overline{a})\varphi = p\overline{a}$ surjektivni je homomorfizam sa jezgrom $\mathbf{A}_1$). $p\mathbf{A}$ je, kao uostalom i cela grupa $\mathbf{A}$, bez elemenata beskonačne visine (videti kontraprimer Kuroša dat uz drugu Prüferovu teoremu – 35.5). Odatle proizilazi i da je $(\mathbf{A}/\mathbf{B})^1 \leq \mathbf{A}_1/\mathbf{B}$; u suprotnom bi pretpostavljeni element iz $(A/B)^1 \setminus (A_1/B)$ implicirao egzistenciju nenula elementa beskonačne visine u faktor grupi $\mathbf{A}/\mathbf{A}_1$ – prirodno homomorfno preslikavanje grupe $\mathbf{G}$ $(= \mathbf{A}/\mathbf{B})$ na grupu $\mathbf{A}/\mathbf{A}_1$ ima za jezgro $\mathbf{A}_1/\mathbf{B}$. $\mathbf{A}_1/\mathbf{B}$ je, jasno, kao ograničena grupa $(p(\mathbf{A}_1/\mathbf{B}) = \mathbf{O})$ bez elemenata beskonačne visine. Prema tome, $\mathbf{G} = \mathbf{A}/\mathbf{B}$ je reducirana $p$-grupa reda kontinuum i tipa 2, a njeni faktori Ulma su (zbog potrebe teksta odstupićemo ovog puta od ranije korišćene notacije):

$$\overline{\mathbf{G}}_0 = (\mathbf{A}/\mathbf{B})/(\mathbf{A}_1/\mathbf{B}) \cong \mathbf{A}/\mathbf{A}_1 \cong p\mathbf{A}, \quad \overline{\mathbf{G}}_1 \cong \mathbf{A}_1/\mathbf{B}.$$

Potpuno analogno prethodnom dokazuje se da je $\mathbf{H}^1 = (\mathbf{A}/\mathbf{C})^1 = \mathbf{A}_1/\mathbf{C}$, kao i da je $(\mathbf{A}_1/\mathbf{C})^1 = \mathbf{O}$. Faktori Ulma grupe $\mathbf{H}$ su, znači:

$$\overline{\mathbf{H}}_0 = (\mathbf{A}/\mathbf{C})/(\mathbf{A}_1/\mathbf{C}) \cong \mathbf{A}/\mathbf{A}_1 \cong p\mathbf{A}, \quad \overline{\mathbf{H}}_1 \cong \mathbf{A}_1/\mathbf{C}.$$

Grupe $\mathbf{A}_1/\mathbf{B}$ i $\mathbf{A}_1/\mathbf{C}$ su pak izomorfne; obe su kardinalnosti kontinuum i sa (nenula) elementima reda $p$, stoga direktne sume kontinuum mnogo cikličnih grupa reda $p$. Za grupu $\mathbf{A}_1/\mathbf{B}$ to je očigledno; $|A_1| = c$ – videti ponovo

kontraprimer Kuroša, a $\mathbf{B}$ je prebrojiva grupa. U slučaju faktor grupe $\mathbf{A}_1/\mathbf{C}$ situacija je za nijansu komplikovanija – i grupa $\mathbf{C}$ je kardinalnosti kontinuum. Pozivamo se na skupovni rezultat (dajemo ga samo u formi koji nam je potreban): postoji podskup $\mathcal{P}$ skupa $P(\{2n+1 \mid n \in \omega\})$ (= partitivni skup skupa neparnih prirodnih brojeva) kardinalnosti kontinuum takav da su svi njegovi elementi (dakle, podskupovi skupa $\{2n+1 \mid n \in \omega\}$) beskonačni, a presek svaka dva (različita) elementa je konačan. Prema tome, ako su $X$ i $Y$ različiti elementi skupa $\mathcal{P}$ i $\overline{a}_X = \langle a_k \rangle_{k\in N}$, $\overline{a}_Y = \langle a'_m \rangle_{m\in N}$, gde je $a_k = \begin{cases} p^{k-1} & k \in X \\ 0 & \text{inače} \end{cases}$, $a'_m = \begin{cases} p^{m-1} & m \in Y \\ 0 & \text{inače} \end{cases}$, onda je $\overline{a}_X + C \neq \overline{a}_Y + C$, tj. $\overline{a}_X - \overline{a}_Y \notin C$ (sve komponente elementa $\overline{a}_X - \overline{a}_Y$ sa neparnim indeksom iz $X \triangle Y \stackrel{\text{def}}{=} (X \setminus Y) \cup (Y \setminus X)$ su različite od nule).

Pokažimo konačno da grupe $\mathbf{G}$ i $\mathbf{H}$ nisu izomorfne. Kako je $\mathbf{G}^1 \leq \mathbf{G}_1$ (= $\mathbf{G}[p]$), $\mathbf{H}^1 \leq \mathbf{H}_1$ (= $\mathbf{H}[p]$), biće dovoljno ako pokažemo da su grupe $\mathbf{G}_1/\mathbf{G}^1$ i $\mathbf{H}_1/\mathbf{H}^1$ različite kardinalnosti. Očigledno je $\mathbf{G}_1 = \mathbf{D}/\mathbf{B}$, gde je $\mathbf{D}$ podgrupa grupe $\mathbf{A}$ čiji domen sadrži uz nulu i sve elemente reda $p$ kao i one elemente reda $p^2$ kod kojih je samo konačno mnogo nenula komponenti reda $p^2$ (ostale su ili nula element ili reda $p$). Grupa $\mathbf{G}_1/\mathbf{G}^1 \cong (\mathbf{D}/\mathbf{B})/(\mathbf{A}_1/\mathbf{B}) \cong \mathbf{D}/\mathbf{A}_1$ je, znači, prebrojiva. Opet, $\mathbf{H}_1 = \mathbf{F}/\mathbf{C}$, gde je $\mathbf{F}$ podgrupa grupe $\mathbf{A}$ čiji domen sadrži uz nulu sve elemente reda $p$ i sve one elemente reda $p^2$ kod kojih je samo konačno mnogo komponenti sa neparnim indeksom reda $p^2$; prema tome može biti beskonačno mnogo komponenti sa parnim indeksom reda $p^2$. Evidentno, grupa $\mathbf{H}_1/\mathbf{H}^1 \cong (\mathbf{F}/\mathbf{C})/(\mathbf{A}_1/\mathbf{C}) \cong \mathbf{F}/\mathbf{A}_1$ je reda kontinuum.□

**Lema 42.6** *Svake dve dekompozicije prebrojive reducirane p-grupe* $\mathbf{A}$ *imaju izomorfna proširenja akko je* $\mathbf{A}$ *tipa* 1.

**Dokaz.** Ako je $\tau(\mathbf{A}) = 1$, tj. ako je $\mathbf{A}$ bez elemenata beskonačne visine, onda je prema drugoj teoremi Prüfera $\mathbf{A}$ direktna suma cikličnih grupa, a prema 35.11 svaka dva razlaganja u direktnu sumu nerazloživih cikličnih grupa su izomorfna (s obzirom da su $p$-ciklične grupe nerazložive, odmah i dobijamo samo razlaganja grupe $\mathbf{A}$ u sumu nerazloživih cikličnih grupa).

Pretpostavimo sada da je $\tau = \tau(\mathbf{A}) > 1$ i neka je, za svako $\alpha < \tau$, $\mathbf{A}_\alpha = \sum_{k\in N} \mathbf{A}_{\alpha,k}$, gde je $\mathbf{A}_{\alpha,k}$ direktna suma cikličnih grupa reda $p^{n_{\alpha,k}}$ i $n_{\alpha,1} < n_{\alpha,2} < \cdots$ (ukoliko je $\alpha < \tau - 1$, u slučaju da je $\tau$ nasledni ordinal, onda je niz $n_{\alpha,1} < n_{\alpha,2} < \cdots$ beskonanačan rastući niz, jer, setimo se, grupa $\mathbf{A}_\alpha$ nije ograničena; jasno, ako je $\tau$ granični ordinal, onda su svi pomenuti nizovi beskonačni). Stavimo: $\mathbf{B}_\alpha = \sum_{m\ parno} \mathbf{A}_{\alpha,m}$, $\mathbf{C}_\alpha = \sum_{m\ neparno} \mathbf{A}_{\alpha,m}$. Prema teoremi Zippina postoje grupe $\mathbf{B}$ i $\mathbf{C}$ tipa $\tau$ sa nizovima Ulma, respektivno, $\mathbf{B}_0, \ldots, \mathbf{B}_\alpha, \ldots, \alpha < \tau$ i $\mathbf{C}_0, \ldots, \mathbf{C}_\alpha, \ldots, \alpha < \tau$. Prema 41.6($b$) je $\mathbf{A} \cong \mathbf{B} \oplus \mathbf{C}$. No, jednako tako postoje grupe $\mathbf{F}$ i $\mathbf{G}$ tipa $\tau$ sa nizovima Ulma, respektivno, $\mathbf{C}_0, \mathbf{B}_1, \ldots, \mathbf{B}_\alpha, \ldots$ i $\mathbf{B}_0, \mathbf{C}_1, \ldots, \mathbf{C}_\alpha, \ldots$, $\alpha < \tau$, i opet je $\mathbf{A} \cong \mathbf{F} \oplus \mathbf{G}$. Odgovarajuće dekompozicije grupe $\mathbf{A}$ nemaju, međutim,



izomorfna proširenja. Ostanimo pri grupama $\mathbf{B} \oplus \mathbf{C}$ i $\mathbf{F} \oplus \mathbf{G}$ i pretpostavimo da postoje dekompozicije grupa $\mathbf{B}$, $\mathbf{C}$, $\mathbf{F}$ i $\mathbf{G}$: $\mathbf{B} = \sum_{i\in I} \mathbf{B}'_i$, $\mathbf{C} = \sum_{j\in J} \mathbf{C}'_j$, $\mathbf{F} = \sum_{k\in K} \mathbf{F}'_k$, $\mathbf{G} = \sum_{l\in L} \mathbf{G}'_l$ takve da je među sumandima direktnih suma $\sum_{i\in I} \mathbf{B}'_i \oplus \sum_{j\in J} \mathbf{C}'_j$ i $\sum_{k\in K} \mathbf{F}'_k \oplus \sum_{l\in L} \mathbf{G}'_l$ moguće uspostaviti uzajamno jednoznačnu korespondenciju za koju su korespondentni sumandi izomorfni. Ali, nijedna od grupa $\mathbf{B}'_i$, $i \in I$, nije izomorfna ni sa jednom od grupa $\mathbf{F}'_k$, $\mathbf{G}'_l$, $k \in K, l \in L$. Zaista, $\mathbf{B}_0 = \sum_{i\in I}(\mathbf{B}'_i)_0$ i $\mathbf{F}_0 = \sum_{k\in K}(\mathbf{F}'_k)_0$ i za dato $i \in I$ i $k \in K$ grupa $(\mathbf{B}'_i)_0$ je direktna suma nekih cikličnih grupa reda $p^{n_{0,m}}$, $m$ parno, $(\mathbf{F}'_k)_0$ je direktna suma nekih cikličnih grupa reda $p^{n_{0,m}}$, $m$ neparno, a po konstrukciji su skupovi $\{n_{0,m} \mid m \text{ je parno }\}$ i $\{n_{0,m} \mid m \text{ je neparno }\}$ disjunktni. Dakle, $(\mathbf{B}'_i)_0 \not\cong (\mathbf{F}'_k)_0$, a onda i $\mathbf{B}'_i \not\cong \mathbf{F}'_k$. U dokazu da za svako $i \in I$ i svako $l \in L$ grupe $\mathbf{B}'_i$ i $\mathbf{G}'_l$ nisu izomorfne, krenuli bismo od $\mathbf{B}_1$ i $\mathbf{G}_1$ (umesto od $\mathbf{B}_0$ i $\mathbf{G}_0$) i uglavnom ponovili prethodnu diskusiju.□

## 43 Torziono slobodne grupe ranga 1

Ove grupe su već ispitane. Prema 33.25 i 34.10, torziono slobodna grupa je ranga 1 akko je podgrupa grupe $\mathbf{Ra}$ akko je torziono slobodna lokalno ciklična grupa. Rezultat 33.25 se, zapravo, lako uopštava (u jednom smeru).

**Lema 43.1** *Torziono slobodna grupa ranga* $\lambda$ *(*$\lambda$ *proizvoljan kardinal) izomorfna je podgrupi deljive grupe* $\sum_{\alpha<\lambda} \mathbf{Ra}_\alpha$, *gde je, za* $\alpha < \lambda$, $\mathbf{Ra}_\alpha$ *"kopija" aditivne grupe racionalnih brojeva.*

**Dokaz.** Već je dat (i to dvaput). Torziono slobodna grupa $\mathbf{A}$ ranga $\lambda$ podgrupa je svog injektivnog omotača – $\mathbf{I}(\mathbf{A})$, koji je, podsećamo, deljiva grupa i esencijalna ekstenzija grupe $\mathbf{A}$ (videti 33.23). Neka je $\{a_\alpha \mid \alpha < \lambda\}$ jedan maksimalan linearno nezavisan sistem grupe $\mathbf{A}$ i $c \in I(\mathbf{A})$. Onda je $\langle c \rangle \cap \mathbf{A} \neq \mathbf{O}$, pa ako je $(0 \neq)\ kc = b_1 + \cdots + b_m$, $b_i \in A$ i $(0 \neq)\ k_i b_i \in \langle \{a_\alpha \mid \alpha < \lambda\} \rangle$, $1 \leq i \leq m$ (31.2($d$)), tada je $(0 \neq)\ (kk_1 \cdot \ldots \cdot k_m)c \in \langle \{a_\alpha \mid \alpha < \lambda\} \rangle$ i $r(\mathbf{I}(\mathbf{A})) = r(\mathbf{A}) = \lambda$.

Drugi dokaz je samo prividno "drugi", tj. različit. Pozivamo se na 37.9 i 33.4 (blažu varijantu teoreme 33.23). Neka je $\mathbf{A}$ podgrupa deljive grupe $\mathbf{D}$ i neka je $\mathbf{B}$ minimalna potpuna podgrupa grupe $\mathbf{D}$ koja sadrži $\mathbf{A}$. Egzistenciju takve podgrupe $\mathbf{B}$ garantuje korolar 37.9, koji ujedno kaže da je $\mathbf{B}$ i esencijalna ekstenzija grupe $\mathbf{A}$. Kao potpuna podgrupe deljive grupe $\mathbf{B}$ je i sama deljiva grupa, dakle, injektivni omotač grupe $\mathbf{A}$.□

Poznatu karakterizaciju torziono slobodnih grupa ranga 1, svejedno, prezentovaćemo još jedanput, opet samo na izgled na drugi način. Visina elementa biće ključni pojam, što je i za očekivati s obzirom da u torziono slobodnim grupama elemente ne možemo razlikovati po redovima. No, prvo nešto opšte priče.

Niz $\alpha : \omega \longrightarrow \omega \cup \{\infty\}$ zvaćemo *visinom*; pisaćemo: $\alpha = (\alpha_0, \ldots, \alpha_n, \ldots)$ (naravno, visina $\beta$ će biti $(\beta_0, \ldots, \beta_n, \ldots)$ i tako dalje). Na skupu visina definišemo relaciju $\leq$ sa: $\alpha \leq \beta$ akko je $\alpha_n \leq \beta_n$ za svako $n \in \omega$; podrazumevamo, jasno, da je $n < \infty$ za svako $n \in \omega$. $\alpha < \beta$ je zamena za $\alpha \leq \beta$ i $\alpha \neq \beta$. Naravno, ako je $\mathcal{H}$ skup svih visina, $\langle \mathcal{H}, \leq \rangle$ je kompletna mreža sa najvećim elementom $(\infty, \ldots, \infty, \ldots)$ i najmanjim elementom $(0, \ldots, 0, \ldots)$. Mogli smo je predstaviti i "algebarski" definišući operacije $\vee$ i $\wedge$ sa:

$$\alpha \vee \beta = (max\{\alpha_0, \beta_0\}, \ldots, max\{\alpha_n, \beta_n\}, \ldots),$$

$$\alpha \wedge \beta = (min\{\alpha_0, \beta_0\}, \ldots, min\{\alpha_n, \beta_n\}, \ldots).$$

Pomenuta mreža dobija sada oblik $\langle \mathcal{H}, \vee, \wedge \rangle$. Visine $\alpha$ i $\beta$ su *slične*, u oznaci $\alpha \sim \beta$, akko imaju iste slike za skoro sve prirodne brojeve, tj. za sve, osim eventualno konačno mnogo, i ako je ispunjeno: ako je $\alpha_n \neq \beta_n$, onda je $\alpha_n, \beta_n \neq \infty$. Relacija $\sim$ je relacija ekvivalencije. Refleksivnost i simetričnost su (više nego) očigledni, a ako je $\alpha \sim \beta$, $\beta \sim \gamma$, $X = \{k \in \omega \mid \alpha_k \neq \beta_k\}$ i $Y = \{m \in \omega \mid \beta_m \neq \gamma_m\}$, onda je $\{n \in \omega \mid \alpha_n \neq \gamma_n\} \subseteq X \cup Y$ i po definiciji relacije $\sim$ ni za jedno $n \in X \cup Y$ nije ni $\alpha_n$ ni $\gamma_n$ jednako $\infty$. Klase ekvivalencije zvaćemo *tipovima* i obeležavaćemo ih, za ovu priliku, sa $\mathbf{a}$, $\mathbf{b}$, ..., ili ako želimo da istaknemo predstavnika klase, sa $[\alpha]$, $[\beta]$, .... Primetimo da su tipovi zatvoreni za operacije $\vee$ i $\wedge$; znači, ako je $\alpha, \alpha' \in \mathbf{a}$, onda je i $\alpha \vee \alpha'$, $\alpha \wedge \alpha' \in \mathbf{a}$. Među tipovima uvodimo dalje relaciju $\preceq$ sa: $\mathbf{a} \preceq \mathbf{b}$ akko postoje visine $\alpha \in \mathbf{a}$ i $\beta \in \mathbf{b}$ takve da je $\alpha \leq \beta$. Neka je $\mathcal{T}$ skup svih tipova. Struktura $\langle \mathcal{T}, \preceq \rangle$ je mreža. Zaista, relacija $\preceq$ je parcijalno uređenje. Refleksivnost i tranzitivnost su očigledni. Pretpostavimo da je $\mathbf{a} \preceq \mathbf{b}$ i $\mathbf{b} \preceq \mathbf{a}$ i neka je, za $\alpha, \alpha' \in \mathbf{a}$, $\beta, \beta' \in \mathbf{b}$ i za svako $n \in \omega$, $\alpha_n \leq \beta_n$, $\beta'_n \leq \alpha'_n$. Ako je $X = \{k \in \omega \mid \alpha_k \neq \alpha'_k\}$ i $Y = \{m \in \omega \mid \beta_m \neq \beta'_m\}$, onda je, za $n \notin X \cup Y$, $\alpha_n \leq \beta_n = \beta'_n \leq \alpha'_n = \alpha_n$, tj. $\alpha_n = \beta_n$. Ako je $k \in X$, onda su $\alpha_k$, $\alpha'_k$ konačni (prirodni) brojevi, pa i $\beta_k$ mora biti prirodan broj (pretpostavka $\beta_k = \infty$ implicirala bi redom: $k \in X \setminus Y$, $\beta'_k = \beta_k \leq \alpha'_k \in \omega$, kontradikcija); analogno rezonujemo i u slučaju $k \in Y$; sada $\beta_k$ i $\beta'_k$ moraju biti prirodni brojevi, a pretpostavka $\alpha_k = \infty$ vodi u protivurečnost. Zaključujemo: $\alpha \sim \beta$, tj. $\mathbf{a} = \mathbf{b}$; dakle, $\preceq$ je antisimetrična relacija. Primetimo da tip $[(\infty, \ldots, \infty, \ldots)]$ sadrži samo jednu visinu. Taj tip zovemo *tip Ra*. Tip $[(0, \ldots, 0, \ldots)]$ zovemo *nula tip* i on, evidentno, sadrži beskonačno prebrojivo mnogo visina. Pokažimo još da je za svaka dva tipa $\mathbf{a} = [\alpha]$ i $\mathbf{b} = [\beta]$ tip $\mathbf{c} = [\alpha \wedge \beta]$ njihov infinum. Uočimo prvo da je tip $\mathbf{c}$ jednoznačno određen; drugim rečima, ako je $\alpha' \in \mathbf{a}$ i $\beta' \in \mathbf{b}$, tada je $[\alpha \wedge \beta] = [\alpha' \wedge \beta']$. Neka je opet $X = \{k \in \omega \mid \alpha_k \neq \alpha'_k\}$ i $Y = \{l \in \omega \mid \beta_l \neq \beta'_l\}$. Onda je, za $m \notin X \cup Y$, $\alpha_m = \alpha'_m$ i $\beta_m = \beta'_m$, te je i $\alpha_m \wedge \beta_m = \alpha'_m \wedge \beta'_m$. Ako je pak $m \in X \cup Y$, recimo, $m \in X$, tada su $\alpha_m, \alpha'_m$ različiti prirodni brojevi, pa su i $min\{\alpha_m, \beta_m\}$, $min\{\alpha'_m, \beta'_m\}$ prirodni (moguće jednaki) brojevi. Prema tome, $\alpha \wedge \beta \sim \alpha' \wedge \beta'$. Pretpostavimo sada da i za tip $\mathbf{d}$ važi: $\mathbf{d} \preceq \mathbf{a}$, $\mathbf{d} \preceq \mathbf{b}$, i neka je, za $\delta^1$ $(= (\delta^1_0, , \ldots, \delta^1_n, \ldots))$, $\delta^2 \in \mathbf{d}$, $\alpha^1 \in \mathbf{a}$ i $\beta^1 \in \mathbf{b}$, $\delta^1 \leq \alpha^1$, $\delta^2 \leq \beta^1$. Prema gore navedenom je $\alpha \wedge \alpha^1 \in \mathbf{a}$, $\beta \wedge \beta^1 \in \mathbf{b}$ i $(\alpha \wedge \beta) \wedge (\alpha^1 \wedge \beta^1) \in \mathbf{c}$. Dalje je $\delta^3 = \alpha \wedge \delta^1$, $\delta^4 = \beta \wedge \delta^2 \in \mathbf{d}$; npr. ako je $Z = \{k \in \omega \mid \alpha_k \neq \alpha^1_k\}$, onda je, za $m \notin Z$, $min\{\alpha_m, \delta^1_m\} = min\{\alpha^1_m, \delta^1_m\} = \delta^1_m$, a ako je $m \in Z$, onda su $\alpha_m$ i $\alpha^1_m$ prirodni brojevi, stoga je i $\delta^1_m$ $(\leq \alpha^1_m)$ prirodan broj; prema tome, $\alpha \wedge \delta^1 \sim \delta^1$. Konačno, $\delta^3 \wedge \delta^4 = (\alpha \wedge \delta^1) \wedge (\beta \wedge \delta^2) \in \mathbf{d}$ i, očigledno, $\delta^3 \wedge \delta^4 \leq \alpha \wedge \beta$ $(\in \mathbf{c})$; znači $\mathbf{d} \preceq \mathbf{c}$. Supremum i infinum tipova $\mathbf{a}$ i $\mathbf{b}$ obeležavaćemo sa, respektivno, $\mathbf{a} \bigvee \mathbf{b}$, $\mathbf{a} \bigwedge \mathbf{b}$; dakle, $[\alpha] \bigvee [\beta] = [\alpha \vee \beta]$, $[\alpha] \bigwedge [\beta] = [\alpha \wedge \beta]$.



Posmatrajmo sada proizvoljnu torziono slobodnu grupu $\mathbf{A}$. Za $a \in A$ niz $H(a) = (h_{p_0}(a), \ldots, h_{p_n}(a), \ldots)$, gde je $h_{p_n}(a)$ visina elementa $a$ u $p_n$ ($p_n$ je $n$-ti po redu prost broj), zove se *visina elementa* $a$ u $\mathbf{A}$. Tip $[H(a)]$ je *tip elementa* $a$. Operacije i relacije koje smo spomenuli u opštoj priči o visinama prenosimo na skupove visina elemenata (datih) grupa.

**Lema 43.2** *Neka je* $\mathbf{A}$ *torziono slobodna grupa i neka su* $a$ *i* $b$ *njeni elementi. Tada važi:*

*(a)* $H(a) = H(-a)$;

*(b)* $h_{p_n}((p_{i_1}^{k_1} \cdot \ldots \cdot p_{i_m}^{k_m} a) = \begin{cases} h_{p_n}(a) & n \notin \{i_1, \ldots, i_m\} \\ h_{p_n}(a) + k_j & n = i_j,\ 1 \leq j \leq m \end{cases}$, *(podrazumevamo, jasno,* $\infty + k = \infty + \infty = \infty$, *kao i da je* $k_j \geq 1$ *za* $j = 1, \ldots, m$*);*

*(c)* $H(a) < H(p_{i_1}^{k_1} \cdot \ldots \cdot p_{i_m}^{k_m} a)$ *akko je* $h_{p_j}(a) \neq \infty$ *za neko* $j \in \{i_1, \ldots, i_m\}$;

*(d)* $H(a) \sim H(p_{i_1}^{k_1} \cdot \ldots \cdot p_{i_m}^{k_m} a)$, *tj.* $[H(a)] = [H(p_{i_1}^{k_1} \cdot \ldots \cdot p_{i_m}^{k_m} a)]$;

*(e) ako je* $ma = nb$ *za neke nenula cele brojeve* $m$ *i* $n$, *onda je* $H(a) \sim H(b)$, *tj.* $[H(a)] = [H(b)]$;

*(f)* $H(a + b) \geq H(a) \wedge H(b)$, *tj.* $[H(a + b)] \succeq [H(a) \wedge H(b)]$;

*(g) ako je* $\mathbf{A}$ *direktna suma podgrupa* $\mathbf{B}$ *i* $\mathbf{C}$ *i ako je* $b \in B$, $c \in C$, *onda je* $H(b + c) = H(a) \wedge H(b)$, *tj.* $[H(b + c)] = [H(a)] \bigwedge [H(b)]$;

*(h) ako je* $\varphi$ *homomorfno preslikavanje grupe* $\mathbf{A}$ *u torziono slobodnu grupu* $\mathbf{G}$, *onda je* $H(a) \leq H((a)\varphi)$, *tj.* $[H(a)] \preceq [H((a)\varphi)]$, *za svako* $a \in A$;

*(i) element* $a$ *je deljiv sa* $m = p_{i_1}^{k_1} \cdot \ldots \cdot p_{i_r}^{k_r}$ *akko je* $k_j \leq h_{p_{i_j}}(a)$ *za svako* $j \in \{1, \ldots, r\}$.

**Dokaz.** Manje više sve je ili očigledno ili već konstatovano; tačke $(c)$ i $(d)$ su direktne posledice tačke $(b)$ (i definicije relacije sličnosti), a tačka $(e)$ je posledica tačke $(d)$:

$H(a) \sim H(ma) = H(nb) \sim H(b)$.

Dokažimo s nešto više detalja tačku $(i)$.

$(i)$ $(\Longleftarrow)$ Treba da pokažemo da jednačina $a = p_{i_1}^{k_1} \cdot \ldots \cdot p_{i_r}^{k_r} x$ ima rešenje (u grupi $\mathbf{A}$). Neka je $a_1$ rešenje jednačine $a = p_{i_1}^{k_1} x_1$ (ono postoji, pošto je

$k_1 \leq h_{p_{i_1}}(a)$, a jedinstveno je jer je **A** torziono slobodna grupa). Element $a_1$ je pak deljiv sa $p_{i_2}^{k_2}$, tj. za neko $a_2$ je $a_1 = p_{i_2}^{k_2} a_2$. Zaista, neka su $u$ i $v$ celi brojevi takvi da je $up_{i_1}^{k_1} + vp_{i_2}^{k_2} = 1$. Tada je $up_{i_1}^{k_1} a_1 + vp_{i_2}^{k_2} a_1 = a_1$, odnosno $ua + vp_{i_2}^{k_2} a_1 = a_1$, a $a$ je deljivo sa $p_{i_2}^{k_2}$. Dobili smo: $a = p_{i_1}^{k_1} a_1 = p_{i_1}^{k_1} p_{i_2}^{k_2} a_2$, gde je sada $a_2$ deljivo sa $p_{i_3}^{k_3}$ (ovog puta bismo krenuli od $(p_{i_1} p_{i_2}, p_{i_3}) = 1$ i ponovili prethodni postupak – za neke cele brojeve $u_1$ i $v_1$ je $u_1 p_{i_1}^{k_1} p_{i_2}^{k_2} + v_1 p_{i_3}^{k_3} = 1$, te je $u_1 p_{i_1}^{k_1} p_{i_2}^{k_2} a_2 + v_1 p_{i_3}^{k_3} a_2 = a_2$, dakle, $u_1 a + v_1 p_{i_3}^{k_3} a_2 = a_2$, a $a$ je deljivo sa $p_{i_3}^{k_3}$). Nastavljajući tako redom došli bismo do rešenja jednačine $a' = a_1 a_2 \cdots a_{i_r}$, gde je za svako $j$, $2 \leq j \leq r$, $a_j$ rešenje jednačine $a_{j-1} = p_{i_j}^{k_j} x_j$.□

**Lema 43.3** *Neka je $a$ element torziono slobodne grupe* **A** *i neka je $\beta$ visina slična visini elementa $a$ u* **A** *– $\beta \sim H(a)$. Tada u* **A** *postoji element $b$ čija je visina baš $\beta$.*

**Dokaz.** Jasno, ako je $H(a) = \beta$ nemamo šta dokazivati (jedno rešenje je samo $a$). Pretpostavimo stoga da je $H(a) \neq \beta$ ($H(a)$ onda ne može biti niz $(\infty, \ldots, \infty, \ldots)$, tj. $a$ ne može biti element beskonačne visine u svakom prostom broju $p$), a zbog pojednostavljenja notacije visinu elementa $a$ u $p_n$ $(h_{p_n}(a))$ obeležićemo sa $\alpha_n$ ($\beta$ je, naravno, niz $(\beta_0, \ldots, \beta_n, \ldots)$). Neka je $X = \{k \in \omega \mid \alpha_k - \beta_k = \mu_k > 0\} = \{i_1, \ldots, i_r\}$, $Y = \{m \in \omega \mid \beta_m - \alpha_m = \nu_m > 0\} = \{j_1, \ldots, j_t\}$ (prema tome je, za svako $l \notin X \cup Y$, $\alpha_l = \beta_l$). Jednačina

$$p_{j_1}^{\nu_{j_1}} \ldots p_{j_t}^{\nu_{j_t}} a = p_{i_1}^{\mu_{i_1}} \ldots p_{i_r}^{\mu_{i_r}} x$$

je rešiva u **A**. U cilju iznalaženja rešenja stavimo: $x = p_{j_1}^{\nu_{j_1}} \ldots p_{j_t}^{\nu_{j_t}} y$. Jednačina se onda svodi na

$$p_{j_1}^{\nu_{j_1}} \ldots p_{j_t}^{\nu_{j_t}} (p_{i_1}^{\mu_{i_1}} \ldots p_{i_r}^{\mu_{i_r}} y - a) = 0,$$

odnosno, s obzirom da je **A** torziono slobodna grupa, na

$$p_{i_1}^{\mu_{i_1}} \ldots p_{i_r}^{\mu_{i_r}} y = a.$$

Prema tački $(i)$ prethodne leme ova jednačina ima rešenje, neka je to $c$. Proizilazi da je rešenje polazne jednačine $b = p_{j_1}^{\nu_{j_1}} \ldots p_{j_t}^{\nu_{j_t}} c$. Iz $p_{j_1}^{\nu_{j_1}} \ldots p_{j_t}^{\nu_{j_t}} a = p_{i_1}^{\mu_{i_1}} \ldots p_{i_r}^{\mu_{i_r}} b$ sledi: za $k \notin X \cup Y$ je $h_{p_k}(b) = h_{p_k}(a) = \alpha_k = \beta_k$. Za $i_m \in X$ imamo: $h_{p_{i_m}}(p_{i_1}^{\mu_{i_1}} \ldots p_{i_m}^{\mu_{i_m}} \ldots p_{i_r}^{\mu_{i_r}} b) = h_{p_{i_m}}(b) + \mu_{i_m} = h_{p_{i_m}}(p_{j_1}^{\nu_{j_1}} \ldots p_{j_t}^{\nu_{j_t}} a) = h_{p_{i_m}}(a) = \alpha_{i_m}$, dakle, $h_{p_{i_m}}(b) = \alpha_{i_m} - \mu_{i_m} = \beta_{i_m}$; analogno se, za $j_n \in Y$, izvodi $h_{p_{j_n}}(b) = \beta_{j_n}$.□

**Teorema 43.4** *Postoji uzajamno jednoznačna korespondencija između klasa izomorfnih torziono slobodnih grupa ranga* 1 *i tipova.*

**Dokaz.** Teorema je idejno već rešena. Preostaje provera tehničkih detalja.



Preslikaćemo "skup" svih klasa izomorfnih torziono slobodnih grupa ranga 1 bijektivno na skup svih tipova na sledeći način: klasi $\mathcal{A}$ (izomornih torziono slobodnih grupa ranga 1) pridružujemo tip $[H(a)]$, gde je $a$ ma koji nenula element ma koje grupe **A** iz $\mathcal{A}$ (naravno, s aspekta teorije skupova se ne može govoriti o skupu čiji su elementi prave klase; imamo takođe u vidu da očigledno takvih klasa može biti najviše kontinuum mnogo, zapravo već sugerišemo da će ih biti baš toliko). Ova korespondencija je dobro definisana. Jer, ako je $a'$ ma koji drugi nenula element grupe **A**, onda je, s obzirom da je $\{a\}$ maksimalni linearno nezavisan sistem, $ma' = na$ za neke nenula cele brojeve $m$ i $n$, pa je i $[H(a')] = [H(a)]$ (tačka $(e)$ prethodne leme); u tom smislu govorimo o *tipu torziono slobodne grupe ranga* 1 – svi nenula elementi takve grupe su istog tipa; opet, ako je $\mathbf{A} \cong \mathbf{B} \in \mathcal{A}$ i $\varphi \in Is(\mathbf{A}, \mathbf{B})$, onda je $[H(a)] = [H((a)\varphi)]$. Pokazujemo dalje da je data korespondencija injektivna. Treba, dakle, da pokažemo da ako su **C** i **D** dve nenula torziono slobodne grupe ranga 1 i ako je $0 \neq c \in C$, $0 \neq d \in D$ i $[H(c)] = [H(d)]$, onda je $\mathbf{C} \cong \mathbf{D}$. Neka je $H(c) = (\gamma_0, \ldots, \gamma_n, \ldots)$, $H(d) = (\delta_0, \ldots, \delta_n, \ldots)$ i neka je $X = \{k \in \omega \mid \gamma_k \neq \delta_k\} = \{i_1, \ldots, i_m\}$. Neka su, dalje, $c' \in C$ i $d' \in D$ rešenja jednačina, respektivno: $c = p_{i_1}^{\gamma_{i_1}} \cdots p_{i_m}^{\gamma_{i_m}} x$, $d = p_{i_1}^{\delta_{i_1}} \cdots p_{i_m}^{\delta_{i_m}} y$ (u grupama, respektivno, **C** i **D**). Onda je $H(c') = H(d')$; za $n \notin X$ su prema tački $(b)$ leme 43.2 visine elemenata $c'$ i $d'$ u $p_n$ jednake, redom, visinama elemenata $c$ i $d$ u $p_n$ – $\gamma_n$, $\delta_n$), a (zbog $n \notin X$ je) $\gamma_n = \delta_n$; za $n \in X$ pak važi: $h_{p_n}(c') = h_{p_n}(d') = 0$ (ponovo prema istoj tački iste leme). Prema tome, jednačina $rc' = sx$ $(r, s \in Z)$ je rešiva u **C** akko je jednačina $rd' = sx$ rešiva u **D**, i kako su u pitanju torziono slobodne grupe, rešenja su, kada postoje, jedinstvena. Preslikavanje $\varphi : C \longrightarrow D$ koje rešenje jednačine $rc' = sx$, ukoliko postoji, preslikava u rešenje jednačine $rd' = sx$ bijekcija je (svaki element iz **C** je rešenje neke jednačine $rc' = sx$ za neke cele brojeve $r$ i $s$, jer je **C** ranga 1; posebno, $c'$ se preslikava na $d'$). No, $\varphi$ je i homomorfno preslikavanje: ako su $c_1$ i $c_2$ rešenja, respektivno, jednačina $r_1 c' = s_1 x$, $r_2 c' = s_2 x$, a $d_1$ i $d_2$ rešenja odgovarajućih jednačina u **D**, tada je $c_1 + c_2$ (jedinstveno) rešenje jednačine $(r_1 s_2 + r_2 s_1)c' = (s_1 s_2)x$, $d_1 + d_2$ je (jedinstveno) rešenje jednačine $(r_1 s_2 + r_2 s_1)d' = (s_1 s_2)x$, pa je $(c_1 + c_2)\varphi = d_1 + d_2 = (c_1)\varphi + (c_2)\varphi$. Preostaje još da se pokaže surjektivnost ustanovljene korespondencije. Neka je $\alpha = (\alpha_0, \ldots, \alpha_n, \ldots)$ ma koja visina, $X = \{k \in \omega \mid \alpha_k$ je prirodan broj $\}$ i $Y = \{m \in \omega \mid \alpha_m = \infty\}$. Evidentno, u podgrupi grupe **Ra** generisanoj skupom $\{\frac{1}{p_k^{\alpha_k}} \mid k \in X\} \cup \bigcup_{m \in Y} \{\frac{1}{p_m^n} \mid n \in N\}$ element 1 je visine $\alpha$.■

**Napomena.** U okviru priče o lokalno cikličnim grupama tip je definisan kao funkcija koja preslikava skup prostih brojeva u skup $Z \cup \{-\infty\}$ i koja je pozitivna za samo konačno mnogo prostih brojeva (34.2). Tom prilikom je pokazano da postoji uzajamno jednoznačna korespondencija između svih tipova i svih nenula podgrupa aditivne grupe racionalnih brojeva – $\mathbf{G} \longleftrightarrow (v_{p_0}(\mathbf{G}), \ldots, v_{p_n}(\mathbf{G}), \ldots)$ (34.3), kao i da su podgrupe **G** i **H** grupe **Ra** izomor-

fne akko je $\sum_{p\in P}|v_p(\mathbf{G})-v_p(\mathbf{H})|<\infty$ (34.4). No, $\sum_{p\in P}|v_p(\mathbf{G})-v_p(\mathbf{H})|<\infty$ upravo znači da se tipovi $(v_{p_0}(\mathbf{G}),\dots,v_{p_n}(\mathbf{G}),\dots)$ i $(v_{p_0}(\mathbf{H}),\dots,v_{p_n}(\mathbf{H}),\dots)$ razlikuju u samo konačno mnogo komponenti, te da su komponente u kojima se ti nizovi razlikuju različite od $-\infty$. U sklopu terminologije ovog paragrafa mogli bismo reći da se radi o relaciji sličnosti. Pokazaćemo da su grupe određene klasama ekvivalencije relacije sličnosti "onih tipova" i "ovih visina" izomorfne. Posmatrajmo jednu klasu ekvivalencije (relacije sličnosti tipova) sa predstavnikom $\varphi=(\varphi_0,\dots,\varphi_n,\dots)$, gde možemo odmah pretpostaviti da je $(p_n)\varphi=\varphi_n\leq 0$ za svako $p_n\in P$ (samo konačno mnogo komponenti nekog tipa može biti pozitivno, pa ako prvi nasumce izabrani predstavnik klase ekvivalencije ima takvih komponenti, zamenjujemo ga tipom koji ima sve ostale komponente iste kao i on, a na mestu "njegovih" pozitivnih komponenti nule). Neka je onda $\beta=(\beta_0,\dots,\beta_n,\dots)$ visina, gde je $\beta_n=-\varphi_n$ (podrazumevamo: $-(-\infty)=\infty$. Tipu $\varphi$ odgovara podgrupa $\mathbf{A}$ grupe $\mathbf{Ra}$ sa domenom $\{0\}\cup\{a\in Ra\mid (a)v_{p_n}\geq\varphi_n\}$ (34.1), visini $\beta$ odgovara podgrupa $\mathbf{B}$ grupe $\mathbf{Ra}$ generisana skupom $\bigcup\{\frac{1}{p_n^{\beta_n}}\ (=p_n^{\varphi_n})\mid \beta_n\neq\infty\}\cup\bigcup\{\frac{1}{p_k^m}\mid \beta_k=\infty, m\in\omega\}$. Grupa $\mathbf{A}$ sadrži 1 i visina tog elementa u $\mathbf{A}$ je baš $\beta$, a to je visina istog elementa i u $\mathbf{B}$. Dalje, prema dokazu prethodne teoreme sledi da su $\mathbf{A}$ i $\mathbf{B}$ izomorfne grupe.

Jednoelementnom tipu $[(\infty,\dots,\infty,\dots)]$ odgovara samo grupa $\mathbf{Ra}$ (videti i 33.29($a$)). Svakom drugom tipu odgovara prebrojivo mnogo izomorfnih podgrupa grupe $\mathbf{Ra}$; na primer, tipu $[(0,\dots,0,\dots)]$ odgovaraju sve podgrupe izomorfne aditivnoj grupi celih brojeva – $\mathbf{Z}$.

**Lema 43.5** *Neka je* $\mathbf{A}$ $(\leq\mathbf{Ra})$ *torziono slobodna grupa ranga* 1. *Tada važi:*

($a$) *Ako je nenula element $a$ iz $A$ visine $H(a)=(\alpha_0,\dots,\alpha_n,\dots)$, tada je* $\overline{\mathbf{A}}=\mathbf{A}/\langle a\rangle\cong\mathbf{P}_0\oplus\cdots\oplus\mathbf{P}_n\oplus\cdots$, *gde je za* $n\in\omega$:

$$\mathbf{P}_n=\begin{cases}\mathbf{Z}_{p_n^{\alpha_n}} & \alpha_n\in\omega\\ \mathbf{p}_n^{\infty} & \alpha_n=\infty\end{cases}.$$

($b$) *Neka je* $\mathbf{B}$ *nenula podgrupa grupe* $\mathbf{A}$ *i neka je nenula element $b$ iz $B$ visina u* $\mathbf{B}$ *i* $\mathbf{A}$, *respektivno,* $\beta=(\beta_0,\dots,\beta_n,\dots)$ *i* $\gamma=(\gamma_0,\dots,\gamma_n,\dots)$. *Tada je* $\mathbf{A}/\mathbf{B}\cong\mathbf{P}'_0\oplus\cdots\oplus\mathbf{P}'_n\oplus\cdots$, *gde je za* $n\in\omega$:

$$\mathbf{P}'_n=\begin{cases}\mathbf{Z}_{p_n^{\gamma_n-\beta_n}} & \gamma_n-\beta_n\in\omega\\ \mathbf{p}_n^{\infty} & \gamma_n-\beta_n=\infty\end{cases};$$

*(podrazumevamo: za svako* $k\in\omega$ *je* $\infty-k=\infty$, $\infty-\infty=0$*).*

**Dokaz.** ($a$) Imamo: $\mathbf{A}/\langle a\rangle\leq\mathbf{Ra}/\langle a\rangle\cong\sum_{p\in P}\mathbf{p}^{\infty}$. Jer, $\mathbf{Ra}/\langle a\rangle$ je deljiva periodična grupa (za svako nenula $a'\in Ra$ postoje nenula celi brojevi $m$ i $n$ takvi da je $ma=na'$). Za svako $p\in P$ postoji bar jedna Prüferova $p$-podgrupa grupe $\mathbf{Ra}/\langle a\rangle$, pošto je $\frac{1}{p}a+\langle a\rangle$ $(\neq\langle a\rangle)$ reda $p$. Opet, ako su



$a'+\langle a\rangle$ i $a''+\langle a\rangle$ elementi redova, respektivno, $p^m$ i $p^n$, $n\geq m$, i ako je $p^ma'=ka$, $p^na''=la$, $(k,p)=(l,p)=1$, onda je $p^{n-m}ka''-la'=0$, tj. $p^{n-m}(ka''+\langle a\rangle)=l(a'+\langle a\rangle)$; dakle, postoji tačno jedna Prüferova $p$-podgrupa (imamo u vidu da je npr. $\langle a''+\langle a\rangle\rangle=\langle k(a''+\langle a\rangle)\rangle$). Proizilazi da je $\overline{\mathbf{A}}_p$ podgrupa Prüferove $p$-grupe, znači, ili je kociklična $p$-grupa ili je nula grupa. Zapravo, ako je $h_{p_n}(a)=\alpha_n\in\omega$ i $a=p_n^{\alpha_n}a_1$, tada je $\overline{\mathbf{A}}_{p_n}=\langle a_1+\langle a\rangle\rangle$ $(\cong\mathbf{Z}_{p_n^{\alpha_n}})$ (pretpostavka da je $\overline{\mathbf{A}}_{p_n}$ ciklična $p_n$-grupa većeg reda ili Prüferova $p_n$-grupa implicirala bi $h_{p_n}(a)>\alpha_n$, kontradikcija); analogno je $\overline{\mathbf{A}}_{p_n}$ Prüferova $p_n$-grupa za $\alpha_n=\infty$.

($b$) Polazimo od:

$$\mathbf{A}/\mathbf{B}\cong(\mathbf{A}/\langle b\rangle)/(\mathbf{B}/\langle b\rangle)=\overline{\mathbf{A}}/\overline{\mathbf{B}}\cong$$

$$(\textstyle\sum_{p\in P}\overline{\mathbf{A}}_p)/(\sum_{p\in P}\overline{\mathbf{B}}_p)\cong\sum_{p\in P}\overline{\mathbf{A}}_p/\overline{\mathbf{B}}_p.$$

Prema tački ($a$) važi: ako je $\beta_n\leq\gamma_n<\infty$ ili $\beta_n=\gamma_n=\infty$, tada je $\overline{\mathbf{A}}_{p_n}/\overline{\mathbf{B}}_{p_n}\cong\mathbf{Z}_{p_n^{\gamma_n-\beta_n}}$; ako je $\beta_n\in\omega$, $\gamma_n=\infty$, tada je $\overline{\mathbf{A}}_{p_n}/\overline{\mathbf{B}}_{p_n}\cong p_n^{\infty}$.□

Sledeća dva rezultata se tiču torziono slobodnih grupa ma kog ranga.

**Lema 43.6** *Neka je* $\mathbf{A}$ *torziono slobodna grupa i* $\mathbf{a}=[\alpha]$ *jedan tip. Tada je* $A(\mathbf{a})\overset{\text{def}}{=}\{a\in A\mid [H(a)]\succeq[\alpha]\}$ *domen potpune podgrupe grupe* $\mathbf{A}$ *– u oznaci* $\mathbf{A}(\mathbf{a})$.

**Dokaz.** $A(\mathbf{a})$ je neprazan skup jer, jasno, sadrži nulu. Tačke ($a$), ($e$) i ($f$) leme 43.2 dokazuju ostalo.□

**Napomena.** Sa $\mathbf{A}'(\mathbf{a})$ obeležićemo podgrupu grupe $\mathbf{A}$ generisanu skupom $\{a\in A\mid [H(a)]\succ\mathbf{a}\}$ (koji može biti i prazan), a sa $\mathbf{A}^*(\mathbf{a})$ faktor grupu $\mathbf{A}(\mathbf{a})/\mathbf{A}'(\mathbf{a})$.

**Definicija 43.7** *Skup tipova torziono slobodne grupe* $\mathbf{A}$, *u oznaci* $\mathcal{T}(\mathbf{A})$, *je skup* $\{[H(a)]\mid a\in A\}$.

$\mathcal{T}(\mathbf{A})$ *ispunjava uslov maksimalnosti (minimalnosti) akko je svaki strogo rastući (opadajući) lanac tipova iz* $\mathcal{T}(\mathbf{A})$: $\mathbf{a}_1\prec\mathbf{a}_2\prec\cdots$ $(\mathbf{a}_1\succ\mathbf{a}_2\succ\cdots)$ *konačne dužine, tj. završava se u konačno mnogo koraka.*

**Lema 43.8** *Skup tipova torziono slobodne grupe konačnog ranga ispunjava uslove maksimalnosti i minimalnosti.*

**Dokaz.** Neka je $\mathbf{a}_1=[H(a_1)]\prec\mathbf{a}_2=[H(a_2)]\prec\cdots$ strogo rastući lanac tipova torziono slobodne grupe konačnog ranga $\mathbf{A}$. Prema prethodnoj lemi podgrupe $\mathbf{A}(\mathbf{a}_1)$, $\mathbf{A}(\mathbf{a}_2)$, ..., obrazuju strogo opadajući niz potpunih podgrupa grupe $\mathbf{A}$ (jasno, $\mathbf{A}(\mathbf{a}_{i+1})\leq\mathbf{A}(\mathbf{a}_i)$, a npr. $a_1\in A(\mathbf{a}_1)\setminus A(\mathbf{a}_2)$). No,

zbog potpunosti tih podgrupa imamo i $r(\mathbf{A}(\mathbf{a}_1)) > r(\mathbf{A}(\mathbf{a}_2)) > \cdots$. Posmatrajmo samo grupe $\mathbf{A}(\mathbf{a}_1)$ i $\mathbf{A}(\mathbf{a}_2)$. Pretpostavimo da je $r(\mathbf{A}(\mathbf{a}_1)) = r(\mathbf{A}(\mathbf{a}_2)) = m$ i neka je $\{b_1, \ldots, b_m\}$ maksimalan linearno nezavisan sistem podgrupe $\mathbf{A}(\mathbf{a}_2)$. Za (svako) dato $a$ iz $A(\mathbf{a}_1)$ postoji nenula ceo broj $k$ takav da je $ka \in \langle b_1, \ldots, b_m\rangle$; recimo $ka = k_1b_1 + \cdots + k_mb_m$. S obzirom na potpunost podgrupe $\mathbf{A}(\mathbf{a}_2)$ je $kb = k_1'b_1 + \cdots + k_mb_m$ za neko $b \in A(\mathbf{a}_2)$, pa je $k(a-b) = 0$, odnosno $a = b \in A(\mathbf{a}_2)$; sledi $A(\mathbf{a}_1) = A(\mathbf{a}_2)$, kontradikcija. Dakle, svaki strogo rastući lanac tipova elemenata iz $\mathbf{A}$ je konačne dužine. Slično rezonujemo i u drugom slučaju.□

**Primer 43.9** (*a*) *Ako je* $\mathbf{A}$ *torziono slobodna grupa ranga* 1, *onda je, za prost broj* $p$, $\bigcap_{n=1}^{\infty} p^n\mathbf{A}$ *ili nula grupa ili cela grupa.*

**Dokaz.** Neka je $p = p_k$ ($k$-ti po redu prost broj). Pretpostavimo da je $p^m\mathbf{A} \neq \mathbf{A}$ za neko $m \in N$. Ako je $a \in A \setminus p^mA$, onda je $k$-ta komponenta visine elementa $a$ ($h_{p_k}(a)$) manja od $m$. Ako je $b$ ma koji drugi nenula element grupe $\mathbf{A}$, mora biti, videli smo, $H(b) \sim H(a)$, pa je i $h_{p_k}(b)$ prirodan broj. Prema tome, za prirodan broj $l$ veći od $h_{p_k}(b)$ element $b$ nije u $p^lA$. Zaključujemo: $\bigcap_{n=1}^{\infty} p^n\mathbf{A} = \mathbf{O}$.

(*b*) *Torziono slobodne grupe* $\mathbf{A}$ *i* $\mathbf{B}$ *ranga* 1 *nisu izomorfne akko postoji skup stepena prostih brojeva* $\Omega$ *takav da je* $\bigcap_{p^k\in\Omega} p^k\mathbf{A} = \mathbf{O}$ *i* $\bigcap_{p^k\in\Omega} p^k\mathbf{B} \neq \mathbf{O}$ *ili obrnuto.*

**Dokaz.** Pretpostavimo da $\mathbf{A}$ i $\mathbf{B}$ nisu izomorfne i neka je $a \in A\setminus\{0\}$, $b \in B\setminus\{0\}$. Onda je $H(a) \not\sim H(b)$, te postoji prost broj $p = p_r$ takav da je $h_{p_r}(a) \neq \infty$ i $h_{p_r}(b) = \infty$ ili obrnuto, ili je pak skup $X = \{s \in \omega \mid h_{p_s}(a) \neq h_{p_s}(b)\}$ beskonačan (naravno, navedene mogućnosti se ne isključuju međusobno). U prvom slučaju je (neka ostane $h_{p_r}(a) \neq \infty$, $h_{p_r}(b) = \infty$), prema prethodnoj tački, $\bigcap_{n=1}^{\infty} p_r^n\mathbf{A} = \mathbf{O}$, $\bigcap_{n=1}^{\infty} p_r^n\mathbf{B} = \mathbf{B}$ (ovde je $\Omega = \{p_r^n \mid n \in N\}$). U drugom slučaju je bar jedan od (disjunktnih) skupova $Y = \{s \in X \mid h_{p_s}(a) > h_{p_s}(b)\}$, $V = \{s \in X \mid h_{p_s}(b) > h_{p_s}(a)\}$, beskonačan. Neka je $|Y| = \aleph_0$. No, onda je $\bigcap\{p_s^{h_{p_s}(a)}\mathbf{A} \mid s \in Y\} \neq \mathbf{O}$ (jer, jasno, $a \in \bigcap\{p_s^{h_{p_s}(a)}A \mid s \in Y\}$), dok je $\bigcap\{p_s^{h_{p_s}(b)}\mathbf{B} \mid s \in Y\} = \mathbf{O}$; hipoteza $(0 \neq)\, b' \in \bigcap\{p_s^{h_{p_s}(a)}B \mid s \in Y\}$ dala bi: za svako $s \in Y$ je $h_{p_s}(b') \geq h_{p_s}(a) > h_{p_s}(b)$, i odatle $H(b') \not\sim H(b)$, kontradikcija.

(*c*) *Ako su torziono slobodne grupe ranga* 1 $\mathbf{A}$ *i* $\mathbf{B}$ *takve da je svaka izomorfna nekoj podgrupi one druge, onda su i izomorfne.*

**Dokaz.** Neka je $\varphi$ izomorfno preslikavanje grupe $\mathbf{A}$ na podgrupu $\mathbf{B}_1$ grupe $\mathbf{B}$, $\psi$ izomorfno preslikavanje grupe $\mathbf{B}$ na podgrupu $\mathbf{A}_1$ grupe $\mathbf{A}$. Tada je za nenula element $a$ iz $A$: $H(a) \leq H((a)\varphi) \leq H((a)(\varphi\circ\psi))$, i kako je $H(a) \sim H((a)(\varphi\circ\psi))$, sledi: $H(a) \sim H((a)\varphi)$. Ali $[H(a)]$ $(= [H((a)\varphi)])$ je upravo je tip grupa $\mathbf{A}$ i $\mathbf{B}$, pa je $\mathbf{A} \cong \mathbf{B}$.□



**Lema 43.10** *Neka je* $\mathbf{G}$ *ma kakva R-grupa. Izolotar ma kog njenog nejediničnog elementa* $a$ ($\mathbf{I}(a)$ – *videti* 4.44) *je Abelova torziono slobodna grupa ranga* 1 *i za svako* $b \in I(a)\setminus\{e\}$ *je* $\mathbf{I}(b) = \mathbf{I}(a)$.

*Za svaka dva elementa* $c, d$ *grupe* $\mathbf{G}$ *je ili* $\mathbf{I}(c) = \mathbf{I}(d)$ *ili* $\mathbf{I}(c)\cap\mathbf{I}(d) = \mathbf{E}$.

**Dokaz.** Neka je $\mathcal{P}_a = \langle\{\mathbf{A} \mid \mathbf{A}$ je Abelova podgrupa ranga 1 grupe $\mathbf{G}$ i $a \in A\}$ $(= P_a), \leq\rangle$. Očigledno je $P_a \neq \emptyset$ jer (barem) $\langle a\rangle \in P_a$, a jasno je i da je ispunjen uslov Zornove leme – unija lanca Abelovih grupa ranga 1 je opet Abelova grupa ranga 1. Neka je $\mathbf{M}_a$ jedan maksimalni element skupa $P_a$. Onda je $\mathbf{M}_a \leq \mathbf{I}(a)$. Jer, važi generalno: ako Abelova podgrupa ranga 1 $\mathbf{B}$ i (ma koja) izolovana podgrupa $\mathbf{H}$ imaju nejedinični presek, tada je $\mathbf{B} \leq \mathbf{H}$; zaista, ako je $x \in B\cap H$ i ako je, za (bilo koje) $y \in B$, $y^m = x^n$ (možemo pretpostaviti da su i $m$ i $n$ prirodni brojevi; po potrebi bismo inače radili sa inverznim jednog od tih ili oba elementa), sledi $y^m \in H$, pa je i $y \in H$. Pretpostavimo da je $a$ element i nekog drugog maksimalnog elementa skupa $P_a$ – $\mathbf{M}$. No, pošto je $\langle a\rangle \leq \mathbf{M}_a\cap\mathbf{M}$, to je za svaki nejedinični element $x \in M_a$ i svaki nejedinični element $y \in M$, za neke pozitivne prirodne brojeve $m, n$, $x^m, y^n \in \langle a\rangle$. Prema tome, elementi $x^m$ i $y^n$ su uzajamno permutabilni, te su prema 4.46 i $x$ i $y$ uzajamno permutabilni. Ali tada je $\langle M_a \cup M\rangle$ Abelova grupa ranga 1, dakle element skupa $P_a$, kontradikcija (koristili smo: ako za $c, c_1$ iz $M_a$ i $d, d_1$ iz $M$ važi $c^m = a^k$, $c_1^r = a^p$, $d^n = a^l$ i $d_1^s = a^q$, onda je $(cd)^{mn(ps+qr)} = (c_1d_1)^{rs(kn+lm)}$). Primetimo još da je $\mathbf{M}_a$ i sama izolovana podgrupa: ako je $b$ nejedinični element i $b^n \in M_a$ za neko $n \in N$, podgrupe $\mathbf{M}_a$ i $\mathbf{M}_b$ imaju neprazan presek, a $\langle M_a\cup M_b\rangle$ je, upravo smo pokazali, Abelova grupa ranga 1 (jasno, $\mathbf{M}_b$ je jedan maksimalni element odgovarajućeg skupa $P_b$); stoga je $\mathbf{M}_b \leq \mathbf{M}_a$ i $b \in M_a$.

Zaključujemo: izolator nejediničnog elementa $a$ je jedinstven maksimalni element parcijalnog uređenja $\mathcal{P}$ – $\mathbf{M}_a$, a odatle trivijalno slede i ostali elementi tvrđenja.□

## 44 Kompletno razložive grupe

Slobodne Abelove grupe su, prema definiciji, direktne sume izomorfnih kopija aditivne grupe celih brojeva (21.10(*i*)), a torziono slobodne deljive grupe izomorfnih kopija aditivne grupe racionalnih brojeva (33.19). U oba slučaja se, dakle, radi o direktnim sumama grupa ranga 1. U ovom paragrafu ćemo reći koju reč o takvim sumama. No prvo

**Definicija 44.1** *Torziono slobodna grupa je kompletno razloživa akko je razloživa u direktnu sumu grupa ranga* 1.

**Lema 44.2** *Sva razlaganja kompletno razložive torziono slobodne grupe* $\mathbf{A}$ *u direktnu sumu grupa ranga* 1 *su izomorfna.*

**Dokaz**. Grupe ranga 1, pokazali smo u prethodnom paragrafu, određeni su (do na izomorfizam) tipom ma kog svog nenula elementa. Pokazaćemo da je broj sumanada određenog tipa nezavisan od dekompozicije grupe $\mathbf{A}$ (u direktnu sumu grupa ranga 1).

Neka je $\mathbf{A} = \sum_{\alpha<\kappa} \mathbf{A}_\alpha$, gde je $r(\mathbf{A}_\alpha) = 1$ za svako $\alpha < \kappa$. Tada je, za fiksni tip $\mathbf{a}$, $\mathbf{A}(\mathbf{a})$ direktna suma onih grupa $\mathbf{A}_\alpha$ čiji je tip veći od ili jednak $\mathbf{a}$ (43.2($g$)); neka je $\mathbf{A}(\mathbf{a}) = \sum_{i\in I} \mathbf{A}_{\alpha_i}$ ($\alpha_i < \kappa$). Isto tako je $\mathbf{A}'(\mathbf{a})$ direktna suma onih grupa $\mathbf{A}_\alpha$ čiji je tip strogo veći od $\mathbf{a}$, recimo $\mathbf{A}'(\mathbf{a}) = \sum_{j\in J} \mathbf{A}_{\alpha_j}$ (dakle, $\{\mathbf{A}_{\alpha_j} \mid j \in J\}$ je skup svih grupa $\mathbf{A}_\alpha$ čiji je tip veći od $\mathbf{a}$); očigledno, $\sum_{j\in J} \mathbf{A}_{\alpha_j} \leq \mathbf{A}'(\mathbf{a})$, a ako je $a = k_1a_1 + \cdots + k_ma_m \in A'(\mathbf{a})$, gde je, za $i = 1,\ldots,m$, $k_i \neq 0$ i $[H(a_i)] > \mathbf{a}$ i ako je $a_i = a_{\alpha_{j_1}} + \cdots + a_{\alpha_{j_{m_i}}} \in A_{\alpha_{j_1}} \oplus \cdots \oplus A_{\alpha_{j_{m_i}}}$, onda je, ponovo prema 43.2($g$), za svako $r = 1,\ldots,m_i$, $[H(a_{\alpha_{j_r}})] > \mathbf{a}$. Jasno, $J \subseteq I$, a $\mathbf{A}^*(\mathbf{a}) = \mathbf{A}(\mathbf{a})/\mathbf{A}'(\mathbf{a}) \cong \sum_{i\in I\setminus J} \mathbf{A}_{\alpha_i}$. Prema tome, $\mathbf{A}^*(\mathbf{a})$ je direktna suma onih sumanada čiji je tip baš $\mathbf{a}$, pa je broj takvih sumanada u datoj dekompoziciji, kao i u svakoj drugoj, jednak rangu grupe $\mathbf{A}^*(\mathbf{a})$.□

Za datu kompletno razloživu torziono slobodnu grupu $\mathbf{A}$ i dati tip $\mathbf{a}$ obeležićemo sa $r_{\mathbf{A}}(\mathbf{a})$ ili, kada je jasno o kojoj je grupi reč, sa $r(\mathbf{a})$ broj sumanada (ranga 1 i) tipa $\mathbf{a}$ u dekompoziciji grupe $\mathbf{A}$ u direktnu sumu grupa ranga 1. Upravo smo pokazali da je taj broj nezavisan od dekompozicije.

**Korolar 44.3** *Dve kompletno razložive torziono slobodne grupe* $\mathbf{A}$ *i* $\mathbf{B}$ *su izomorfne akko je* $r_{\mathbf{A}}(\mathbf{a}) = r_{\mathbf{B}}(\mathbf{a})$ *za svaki tip* $\mathbf{a}$.

Jasno, prvi problem vezan za potpuno razložive grupe je njihova karakterizacija. Na njega još nije adekvatno odgovoreno, u smislu da su ponuđene karakterizacije pre "nategnute veze" nego ekvivalenti koji bi omogućili lakše ispitivanje ovih grupa. Mi ćemo ovom prilikom izneti samo neke od rezultata koji se tiču pitanja: kada je direktni sumand potpuno razložive torziono slobodne grupe i sam potpuno razloživ?

**Lema 44.4** *Neka je* $\mathbf{B}$ *prava potpuna podgrupa torziono slobodne grupe* $\mathbf{A}$ *takva da su svi elementi iz* $A \setminus B$ *kao i nenula elementi faktor grupe* $\mathbf{A}/\mathbf{B}$ *istog tipa. Tada u svakom kosetu* $a + B$ *različitom od* $B$ *postoji element* $a_1$ *takav da je* $H(a_1) = H(a + B)$.

**Dokaz**. U vezi sa uslovom potpunosti podgrupe $\mathbf{B}$ videti 37.8($d$).

Krenimo od elementa $a$ iz $a+B$ (izbor predstavnika je nebitan). Očigledno, $H(a) \leq H(a + B)$ (iz $a = p^lc$ sledi $a + B = p^l(c + B)$). S druge strane, zbog $H(a) \sim H(a + B)$ razlikuju se visine elementa $a$ (u $\mathbf{A}$) i elementa $a + B$ (u $\mathbf{A}/\mathbf{B}$) u samo konačno mnogo komponenti i te različite komponente su prirodni brojevi. Ako nema različitih komponenti dokaz je gotov – $a$ je traženi element. Pretpostavimo stoga da ima različitih komponenti. Neka je $H(a) =$



$(\alpha_0,\ldots,\alpha_n,\ldots)$, $H(a+B) = (\beta_0,\ldots,\beta_n,\ldots)$ i neka je $\{k \in \omega \mid \beta_k - \alpha_k = \gamma_k > 0\} = \{i_1,\ldots,i_r\}$. Tada je, za $m = p_{i_1}^{\gamma_{i_1}} \cdot \ldots \cdot p_{i_r}^{\gamma_{i_r}}$, $H(ma) = H(a + B)$. Ako je $\overline{m} = p_{i_1}^{\beta_{i_1}} \cdot \ldots \cdot p_{i_r}^{\beta_{i_r}}$, onda je $a+B$ deljivo sa $\overline{m}$ (43.2($i$)), pa je $a+B = \overline{m}(c+B) = \overline{m}c + B$ za neki element $c + B$ faktor grupe $\mathbf{A}/\mathbf{B}$. Kao maločas proizilazi da je $H(n\overline{m}c) = H(\overline{m}c + B) = H(a + B)$ za neki prirodan broj $n$. Naravno, $(\overline{m}, n) = 1$ (u suprotnom bismo, za $p_{i_j}|(\overline{m}, n)$ za neko $j$, $1 \leq j \leq r$, dobili $h_{p_{i_j}}(a+B) < h_{p_{i_j}}(n\overline{m}c)$, jer bi $n\cdot\overline{m}$ bilo deljivo sa $p_{i_j}^{\beta_{i_j}+1}$), te je i $(m, n) = 1$. Ako je, za cele brojeve $u$ i $v$, $um + nv = 1$ i $a_1 = (um)a + (nv)\overline{m}c$, tada je $a - a_1 = (um)a + (vn)a - (um)a - (nv)\overline{m}c = nv(a - \overline{m}c) \in B$, tj. $a_1 \in a + B$ i $H(a_1) \leq H(a + B) = H(ma) \wedge H(n\overline{m}c) \leq H(uma) \wedge H((nv)\overline{m}c) \leq H(a_1)$ (jer je, za svaki prost broj $p$, $h_p(a_1) \geq min\{h_p(uma), h_p((nv)\overline{m}c)\}$. Znači, $H(a_1) = H(a + B)$.□

**Lema 44.5** *Neka je* $\mathbf{B}$ *potpuna podgrupa torziono slobodne grupe* $\mathbf{A}$ *takva da je faktor grupa* $\mathbf{A}/\mathbf{B}$ *ranga* 1 *a svi elementi iz* $A \setminus B$ *su istog tipa kao i faktor grupa* $\mathbf{A}/\mathbf{B}$. *Tada je* $\mathbf{B}$ *direktni sumand grupe* $\mathbf{A}$.

**Dokaz**. Neka je $a+B$ proizvoljan nenula elemenat faktor grupe $\mathbf{A}/\mathbf{B}$ i neka je $H(a_1) = H(a+B)$ za $a_1 \in a+B$. Potpuna podgrupa $\mathbf{A}_1$ grupe $\mathbf{A}$ generisana elementom $a_1$ (setimo se, njen domen je $A_1 = \{g \in A \mid mg \in \langle a_1\rangle$ za neki nenula ceo broj $m$ koji zavisi od $g\}$ – 37.9) ima svojstvo da sadrži po tačno jedan element iz svakog koseta podgrupe $\mathbf{B}$. Jer, za ma koji koset $c+B$ postoje celi uzajamno prosti brojevi $k$ i $l$ takvi da je $k(c + B) = l(a_1 + B)$. Kako je $l(a_1 + B)$ deljivo sa $k$, a onda i $a_1 + B$, dakle i $a_1$, to je $a_1 = ka_2$ za neko $a_2$. Sledi: $k((c + B) - l(a_2 + B)) = B$, tj. $c + B = l(a_2 + B)$, pa je, za neko $b \in B$, $c + b = la_2 \in A_1$ ($k(la_2) = la_1 \in \langle a_1\rangle$). Pretpostavimo da je $c + b_1 \in A_1$ i za neko $b_1$ iz $B$, različito od $b$. Ali tada je $c + b - (c + b_1) = b - b_1 \in A_1$, znači, za neke nenula cele brojeve $u$ i $v$ je $u(b - b_1) = va_1$. Odatle je $v(a_1 + B) = B$; prema tome, $v = 0$ (a onda i $u = 0$), kontradikcija.

Sada direktno proizilazi: $\mathbf{A} = \mathbf{B} \oplus \mathbf{A}_1$ ($\mathbf{B} \cap \mathbf{A}_1 = \mathbf{O}$ jer je, trivijalno, $|A_1 \cap B| = 1$), a za $c \notin B$ postoji $b \in B$ takvo da je $c + b \in A_1$, te je $\mathbf{B} \oplus \mathbf{A}_1 = \mathbf{A}$.□

**Korolar 44.6** *Neka je* $\mathbf{B}$ *potpuna podgrupa torziono slobodne grupe* $\mathbf{A}$ *takva da je* $\mathbf{A}/\mathbf{B}$ *(torziono slobodna) grupa konačnog ranga a svi elementi iz* $A \setminus B$ *su istog tipa* – $\mathbf{a}$. *Tada je* $\mathbf{A}$ *direktna suma podgrupe* $\mathbf{B}$ *i kompletno razložive podgrupe ako su svi nenula elementi svake faktor grupe* $\mathbf{A}/\mathbf{C}$, *gde je* $\mathbf{C}$ *(prava) potpuna podgrupa koja sadrži* $\mathbf{B}$, *tipa* $\mathbf{a}$.

**Dokaz**. Pretpostavimo da važi navedeni uslov. Ako je $\mathbf{A}/\mathbf{B}$ baš ranga 1, pozivamo se direktno na prethodnu lemu. U suprotnom, neka $a_1 \notin B$ i neka je $\mathbf{B}_1$ minimalna potpuna podgrupa grupe $\mathbf{A}$ koja sadrži podgrupu $\mathbf{B} \oplus \langle a_1\rangle$. $\mathbf{B}_1/\mathbf{B}$ je ranga 1 i tipa $\mathbf{a}$ (ako je $(B \neq) c + B \in B_1/B$, onda je, za neke nenula

cele brojeve $k, l$ i neko $b \in B$, $kc = b + la_1$, te je $k(c + B) = l(a_1 + B))$ i opet je prema prethodnoj lemi $\mathbf{B}_1$ direktna suma podgrupe $\mathbf{B}$ i neke podgrupe $\mathbf{C}_1$ ranga 1. Postupak nastavljamo. Neka $a_2 \notin B_1$ i neka je $\mathbf{B}_2$ minimalna potpuna podgrupa grupe $\mathbf{A}$ koja sadrži podgrupu $\mathbf{B}_1 \oplus \langle a_2 \rangle$. $\mathbf{B}_2/\mathbf{B}_1$ je ranga 1 i tipa $\mathbf{a}$ (po uslovu leme je svaki element faktor grupe $\mathbf{A}/\mathbf{B}_1$ tipa $\mathbf{a}$), pa je $\mathbf{B}_2 = \mathbf{B}_1 \oplus \mathbf{C}_2$ za neku podgrupu $\mathbf{C}_2$ ranga 1. Ako je $\mathbf{B}_2 \neq \mathbf{A}$ idemo dalje. U svakom slučaju, s obzirom da je $\mathbf{A}/\mathbf{B}$ konačnog ranga, posle konačno mnogo koraka, recimo $k$, doći ćemo do grupe $\mathbf{A} - \mathbf{A} = \mathbf{B}_k$, i prema navedenom imamo: $\mathbf{A} = \mathbf{B}_k = \mathbf{B}_{k-1} \oplus \mathbf{C}_k = \mathbf{B}_{k-2} \oplus \mathbf{C}_{k-1} \oplus \mathbf{C}_k = \cdots = \mathbf{B} \oplus \mathbf{C}_1 \oplus \cdots \mathbf{C}_k$.□

**Definicija 44.7** *Koset $a + B$ pogrupe $\mathbf{B}$ torziono slobodne grupe $\mathbf{A}$ je regularan akko sadrži element $a_1$ takav da je $H(c) \leq H(a_1)$ za svako $c \in a + B$.*

Kada je $\mathbf{B}$ direktni sumand grupe $\mathbf{A}$ – $\mathbf{A} = \mathbf{B} \oplus \mathbf{C}$, onda je svaki koset podgrupe $\mathbf{B}$ regularan; jer, koseti su oblika $c + B$, gde je $c \in C$, pa je, za $c + b \in c + B$, $H(c + b) = H(c) \wedge H(b) \leq H(c)$.

**Teorema 44.8** *Neka je $\mathbf{B}$ podgrupa torziono slobodne grupe $\mathbf{A}$ takva da je faktor grupa $\mathbf{A}/\mathbf{B}$ potpuno razloživa torziono slobodna grupa. Onda je $\mathbf{A}$ direktna suma podgrupe $\mathbf{B}$ i potpuno razložive podgrupe akko je svaki koset podgrupe $\mathbf{B}$ regularan.*

**Dokaz.** ($\Longrightarrow$) Upravo smo konstatovali da ovaj pravac važi generalno; ne trebaju nam ostali uslovi, dovoljno je što je $\mathbf{B}$ direktni sumand.

($\Longleftarrow$) Neka je $\mathbf{A}/\mathbf{B} = \sum_{\alpha<\lambda} \overline{\mathbf{C}}_\alpha$, gde je $\overline{\mathbf{C}}_\alpha = \mathbf{C}_\alpha/\mathbf{B}$ torziono slobodna grupa ranga 1. Iz svake podgrupe $\overline{\mathbf{C}}_\alpha$ izaberimo jedan nenula element $c_\alpha + B$ koji kao koset podgrupe $\mathbf{B}$, po uslovu teoreme, sadrži element $a_\alpha$ takav da je $H(c) \leq H(a_\alpha)$ za svaki drugi element $c \in c_\alpha + B$. Neka je, dalje, $\mathbf{D}_\alpha$ potpuna podgrupa grupe $\mathbf{A}$ generisana elementom $a_\alpha$ (ponavljamo: $D_\alpha = \{g \in A \mid kg \in \langle a_\alpha \rangle$ za neki nenula ceo broj $k$ koji zavisi od $g\}$); dakle, $r(\mathbf{D}_\alpha) = 1$. Sledi da je $\mathbf{C}_\alpha = \mathbf{B} \oplus \mathbf{D}_\alpha$. Zaista, $\mathbf{B} \cap \mathbf{D}_\alpha = \mathbf{O}$; pretpostavka $0 \neq g \in B \cap D_\alpha$ dala bi, zbog potpunosti podgrupe $\mathbf{B}$ i činjenice da je $\mathbf{D}_\alpha$ ranga 1, $\mathbf{D}_\alpha \leq \mathbf{B}$, posebno $a_\alpha \in B$, kontradikcija (ako $0 \neq h \in D_\alpha$, onda bi, za neke nenula cele brojeve $u$ i $v$ bilo $uh = vg \in B$, pa bismo za neko $b \in B$ imali $uh = ub$, tj. $u(h - b) = 0$, odnosno $h = b \in B$). Ako je pak $0 \neq c \in C_\alpha \setminus B$ (znači, $c + B \neq B$), tada je $k(c + B) = l(a_\alpha + B)$ za neke nenula uzajamno proste cele brojeve $k$ i $l$. Odatle je $kc = la_\alpha + b$ za neko $b \in B$. Neka je, za cele brojeve $m$ i $n$, $mk + nl = 1$. Onda je $k(nc + ma_\alpha) = n(kc) + (km)a_\alpha = (nl)a_\alpha + nb + (km)a_\alpha = a_\alpha + nb \in a_\alpha + B$, pa pošto je $H(a_\alpha + nb) \leq H(a_\alpha)$ i $a_\alpha + nb$ deljivo sa $k$, to je i $a_\alpha$ deljivo sa $k$. Ako je $a_\alpha = ka'_\alpha$, onda je $a'_\alpha \in D_\alpha$ i $b = kc - la_\alpha = k(c - la'_\alpha)$, a odatle je, zbog potpunosti grupe $\mathbf{B}$, $c - la'_\alpha \in B$, tj. $c \in B \oplus D_\alpha$ (ponavljamo:



za neko $b' \in B$ je $k(c - la'_\alpha) = kb'$, odnosno $k(c - la'_\alpha - b') = 0$ i stoga je $c - la'_\alpha = b'$). Konačno, $\mathbf{A}/\mathbf{B} = \sum_{\alpha<\lambda} \overline{\mathbf{C}}_\alpha = \sum_{\alpha<\lambda} (\mathbf{B} \oplus \mathbf{D}_\alpha)/\mathbf{B}$ implicira, prema 10.16, $\mathbf{A} = \mathbf{B} \oplus \sum_{\alpha<\lambda} \mathbf{D}_\alpha$.■

**Korolar 44.9** *Neka je $\mathbf{B}$ potpuna podgrupa torziono slobodne grupe $\mathbf{A}$ takva da su svi elementi skupa $A \setminus B$ istog tipa – $\mathbf{a}$, a faktor grupa $\mathbf{A}/\mathbf{B}$ je direktna suma grupa ranga 1 i istog tipa $\mathbf{a}$. Tada je $\mathbf{B}$ direktni sumand grupe $\mathbf{A}$.*

**Dokaz.** Prema 44.4 (i 43.2($g$)) svaki koset ($B \neq$) $a + B$ sadrži element $a_1$ za koji je $H(a_1) = H(a + B)$. Prema tome, svaki koset je regularan pa imamo ispunjene uslove prethodne teoreme.□

**Teorema 44.10** *Ako je $\mathbf{A} = \sum_{\alpha<\lambda} \mathbf{A}_\alpha$, gde je, za svako $\alpha < \lambda$, $\mathbf{A}_\alpha$ torziono slobodna grupa ranga 1 i (istog) tipa $\mathbf{a}$, onda je i svaka potpuna podgrupa grupe $\mathbf{A}$ takođe direktna suma grupa ranga 1 i tipa $\mathbf{a}$.*

**Dokaz.** Neka je $\mathbf{B}$ potpuna podgrupa grupe $\mathbf{A}$ i neka je, za $\beta < \lambda$, $\mathbf{A}^{(\beta)} = \sum_{\alpha<\beta} \mathbf{A}_\alpha$ i $\mathbf{B}^{(\beta)} = \mathbf{B} \cap \mathbf{A}^{(\beta)}$. Jasno, $\mathbf{B}^{(\beta)} \leq \mathbf{B}^{(\beta+1)}$ i $\mathbf{B}^{(\beta+1)}/\mathbf{B}^{(\beta)}$ je ili nula grupa ili grupa izomorfna podgrupi grupe $\mathbf{A}_\beta$, jer je prema drugoj teoremi o izomorfizmu:

$$\mathbf{B}^{(\beta+1)}/\mathbf{B}^{(\beta)} = \mathbf{B}^{(\beta+1)}/(\mathbf{B}^{(\beta+1)} \cap \mathbf{A}^{(\beta)}) \cong$$

$$(\mathbf{B}^{(\beta+1)} + \mathbf{A}^{(\beta)})/\mathbf{A}^{(\beta)} \leq \mathbf{A}^{(\beta+1)}/\mathbf{A}^{(\beta)} \cong \mathbf{A}_\beta.$$

Dalje je, prema 37.8($c$), $\mathbf{B}^{(\beta+1)} = \mathbf{B} \cap \mathbf{A}^{(\beta+1)}$ potpuna podgrupa grupe $\mathbf{A}$, pa je (svaki) element $a \in B^{(\beta+1)} \setminus B^{(\beta)}$ tipa $\mathbf{a}$ (imamo u vidu 43.2($g$)), dok prema gornjoj relaciji koset $a + B^{(\beta)}$ ne može biti tipa većeg od $\mathbf{a}$ (dakle, baš je tipa $\mathbf{a}$). Prema lemi 44.5 je $\mathbf{B}^{(\beta)}$ direktni sumand grupe $\mathbf{B}^{(\beta+1)}$ – $\mathbf{B}^{(\beta+1)} = \mathbf{B}^{(\beta)} \oplus \mathbf{C}_\beta$, gde je $\mathbf{C}_\beta \cong \mathbf{B}^{(\beta+1)}/\mathbf{B}^{(\beta)}$ ili nula grupa ili grupa ranga 1 i, prema prethodnom, tipa $\mathbf{a}$ ($\mathbf{C}_\beta$ je potpuna podgrupa grupe $\mathbf{A}$ – videti 37.8($a$)). Transfinitnom indukcijom se pokazuje da je $\mathbf{B}^{(\beta)} = \sum_{\alpha<\beta} \mathbf{C}_\alpha$. Slučaj $\beta = 0, 1$ je trivijalan. ($\mathbf{B}^{(0)} = \mathbf{O}$, $\mathbf{B}^{(1)} = \mathbf{B} \cap \mathbf{A}_0 = \mathbf{C}_0$). Za $\beta = \gamma + 1$ imamo: $\mathbf{B}^{(\gamma+1)} = \mathbf{B}^{(\gamma)} \oplus \mathbf{C}_\gamma = \sum_{\alpha<\gamma} \mathbf{C}_\alpha \oplus \mathbf{C}_\gamma$ (prema induktivnoj hipotezi) $= \sum_{\alpha\leq\gamma} \mathbf{C}_\alpha$. Ako je $\beta$ granični ordinal, onda je $\mathbf{B}^{(\beta)} = \bigcup_{\gamma<\beta} \mathbf{B}^{(\gamma)} = \bigcup_{\gamma<\beta} (\sum_{\alpha<\gamma} \mathbf{C}_\alpha)$ (prema induktivnoj hipotezi) $= \sum_{\alpha<\beta} \mathbf{C}_\alpha$. Isto tako je $\mathbf{B} = \sum_{\alpha<\lambda} \mathbf{C}_\alpha = \sum \{\mathbf{C}_\alpha \mid \alpha < \lambda, \mathbf{C}_\alpha \neq \mathbf{O}\}$.■

Prethodna teorema se u slučaju direktnih sumanada može uopštiti.

**Teorema 44.11** *Neka je $\mathbf{A}$ torziono slobodna potpuno razloživa grupa – $\mathbf{A} = \sum_{\alpha<\lambda} \mathbf{A}_\alpha$, gde je, za $\alpha < \lambda$, $\mathbf{A}_\alpha$ grupa ranga 1 i tipa $\mathbf{a}_\alpha$, i neka je skup tipova sumanada konačan. Tada je svaki direktni sumand grupe $\mathbf{A}$ takođe potpuno razloživa grupa.*

**Dokaz.** Neka je $\{\mathbf{a}_\alpha \mid \alpha < \lambda\} = \{\mathbf{d}_1, \ldots, \mathbf{d}_n\}$ i neka je $\mathbf{D}_i$, $i = 1, \ldots, n$, direktna suma sumanada tipa $\mathbf{d}_i$; dakle, $\mathbf{A} = \mathbf{D}_1 \oplus \cdots \oplus \mathbf{D}_n$. S druge strane, neka je $\mathbf{A} = \sum_{\beta<\mu} \mathbf{B}_\beta$. Pokazaćemo, a time i dokazati teoremu, da data razlaganja grupe $\mathbf{A}$ imaju izomorfna proširenja (jer je onda, za svako $\beta < \mu$, $\mathbf{B}_\beta$ direktna suma podgrupa izomorfnih podgrupama nekih grupa $\mathbf{D}_i$, koje su pak prema prethodnoj teoremi potpuno razložive). Dokaz je indukcijom po $n$. Slučaj $n = 1$ je prethodna teorema. Pretpostavimo da tvrđenje važi za svako $k < n$ i neka je $\mathbf{d}_1$ jedan (možda i jedini) maksimalan tip među $\{\mathbf{d}_1, \ldots, \mathbf{d}_n\}$. Tada za projekciju $\pi_\beta$ grupe $\mathbf{A}$ na $\mathbf{B}_\beta$ važi: $(\mathbf{D}_1)\pi_\beta = \mathbf{D}_1 \cap \mathbf{B}_\beta = \mathbf{C}_\beta$. Inkluzija $\geq$ važi uvek, a inkluzija $\leq$ je posledica maksimalnosti tipa $\mathbf{d}_1$ (zbog koje je podgrupa $\mathbf{D}_1$ potpuno invarijantna). Proizilazi: $\mathbf{D}_1 = \sum_{\beta<\mu}(\mathbf{D}_1 \cap \mathbf{B}_\beta) = \sum_{\beta<\mu} \mathbf{C}_\beta$. Prema tome je

$$\mathbf{A} = \sum\nolimits_{\beta<\mu} \mathbf{C}_\beta \oplus \mathbf{D}_2 \oplus \cdots \oplus \mathbf{D}_n \qquad (1).$$

Kako je $\mathbf{C}_\beta = \mathbf{D}_1 \cap \mathbf{B}_\beta$ ($\leq \mathbf{B}_\beta$) direktni sumand grupe, to je (za neku podgrupu $\mathbf{C}'_\beta$ grupe $\mathbf{B}_\beta$) $\mathbf{B}_\beta = \mathbf{C}_\beta \oplus \mathbf{C}'_\beta$. Odatle je

$$\mathbf{A} = \sum\nolimits_{\beta<\mu} \mathbf{C}_\beta \oplus \sum\nolimits_{\beta<\mu} \mathbf{C}'_\beta \qquad (2).$$

Prema (1) i (2) su podgrupe $\mathbf{D}_2 \oplus \cdots \oplus \mathbf{D}_n$ i $\sum_{\beta<\mu} \mathbf{C}'_\beta$ izomorfne, pa po induktivnoj hipotezi postoje izomorfna proširenja datih dekompozicija.■

**Korolar 44.12** *Svaki direktni sumand kompletno razložive torziono slobodne grupe konačnog ranga i sam je kompletno razloživ.*

**Napomena.** Jedan od brojnih rezultata Baera uopštava prethodnu teoremu; uslov o konačnosti tipova može se u njoj zameniti slabijim uslovom: skup tipova sumanada (ranga 1) ispunjava uslov maksimalnosti. Kulikov je opet pokazao, uostalom njegova je i prethodna teorema, da je svaki direktni sumand prebrojive potpuno razložive torziono slobodne grupe takođe kompletno razloživa grupa.

Navedimo i sledeći rezultat koji nije neposredno vezan za kompletnu razloživost ali je u okviru priče o njoj.

**Teorema 44.13** *Svaka potpuna podgrupa torziono slobodne grupe* $\mathbf{A}$ *je direktni sumand akko je* $\mathbf{A}$ *direktna suma neke deljive grupe* $\mathbf{D}$ *i direktne sume konačnog broja izomorfnih grupa ranga* 1.

**Dokaz.** Neka je $\mathbf{A} = \mathbf{D} \oplus \mathbf{C}$, gde je $\mathbf{D}$ maksimalna deljiva podgrupa grupe $\mathbf{A}$, $\mathbf{C} = \sum_{i\in I} \mathbf{C}_i$ i, za $i, j \in I$, $\mathbf{C}_i$ i $\mathbf{C}_j$ su izomorfne grupe ranga 1. Grupa $\mathbf{A}$ ima svojstvo da joj je svaka potpuna podgrupa direktni sumand akko isto to svojstvo ima i podgrupa $\mathbf{C}$. Jer, neka je $\mathbf{C}$ sa tim svojstvom i neka je $\mathbf{B}$



potpuna podgrupa grupe $\mathbf{A}$. Onda je $\mathbf{B} \cap \mathbf{D}$ deljiva podgrupa grupe $\mathbf{B}$ (zbog potpunosti grupe $\mathbf{B}$), pa je $\mathbf{B} = (\mathbf{B} \cap \mathbf{D}) \oplus \mathbf{B}_1$, gde možemo pretpostaviti da je $\mathbf{B}_1$ podgrupa grupe $\mathbf{C}$ (u suprotnom, $\mathbf{B}_1$ je podgrupa nekog komplementa grupe $\mathbf{D}$ koji je, evidentno, izomorfan sa $\mathbf{C}$). $\mathbf{B} \cap \mathbf{D}$ je direktni sumand (deljive) podgrupe $\mathbf{D}$, a $\mathbf{B}_1$ je potpuna podgrupa podgrupe $\mathbf{C}$ i po pretpostavci njen direktni sumand; znači, i $\mathbf{B}$ je direktni sumand grupe $\mathbf{A}$. Zbog navedenog, u nastavku razmatramo samo reducirane torziono slobodne grupe.

($\Longrightarrow$) Neka je $\mathbf{C}$ reducirana torziono slobodna grupa sa svojstvom da joj je svaka potpuna podgrupa direktni sumand. Pretpostavimo da je $\{c_1, \ldots, c_n, \ldots\}$ jedan njen beskonačan linearno nezavisan sistem i neka je $\mathbf{G}$ potpuna podgrupa grupe $\mathbf{C}$ generisana skupom $X = \{c_1 - 2c_2, c_2 - 3c_3, \ldots, c_n - (n+1)c_{n+1}, \ldots\}$ (37.9). $\mathbf{G}$ je prava podgrupa jer npr. $c_1 \notin G$; pretpostavka da je $kc_1 \in \langle X \rangle$ za neki nenula ceo broj $k$ vodi u kontradikciju: iz $kc_1 = k_1(c_1 - 2c_2) + k_2(c_2 - 3c_3) + \cdots + k_n(c_n - (n+1)c_{n+1})$ sledi $k_1 = k$, $k_2 = 2!k, \ldots, k_n = n!k$ i $(n+1)!kc_{n+1} = 0$. S druge strane, podgrupa generisana skupom $\{c_n + G \mid n \in N\}$ faktor grupe $\mathbf{C}/\mathbf{G}$ je deljiva; u stvari, radi se o kopiji aditivne grupe racionalnih brojeva: $c_1 + G = 2(c_2 + G)$, $c_2 + G = 3(c_3 + G)$, ..., $c_n + G = (n+1)(c_{n+1} + G)$, ... (21.10($p$)). Kako je $\mathbf{C}$ reducirana grupa, proizilazi da $\mathbf{G}$ ne može biti direktni sumand grupe $\mathbf{C}$, protivno našoj pretpostavci, dakle, $\mathbf{C}$ je konačnog ranga. Ako je $\mathbf{C}_1$ potpuna podgrupa grupe $\mathbf{C}$ generisana jednim od elemenata maksimalnog linearno nezavisnog sistema, znači ranga 1, onda je, po uslovu, $\mathbf{C} = \mathbf{C}_1 \oplus \mathbf{C}'$. Ako je $\mathbf{C}_1$ prava podgrupa, razlažemo dalje $\mathbf{C}'$ i tako ćemo, ponavljajući postupak, dobiti razlaganje grupe $\mathbf{C}$ u direktnu sumu grupa ranga 1: $\mathbf{C} = \mathbf{C}_1 \oplus \cdots \oplus \mathbf{C}_n$ (grupa $\mathbf{C}'$ zadržava svojstvo da joj je svaka potpuna podgrupa direktni sumand, jer su njene potpune podgrupe ujedno i potpune podgrupe grupe $\mathbf{C}$ – videti i 10.17).

Pođimo sada od toga da je $n > 1$ i da su, recimo, grupe $\mathbf{C}_1$ i $\mathbf{C}_2$ tipova, respektivno, $\mathbf{c}_1$ i $\mathbf{c}_2$, neizomorfne (drugim rečima, $\mathbf{c}_1 \neq \mathbf{c}_2$). Podgrupa $\mathbf{C}_1 \oplus \mathbf{C}_2$ sadrži elemente dva ili tri različita tipa već u zavisnosti od toga da li su tipovi $\mathbf{c}_1$ i $\mathbf{c}_2$ uporedivi. Neka su $c'_1$ i $c'_2$ nenula elementi grupa, respektivno, $\mathbf{C}_1$ i $\mathbf{C}_2$. Uzmimo prvo da je npr. $\mathbf{c}_1 \prec \mathbf{c}_2$. Za neki prirodan broj $n$ ($> 1$) jednačina $c'_2 = nx$ nema rešenje ($H(c'_2) \neq (\infty, \ldots, \infty, \ldots)$ jer nemamo deljivih podgrupa). Ako je $\mathbf{H}_1$ potpuna podgrupa grupe $\mathbf{C}_1 \oplus \mathbf{C}_2$ generisana elementom $nc'_1 + c'_2$, onda je za neku podgrupu $\mathbf{H}_2$ tipa $\mathbf{c}_2$: $\mathbf{C}_1 \oplus \mathbf{C}_2 = \mathbf{H}_1 \oplus \mathbf{H}_2$ ($\mathbf{H}_1$ je, naravno, tipa $\mathbf{c}_1$ – 43.2($g$)). Odatle je $\mathbf{H}_2 = \mathbf{C}_2$; $\mathbf{H}_2$ je očigledno podgrupa grupe $\mathbf{C}_2$, čiji domen sadrži pored nule sve elemente grupe $\mathbf{C}_1 \oplus \mathbf{C}_2$ tipa $\mathbf{c}_2$, dakle i direktni sumand te grupe, pa važi jednakost tih grupa. No, ispada da element $c'_1$ nije u $\mathbf{H}_1 \oplus \mathbf{C}_2$ ($= \mathbf{C}_1 \oplus \mathbf{C}_2$), kontradikcija. Jer, neka je $c'_1 = h + c''_2$ za neko $h \in H_1$ i neko $c''_2 \in C_2$. Onda je, za neke nenula cele brojeve $k, l, q, t$, $kh = l(nc'_1 + c'_2)$, $qc''_2 = tc'_2$ i $(k, l) = (q, t) = 1$, te je $(kq)c'_1 = lq(nc'_1 + c'_2) + ktc'_2$. Odatle sledi $(kq - lqn)c'_1 = (lq + kt)c'_2 = 0$ i dalje, redom: $k = ln$, $(q + nt)c'_2 = 0$. Ako je $|q| = |t| = 1$ ili samo $|t| = 1$, proizilazi da je $c'_2$ deljivo sa $n$, a

ako je $|t| > 1$, dobijamo da je $q$ deljivo sa $t$, suprotno uslovu $(q,t) = 1$. Ako tipovi $\mathbf{c}_1$ i $\mathbf{c}_2$ nisu uporedivi, neka je $\mathbf{G}_1$ potpuna podgrupa generisana elementom $c_1' + c_2'$. Ali sada $\mathbf{G}_1$ ne može biti direktni sumand s obzirom da je $[H(c_1') \wedge H(c_2')] = [H(c_1')] \wedge [H(c_2')] = \mathbf{c}_1 \wedge \mathbf{c}_2$; ako bi bilo na primer $\mathbf{C}_1 \oplus \mathbf{C}_2 = \mathbf{G}_1 \oplus \mathbf{G}_2$ i $\mathbf{G}_2$ tipa $\mathbf{c}_1$, onda grupa $\mathbf{C}_1 \oplus \mathbf{C}_2$ ne bi imala element tipa $\mathbf{c}_2$.

($\Longleftarrow$) Neka je $\mathbf{C}$ torziono slobodna reducirana grupa i $\mathbf{C} = \mathbf{C}_1 \oplus \cdots \oplus \mathbf{C}_r$, gde su, za $i,j = 1,\ldots,r$, $\mathbf{C}_i$ i $\mathbf{C}_j$ izomorfne grupe ranga 1. Pretpostavićemo da su te grupe baš podgrupe grupe $\mathbf{Ra}$; onda je svaka grupa $\mathbf{C}_i$ oblika $\mathbf{R}c_i$, gde je $\mathbf{R}$ prava podgrupa grupe $\mathbf{Ra}$, a $c_i$, $i = 1,\ldots,r$, su pogodno izabrani elementi (videti dokaz teoreme 43.4). Neka je dalje $\mathbf{F}$ potpuna podgrupa grupe $\mathbf{C}$ i $f \in F$ element s najvišim "indeksom" $(k)$ takav da je, za neke cele brojeve $n_1,\ldots,n_k$, $f_1 = n_1c_1 + \cdots + n_kc_k$ i $(n_1,\ldots,n_k) = 1$. Egzistencija ovakvog elementa proizilazi iz potpunosti podgrupe $\mathbf{C}$: ako je $f' = \frac{r_1}{s_1}c_1 + \cdots + \frac{r_k}{s_k}c_k$, onda je $NZS(s_1,\ldots,s_k)f' = r_1r_1'c_1 + \cdots + r_kr_k'c_k$ (gde je $r_i' = \frac{NZS(s_1,\ldots,s_k)}{s_i}$). Ako je $(r_1r_1',\ldots,r_kr_k') = m$ i $r_ir_i' = mn_i$, tada je $NZS(s_1,\ldots,s_k)f' = m(n_1c_1 + \cdots + n_kc_k)$, pa je, za neko $f \in F$, $NZS(s_1,\ldots,s_k)f' = mf_1$ i odatle $f_1 = n_1c_1 + \cdots + n_kc_k$. Prema analogonu leme 32.3 (dokaz je isti) grupa $\mathbf{R}c_1 \oplus \cdots \oplus \mathbf{R}c_k$ se može predstaviti u obliku $\mathbf{R}f_1 \oplus \mathbf{R}c_2' \oplus \cdots \oplus \mathbf{R}c_k'$ za neke elemente $c_2',\ldots,c_k'$. Opet je zbog potpunosti podgrupe $\mathbf{F}$ $\mathbf{R}f_1 \leq \mathbf{F}$ i $\mathbf{R}f_1$ je direktni sumand grupe $\mathbf{F}$. Ako je $\mathbf{F} = \mathbf{R}f_1 \oplus \mathbf{F}_1$, postupak nastavljamo polazeći od potpune podgrupe $\mathbf{F}_1$ grupe $\mathbf{R}c_1' \oplus \cdots \oplus \mathbf{R}c_k'$. U konačno mnogo koraka stići ćemo do dekompozicije grupe $\mathbf{C}$: $\mathbf{C} = \mathbf{R}f_1 \oplus \mathbf{R}f_2 \oplus \cdots \oplus \mathbf{R}f_s \oplus \cdots \oplus \mathbf{R}g_{r-s}$, $s \leq r$, gde je $\mathbf{F} = \mathbf{R}f_1 \oplus \cdots \oplus \mathbf{R}f_s$.■

**Primer 44.14** *(a) Kartezijanska suma beskonačne familije beskonačnih cikličnih grupa nije potpuno razloživa, prema tome nije ni slobodna A va grupa.*

**Dokaz.** Neka je $\mathbf{A} = \sum_{\alpha<\lambda}^{c} \mathbf{Z}_\alpha$, gde je $\lambda \geq \aleph_0$ i $\mathbf{Z}_\alpha$, $\alpha < \lambda$, kopija aditivne grupe celih brojeva (sa domenom $Z_\alpha = \{k_\alpha \mid k \in Z\}$). Nenula elementi grupe $\mathbf{A}$ su tipa $[(0,\ldots,0,\ldots)]$ (element $\langle k_\alpha\rangle_{\alpha<\lambda}$ je deljiv sa $p$ akko $p|k_\alpha$ za svako $\alpha < \lambda$). Stoga bi pretpostavka da je $\mathbf{A}$ kompletno razloživa grupa značila da je $\mathbf{A}$ slobodna Abelova grupa, pa bi i njena podgrupa $\mathbf{B} = \sum_{\alpha<\aleph_0}^{c} \mathbf{Z}_\alpha$ bila slobodna Abelova grupa. Pokazaćemo da nije tako. Znači, u daljem razmatranju polazimo od kartazijanske sume beskonačno prebrojivo mnogo beskonačnih cikličnih grupa. Neka to ostane (u oznaci) $\mathbf{B}$ sa elementima $\langle k_n\rangle_{n\in\omega}$ i neka je $\mathbf{C}$ njena podgrupa čiji je domen skup elemenata $\langle l_n\rangle_{n\in\omega}$ sa svojstvom da su za svaki prirodan broj $r$ skoro sve komponente $l_n$ (sve sem eventualno konačno mnogo) deljive sa $2^r$. Grupe $\mathbf{B}$ i $\mathbf{C}$ su reda kontinuum. Što se tiče grupe $\mathbf{B}$ to je (više nego) očigledno, a kada je u pitanju grupa $\mathbf{C}$, možemo ovako rezonovati: postoji kontinuum mnogo beskonačnih podskupova skupa $\omega$ i za svaki takav podskup $X$ $(\subseteq \omega - |X| = \aleph_0)$ neka je $c_X = \langle l_n^X\rangle_{n\in\omega}$,



gde je $l_n^X = \begin{cases} 0 & n \in X \\ 2^n & n \notin X \end{cases}$; tako smo već dobili kontinuum mnogo elemenata iz $C$ (a više ih i nema). Ako je $\mathbf{B}$ slobodna Abelova grupa, onda je to i grupa $\mathbf{C}$, a faktor grupa $\mathbf{C}/2\mathbf{C}$ je takođe reda kontinuum, jer $\mathbf{C}$ je direktna suma kontinuum mnogo beskonačnih cikličnih grupa, skup kardinalnosti kontinuum sadrži kontinuum mnogo konačnih, možemo pretpostaviti i disjunktnih, podskupova, te je lako naći kontinuum mnogo elemenata grupe $\mathbf{C}$ koji određuju različite kosete podgrupe $2\mathbf{C}$. Ali, s druge strane, proizilazi da je $\mathbf{C}/2\mathbf{C}$ prebrojiva grupa. Zaista, neka je $\mathbf{G}$ prebrojiva podgrupa grupe $\mathbf{C}$ sa domenom $\{\langle k_n\rangle_{n\in\omega} \mid$ samo konačno mnogo komponenti $k_n$ je različito od nule$\}$. Tada za svaki element $c \in C$ postoji element $g_c \in G$ takav da je $c - g_c \in 2C$; ako je $c = \langle k_n\rangle_{n\in\omega}$ i $Y = \{n \in \omega \mid k_n$ nije deljivo sa $2\}$ ($Y$ je konačan skup), možemo za $g_c$ uzeti element $\langle l_n\rangle_{n\in\omega}$, gde je $l_n = \begin{cases} k_n & n \in Y \\ 0 & n \notin Y \end{cases}$. Prema tome, $c + 2C = g_c + 2C$ i $|C/2C| = \aleph_0$.

Za razliku od prethodne tačke gde je grupa bila razloživa ali ne i potpuno razloživa, u narednoj imamo generalnu nerazloživost.

*(b) Nijedna potpuna podgrupa p-adične grupe celih brojeva (30.7(c)) nije razloživa (dekompozibilna).*

**Dokaz.** Neka je $\mathbf{P}$ $p$-adična grupa celih brojeva. Tada je domen podgrupe $p\mathbf{P}$ skup $\{\langle k_n\rangle_{n\in N} \in P \mid k_1 = 0\}$, a faktor grupa $\mathbf{P}/p\mathbf{P}$ je reda $p$; za $\langle k_n\rangle_{n\in N}$, $\langle l_n\rangle_{n\in N} \in P$, iz $k_1 = l_1$ sledi $p|(k_n - l_n)$, tj. $\langle k_n\rangle_{n\in N} - \langle l_n\rangle_{n\in N} \in pP$ (dokaz je indukcijom po $n$: za $n = 1$ to je dato, a ako $p|(k_n - l_n)$, onda iz $k_{n+1} \equiv k_n \,(mod\, p^n)$, $l_{n+1} \equiv l_n \,(mod\, p^n)$ sledi $p^n|(k_{n+1} - l_{n+1} - (k_n - l_n))$ pa $p|(k_{n+1} - l_{n+1})$). Kao podgrupa prostog indeksa $p\mathbf{P}$ je maksimalna podgrupa grupe $\mathbf{P}$. Neka je $\mathbf{H}$ nenula potpuna podgrupa grupe $\mathbf{P}$. Onda je $p\mathbf{H} = \mathbf{H} \cap p\mathbf{P}$. Dalje, $\mathbf{H}$ sadrži element koji nije u $\mathbf{P}$. Stvarno, ako je $h = \langle 0, h_2,\ldots,h_n,\ldots\rangle \in H \cap pP$ i, recimo, $h_2 \neq 0$, onda je zbog potpunosti podgrupe $\mathbf{H}$, za neko $h' = \langle h_1', h_2',\ldots,h_n',\ldots\rangle \in H$, $h = ph'$. No, $h_1' \neq 0$, u suprotnom je $h_2'$ neki broj $sp$, $1 \leq s \leq p-1$, i $h_2 = \underbrace{h_2' +_{p^2} \cdots +_{p^2} h_2'}_{p-puta} = p \cdot_{p^2} h_2' = 0$, kontradikcija. Analogno bismo rezonovali u slučaju da je $h_2 = \cdots = h_n = 0$, $h_{n+1} \neq 0$. Zbog maksimalnosti podgrupe $p\mathbf{P}$ važi $\mathbf{P} = \mathbf{H} + p\mathbf{P}$, te je prema drugoj teoremi o izomorfizmu:

$$\mathbf{P}/p\mathbf{P} = (\mathbf{H} + p\mathbf{P})/p\mathbf{P} \cong \mathbf{H}/(\mathbf{H} \cap p\mathbf{H}) = \mathbf{H}/p\mathbf{H},$$

i $\mathbf{H}/p\mathbf{H}$ je ciklična grupa reda $p$. Ako bi $\mathbf{H}$ bila dekompozibilna - $\mathbf{H} = \mathbf{H}_1 \oplus \mathbf{H}_2$, $\mathbf{H}_1, \mathbf{H}_2 \neq \mathbf{O}$, onda bi podgrupe $\mathbf{H}_i$, $i = 1,2$, bile potpune podgrupe grupe $\mathbf{H}$, stoga i grupe $\mathbf{P}$ i, kao i maločas, $\mathbf{H}_i/p\mathbf{H}_i$ bi bila ciklična grupa reda $p$. Ali, $p\mathbf{H} = p\mathbf{H}_1 \oplus p\mathbf{H}_2$ (opet imamo u vidu potpunost podgrupa) i $\mathbf{H}/p\mathbf{H} = (\mathbf{H}_1 \oplus \mathbf{H}_2)/(p\mathbf{H}_1 \oplus p\mathbf{H}_2) \cong \mathbf{H}_1/p\mathbf{H}_1 \oplus \mathbf{H}_2/p\mathbf{H}_2$, kontradikcija.□

**Napomena.** Poslednji primer ukazuje na egzistenciju nerazloživih torziono slobodnih grupa konačnog ili beskonačnog ranga kardinalnosti manje od ili jednake kontinuum. L. Fuks je međutim generalno dokazao: *za svaki beskonačan kardinal $\lambda$ postoji $2^\lambda$ neizomorfnih nerazloživih torziono slobodnih Abelovih grupa reda $\lambda$.*

Jedno uopštenje pojma potpune razloživosti je separabilnost.

**Definicija 44.15** *Torziono slobodna grupa je separabilna akko je svaki konačan podskup njenog domena sadržan u kompletno razloživom direktnom sumandu.*

Očigledno, svaka kompletno razloživa (dekompozibilna) grupa je separabilna. U slučaju prebrojivosti važi i obrat.

**Lema 44.16** *Svaka prebrojiva separabilna grupa je potpuno razloživa.*

**Dokaz.** Neka je $\mathbf{A}$ prebrojiva separabilna grupa sa domenom $\{a_n \mid n \in N\}$ i neka je $\mathbf{A}_0 = \mathbf{O}$. Za elemente $a_1, \ldots, a_n$ neka je $\mathbf{A}_n$ kompletno razloživi direktni sumand konačnog ranga koji ih sadrži (pretpostavka o konačnosti ranga nije, naravno, nikakvo ograničenje; ako neki direktni kompletno razloživi sumand grupe $\mathbf{A}$ sadrži elemente $a_1, \ldots, a_n$, onda se u okviru njega može naći i kompletno razloživi direktni sumand konačnog ranga koji sadrži te elemente). $\mathbf{A}_{n+1}$ je onda kompletno razloživi direktni sumand konačnog ranga grupe $\mathbf{A}$ koji sadrži $a_{n+1}$ i maksimalan linearno nezavisan sistem podgrupe $\mathbf{A}_n$; neka je to $\{b_1, \ldots, b_k\}$ ($b_j = a_{i_j}$ za neko $i_j \in N$). $\mathbf{A}_n$ je podgrupa grupe $\mathbf{A}_{n+1}$ jer je ova potpuna. Zaista, neka je $a$ nenula element podgrupe $\mathbf{A}_n$ i neka je, za nenula ceo broj $m$, $ma = m_1b_1 + \cdots + m_kb_k \in A_{n+1}$. Tada je, za neki element $a' \in A_{n+1}$, $ma' = m_1b_1 + \cdots + m_kb_k$, pa je $m(a - a') = 0$, tj. $a = a'$. Ako je $\mathbf{A} = \mathbf{A}_n \oplus \mathbf{B}_n = \mathbf{A}_{n+1} \oplus \mathbf{B}_{n+1}$, onda je $\mathbf{A}_{n+1} = \mathbf{A}_n \oplus (\mathbf{A}_{n+1} \cap \mathbf{B}_n) = \mathbf{A}_n \oplus \mathbf{C}_{n+1}$ (stavili smo: $\mathbf{C}_{n+1} = \mathbf{A}_{n+1} \cap \mathbf{B}_n$). $\mathbf{C}_{n+1}$ je prema 44.12 takođe potpuno razloživa grupa. Iz $\mathbf{A} = \bigcup_{n \in N} \mathbf{A}_n$ sledi $\mathbf{A} = \sum_{n \in N} \mathbf{C}_n$ i $\mathbf{A}$ je kompletno razloživa grupa (imamo u vidu: $\mathbf{A}_{n+1} = \mathbf{A}_n \oplus \mathbf{C}_{n+1} = (\mathbf{A}_{n-1} \oplus \mathbf{C}_n) \oplus \mathbf{C}_{n+1} = \cdots = (\mathbf{A}_0 \oplus \mathbf{C}_1) \oplus \cdots \oplus \mathbf{C}_n \oplus \mathbf{C}_{n+1} = \mathbf{C}_1 \oplus \cdots \oplus \mathbf{C}_n \oplus \mathbf{C}_{n+1}$).□

Sledeći već poznati primer pokazuje da je svojstvo separabilnosti pravo uopštenje svojstva potpune razloživosti.

**Primer 44.17** *Kartezijanska suma beskonačne familije beskonačnih cikličnih grupa je separabilna. Svaki konačan skup je sadržan u nekom konačno generisanom sumandu čiji je (direktni) komplement opet kartezijanska suma beskonačnog skupa beskonačnih cikličnih grupa. Osim toga, svaka prebrojiva podgrupa je slobodna Abelova grupa.*

**Dokaz.** Neka je $\mathbf{A} = \sum^c_{\alpha<\lambda} \mathbf{Z}_\alpha$, gde je kao i ranije, za $\alpha < \lambda$, $\mathbf{Z}_\alpha$ kopija aditivne grupe celih brojeva. Za $0 \neq a = \langle k_\alpha \rangle_{\alpha<\lambda}$ neka je $k(a) = min\{|k_\alpha| \mid$



$k_\alpha \neq 0, \alpha < \lambda\}$ (uzimamo da je domen podgrupe $\mathbf{Z}_\alpha$ baš $Z$, s tim što indeks $\alpha$ označava odakle je data komponenta). Indukcijom po $k(a)$ pokazujemo da je nenula element $a$ iz $A$ sadržan u konačno generisanom direktnom sumandu grupe $\mathbf{A}$, dok je drugi sumand kartezijanska suma beskonačne familije beskonačnih cikličnih grupa. Ako je $k(a) = 1$, onda je $k_\beta \in \{1, -1\}$ za neko $\beta < \lambda$ i $\mathbf{A} = \langle a \rangle \oplus \mathbf{A}_\beta$, gde je $\mathbf{A}_\beta$ podgrupa grupe $\mathbf{A}$ čiji su elementi sa $\beta$-komponentom nula ($\mathbf{A}_\beta \cong \sum^c_{\delta \neq \beta} \mathbf{A}_\delta$). Ako je $k(a) > 1$, delimo svako $k_\alpha$ sa $k(a)$; neka je $k_\alpha = q_\alpha k(a) + r_\alpha$, $0 \leq r_\alpha < k(a)$. Sada je $a = k(a) \cdot a_1 + a_2$, gde je $a_1 = \langle q_\alpha \rangle_{\alpha<\lambda}$, $a_2 = \langle r_\alpha \rangle_{\alpha<\lambda}$. Naravno, $k(a_1) = 1$ (za neko $\gamma < \lambda$ je $|k_\gamma| = k(a)$, pa je $q_\gamma \in \{1, -1\}$, $r_\gamma = 0$). Kao što smo već konstatovali, tada je $\mathbf{A} = \langle a_1 \rangle \oplus \mathbf{A}_\gamma$. Tako je $a_2 \in A_\gamma$ i, jasno, za $a_2 \neq 0$ je $k(a_2) < k(a)$. Prema induktivnoj hipotezi je $a_2$ sadržan u konačno generisanom direktnom sumandu grupe $\mathbf{A}_\gamma$, recimo $\mathbf{B}_\gamma$: $\mathbf{A}_\gamma = \mathbf{B}_\gamma \oplus \mathbf{C}_\gamma$, $a_2 \in B_\gamma$ i $\mathbf{C}_\gamma$ je kartezijanska suma beskonačne familije beskonačnih cikličnih grupa. Onda je $a$ sadržan u konačno generisanom direktnom sumandu $\langle a_1 \rangle \oplus \mathbf{B}_\gamma$.

Dalje, indukcijom po broju elemenata pokazujemo da je svaki konačan podskup domena $A$ sadržan u konačno generisanom direktnom sumandu, dok drugi sumand ostaje kartezijanska suma beskonačne familije beskonačnih cikličnih grupa. Slučaj $n = 1$ je upravo dokazan. Pretpostavimo da je trvđenje tačno za svako $k < n$ ($> 1$) i posmatrajmo skup od $n$ elemenata – $\{a_1, \ldots, a_n\}$. Prema induktivnoj hipotezi elementi $a_1, \ldots, a_{n-1}$ su sadržani u nekom konačno generisanom direktnom sumandu, neka to bude $\mathbf{B}$: $\mathbf{A} = \mathbf{B} \oplus \mathbf{C}$, a $\mathbf{C}$ je, ponavljamo, kartezijanska suma beskonačne familije beskonačnih cikličnih grupa. Ako je $a_{n+1} = b + c$, $b \in B$, $c \in C$, prema prethodnom, $c$ je sadržan u konačno generisanom direktnom sumandu – $\mathbf{C}_1$ – grupe $\mathbf{C}$. Zaključujemo: $\langle a_1, \ldots, a_n \rangle \leq \mathbf{B} \oplus \mathbf{C}_1$.

Pretpostavimo u nastavku da prebrojiva podgrupa $\mathbf{D}$ grupe $\mathbf{A}$ nije slobodna. Prema 32.12 postoji podgrupa konačnog ranga $\mathbf{G}$ grupe $\mathbf{D}$ koja nije slobodna. Neka je $Y$ maksimalan linearno nezavisan sistem grupe $\mathbf{G}$. Prema upravo konstatovanom $Y$ se sadrži u nekom konačno generisanom direktnom sumandu $\mathbf{H}$ grupe $\mathbf{A}$ (čiji je komplement kartezijanska suma beskonačne familije beskonačnih cikličnih grupa). No, ako je $a \in G$, onda je $ma \in \langle Y \rangle \subseteq H$ za neki pozitivan prirodan broj $m$. Kako je $\mathbf{A}/\mathbf{H}$ torziono slobodna grupa, to je $a \in H$, pa je $\mathbf{G}$ podgrupa grupe $\mathbf{H}$. Ali $\mathbf{H}$ je slobodna Abelova grupa, znači i $\mathbf{G}$ je slobodna Abelova grupa, kontradikcija.□

## 45 Mešovite grupe

Mešovite Abelove grupe su najopštija klasa Abelovih grupa, samim tim o njima se najmanje zna. Poseban je (i lepši) slučaj kada je mešovita grupa direktna suma svog periodičnog dela i torziono slobodne grupe. U ovom paragrafu biće reči o takvim grupama.

**Definicija 45.1** *Mešovita grupa se deli (eng. split) akko je direktna suma svog periodičnog dela i neke torziono slobodne podgrupe. Grupe koje se dele zvaćemo i rastavljajućim grupama.*

Sledeći problemi se prirodno nameću:

(1) okarakterisati periodične grupe – $\mathbf{T}$ – za koje važi: ako je $\mathbf{T}$ periodični deo mešovite grupe $\mathbf{A}$, onda se $\mathbf{A}$ deli;

(2) okarakterisati torziono slobodne grupe – $\mathbf{G}$ – za koje važi: ako je, za mešovitu grupu $\mathbf{A}$, $\mathbf{A}/t(\mathbf{A}) \cong \mathbf{G}$, onda se $\mathbf{A}$ deli;

(3) okarakterisati periodične grupe – $\mathbf{T}$ – i torziono slobodne grupe – $\mathbf{G}$ – za koje važi: mešovita grupa $\mathbf{A}$ se deli akko je $t(\mathbf{A}) \cong \mathbf{T}$ i $\mathbf{A}/t(\mathbf{A}) \cong \mathbf{G}$.

Kompletno je rešen samo prvi od njih. Odgovor dajemo u prvoj narednoj teoremi. No pre toga jedna konstatacija u cilju distanciranja pojmova razloživosti i rastavljivosti.

**Lema 45.2** *Svaka mešovita Abelova grupa je razloživa.*

**Dokaz.** Ako je periodični deo mešovite Abelove grupe $\mathbf{A}$ deljiva grupa, onda je i njen direktni sumand (33.7). Ako $t(\mathbf{A})$ nije deljiva grupa, onda prema 37.24 sadrži konačan ciklični direktni sumand. Ovaj je, kao potpuna podgrupa grupe $t(\mathbf{A})$, potpuna podgrupa i cele grupe $\mathbf{A}$, stoga i njen direktni sumand (37.18).□

**Lema 45.3** *Neka su $\mathbf{B}$ i $\mathbf{C}$ podgrupe mešovite grupe $\mathbf{A}$ takve da je $\mathbf{A} \geq \mathbf{B} \geq t(\mathbf{A}) \geq \mathbf{C}$. Ako se faktor grupa $\mathbf{B}/\mathbf{C}$ ne deli, ne deli se ni grupa $\mathbf{A}$.*

**Dokaz.** Pretpostavimo da je $\mathbf{A} = t(\mathbf{A}) \oplus \mathbf{G}$. No, onda je $\mathbf{B} = t(\mathbf{A}) \oplus (\mathbf{B} \cap \mathbf{G})$, pa je prema 10.3 i 10.17 $\mathbf{B}/\mathbf{C} = (t(\mathbf{A}) \oplus (\mathbf{B} \cap \mathbf{G}))/\mathbf{C} \cong t(\mathbf{A})/\mathbf{C} \oplus (\mathbf{B} \cap \mathbf{G})$; znači, i $\mathbf{B}/\mathbf{C}$ se deli.□

Iskoristićemo prethodnu lemu za još jedan dokaz leme 30.4.

**Primer 45.4** *(a) Neka je $\mathbf{A} = \sum^{c}_{p \in Q} \mathbf{Z}_p$, gde je $Q$ beskonačan podskup skupa prostih brojeva $P$. Grupa $\mathbf{A}$ se ne deli.*

**Dokaz.** Neka je $Q = \{q_k \mid k \in \omega\}$ ($q_0$ je prvi, po prirodnom redosledu, prost broj koji se javlja u $Q$ i tako dalje). Elementi grupe $\mathbf{A}$ biće za nas nizovi $\langle k_n \rangle_{n \in \omega}$, gde je $k_n \in Z_{q_n}$. Već je pokazano u 30.4 da je $t(\mathbf{A}) = \sum_{p \in Q} \mathbf{Z}_p$. Neka je $\mathbf{1} = \langle 1_n \rangle_{n \in \omega}$, gde je $1_n$ generatorni element grupe $\mathbf{Z}_{q_n}$, $\mathbf{1}_n$ element čija je $n$-ta komponenta $1_n$ a ostale su nula i $\overline{\mathbf{1}}_n$ element čije su sve komponente "jedinica" osim $n$-te koja je nula. Kako je za dato $k$, za svako $n \neq k$, $1_n$ deljivo sa $q_k$ (u grupi $\mathbf{Z}_{q_n}$), postoji element $\mathbf{a}_k$ takav da je $q_k \mathbf{a}_k = \overline{\mathbf{1}}_k = \mathbf{1} - \mathbf{1}_k$. Neka je dalje $\mathbf{B} = \langle t(A) \cup \{\mathbf{1}\} \cup \{\mathbf{a}_k \mid k \in \omega\} \rangle$ i $\mathbf{C} = \mathbf{O}$. Podgrupa $\mathbf{B}$ ($\cong \mathbf{B}/\mathbf{O}$) se ne deli (primetimo da je $\mathbf{B}$ prebrojiva, dakle i prava podgrupa grupe $\mathbf{A}$). Jer, pretpostavimo: $\mathbf{B} = t(\mathbf{B}) \oplus \mathbf{G}$. Onda je $\mathbf{1} = \mathbf{1}' + \mathbf{1}''$ i, za svako $k \in \omega$, $\mathbf{a}_k = \mathbf{a}'_k + \mathbf{a}''_k$, gde je $\mathbf{1}', \mathbf{a}'_k \in t(B) = t(A)$, $\mathbf{1}'', \mathbf{a}''_k \in G$. Stoga za (svako) $k \in \omega$ imamo $q_k \mathbf{a}_k = q_k \mathbf{a}'_k + q_k \mathbf{a}''_k = \mathbf{1} - \mathbf{1}_k = (\mathbf{1}' - \mathbf{1}_k) + \mathbf{1}''$ i odatle $\mathbf{1}' - \mathbf{1}_k = q_k \mathbf{a}'_k$. Kako je $\mathbf{1}'$ konačnog reda, za prost broj $q_m$ iz $Q$ koji ne deli red elementa $\mathbf{1}'$ postoji u $t(\mathbf{B})$ rešenje jednačine $q_m x = \mathbf{1}'$; recimo da je to $\mathbf{c}'$. No, tada zbog $1_m = q_m(c'_m - a'_m)$ (gde su $c'_m$ i $a'_m$, jasno, $m$-te komponente elemenata, respektivno, $\mathbf{c}'$ i $\mathbf{a}'_m$) sledi da je generatorni element grupe $\mathbf{Z}_{q_m}$ ($1_m$) deljiv sa $q_m$, kontradikcija.

*(b) Neka je $\mathbf{A} = \sum^{c}_{n \in N} \mathbf{Z}_{p^{2n}}$, $p$ prost broj, $\mathbf{T} = \sum_{n \in N} \mathbf{Z}_{p^{2n}}$ i neka je, za $n \in N$, $\mathbf{a}_n = \langle 0, \ldots, 0, 1_n, p1_{n+1}, p^2 1_{n+2}, \ldots \rangle$, gde je $1_k$ generatorni element grupe $\mathbf{Z}_{p^{2k}}$. Podgrupa $\mathbf{B} = \langle T \cup \{a_n \mid n \in \omega\} \rangle$ se ne deli.*

**Dokaz.** Elementi $\mathbf{a}_n$ su, očigledno, beskonačnog reda, zapravo jednako tako je očigledno da je $t(\mathbf{B}) = \mathbf{T}$. Zaista, pretpostavka da je $m_1 \mathbf{a}_{i_1} + \cdots + m_k \mathbf{a}_{i_k}$ ($m_j \neq 0$ za $1 \leq j \leq k$) reda $p^t$ vodi u kontradikciju: za dovoljno veliko $n$ broj $p^t(m_1 p^{n-i_1} + \cdots + m_k p^{n-i_k})$ nije deljiv sa $p^{2n}$. Ako bi bilo $\mathbf{B} = \mathbf{T} \oplus \mathbf{G}$, element $\mathbf{a}_n + T$ faktor grupe $\mathbf{B}/\mathbf{T}$ ($\cong \mathbf{G}$) bio bi, zbog $p^k \mathbf{a}_{n+k} - \mathbf{a}_n \in T$, tj. $\mathbf{a}_n + T = p^k(\mathbf{a}_{n+k} + T)$, beskonačne visine po $p$. No grupa $\mathbf{A}$, a onda i njena podgrupa $\mathbf{G}$, nema elemente beskonačne visine po $p$; ako je element $\mathbf{a} = \langle k_n \rangle_{n \in N}$ deljiv sa $p^{2m}$, onda je prvih njegovih $m$ komponenti jednako nuli.□



**Teorema 45.5** *Periodična Abelova grupa $\mathbf{T}$ ima svojstvo da se svaka Abelova grupa čiji je periodični deo izomorfan sa $\mathbf{T}$ deli akko je direktna suma deljive i ograničene grupe.*

**Dokaz.** ($\Longleftarrow$) Neka je periodična grupa $\mathbf{T} = \mathbf{D} \oplus \mathbf{G}$, gde je $\mathbf{D}$ deljiva grupa i $\mathbf{G}$ ograničena grupa, periodični deo Abelove grupe $\mathbf{A}$. S obzirom da je $\mathbf{D}$, kao deljiva grupa, apsolutni direktni sumand grupe $\mathbf{A}$ (33.11), to je, za neku podgrupu $\mathbf{F}$ grupe $\mathbf{A}$ koja sadrži $\mathbf{G}$, $\mathbf{A} = \mathbf{D} \oplus \mathbf{F}$. Jasno, $t(\mathbf{F}) = \mathbf{G}$, pa je $\mathbf{G}$ potpuna ograničena podgrupa grupe $\mathbf{F}$, stoga i njen direktni sumand (37.18).

($\Longrightarrow$) Neka je sada periodična grupa $\mathbf{T}$ direktna suma deljive grupe $\mathbf{D}$ i reducirane i neograničene grupe $\mathbf{G}$. Pokazaćemo da postoji grupa čiji je periodični deo grupa $\mathbf{T}$ i koja se ne deli. Pošto je $\mathbf{G} = \sum_{p \in P} \mathbf{G}_p$ (gde je, podsećamo, $\mathbf{G}_p$ podgrupa grupe $\mathbf{G}$ sa domenom $G_p = \{g \in G \mid$ red elementa $g$ je stepen prostog broja $p\}$) neograničena, imamo: za beskonačan podskup $Q$ skupa prostih brojeva $P$ podgrupe $\mathbf{G}_p$, $p \in Q$, su različite od nula-grupe ili je za neki prost broj $p$ podgrupa $\mathbf{G}_p$ neograničena (ili i jedno i drugo).

U prvom slučaju možemo pretpostaviti da je svaka grupa $\mathbf{G}_p$, $p \in Q$, ograničena; u suprotnom bismo odmah prešli na drugi slučaj. Neka je, dakle, $\mathbf{G} = \sum_{p \in Q} \mathbf{G}_p$, gde je (za $p \in Q$) $\mathbf{G}_p$ nenula ograničena podgrupa. $\mathbf{G}_p$ je prema 35.2 direktna suma cikličnih grupa i ciklična grupa $\mathbf{Z}_p$ je jedna njena homomorfna slika, te je $\sum_{p \in Q} \mathbf{Z}_p$ (jedna) homomorfna slika grupe $\mathbf{G}$ za, recimo, homomorfizam $\varphi$. Prema lemi 33.30 postoji grupa $\mathbf{F}$ koja sadrži $\mathbf{G}$ i

takva je da je $\mathbf{F}/\mathbf{Ker}(\varphi) \cong \mathbf{B}$, gde je $\mathbf{B}$ grupa iz tačke $(a)$ prethodnog primera. Grupa $\mathbf{H} = \mathbf{D} \oplus \mathbf{F}$ je mešovita grupa sa periodičnim delom $\mathbf{D} \oplus \mathbf{G} = \mathbf{T}$ jer je $t(\mathbf{F}/\mathbf{Ker}(\varphi)) = \mathbf{G}/\mathbf{Ker}(\varphi)$ (pošto je $\sum_{p\in Q} \mathbf{Z}_p$ periodični deo grupe $\mathbf{B}$). Iz $t(\mathbf{H}) = \mathbf{D} \oplus \mathbf{G} \geq \mathbf{Ker}(\varphi)$ i činjenice da se $\mathbf{H}/\mathbf{Ker}(\varphi) = (\mathbf{D} \oplus \mathbf{F})/\mathbf{Ker}(\varphi)$ ($\cong \mathbf{D} \oplus \mathbf{F}/\mathbf{Ker}(\varphi) \cong \mathbf{D} \oplus \mathbf{B}$) ne deli (s obzirom da se i $\mathbf{B}$ ne deli – pretpostavka $\mathbf{D} \oplus \mathbf{B} = t(\mathbf{D} \oplus \mathbf{B}) \oplus \mathbf{K}$, gde je $\mathbf{K}$ torziono slobodna grupa, dala bi, zbog $t(\mathbf{D} \oplus \mathbf{B}) = \mathbf{D} \oplus (\mathbf{B} \cap t(\mathbf{D} \oplus \mathbf{B}))$, $\mathbf{B} \cong (\mathbf{B} \cap t(\mathbf{D} \oplus \mathbf{B})) \oplus \mathbf{K}$) sledi prema lemi 45.3 da se ni $\mathbf{H}$ ne deli.

Pretpostavimo sada da je za neko $p$ grupa $\mathbf{G}_p$ neograničena. Svaka njena bazična podgrupa (a sve su nenula podgrupe) takođe je neograničena. Jer, ako je $\mathbf{B}_p$ bazična podgrupa, onda je prema 39.14 $p^m\mathbf{B}_p$ bazična podgrupa grupe $p^m\mathbf{G}_p$, pa bi $p^m\mathbf{B}_p = \mathbf{O}$ impliciralo da je $p^m\mathbf{G}_p$ deljiva grupa. Prema 39.26 grupa $\mathbf{G}_p$ se, a onda i grupa $\mathbf{G}$, homomorfno preslikava na $\mathbf{B}_p$, a ova se pak može homomorfno preslikati na grupu $\sum_{k\in N} \mathbf{Z}_{p^{2k}}$ (pozivamo se na poznatu činjenicu da je za svako $i \leq m$ grupa $\mathbf{Z}_{p^i}$ homomorfna slika grupe $\mathbf{Z}_{p^m}$). Priča se dalje ponavlja kao i u prethodnom slučaju, s tim što sada, jasno, koristimo tačku $(b)$ prethodnog primera.■

Jedno od zapažanja iz dokaza prethodne teoreme "promovisaćemo" i zvanično.

**Lema 45.6** *Ako je periodična grupa* $\mathbf{T}$ *direktna suma grupa* $\mathbf{T}'$ *i* $\mathbf{T}''$ *i ako je za grupu* $\mathbf{A}$ *koja se ne deli* $t(\mathbf{A}) = \mathbf{T}'$, *onda se ne deli ni grupa* $\mathbf{T}'' \oplus \mathbf{A}$.

**Korolar 45.7** *Mešovita Abelova grupa sa ograničenim periodičnim delom je rastavljajuća.*

**Lema 45.8** *Ako je za mešovitu Abelovu grupu* $\mathbf{A}$, *za neko* $n \in N$, $n\mathbf{A}$ *rastavljajuća grupa, onda je i* $\mathbf{A}$ *rastavljajuća grupa.*

**Dokaz**. Dovoljno je razmotriti samo slučaj kada je $n$ prost broj. Zaista, pod pretpostavkom da tvrđenje važi za sve proste brojeve, iz $n\mathbf{A}$ je rastavljajuća grupa, gde je $n = p_1^{\alpha_1}p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, sledi, sukcesivno: $p_1^{\alpha_1-1}p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}\mathbf{A}$ je rastavljajuća, ..., $p_k\mathbf{A}$ je rastavljajuća, $\mathbf{A}$ je rastavljajuća. Krenimo, dakle, od toga da je za mešovitu grupu $\mathbf{A}$, i neki prost broj $p$, $p\mathbf{A} = t(p\mathbf{A}) \oplus \mathbf{G}$, gde je, jasno, $\mathbf{G}$ torziono slobodna grupa. Neka je dalje $\mathbf{F}$ (jedna) maksimalna torziono slobodna podgrupa grupe $\mathbf{A}$ takva da je $\mathbf{G} \leq \mathbf{F}$ (egzistencija podgrupe $\mathbf{F}$ zagarantovana je lemom Zorna: posmatramo parcijalno uređeni skup $\langle\{\mathbf{B} \leq \mathbf{A} \mid \mathbf{G} \leq \mathbf{B},\ \mathbf{B} \cap t(\mathbf{A}) = \mathbf{O}\}, \leq\rangle$). Pretpostavimo da element $a\ (\in A)$ nije u $t(\mathbf{A}) \oplus \mathbf{F}$. No, $pa \in pA = t(pA) \oplus G$, pa je $pa = b + c$ za neko $b \in t(pA)$ i neko $c \in G$, i kako je, očigledno, $t(p\mathbf{A}) = pt(\mathbf{A})$, to je $b = pb'$ za neko $b' \in t(A)$. Prema tome, $a - b' \notin t(A) \oplus F$, dok je $p(a - b') = c \in G \subseteq F$. Stoga je $\langle F \cup \{a - b'\}\rangle \cap t(A) \neq \{0\}$. Neka je $m(a - b') + f = d \neq 0$, gde je $0 < m < p$, $f \in F$ i $d \in t(A)$. Sledi: $m(a - b') = d + (-f) \in t(A) \oplus F$, a tada i $a - b' \in t(A) \oplus F$ (zbog $(m, p) = 1$), kontradikcija.□

# Glava 4

# Nilpotentne i rešive grupe

## 46 Normalni nizovi podgrupa

Celo ovo poglavlje se odnosi na ispitivanje grupa sa određenim sistemima podgrupa. Upoznajemo se prvo sa formulacijama i osnovnim osobinama nekih najinteresantnijih sistema (podgrupa), koje ćemo pak kasnije koristiti u definisanju klasa grupa od posebnog interesa – nilpotentne grupe, rešive grupe, $Z$-grupe, $ZA$-grupe, $SD$-grupe, $SN$- grupe, ....

**Definicija 46.1** *Normalni niz grupe* $\mathbf{G}$ *je konačan opadajući niz podgrupa grupe* $\mathbf{G}$ – $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_k = \mathbf{E}$, *gde je, za svako* $i$, $1 \leq i \leq k$, $\mathbf{G}_i$ *prava normalna podgrupa grupe* $\mathbf{G}_{i-1}$.

*Faktor grupe* $\mathbf{G}/\mathbf{G}_1, \mathbf{G}_1/\mathbf{G}_2, \ldots, \mathbf{G}_{k-1}/\mathbf{E}$ *su faktori datog normalnog niza, a broj faktora* $(k)$ *je dužina niza.*

**Napomena**. U nekim engleskim knjigama se opisani nizovi nazivaju *subnormal series*; shodno tome, invarijantni nizovi (videti definiciju 46.12) se u tim knjigama zovu *normal series*. U svakom slučaju, termini koje mi koristimo standardniji su, tj. češće su u upotrebi. Pored toga, često se ne postavlja uslov da je $\mathbf{G}_i$ prava podgrupa grupe $\mathbf{G}_{i-1}$.

Već smo videli da svojstvo normalnosti nije tranzitivno. U prethodnoj definiciji zahteva se samo da je $\mathbf{G}_i$ (prava) normalna podgrupa grupe $\mathbf{G}_{i-1}$; prema tome, $\mathbf{G}_i$ nije nužno normalna podgrupa i grupe $\mathbf{G}_{i-2}$.

Za nejediničnu grupu $\mathbf{G}$ imamo, trivijalno, normalni niz $\mathbf{G} > \mathbf{E}$. Svaka netrivijalna normalna podgrupa $\mathbf{H}$ grupe $\mathbf{G}$ član je (bar jednog) normalnog niza: $\mathbf{G} > \mathbf{H} > \mathbf{E}$. Uopšte, podgrupa grupe $\mathbf{G}$ koja se javlja kao član nekog normalnog niza zove se *dostižna* ili *podnormalna* (eng. *accessible* ili *subnormal subgroup*). Jasno, dostižna podgrupa dostižne podgrupe je dostižna.

**Definicija 46.2** *Normalni niz* $\mathbf{G} = \mathbf{H}_0 > \mathbf{H}_1 > \cdots > \mathbf{H}_l = \mathbf{E}$ *je proširenje (eng. refinement) normalnog niza* $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_k = \mathbf{E}$ *akko*

*se svaka podgrupa $\mathbf{G}_i$ javlja u njemu (drugim rečima: $\{\mathbf{G}_i \mid i = 0, \ldots, k\} \subseteq \{\mathbf{H}_j \mid j = 0, \ldots, l\}$).*

*Kompozicioni niz je normalni niz bez pravih proširenja.*

**Definicija 46.3** *Dva normalna niza su izomorfna akko su iste dužine i ako se među njihovim faktorima može uspostaviti uzajamno jednoznačna korespondencija takva da su korespondentni faktori izomorfne grupe.*

Korespondencija faktora o kojoj je reč u definiciji ne podrazumeva "vezivanje" po redu. Na primer, ciklična grupa $\mathbf{Z}_{p_1 \cdot \ldots \cdot p_n}$, $p_i$ – prost broj, $n \geq 2$, ima normalne nizove

$$\mathbf{Z}_{p_1 \ldots p_n} > \langle p_1 \rangle > \langle p_1 p_2 \rangle > \cdots > \langle p_1 p_2 \ldots p_{n-1} \rangle > \mathbf{O}$$

i

$$\mathbf{Z}_{p_1 \ldots p_n} > \langle p_n \rangle > \langle p_{n-1} p_n \rangle > \cdots > \langle p_2 \ldots p_{n-1} p_n \rangle > \mathbf{O}$$

čiji su faktori ciklične grupe redova $p_1, \ldots, p_n$; ovde prvi faktor prvog niza odgovara poslednjem faktoru drugog niza, drugi pretposlednjem, ..., poslednji prvom.

Sledeća teorema je od suštinskog značaja za ispitivanje normalnih nizova.

**Teorema 46.4** *(Teorema Schreiera). Svaka dva normalna niza ma koje grupe imaju izomorfna proširenja.*

**Dokaz.** Neka su dati normalni nizovi grupe $\mathbf{G}$:

$$\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_k = \mathbf{E}$$

i

$$\mathbf{G} = \mathbf{H}_0 > \mathbf{H}_1 > \cdots > \mathbf{H}_l = \mathbf{E},$$

i neka je, za $j = 0, 1, \ldots, l$, $\mathbf{G}_{ij} = \mathbf{G}_i \cdot (\mathbf{G}_{i-1} \cap \mathbf{H}_j)$, za $i = 0, 1, \ldots, k$, $\mathbf{H}_{ij} = \mathbf{H}_j \cdot (\mathbf{H}_{j-1} \cap \mathbf{G}_i)$. $\mathbf{G}_{ij}$ je zaista podgrupa grupe $\mathbf{G}_{i-1}$ jer je $\mathbf{G}_i \lhd \mathbf{G}_{i-1}$, a isto tako je $\mathbf{H}_{ij}$ podgrupa grupe $\mathbf{H}_{j-1}$. Prema lemi Zassenhausa važi: $\mathbf{G}_{ij} \lhd \mathbf{G}_{i,j-1}$, $\mathbf{H}_{ij} \lhd \mathbf{H}_{i-1,j}$ i $\mathbf{G}_{i,j-1}/\mathbf{G}_{ij} \cong \mathbf{H}_{i-1,j}/\mathbf{H}_{ij}$, pa ako je $\mathbf{G}_{ij} = \mathbf{G}_{i,j-1}$, onda je i $\mathbf{H}_{ij} = \mathbf{H}_{i-1,j}$. Eliminisanjem po parovima identičnih uzastopnih grupa, ukoliko takve postoje, ostaju izomorfna proširenja polaznih normalnih nizova.■

**Korolar 46.5** *(Teorema Jordan-Höldera). Ako grupa ima kompozicioni niz, onda su svaka dva njena kompoziciona niza izomorfna.*

**Korolar 46.6** *Ako grupa ima kompozicioni niz, onda svaki njen normalni niz ima proširenje koje je kompozicioni niz. Posebno, svaka dostižna grupa je član nekog kompozicionog niza.*



Jordan-Hölderova teorema nam dozvoljava da uvedemo termine: *kompoziciona dužina* (svi kompozicioni nizovi date grupe su iste dužine) i *kompozicioni faktori*.

Trivijalno, konačne i proste grupe imaju kompozicioni niz (u slučaju prostih grupa ti su nizovi jedinstveni – dužine 1). Ali, Abelova grupa ima kompozicioni niz akko je konačna. Jer, kompozicioni faktori su proste grupe (videti 8.7), pa su u slučaju Abelove grupe kompozicioni faktori ciklične grupe prostog reda (to su jedine Abelove proste grupe). I tako, ako je $\mathbf{A}$ Abelova grupa i $\mathbf{A} = \mathbf{A}_0 > \mathbf{A}_1 > \cdots > \mathbf{A}_k = \mathbf{O}$ njen kompozicioni niz, tada je $\mathbf{A}_{k-1}/\mathbf{O} \cong \mathbf{A}_{k-1}$ konačna grupa, $\mathbf{A}_{k-2}$ je konačna grupa, pošto su $\mathbf{A}_{k-1}$ i $\mathbf{A}_{k-2}/\mathbf{A}_{k-1}$ konačne grupe i, generalno, svaka grupa $\mathbf{A}_i$ je konačna (formalni dokaz bi išao indukcijom po $i$, $i = 1, \ldots, k$; dokazuje se: grupa $\mathbf{A}_{k-i}$ je konačna za svako $i \in \{1, \ldots, k\}$). Posebno, $\mathbf{A}$ je konačna grupa.

**Korolar 46.7** *Grupa sa kompozicionim nizom nastaje od (odgovarajuće) proste grupe uzastopnim formiranjem ekstenzija konačno mnogo puta.*

U kriterijumu koji ćemo dati za egzistenciju kompozicionog niza koriste se pojmovi koje upravo definišemo.

**Definicija 46.8** *Opadajući normalni lanac podgrupa grupe $\mathbf{G}$ je opadajući lanac podgrupa $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{i-1} > \mathbf{G}_i > \cdots$, gde je, za svako $i = 1, 2, \ldots$, $\mathbf{G}_i$ prava normalna podgrupa grupe $\mathbf{G}_{i-1}$.*

*Rastući lanac podgrupa grupe $\mathbf{G}$ – $\mathbf{E} = \mathbf{H}_0 < \mathbf{H}_1 < \cdots < \mathbf{H}_i < \mathbf{H}_{i+1} < \cdots$ – je rastući normalni lanac podgrupa akko je, za svako $i = 0, 1, \ldots$, $\mathbf{H}_i$ prava normalna podgrupa grupe $\mathbf{H}_{i+1}$ i ako je svaka podgrupa $\mathbf{H}_i$ dostižna.*

Uočimo da su elementi bilo kog opadajućeg normalnog lanca dostižne podgrupe (dokaz, indukcijom po $i$, koristi već pomenutu tranzitivnost svojstva dostižnosti).

**Napomena.** U nekim knjigama koriste se termini: *opadajući (rastući) normalni niz* (umesto opadajući (rastući) normalni lanac). Mi smo, međutim, držeći se terminologije A. Kuroša, ove izraze sačuvali za "druge stvari" (videti 47.4).

**Lema 46.9** *Grupa $\mathbf{G}$ ima kompozicioni niz akko su svi njeni opadajući i rastući normalni lanci konačni.*

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{G}$ sa kompozicionim nizom dužine $k$. Ako bi $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{i-1} > \mathbf{G}_i > \cdots$, gde je $i \geq k$, bio njen opadajući normalni lanac, onda bi niz $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_i > \mathbf{E}$ bio normalni niz dužine $i + 1 > k$, kontradikcija; prema 46.5 i 46.6, dužina bilo kog normalnog niza jednaka je ili manja od kompozicione dužine. Analogno rezonujemo i u slučaju

rastućih normalnih lanaca: ako bi $\mathbf{E} = \mathbf{H}_0 < \mathbf{H}_1 < \cdots < \mathbf{H}_i < \cdots$, gde je $i \geq k$, bio rastući normalni lanac i $\mathbf{H}_i \neq \mathbf{G}$, tada bismo, polazeći od uslova da je $\mathbf{H}_i$ dostižna grupa, našli jedan normalni niz oblika $\mathbf{G} > \mathbf{K}_1 > \cdots > \mathbf{K}_m = \mathbf{H}_i > \mathbf{E}$, pa bi opet $\mathbf{G} > \cdots > \mathbf{K}_m = \mathbf{H}_i > \mathbf{H}_{i-1} > \cdots > \mathbf{H}_1 > \mathbf{E}$ bio normalni niz dužine veće od kompozicione.

($\Longleftarrow$) Iz uslova da je svaki rastući normalni lanac konačan sledi da svaka dostižna podgrupa sadrži maksimalnu normalnu podgrupu; u suprotnom bi dostižna podgrupa bez tog svojstva imala beskonačan rastući normalni lanac koji bi ujedno bio i rastući normalni lanac grupe $\mathbf{G}$. Posebno, $\mathbf{G}$ sadrži maksimalnu normalnu podrupu (ne nužno jedinstvenu), neka je to $\mathbf{G}_1$, koja pak sadrži maksimalnu normalnu podgrupu $\mathbf{G}_2$. Nastavljajući tako formiramo opadajući normalni lanac $\mathbf{G} > \mathbf{G}_1 > \cdots > \mathbf{G}_{i-1} > \mathbf{G}_i > \cdots$, gde je $\mathbf{G}_i$ maksimalna normalna podgrupa grupe $\mathbf{G}_{i-1}$, a koji je, kao i svaki drugi, konačan. Stoga je za neko $n$ grupa $\mathbf{G}_n$ prosta (te je $\mathbf{G}_{n+1} = \mathbf{E}$), a niz $\mathbf{G} > \mathbf{G}_1 > \cdots > \mathbf{G}_n > \mathbf{E}$ je, jasno, kompozicioni.□

**Korolar 46.10** *Ako grupa* $\mathbf{G}$ *ima kompozicioni niz, onda i svaka njena dostižna podgrupa* $\mathbf{H}$ *ima kompozicioni niz. Kompoziciona dužina prave dostižne podgrupe* $\mathbf{H}$ *manja je od kompozicione dužine grupe* $\mathbf{G}$ *i (svaki) kompozicioni niz podgrupe* $\mathbf{H}$ *deo je nekog kompozicionog niza grupe* $\mathbf{G}$.

**Dokaz.** Svaki rastući normalni lanac podgrupe $\mathbf{H}$ ujedno je i rastući normalni lanac grupe $\mathbf{G}$ (jer je $\mathbf{H}$ dostižna podgrupa, a svojstvo dostižnosti je, ponavljamo, tranzitivno), pa je prema prethodnoj teoremi konačan. Iz dokaza (iste) teoreme videli smo i da je svaki opadajući normalni lanac podgrupe $\mathbf{H}$ deo nekog opadajućeg normalnog lanca grupe $\mathbf{G}$, stoga su i opadajući normalni lanci podgrupe $\mathbf{H}$ konačni.□

**Napomena.** Svojstvo dostižnosti podgrupe $\mathbf{H}$ nije moguće isključiti (u prethodnom korolaru). Recimo, beskonačna alternativna grupa $\mathbf{A}_\infty$ (videti 9.27) je (beskonačna) prosta grupa, znači grupa sa kompozicionim nizom, ali njena podgrupa generisana skupom permutacija $\{(4n\ \ 4n+1)(4n+2\ \ 4n+3) \mid n = 0, 1, \ldots\}$ je beskonačna Abelova grupa (elementi generatornog skupa su disjunktne, dakle i uzajamno permutabilne permutacije), znači grupa bez kompozicionog niza.

**Lema 46.11** *Neka je* $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_k = \mathbf{E}$ *normalni niz grupe* $\mathbf{G}$ *i* $\mathbf{H}$ *jedna njena podgrupa. Tada* $\mathbf{H}$ *ima normalni niz čiji su faktori izomorfni podgrupama nekih faktora datog normalnog niza grupe* $\mathbf{G}$.

**Dokaz.** Posmatrajmo opadajući niz podgrupa grupe $\mathbf{H}$: $\mathbf{H} = \mathbf{H}_0 = \mathbf{H} \cap \mathbf{G}_0 \geq \mathbf{H}_1 = \mathbf{H} \cap \mathbf{G}_1 \geq \cdots \geq \mathbf{H}_k = \mathbf{E} = \mathbf{H} \cap \mathbf{G}_k$. Kako je $\mathbf{G}_i$ normalna podgrupa grupe $\mathbf{G}_{i-1}$ i, trivijalno, $\mathbf{E} \lhd \mathbf{H}$, prema lemi Zassenhausa važi: $\mathbf{E} \cdot (\mathbf{G}_i \cap \mathbf{H}) \lhd \mathbf{E} \cdot (\mathbf{G}_{i-1} \cap \mathbf{H})$, tj. $\mathbf{H}_i \lhd \mathbf{H}_{i-1}$, $\mathbf{G}_i \cdot (\mathbf{G}_{i-1} \cap \mathbf{E}) \lhd \mathbf{G}_i \cdot (\mathbf{G}_{i-1} \cap \mathbf{H})$, tj. $\mathbf{G}_i \lhd \mathbf{G}_i \cdot \mathbf{H}_{i-1}$ (ovo smo i inače znali) i

$$\mathbf{H}_{i-1}/\mathbf{H}_i \cong (\mathbf{G}_i \cdot \mathbf{H}_{i-1})/\mathbf{G}_i \leq \mathbf{G}_{i-1}/\mathbf{G}_i.$$



Uklanjanjem "viška" podgrupa (ukoliko se neke podgrupe ponavljaju) ostaje normalni niz podgrupe $\mathbf{H}$ sa navedenim svojstvom.□

**Definicija 46.12** *Invarijantni niz podgrupa grupe* $\mathbf{G}$ *je konačni opadajući niz njenih normalnih podgrupa* $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_k = \mathbf{E}$, *gde je, kao i u slučaju normalnih nizova, za svako* $i = 1, \ldots, k$, $\mathbf{G}_i$ *prava podgrupa grupe* $\mathbf{G}_{i-1}$.

*Proširenje invarijantnog niza definiše se kao u u slučaju normalnih nizova.*

*Glavni niz (eng. principal ili chief series) je invarijantni niz bez pravih (invarijantnih) proširenja.*

*Opadajuće i rastuće lance normalnih podgrupa definišemo kao i opadajuće odnosno rastuće normalne lance uz dodatni uslov: sve podgrupe tih lanaca su normalne.*

*Invarijantni niz čiji su svi članovi karakteristične podgrupe zove se karakteristični niz. Analogno se definiše potpuno invarijantni niz.*

**Korolar 46.13** *Grupa* $\mathbf{G}$ *ima glavni niz akko je svaki opadajući i svaki rastući lanac normalnih podgrupa konačan.*

**Dokaz.** Kopija odgovarajućeg dokaza za kompozicione nizove.□

**Korolar 46.14** *Svaka dva invarijantna niza grupe* $\mathbf{G}$ *imaju izomorfna invarijantna proširenja.*

**Dokaz.** Kopija dokaza Schreierove teoreme, uz napomenu: presek i proizvod normalnih podgrupa je normalna podgrupa.□

**Korolar 46.15** *Ako grupa ima glavni niz, onda su svaka dva njena glavna niza izomorfna.*

**Napomena.** Kako svojstvo normalnosti (za razliku od svojstva dostižnosti) nije tranzitivno, ne važi u opštem analogon korolara 46.11: glavni niz podgrupe $\mathbf{H}$ grupe $\mathbf{G}$ može biti pravo proširenje segmenta između $\mathbf{H}$ i $\mathbf{E}$ glavnog niza grupe $\mathbf{G}$ koji "prolazi" kroz $\mathbf{H}$. Takav jedan primer nam daju grupa $\mathbf{A}_4$ i njena jedina netrivijalna normalna podgrupa

$$\mathbf{H} = \langle \{\imath, (0\ 1)(2\ 3), (0\ 2)(1\ 3), (0\ 3)(1\ 2)\}, \circ \rangle$$

(videti 9.23), koja pak ima normalnu podgrupu $\langle \{\imath, (0\ 1)(2\ 3)\}, \circ \rangle$.

**Lema 46.16** *Grupa sa glavnim nizom je karakteristično prosta akko je direktni proizvod familije izomorfnih, prostih (i, jasno, normalnih) podgrupa.*

**Dokaz.** Pravac ($\Longrightarrow$) je već dokazan (10.40 – grupa sa glavnim nizom ima minimalnu normalnu podgrupu), a pravac ($\Longleftarrow$) važi uvek (10.34($c$)).□

**Lema 46.17** *Neka je* $\mathbf{G}$ *konačna grupa. Tada važi:*

($a$) *Ako je* $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{n-1} > \mathbf{G}_n = \mathbf{E}$ *glavni niz grupe* $\mathbf{G}$, *onda je, za svako* $i = 1, \ldots, n$, $\mathbf{G}_{i-1}/\mathbf{G}_i$ *direktni proizvod izomorfnih prostih grupa;*

($b$) *Ako je* $\mathbf{G} = \mathbf{G}_0 > \cdots > \mathbf{G}_{n-1} > \mathbf{G}_n = \mathbf{E}$ *invarijantni niz grupe* $\mathbf{G}$, *gde je (za* $i = 1, \ldots, n$*)* $\mathbf{G}_i$ *maksimalna karakteristična podgrupa grupe* $\mathbf{G}_{i-1}$, *onda je, za svako* $i$, $\mathbf{G}_{i-1}/\mathbf{G}_i$ *direktni proizvod izomorfnih prostih grupa;*

($c$) *Ako je* $\mathbf{G} = \mathbf{G}_0 > \cdots > \mathbf{G}_{n-1} > \mathbf{G}_n = \mathbf{E}$ *invarijantni niz grupe* $\mathbf{G}$, *gde je (za svako* $i = 1, \ldots, n$*)* $\mathbf{G}_i$ *maksimalna karakteristična podgrupa grupe* $\mathbf{G}$ *sadržana u* $\mathbf{G}_{i-1}$, *tada je, za svako* $i$, $\mathbf{G}_{i-1}/\mathbf{G}_i$ *direktni proizvod izomorfnih prostih grupa.*

**Dokaz.** ($a$) Konstatujmo samo: za svako $i = 1, \ldots, n$ (faktor) grupa $\mathbf{G}_{i-1}/\mathbf{G}_i$ je konačna, karakteristično prosta grupa; ako bi $\mathbf{H}/\mathbf{G}_i$ bila netrivijalna karakteristična podgrupa grupe $\mathbf{G}_{i-1}/\mathbf{G}_i$, onda bi bila i normalna podgrupa grupe $\mathbf{G}/\mathbf{G}_i$ (4.34), te bi $\mathbf{H}$ bila normalna podgrupa grupe $\mathbf{G}$ "uklještena" između $\mathbf{G}_{i-1}$ i $\mathbf{G}_i$, kontradikcija.

($b$) i ($c$) Kao i u prethodnoj tački, svi faktori $\mathbf{G}_{i-1}/\mathbf{G}_i$ su karakteristično proste grupe – videti 8.10.

Vežbe radi dajemo i drugi dokaz koji je u osnovi ponavljanje dokaza korolara 10.40.

($a$) Neka je $\overline{\mathbf{H}} = \mathbf{H}/\mathbf{G}_i$ minimalna normalna podgrupa grupe $\overline{\mathbf{G}}_{i-1} = \mathbf{G}_{i-1}/\mathbf{G}_i$. Ako je baš $\mathbf{H} = \mathbf{G}_{i-1}$, $\overline{\mathbf{G}}_{i-1}$ je prosta grupa. Pretpostavimo stoga da je $\mathbf{H}$ prava (normalna) podgrupa grupe $\mathbf{G}_{i-1}$ (dok je $\mathbf{G}_i$ prava podgrupa grupe $\mathbf{H}$) i neka su $\mathbf{H}_0 = \mathbf{H}, \mathbf{H}_1 = (\mathbf{H})u_{g_1}, \ldots, \mathbf{H}_{m-1} = (\mathbf{H})u_{g_{m-1}}$ svi njeni konjugati u $\mathbf{G}$. Naravno, $m > 1$, jer $\mathbf{H}$ nije normalna podgrupa grupe $\mathbf{G}$, svaki konjugat je sadržan u $\mathbf{G}_{i-1}$, sadrži $\mathbf{G}_i$ i za $0 \leq k < j \leq m-1$ je $\mathbf{H}_k \cap \mathbf{H}_j = \mathbf{G}_i$, tj. $\mathbf{H}_k/\mathbf{G}_i \cap \mathbf{H}_j/\mathbf{G}_i = \overline{\mathbf{H}}_k \cap \overline{\mathbf{H}}_j = \overline{\mathbf{E}}$ (zbog $(\mathbf{H}_k \cap \mathbf{H}_j)/\mathbf{G}_i \lhd \mathbf{G}_{i-1}/\mathbf{G}_i$). Prema 10.41, $\overline{\mathbf{K}} = \langle \overline{H}_0 \cup \ldots \cup \overline{H}_{m-1} \rangle = \langle H_0 \cup \ldots \cup H_{m-1} \rangle / \mathbf{G}_i = \mathbf{K}/\mathbf{G}_i$ je direktan proizvod nekih podgrupa $\overline{\mathbf{H}}_{i_0}, \ldots, \overline{\mathbf{H}}_{i_r}$, $i_0, \ldots, i_r \in \{0, \ldots, m-1\}$. Ali $\mathbf{K}$ je normalna podgrupa grupe $\mathbf{G}$, pa je $\overline{\mathbf{K}} = \overline{\mathbf{G}}_{i-1}$ (ponavljamo: ne postoji normalna podgrupa grupe $\mathbf{G}$ između $\mathbf{G}_{i-1}$ i $\mathbf{G}_i$). Odatle odmah sledi i da je $\overline{\mathbf{H}}$ prosta grupa; u suprotnom, nijedna od podgrupa $\overline{\mathbf{H}}_i$, $i = 0, \ldots, m-1$, ne bi bila prosta, no netrivijalna normalna podgrupa nekog od faktora bila bi normalna podgrupa i grupe $\overline{\mathbf{G}}_{i-1}$, kontradikcija. Mogli smo, naravno, i odmah pretpostaviti da je $\overline{\mathbf{H}}$ jedan od direktnih faktora.



($b$) Dokaz je u osnovi isti. Opet polazimo od minimalne normalne podgrupe $\mathbf{H}/\mathbf{G}_i$ grupe $\mathbf{G}_{i-1}/\mathbf{G}_i$, pa ako je $\mathbf{H}$ prava podgrupa grupe $\mathbf{G}_{i-1}$, stoga ne i njena karakteristična podgrupa (moguće je, međutim, da je karakteristična podgrupa grupe $\mathbf{G}$ – videti komentar uz 4.34), nalazimo sve njene različite slike za automorfizme grupe $\mathbf{G}_{i-1}$. Neka su to $\mathbf{H}_0 = \mathbf{H} = (\mathbf{H})\imath$, $\mathbf{H}_1 = (\mathbf{H})\varphi_1, \ldots, \mathbf{H}_{r-1} = (\mathbf{H})\varphi_{r-1}$, $\varphi_j \in Aut(\mathbf{G}_{i-1})$. Ponovo je, za $0 \leq j < k \leq r-1$, $\mathbf{H}_j \cap \mathbf{H}_k = \mathbf{G}_i$ ($\mathbf{G}_i$ je karakteristična podgrupa grupe $\mathbf{G}_{i-1}$ i $\mathbf{G}_i \leq (\mathbf{H})\varphi_j \cap (\mathbf{H})\varphi_k \lhd \mathbf{G}_{i-1}$) i opet je $\overline{\mathbf{K}} = \langle \overline{H}_0 \cup \ldots \cup \overline{H}_{m-1} \rangle = \langle H_0 \cup \ldots \cup H_{m-1} \rangle / \mathbf{G}_i = \mathbf{K}/\mathbf{G}_i$ direktni proizvod nekih podgrupa $\overline{\mathbf{H}}_{i_0}, \ldots, \overline{\mathbf{H}}_{i_r}$. $\mathbf{K}$ je, međutim, karakteristična podgrupa grupe $\mathbf{G}_{i-1}$, te je $\overline{\mathbf{K}} = \overline{\mathbf{G}}_{i-1}$. Iz razloga navedenog u prethodnoj tački $\overline{\mathbf{H}}$ je prosta grupa.

($c$) Isto. S uvedenom notacijom, ako je $\overline{\mathbf{H}} = \mathbf{H}/\mathbf{G}_i$ minimalna normalna prava podgrupa grupe $\overline{\mathbf{G}}_{i-1}$, onda $\mathbf{H}$ nije karakteristična podgrupa grupe $\mathbf{G}$ (pa dakle ni grupe $\mathbf{G}_{i-1}$). Sada nalazimo sve različite slike podgrupe $\mathbf{H}$ za automorfizme grupe $\mathbf{G}$, neka su to $\mathbf{H}_0 = \mathbf{H}$, $\mathbf{H}_1 = (\mathbf{H})\psi_1, \ldots, \mathbf{H}_{m-1} = (\mathbf{H})\psi_{m-1}$. Tada je $\overline{\mathbf{K}} = \langle \overline{H}_0 \cup \ldots \cup \overline{H}_{m-1} \rangle = \langle H_0 \cup \ldots \cup H_{m-1} \rangle / \mathbf{G}_i = \mathbf{K}/\mathbf{G}_i$ direktni proizvod nekih od datih podgrupa i $\overline{\mathbf{K}} = \overline{\mathbf{G}}_{i-1}$, tj. $\mathbf{K} = \mathbf{G}_{i-1}$ (jer je $\langle H_0 \cup \ldots \cup H_{m-1} \rangle$ karakteristična podgrupa grupe $\mathbf{G}$).□

**Lema 46.18** ($a$) *Neka je* $\mathbf{G} > \mathbf{K} > \mathbf{H} > \mathbf{E}$ *invarijantni niz grupe* $\mathbf{G}$, *gde je* $\mathbf{H}$ *konačna grupa a* $\mathbf{K}/\mathbf{H}$ *beskonačna ciklična grupa. Tada postoji invarijantni niz* $\mathbf{G} > \mathbf{K} > \mathbf{M} > \mathbf{E}$, *gde je* $\mathbf{M}$ *beskonačna ciklična grupa a* $\mathbf{K}/\mathbf{M}$ *konačna grupa;*

($b$) *Neka je* $\mathbf{G} > \mathbf{K} > \mathbf{H} > \mathbf{E}$ *invarijantni niz grupe* $\mathbf{G}$, *gde je* $|H| = p$ *i* $|K/H| = q$, $p, q$ *su prosti brojevi i* $p < q$. *Tada postoji invarijantni niz* $\mathbf{G} > \mathbf{K} > \mathbf{M} > \mathbf{E}$, *gde je* $|M| = q$ *i* $|K/M| = p$.

**Dokaz.** ($a$) Direktna posledica leme 32.9. Prema njoj $\mathbf{K}$ sadrži karakterističnu, slobodnu Abelovu podgrupu $\mathbf{M}$ ranga jednakog rangu grupe $\mathbf{K}/\mathbf{H}$, dakle u ovom slučaju ranga 1, i takvu da je $\mathbf{K}/\mathbf{M}$ konačna grupa. $\mathbf{M}$ je, jasno, i normalna podgrupa grupe $\mathbf{G}$ (4.34).

($b$) $\mathbf{K}$ je grupa reda $pq$ i s obzirom na uslov $p < q$ ima jedinstvenu, stoga i karakterističnu (štaviše potpunu invarijantnu) Sylowu $q$-podgrupu $\mathbf{M}$. Prema tome, $\mathbf{G} > \mathbf{K} > \mathbf{M} > \mathbf{E}$ je invarijantni niz, a i ostali zahtevi su ispunjeni.□

**Lema 46.19** *Neka je elementarna Abelova grupa* $\mathbf{A}$ *karakteristična podgrupa konačnog reda grupe* $\mathbf{G}$, *čija je faktor grupa* $\mathbf{G}/\mathbf{A}$ *slobodna Abelova grupa konačnog ranga* $r$. *Tada postoji karakteristični niz grupe* $\mathbf{G}$ *čiji su faktori elementarne Abelove grupe i slobodna Abelova grupa ranga* $r$, *s tim što se ova javlja "na kraju".*

**Dokaz.** Prema 32.9 $\mathbf{G}$ ima karakterističnu podgrupu konačnog indeksa $\mathbf{B}$, koja je slobodna Abelova grupa ranga $r$. Kako je $\mathbf{A} \cap \mathbf{B} = \mathbf{E}$, prema dokazu

Schreierove teoreme dobijamo karakteristična izomorfna proširenja karakterističnih nizova, respektivno, $\mathbf{G} > \mathbf{A} > \mathbf{E}$ i $\mathbf{G} > \mathbf{B} > \mathbf{E}$: $\mathbf{G} \geq \mathbf{AB} > \mathbf{A} > \mathbf{E}$ i $\mathbf{G} \geq \mathbf{AB} > \mathbf{B} > \mathbf{E}$. Faktor $(\mathbf{AB})/\mathbf{B}$ $(\cong \mathbf{A})$ je elementarna Abelova grupa, a $\mathbf{G}/(\mathbf{AB})$ je (kao konačna homomorfna slika slobodne Abelove grupe konačnog ranga $\mathbf{G}/\mathbf{A}$) konačna direktna suma konačnih direktnih suma $p$-primarnih cikličnih grupa. No, svaka takva grupa ima karakteristični niz čiji su članovi elementarne Abelove grupe. Jer, ako je npr. $\mathbf{C} = \mathbf{C}_1 \oplus \mathbf{C}_2 \oplus \cdots \oplus \mathbf{C}_m$, gde je, za $i = 1, \ldots, m$, $\mathbf{C}_i = \mathbf{Z}_{p_i^{n_1^i}} \oplus \cdots \oplus \mathbf{Z}_{p_i^{n_{k_i}^i}}$ i $n_i = max\,\{n_1^i, \ldots, n_{k_i}^i\}$, onda je jedan takav karakteristični niz dat, sa recimo:

$$\mathbf{C} > p_1\mathbf{C}_1 \oplus (\mathbf{C}_2 \oplus \cdots \oplus \mathbf{C}_m) > p_1^2\mathbf{C}_1 \oplus (\mathbf{C}_2 \oplus \cdots \oplus \mathbf{C}_m) > \cdots >$$

$$p_1^{n_1-1}\mathbf{C}_1 \oplus (\mathbf{C}_2 \oplus \cdots \oplus \mathbf{C}_m) > \mathbf{C}_2 \oplus \cdots \oplus \mathbf{C}_m > p_2\mathbf{C}_2 \oplus (\mathbf{C}_3 \oplus \cdots \oplus \mathbf{C}_m) > \cdots$$

$$> p_2^{n_2-1}\mathbf{C}_2 \oplus (\mathbf{C}_3 \oplus \cdots \oplus \mathbf{C}_m) > \mathbf{C}_3 \oplus \cdots \oplus \mathbf{C}_m > \cdots > \mathbf{C}_m >$$

$$p_m\mathbf{C}_m > p_m^2\mathbf{C}_m > \cdots > p_m^{n_m-1}\mathbf{C}_m > E.$$

Preostaje još da se pozovemo na 8.10.□

**Definicija 46.20** *Invarijantni niz grupe* $\mathbf{G}$ - $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{k-1} > \mathbf{G}_k = \mathbf{E}$ - *je centralni niz akko je* $\mathbf{G}_{i-1}/\mathbf{G}_i \leq \mathbf{Z}(\mathbf{G}/\mathbf{G}_i)$ *za svako* $i = 1, \ldots, k$.

**Lema 46.21** *Invarijantni niz* $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{k-1} > \mathbf{G}_k = \mathbf{E}$ *je centralni niz akko je* $[\mathbf{G}_{i-1}, \mathbf{G}] \leq \mathbf{G}_i$ *za svako* $i = 1, \ldots, k$.

**Dokaz.** Podsećamo se prvo: za podgrupe $\mathbf{A}$ i $\mathbf{B}$ grupe $\mathbf{G}$ je $[\mathbf{A}, \mathbf{B}]$ podgrupa grupe $\mathbf{G}$ generisana skupom komutatora $\{[a, b] \mid a \in A, b \in B\}$; domen te podgrupe označavamo sa $[A, B]$.

Za svako $i$ $(= 1, \ldots, k)$ imamo: $\mathbf{G}_{i-1}/\mathbf{G}_i \leq \mathbf{Z}(\mathbf{G}/\mathbf{G}_i)$ akko je, za svako $a \in G_{i-1}$ i svako $g \in G$, $agG_i = aG_i \cdot gG_i = gG_i \cdot aG_i = gaG_i$ akko je, za svako $a \in G_{i-1}$ i svako $g \in G$, $[a, g] \in G_i$ akko je $[\mathbf{G}_{i-1}, \mathbf{G}] \leq \mathbf{G}_i$.□

**Korolar 46.22** *Normalni niz* $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{k-1} > \mathbf{G}_k = \mathbf{E}$ *je centralni niz akko je* $[\mathbf{G}_{i-1}, \mathbf{G}] \leq \mathbf{G}_i$ *za svako* $i = 1, \ldots, k$.

**Dokaz.** Primetimo samo: iz $[\mathbf{G}_{i-1}, \mathbf{G}] \leq \mathbf{G}_i$ sledi da je svaka podgrupa $\mathbf{G}_i$ normalna podgrupa grupe $\mathbf{G}$.□

**Definicija 46.23** *Niži centralni lanac grupe* $\mathbf{G}$ *(eng. lower central chain) je lanac podgrupa* $\gamma_0\mathbf{G} \geq \gamma_1\mathbf{G} \geq \cdots \geq \gamma_k\mathbf{G} \geq \cdots$, *gde je:*

$\gamma_0\mathbf{G} = \mathbf{G}$

$\gamma_1\mathbf{G} = [\gamma_0\mathbf{G}, \mathbf{G}]\ (= \mathbf{G}')$



$\gamma_{k+1}\mathbf{G} = [\gamma_k\mathbf{G}, \mathbf{G}]$

$\vdots$

*Ako taj lanac u konačno mnogo koraka "stiže" do jedinične grupe, onda imamo niži centralni niz.*

*Viši centralni lanac (eng. upper central chain) grupe* $\mathbf{G}$ *je lanac podgrupa* $\mathbf{E} = \zeta_0\mathbf{G} \leq \zeta_1\mathbf{G} \leq \cdots \leq \zeta_k\mathbf{G} \leq \cdots$, *gde je* $\zeta_1\mathbf{G} = \mathbf{Z}(\mathbf{G})$ *i, generalno,* $\zeta_{k+1}\mathbf{G}/\zeta_k\mathbf{G} = \mathbf{Z}(\mathbf{G}/\zeta_k\mathbf{G})$.

*Ako taj lanac u konačno mnogo koraka "stiže" do grupe* $\mathbf{G}$, *onda imamo viši centralni niz.*

*Transfinitno produženi niži centralni lanac grupe* $\mathbf{G}$ *je opadajući lanac podgrupa sa elementima* $\gamma_\alpha\mathbf{G}$ *($\alpha$ ordinal), gde je* $\gamma_0\mathbf{G} = \mathbf{G}$, *za nasledni ordinal* $\alpha$ *je* $\gamma_\alpha\mathbf{G} = [\gamma_{\alpha-1}\mathbf{G}, \mathbf{G}]$, *a za granični ordinal* $\alpha$ *je* $\gamma_\alpha\mathbf{G} = \bigcap_{\beta<\alpha} \gamma_\beta\mathbf{G}$. *Ako taj lanac stiže do jedinične grupe, zvaćemo ga transfinitno produženi niži centralni niz.*

*Transfinitno produženi viši centralni lanac grupe* $\mathbf{G}$ *je rastući lanac podgrupa sa elementima* $\zeta_\alpha\mathbf{G}$ *($\alpha$ ordinal), gde je* $\zeta_0\mathbf{G} = \mathbf{E}$, *za nasledni ordinal* $\alpha$ *je* $\zeta_\alpha\mathbf{G}/\zeta_{\alpha-1}\mathbf{G} = \mathbf{Z}(\mathbf{G}/\zeta_{\alpha-1}\mathbf{G})$, *i za granični ordinal* $\alpha$ *je* $\zeta_\alpha\mathbf{G} = \bigcup_{\beta<\alpha} \zeta_\beta\mathbf{G}$. *Ako taj lanac stiže do grupe* $\mathbf{G}$, *zvaćemo ga transfinitno produženi viši centralni niz.*

**Napomena.** Treba reći i da je prilično uobičajeno da se niži (viši) centralni lanac naziva niži (viši) centralni niz (pa se onda niži (viši) centralni nizovi iz "naše" terminologije posebno dodefinišu). Mi smo u skladu sa dosadašnjim korišćenjem pojma niz (*series*) prihvatili "dvojne" nazive koje koristi u svojoj knjizi A.G. Kuroš.

Jasno, transfinitno produženi niži centralni lanac je produženje nižeg centralnog lanca, ukoliko ovaj već nije stigao do jedinične grupe u konačno mnogo koraka; transfinitno produženi viši centralni lanac je produženje višeg centralnog lanca, ukoliko ovaj nije stigao do cele grupe u konačno mnogo koraka. U svakom slučaju bilo koje transfinitno produženje će postati stacionarno u nekom ordinalu kardinalnosti manje od ili jednake $|G|$, tj. od nekog ordinala su sve podgrupe lanca jednake. Transfinitno produženi niži (viši) centralni niz će se "stacionirati" baš u jediničnoj (celoj) grupi i pre toga neće imati jednakih elemenata; npr. ako je za transfinitno produženi viši centralni niz grupe $\mathbf{G}$ $\alpha$ prvi ordinal za koje je $\zeta_\alpha\mathbf{G} = \mathbf{G}$, tada je za sve ordinale $\beta, \gamma$, gde je $\beta < \gamma < \alpha$, $\zeta_\beta\mathbf{G}$ prava podgrupa grupe $\zeta_\gamma\mathbf{G}$.

**Lema 46.24** *Za ma koju grupu* $\mathbf{G}$ *je, za svaki ordinal* $\alpha$, $\gamma_\alpha\mathbf{G}$ *potpuno invarijantna,* $\zeta_\alpha\mathbf{G}$ *karakteristična podgrupa i* $\gamma_\alpha\mathbf{G}/\gamma_{\alpha+1}\mathbf{G} \leq \mathbf{Z}(\mathbf{G}/\gamma_{\alpha+1}\mathbf{G})$.

**Dokaz.** Transfinitnom indukcijom. $\gamma_0\mathbf{G} = \mathbf{G}$ je trivijalno potpuno invarijantna podgrupa, a ako je $\gamma_\alpha\mathbf{G}$ potpuno invarijantna podgrupa, onda je i

$\gamma_{\alpha+1}\mathbf{G} = [\gamma_\alpha\mathbf{G}, \mathbf{G}]$ potpuno invarijantna podgrupa (videti dokaz leme 6.10($a$)). Ako je $\alpha$ granični ordinal i ako su sve podgrupe $\gamma_\beta\mathbf{G}$, $\beta < \alpha$, potpuno invarijantne, onda je i $\gamma_\alpha\mathbf{G} = \bigcap_{\beta<\alpha}\gamma_\beta\mathbf{G}$ potpuno invarijantna podgrupa (5.24).

Pretpostavimo sada da je $\zeta_\alpha\mathbf{G}$ karakteristična podgrupa ($\zeta_0\mathbf{G} = \mathbf{E}$ je to sigurno) i neka je $\varphi \in Aut(\mathbf{G})$. Tada je preslikavanje $\psi : G/\zeta_\alpha G \longrightarrow G/\zeta_\alpha G$, dato sa $(g\,\zeta_\alpha G)\psi = (g)\varphi\,\zeta_\alpha G$, automorfizam grupe $\mathbf{G}/\zeta_\alpha\mathbf{G}$. Homomorfnost i surjektivnost su očigledni, a dobra definisanost i injektivnost su posledica karakterističnosti podgrupe $\zeta_\alpha\mathbf{G}$; tako je za $g, h \in G$: $g\,\zeta_\alpha G = h\,\zeta_\alpha G$ akko je $h^{-1}g \in \zeta_\alpha G$ akko je $(h^{-1}g)\varphi \in \zeta_\alpha G$ akko je $(g)\varphi\,\zeta_\alpha G = (h)\varphi\,\zeta_\alpha G$. Kako je centar uvek karakteristična podgrupa, to je, za dato $a \in \zeta_{\alpha+1}G$, $(a\,\zeta_\alpha G)\psi = (a)\varphi\,\zeta_\alpha G \in Z(\mathbf{G}/\zeta_\alpha\mathbf{G}) = \zeta_{\alpha+1}G/\zeta_\alpha G$, pa je, za neko $b \in \zeta_{\alpha+1}G$, $(a)\varphi\,\zeta_\alpha G = b\,\zeta_\alpha G$ i, stoga $(a)\varphi \in \zeta_{\alpha+1}G$.

Ako je $\alpha$ granični ordinal, ponovo se pozivamo na 5.24 – unija karakterističnih podgrupa je karakteristična podgrupa.

Poslednji deo tvrđenja direktno proveravamo. Neka je $a \in \gamma_\alpha G$ i $g \in G$. Onda je $(a\,\gamma_{\alpha+1}G)^{-1}\cdot(g\,\gamma_{\alpha+1}G)^{-1}\cdot(a\,\gamma_{\alpha+1}G)\cdot(g\,\gamma_{\alpha+1}G) = a^{-1}g^{-1}ag\,\gamma_{\alpha+1}G = [a,g]\,\gamma_{\alpha+1}G = \gamma_{\alpha+1}G$, te je $a\,\gamma_{\alpha+1}G \cdot g\,\gamma_{\alpha+1}G = g\,\gamma_{\alpha+1}G \cdot a\,\gamma_{\alpha+1}G$.□

**Lema 46.25** *Za ma koju grupu* $\mathbf{G}$, *(ma koju) njenu normalnu podgrupu* $\mathbf{N}$ *i ma koje prirodne brojeve* $i, j$ *važi:*

(1) $[\gamma_i\mathbf{G}, \gamma_j\mathbf{G}] \leq \gamma_{i+j+1}\mathbf{G}$;

(2) $\gamma_i(\gamma_j\mathbf{G}) \leq \gamma_{(i+1)j}\mathbf{G}$;

(3) $[\gamma_i\mathbf{G}, \zeta_j\mathbf{G}] \leq \zeta_{j-(i+1)}\mathbf{G}$ *ako je* $j \geq i+1$; *posebno,* $[\gamma_i\mathbf{G}, \zeta_{i+1}\mathbf{G}] = \mathbf{E}$;

(4) $\zeta_i(\mathbf{G}/\zeta_j\mathbf{G}) = \zeta_{i+j}\mathbf{G}/\zeta_j\mathbf{G}$;

(5) $\gamma_n(\mathbf{G}/\mathbf{N}) = (\gamma_n\mathbf{G}\cdot\mathbf{N})/\mathbf{N}$.

**Dokaz.** (1) Indukcijom po $i$. Slučaj $i = 0$ je trivijalan: $[\gamma_0\mathbf{G}, \gamma_j\mathbf{G}] = \gamma_{j+1}\mathbf{G}$. Pretpostavimo da je $[\gamma_k\mathbf{G}, \gamma_l\mathbf{G}] \leq \gamma_{k+l+1}\mathbf{G}$ za svako $k \leq i$ i svako $l$. Tada je, prema 6.10($b$), prethodnoj lemi i induktivnoj hipotezi:

$$[\gamma_{i+1}\mathbf{G}, \gamma_j\mathbf{G}] = [[\gamma_i\mathbf{G}, \mathbf{G}], \gamma_j\mathbf{G}] \leq [[\gamma_j\mathbf{G}, \gamma_i\mathbf{G}], \mathbf{G}]\cdot[[\mathbf{G}, \gamma_j\mathbf{G}], \gamma_i\mathbf{G}] \leq$$

$$[\gamma_{i+j+1}\mathbf{G}, \mathbf{G}]\cdot[\gamma_{j+1}\mathbf{G}, \gamma_i\mathbf{G}] \leq \gamma_{i+j+2}\mathbf{G}\cdot\gamma_{i+j+2}\mathbf{G} = \gamma_{(i+1)+j+1}\mathbf{G}.$$

(2) Indukcijom po $i$. Za $i = 0$ je očigledno $\gamma_0(\gamma_j\mathbf{G}) = \gamma_j\mathbf{G} = \gamma_{1\cdot j}\mathbf{G}$. Neka je tvrđenje tačno za svako $k \leq i$. Onda je prema induktivnoj hipotezi i prethodnoj tački

$$\gamma_{i+1}(\gamma_j\mathbf{G}) = [\gamma_i(\gamma_j\mathbf{G}), \gamma_j\mathbf{G}] \leq [\gamma_{(i+1)j}\mathbf{G}, \gamma_j\mathbf{G}] \leq \gamma_{(i+1)j+j+1}\mathbf{G} \leq \gamma_{((i+1)+1)j}\mathbf{G}.$$

(3) Indukcijom po $i$. Za $i = 0$ (dakle, $j \geq 1$) je trivijalno $[\gamma_0\mathbf{G}, \zeta_j\mathbf{G}] = [\mathbf{G}, \zeta_j\mathbf{G}] \leq \zeta_{j-1}\mathbf{G}$ (46.21). Pretpostavimo da je tvrđenje tačno za svako $k \leq i$ i svako $l \geq k+1$. Onda je, prema induktivnoj hipotezi i (opet) 46.21, za $j \geq i+2$: $[\gamma_{i+1}\mathbf{G}, \zeta_j\mathbf{G}] = [[\gamma_i\mathbf{G}, \mathbf{G}], \zeta_j\mathbf{G}] \leq [[\zeta_j\mathbf{G}, \gamma_i\mathbf{G}], \mathbf{G}]\cdot[[\mathbf{G}, \zeta_j\mathbf{G}], \gamma_i\mathbf{G}] \leq [\zeta_{j-(i+1)}\mathbf{G}, \mathbf{G}]\cdot[\zeta_{j-1}\mathbf{G}, \gamma_i\mathbf{G}] \leq \zeta_{j-(i+2)}\mathbf{G}$.

(4) Indukcijom po $i$. Slučaj $i = 0$ je trivijalan: $\zeta_0(\mathbf{G}/\zeta_j\mathbf{G})$ i $\zeta_j\mathbf{G}/\zeta_j\mathbf{G}$ su jedinične grupe. U induktivnom koraku imamo:

$$\zeta_{i+1}(\mathbf{G}/\zeta_j\mathbf{G})/\zeta_i(\mathbf{G}/\zeta_j\mathbf{G}) = \mathbf{Z}((\mathbf{G}/\zeta_j\mathbf{G})/\zeta_i(\mathbf{G}/\zeta_j\mathbf{G})) =$$

$$\mathbf{Z}((\mathbf{G}/\zeta_j\mathbf{G})/(\zeta_{i+j}\mathbf{G}/\zeta_j\mathbf{G})) \cong \mathbf{Z}(\mathbf{G}/\zeta_{i+j}\mathbf{G}) = \zeta_{i+j+1}\mathbf{G}/\zeta_{i+j}\mathbf{G} \cong$$

$$(\zeta_{i+j+1}\mathbf{G}/\zeta_j\mathbf{G})/(\zeta_{i+j}\mathbf{G}/\zeta_j\mathbf{G}) = (\zeta_{i+j+1}\mathbf{G}/\zeta_j\mathbf{G})/\zeta_i(\mathbf{G}/\zeta_j\mathbf{G}),$$

i stoga je $\zeta_{i+1}(\mathbf{G}/\zeta_j\mathbf{G}) = \zeta_{i+j+1}\mathbf{G}/\zeta_j\mathbf{G}$ (primetimo da se u slučaju datih izomorfizama radi zapravo o inverznim preslikavanjima).

(5) Tvrđenje je očigledno za $i = 0$, a za $i = 1$ tu je lema 6.22: $\gamma_1(\mathbf{G}/\mathbf{N}) = (\mathbf{G}/\mathbf{N})' = (\mathbf{G}'\cdot\mathbf{N})/\mathbf{N} = (\gamma_1\mathbf{G}\cdot\mathbf{N})/\mathbf{N}$. U induktivnom koraku imamo: $\gamma_{i+1}(\mathbf{G}/\mathbf{N}) = [\gamma_i(\mathbf{G}/\mathbf{N}), \mathbf{G}/\mathbf{N}] = [(\gamma_i\mathbf{G}\cdot\mathbf{N})/\mathbf{N}, \mathbf{G}/\mathbf{N}] = (\gamma_{i+1}\mathbf{G}\cdot\mathbf{N})/\mathbf{N}$ – dokaz poslednje jednakosti u potpunosti je analogan dokazu leme 6.22.□



**Lema 46.26** *Neka je* $\mathbf{G} = \mathbf{HK}$, *gde je* $\mathbf{K}$ *normalna podgrupa. Tada za svaki prirodan broj* $m$ *važi:*

$\mathbf{G}^{(m)} \leq \mathbf{H}^{(m)}\mathbf{K}$;

$\gamma_m\mathbf{G} \leq \gamma_m\mathbf{H}\,\mathbf{K}$.

**Dokaz.** Trivijalan; indukcijom po $m$ sa korišćenjem tačaka ($d$) i ($e$) leme 6.2.□

**Lema 46.27** *Ako je* $\mathbf{A}$ *normalna podgrupa grupe* $\mathbf{G}$, *tada za (svaki) prirodan broj* $n$ *važi:* $\mathbf{A} \leq \zeta_n\mathbf{G}$ *akko je* $[\mathbf{A}, \underbrace{\mathbf{G}, \ldots, \mathbf{G}}_{n-puta}] = \mathbf{E}$.

**Dokaz.** ($\Longrightarrow$) Indukcijom po $n$. Ako je $n = 0$, onda je $\mathbf{A} = \mathbf{E}$ i po definiciji je $[\mathbf{E}] = \mathbf{E}$. Slično, za $n = 1$ je $[\mathbf{A}, \mathbf{G}] \leq [\mathbf{Z}(\mathbf{G}), \mathbf{G}] = \mathbf{E}$. Pretpostavimo da je tvrđenje tačno za svako $k < n+1$ i neka je $\mathbf{A} \leq \zeta_{n+1}\mathbf{G}$. Tada je, prema 46.21, $[\mathbf{A}, \mathbf{G}] \leq [\zeta_{n+1}\mathbf{G}, \mathbf{G}] \leq \zeta_n\mathbf{G}$, pa je prema induktivnoj hipotezi

$$[[\mathbf{A}, \mathbf{G}], \underbrace{\mathbf{G}, \ldots, \mathbf{G}}_{n-puta}] = [\mathbf{A}, \underbrace{\mathbf{G}, \ldots, \mathbf{G}}_{n+1-puta}] = \mathbf{E}.$$

($\Longleftarrow$) Analogno, indukcijom po $n$. Slučajevi $n = 0, 1$ su trivijalni, a ako tvrđenje važi za $n$ ($\geq 1$) izvodimo: ako je $[\mathbf{A}, \underbrace{\mathbf{G}, \ldots, \mathbf{G}}_{n+1-puta}] = [[\mathbf{A}, \mathbf{G}], \underbrace{\mathbf{G}, \ldots, \mathbf{G}}_{n-puta}] = \mathbf{E}$, tada je prema induktivnoj pretpostavci $[\mathbf{A}, \mathbf{G}] \leq \zeta_n\mathbf{G}$ i stoga je:

$$[(\mathbf{A}\zeta_n\mathbf{G})/\zeta_n\mathbf{G}, \mathbf{G}/\zeta_n\mathbf{G}] = ([\mathbf{A}, \mathbf{G}]\zeta_n\mathbf{G})/\zeta_n\mathbf{G}\ (= \overline{\mathbf{E}});$$

dakle, $(\mathbf{A}\zeta_n\mathbf{G})/\zeta_n\mathbf{G} \leq \mathbf{Z}(\mathbf{G}/\zeta_n\mathbf{G}) = \zeta_{n+1}\mathbf{G}/\zeta_n\mathbf{G}$, a onda je i $\mathbf{A} \leq \zeta_{n+1}\mathbf{G}$.□

**Lema 46.28** *Neka je* $\{g_\alpha \mid \alpha < \lambda\}$ *generatorni skup grupe* $\mathbf{G}$. *Tada je* $\{[g_{\alpha_1}, \dots, g_{\alpha_i}]\gamma_i G \mid \alpha_j < \lambda\}$ *generatorni skup grupe* $\gamma_{i-1}\mathbf{G}/\gamma_i\mathbf{G}$ *za svaki pozitivan prirodan broj* $i$.

**Dokaz**. Ovde, posebno, za $i = 1$ uzimamo da je $[g_\alpha] = g_\alpha$. Dokaz je indukcijom po $i$. S obzirom na uvedenu konvenciju, za $i = 1$ tvrđenje trivijalno važi. Pretpostavimo da je tvrđenje tačno za svako $j < i$. Kako je $\gamma_i\mathbf{G} = [\gamma_{i-1}\mathbf{G}, \mathbf{G}]$, to je grupa $\gamma_i\mathbf{G}/\gamma_{i+1}\mathbf{G}$ generisana skupom $\{[x,y]\gamma_{i+1}G \mid x \in \gamma_{i-1}G,\ y \in G\}$. Prema induktivnoj hipotezi je svako $x$ iz $\gamma_{i-1}G$ oblika $(b_1 \dots b_m)z$, gde je, opet, svako $b_j$ iz $\gamma_{i-1}G$ oblika $[g_{\alpha_1}, \dots, g_{\alpha_i}]^k$, $k \in \{1, -1\}$, dok je $z \in \gamma_i G$. Stavimo: $b = b_1 \dots b_m$. Onda je prema 6.2($d$): $[x,y] = [bz,y] = z^{-1}[b,y]z \cdot [z,y] = [b,y] \cdot [[b,y],z] \cdot [z,y]$ $(= [b,y] \cdot [b,y,z] \cdot [z,y])$, i pošto je $[b,y,z], [z,y] \in \gamma_{i+1}G$, to je $[x,y]\gamma_{i+1}G = [b,y]\gamma_{i+1}G$. No, $[b_1 \dots b_m, y]\gamma_{i+1}G = [b_1,y] \dots [b_m,y]\gamma_{i+1}G$; jer, za $m = 2$ (a taj slučaj objašnjava sve) izvodimo kao i maločas: $[b_1b_2,y]\gamma_{i+1}G = ([b_1,y] \cdot [[b_1,y],b_2] \cdot [b_2,y])\gamma_{i+1}G = ([b_1,y] \cdot [b_2,y])\gamma_{i+1}G$ ($b_1 \in \gamma_{i-1}G$ implicira $[[b_1,y],b_2] \in \gamma_{i+1}G$). Ako je za neko $j$, $1 \le j \le m$, $b_j = [g_{\alpha_1}, \dots, g_{\alpha_i}]^{-1}$, tada je prema 6.2($c$):

$$[[g_{\alpha_1}, \dots, g_{\alpha_i}]^{-1}, y]\gamma_{i+1}G =$$

$$([g_{\alpha_1}, \dots, g_{\alpha_i}] \cdot [[g_{\alpha_1}, \dots, g_{\alpha_i}], y]^{-1} \cdot [g_{\alpha_1}, \dots, g_{\alpha_i}]^{-1})\gamma_{i+1}G =$$

$$([[g_{\alpha_1}, \dots g_{\alpha_i}], y]^{-1} \cdot [[[g_{\alpha_1}, \dots, g_{\alpha_i}], y]^{-1}, [g_{\alpha_1}, \dots, g_{\alpha_i}]^{-1}])\gamma_{i+1}G =$$

$$([[g_{\alpha_1}, \dots, g_{\alpha_i}], y]\gamma_{i+1}G)^{-1}$$

(zbog $[[g_{\alpha_1}, \dots, g_{\alpha_i}], y]^{-1} \in \gamma_i G$). Konačno, ako je $g = g_{\beta_1}^{k_1} \dots g_{\beta_n}^{k_n}$, $\beta_j < \lambda$, $k_j \in \{1, -1\}$, i $a = [g_{\alpha_1}, \dots, g_{\alpha_i}]$, imamo:

$$[a,g]\gamma_{i+1}G = [a, g_{\beta_1}^{k_1} \dots g_{\beta_n}^{k_n}]\gamma_{i+1}G = ([a,g_{\beta_n}]\gamma_{i+1}G)^{k_n} \dots ([a,g_{\beta_1}]\gamma_{i+1}G)^{k_1}.$$

Dokažimo ovo za slučaj $n = 2$ koristeći 6.2($e$) (indukcija lako sve uopštava):

$$[a, g_{\beta_1}^{k_1} g_{\beta_2}^{k_2}]\gamma_{i+1}G = ([a, g_{\beta_2}^{k_2}]g_{\beta_2}^{-k_2}[a, g_{\beta_1}^{k_1}]g_{\beta_2}^{k_2})\gamma_{i+1}G =$$

$$([a, g_{\beta_2}^{k_2}] \cdot [a, g_{\beta_1}^{k_1}] \cdot [[a, g_{\beta_1}^{k_1}], g_{\beta_2}^{k_2}])\gamma_{i+1}G = ([a, g_{\beta_2}^{k_2}]\gamma_{i+1}G) \cdot ([a, g_{\beta_1}^{k_1}]\gamma_{i+1}G),$$

a recimo,

$$[a, g_\beta^{-1}]\gamma_{i+1}G = (g_\beta[a,g_\beta]^{-1}g_\beta^{-1})\gamma_{i+1}G =$$

$$([a,g_\beta]^{-1} \cdot [[a,g_\beta]^{-1}, g_\beta^{-1}])\gamma_{i+1}G = ([a,g_\beta]\gamma_{i+1}G)^{-1}.\square$$

**Korolar 46.29** *Ako je grupa* $\mathbf{G}$ *konačno generisana, onda je za svaki pozitivan prirodan broj* $m$ *i grupa* $\gamma_{m-1}\mathbf{G}/\gamma_m\mathbf{G}$ *konačno generisana.*

**Lema 46.30** *Neka je* $\mathbf{G} = \mathbf{H}\gamma_1\mathbf{K}$, *gde je* $\mathbf{H}$ *podgrupa i* $\mathbf{K}$ *normalna podgrupa grupe* $\mathbf{G}$. *Tada je* $\mathbf{G} = \mathbf{H}\gamma_i\mathbf{K}$ *za svako pozitivno* $i$.



**Dokaz**. Indukcijom. Slučaj $i = 1$ je upravo uslov korolara. Pretpostavimo da je $\mathbf{G} = \mathbf{H}\gamma_i\mathbf{K}$ za $i$ ($\ge 1$). Pokazujemo da je $\gamma_i\mathbf{K} \le \mathbf{H}\gamma_{i+1}\mathbf{K}$, a onda je, naravno, $\mathbf{G} = \mathbf{H}\gamma_{i+1}\mathbf{K}$. Ako je u $[a_1, \dots, a_{i+1}]$, $a_j \in K$, $j = 1, \dots, i+1$, bar jedan od elemenata $a_j$ iz $\gamma_m K$, $m \ge 1$, tada je $[a_1, \dots, a_{i+1}] \in \gamma_{i+1}K$. Nije problem ni ako su svi elementi iz $\mathbf{H}$. Neka je stoga $a_j \in K \setminus \gamma_1 K$ za svako $j$, $1 \le j \le i+1$, i neka je $a_j = b_j h_j$, gde je $b_j \in \gamma_1 K$, $h_j \in H$ $(\cap K \setminus \gamma_1 K)$. Tada je prema 6.2($e$):

$$[a_1, \dots, a_i, b_{i+1}h_{i+1}] = [a_1, \dots, a_i, h_{i+1}] \cdot h_{i+1}^{-1}[a_1, \dots, a_i, b_{i+1}]h_{i+1}.$$

Kako je $h_{i+1}^{-1}[a_1, \dots, a_i, b_{i+1}]h_{i+1} \in \gamma_{i+1}K$, skoncentrišimo se na $[a_1, \dots, a_i, h_{i+1}] = [[[a_1, \dots, a_{i-1}], b_i h_i], h_{i+1}]$. Ponovo je prema 6.2($e$):

$$[[[a_1, \dots, a_{i-1}], b_i h_i], h_{i+1}] = [[a_1, \dots, a_{i-1}, h_i] \cdot h_i^{-1}[a_1, \dots, a_{i-1}, b_i]h_i, h_{i+1}] =$$

$$(h_i^{-1}[a_1, \dots, a_{i-1}, b_i]h_i)^{-1}[a_1, \dots, a_{i-1}, h_i, h_{i+1}]h_i^{-1}[a_1, \dots, a_{i-1}, b_i]h_i \cdot$$
$$[h_i^{-1}[a_1, \dots, a_{i-1}, b_i]h_i, h_{i+1}] =$$
$$[a_1, \dots, a_{i-1}, h_i, h_{i+1}] \cdot [[a_1, \dots, a_{i-1}, h_i, h_{i+1}], h^{-1}[a_1, \dots, a_{i-1}, b_i]h_i] \cdot$$
$$[h_i^{-1}[a_1, \dots, a_{i-1}, b_i]h_i, h_{i+1}].$$

Očigledno je

$$[[a_1, \dots, a_{i-1}, h_i, h_{i+1}], h^{-1}[a_1, \dots, a_{i-1}, b_i]h_i] \cdot [h_i^{-1}[a_1, \dots, a_{i-1}, b_i]h_i, h_{i+1}]$$

element grupe $\gamma_{i+1}\mathbf{K}$ i, evidentno, sukcesivnim ponavljanjem postupka dobili bismo da su svi faktori polaznog elementa ili iz $\gamma_{i+1}\mathbf{K}$ ili iz $\mathbf{H}$.$\square$

**Lema 46.31** *Ako je centar grupe* $\mathbf{G}$ *torziono slobodna grupa, onda su i svi faktori višeg centralnog lanca torziono slobodne grupe.*

**Dokaz**. Pretpostavimo da je, za neko $a \in \zeta_2 G$ i neki pozitivan prirodan broj $m$, $a^m \in \zeta_1 G = Z(\mathbf{G})$. Pošto je $[a,g] \in \zeta_1 G$ za svako $g \in G$ (jer je $\zeta_2\mathbf{G}/\zeta_1\mathbf{G} = \mathbf{Z}(\mathbf{G}/\zeta_1\mathbf{G})$ i odatle: $a\zeta_1 G \cdot g\zeta_1 G = g\zeta_1 G \cdot a\zeta_1 G$, tj. $[a,g]\zeta_1 G = \zeta_1 G$), sledi prema 6.2($h$): $[a,g]^m = [a^m, g] = e$. No tada je $[a,g] = e$ ($\zeta_1\mathbf{G}$ je po pretpostavci torziono slobodna grupa), pa je $a \in \zeta_1 G$ $(= Z(\mathbf{G}))$. Analogno se pokazuje da je $\zeta_3\mathbf{G}/\zeta_2\mathbf{G}$ torziono slobodna grupa. Centar grupe $\overline{\mathbf{G}}_1 = \mathbf{G}/\zeta_1\mathbf{G} - \zeta_2\mathbf{G}/\zeta_1\mathbf{G}$ – je, upravo smo pokazali, torziono slobodna grupa, a prema 46.25(4) je $\zeta_2\overline{\mathbf{G}}_1 = \zeta_2(\mathbf{G}/\zeta_1\mathbf{G}) = \zeta_3\mathbf{G}/\zeta_1\mathbf{G}$, te je (déjà vu)

$$(\zeta_3\mathbf{G}/\zeta_1\mathbf{G})/(\zeta_2\mathbf{G}/\zeta_1\mathbf{G}) \cong \zeta_3\mathbf{G}/\zeta_2\mathbf{G}$$

torziono slobodna grupa. Jasno, da bismo pokazali da je $\zeta_4\mathbf{G}/\zeta_3\mathbf{G}$ torziono slobodna grupa, krenuli bismo od grupe $\overline{\mathbf{G}}_2 = \mathbf{G}/\zeta_2\mathbf{G}$ (sa centrom $\zeta_3\mathbf{G}/\zeta_2\mathbf{G}$) i tako dalje.$\square$

**Lema 46.32** *Članovi transfinitno produženog višeg centralnog lanca R-grupe* $\mathbf{G}$ *su izolovane podgrupe, faktori* $\zeta_{\alpha+1}\mathbf{G}/\zeta_\alpha\mathbf{G}$ *su Abelove torziono slobodne grupe, a* $\mathbf{G}/\zeta_\alpha\mathbf{G}$ *R-grupe.*

**Dokaz**. Transfinitnom indukcijom po $\alpha \geq 1$. $\zeta_1\mathbf{G} = \mathbf{Z}(\mathbf{G})$ je, već smo videli – 4.45($b$), izolovana podgrupa, pokazali smo i da je $\mathbf{G}/\zeta_1\mathbf{G}$ $R$-grupa – 4.47, a trivijalno, $\zeta_1\mathbf{G}/\zeta_0\mathbf{G}$ ($\cong \zeta_1\mathbf{G}$) je Abelova torziono slobodna grupa. Pretpostavimo da je tvrđenje tačno za svako $\beta < \alpha$ ($> 1$). Ako je $\alpha$ naredni ordinal, onda pošto je $\mathbf{G}/\zeta_{\alpha-1}\mathbf{G}$ $R$-grupa, to je i njen centar – $\zeta_\alpha\mathbf{G}/\zeta_{\alpha-1}\mathbf{G}$ – Abelova torziono slobodna i izolovana podgrupa, te je prema 8.17 $\zeta_\alpha\mathbf{G}$ izolovana podgrupa grupe $\mathbf{G}$. Takođe je, opet prema 4.47,

$$\mathbf{G}/\zeta_\alpha\mathbf{G} \cong (\mathbf{G}/\zeta_{\alpha-1}\mathbf{G})/(\zeta_\alpha\mathbf{G}/\zeta_{\alpha-1}\mathbf{G})$$

$R$-grupa. Ako je $\alpha$ granični ordinal, očigledno je $\zeta_\alpha\mathbf{G} = \bigcup_{\beta<\alpha}\zeta_\beta\mathbf{G}$, kao unija izolovanih podgrupa, izolovana podgrupa. Isto tako, ako za $a, b \in G$ važi $(a\,\zeta_\alpha G)^n = (b\,\zeta_\alpha G)^n$, sledi $a^{-n}b^n \in \zeta_\alpha G$, tj. $a^{-n}b^n \in \zeta_\beta G$ za neko $\beta < \alpha$. Pošto je po pretpostavci $\mathbf{G}/\zeta_\beta\mathbf{G}$ $R$-grupa, iz $(a\,\zeta_\beta G)^n = (b\,\zeta_\beta G)^n$ sledi $a\,\zeta_\beta G = b\,\zeta_\beta G$, a onda i $a\,\zeta_\alpha G = b\,\zeta_\alpha G$.□

## 47 Normalni i invarijantni sistemi

U ovom paragrafu ćemo razmotriti uopštenja nekih od rezultata iz prethodnog.

**Definicija 47.1** *Sistem (familija) podgrupa grupe* $\mathbf{G}$ *koji sadrži jediničnu podgrupu i celu grupu i linearno je uređen relacijom inkluzije zove se uređen sistem podgrupa, a njegovi elementi su termi. Ako između dva terma nema trećeg, onda kažemo da oni čine (obrazuju, formiraju) skok (eng. jump).*

*Uređen sistem je potpun (kompletan) akko je unija i presek svakog njegovog podsistema ujedno i njegov term.*

Kada pišemo za uređeni sistem podgrupa $\mathcal{S}$ grupe $\mathbf{G}$: $\mathcal{S} = \{\mathbf{H}_\alpha \mid 0 \leq \alpha \leq \mu\}$ ili, recimo, $\mathcal{S} = \{\mathbf{H}_\alpha \mid \alpha \in \Omega\}$, onda podrazumevamo da $\alpha$ "ide" nekim skupom indeksa ($\Omega$) linearno uređenim relacijom $\leq$ (koristimo istu oznaku kao i za uređenje grupa), kao i da je $\mathbf{H}_0 = \mathbf{E}$, $\mathbf{H}_\mu = \mathbf{G}$, a za $\alpha < \beta$ (tj. $\alpha \leq \beta$ i $\alpha \neq \beta$) $\mathbf{H}_\alpha$ prava podgrupa grupe $\mathbf{H}_\beta$; i kad stavimo samo $\Omega$, 0 će biti, u opštoj priči, najmanji element. Naslednika elementa $\alpha$ (odnosno element kome neposredno prethodi $\alpha$), ukoliko postoji, označavaćemo sa $\alpha + 1$ (po uzoru na notaciju ordinalne aritmetike). Jasno, parovi elemenata i njihovih naslednika su u uzajamno jednoznačnoj korespondenciji sa skokovima u $\mathcal{S}$.

**Lema 47.2** *Svaki uređen sistem podgrupa* $\mathcal{S}$ *(ma koje) grupe* $\mathbf{G}$ *može se kompletirati.*



**Dokaz**. Uređen par $(\mathcal{S}_1, \mathcal{S}_2)$, gde su $\mathcal{S}_1$ i $\mathcal{S}_2$ neprazni disjunktni podskupovi sistema $\mathcal{S}$ takvi da važi: $\mathcal{S}_1 \cup \mathcal{S}_2 = \mathcal{S}$, $\mathcal{S}_1$ je zatvoren naniže (ako je podgrupa $\mathbf{H}$ u $\mathcal{S}_1$, onda su u $\mathcal{S}_1$ i sve njene podgrupe koje su elementi sistema $\mathcal{S}$) i $\mathcal{S}_1$ je bez maksimalnog elementa, zove se *Dedekindov presek* sistema $\mathcal{S}$ (videti komentar uz lemu 33.42). Evidentno, $\mathcal{S}$ je potpun sistem akko sadrži uniju prve i presek druge "komponente" svakog (svog) Dedekindovog preseka $(\mathcal{S}_1, \mathcal{S}_2)$ – $\bigcup\mathcal{S}_1 \stackrel{\text{def}}{=} \bigcup\{\mathbf{H} \mid \mathbf{H} \in \mathcal{S}_1\}$, $\bigcap\mathcal{S}_2 \stackrel{\text{def}}{=} \bigcap\{\mathbf{K} \mid \mathbf{K} \in \mathcal{S}_2\}$. Stoga je dovoljno za sve Dedekindove preseke "ubaciti" u $\mathcal{S}$ (ukoliko već nisu tamo) unije prvih i preseke drugih klasa (nije isključeno da se koji put radi o istim podgrupama). Neka je $\overline{\mathcal{S}}$ novodobijeni sistem. Proveravamo prvo da je i on linearno uređen. Pretpostavimo suprotno: neka $\mathbf{H}, \mathbf{K} \in \overline{\mathcal{S}}$ i neka nijedna od ovih podgrupa nije sadržana u onoj drugoj. Jasno, bar jedna od njih nije u $\mathcal{S}$, recimo da nijedna nije u $\mathcal{S}$. Neka je $\mathbf{H} = \bigcup\mathcal{S}_1$, $\mathbf{K} = \bigcup\mathcal{T}_1$, gde su, naravno, $\mathcal{S}_1$ i $\mathcal{T}_1$ "prve" klase Dedekindovih preseka (sistema $\mathcal{S}$). No, ili je $\mathcal{T}_1 \subset \mathcal{S}_1$ ili je $\mathcal{S}_1 \subset \mathcal{T}_1$ (zaista, ako bismo imali $\mathbf{M} \in \mathcal{S}_1 \setminus \mathcal{T}_1$, $\mathbf{N} \in \mathcal{T}_1 \setminus \mathcal{S}_1$ i na primer $\mathbf{N} < \mathbf{M}$, sledilo bi, zbog zatvorenosti naniže klase $\mathcal{S}_1$, $\mathbf{N} \in \mathcal{S}_1$, kontradikcija). Ali, $\mathcal{T}_1 \subset \mathcal{S}_1$ povlači $\mathbf{K} \leq \mathbf{H}$ i opet kontradikcija. Slično bismo rezonovali i u slučaju $\mathbf{H} = \bigcap\mathcal{S}_2$, $\mathbf{K} = \bigcap\mathcal{T}_2$. Ako je pak $\mathbf{H} = \bigcup\mathcal{S}_1$, $\mathbf{K} = \bigcap\mathcal{T}_2$ i npr. $\mathcal{S}_1 \subseteq \mathcal{T}_1$, tada je $\mathbf{H} \leq \bigcup\mathcal{T}_1 \leq \bigcap\mathcal{T}_2 = \mathbf{K}$; s druge strane, ako je $\mathcal{T}_1 \subset \mathcal{S}_1$ i $\mathbf{M} \in \mathcal{S}_1 \setminus \mathcal{T}_1$, tada je $\mathbf{M} \in \mathcal{T}_2$ i $\mathbf{K} = \bigcap\mathcal{T}_2 \leq \mathbf{M} < \bigcup\mathcal{S}_1 = \mathbf{H}$, kontradikcija svakako. $\overline{\mathcal{S}}$ je i potpun sistem. Jer, neka je $\overline{\mathcal{T}} \subset \overline{\mathcal{S}}$, $\bigcup\overline{\mathcal{T}} \neq \mathbf{G}$ i neka je $\overline{\mathcal{T}}$ bez maksimalnog elementa. Ako je $\overline{\mathcal{S}}_1 = \{\mathbf{H} \in \overline{\mathcal{S}} \mid \mathbf{H} \leq \mathbf{K}$ za neko $\mathbf{K} \in \overline{\mathcal{T}}\}$, onda je $\bigcup\overline{\mathcal{S}}_1 = \bigcup\overline{\mathcal{T}}$. Neka je dalje $\mathcal{S}_1 = \{\mathbf{M} \in \mathcal{S} \mid \mathbf{M} \in \overline{\mathcal{S}}_1\}$. $\mathcal{S}_1$ je prva klasa Dedekindovog preseka: neprazna je, očigledno je zatvorena naniže a nema ni maksimalnog elementa. Na primer, ako je $\mathbf{N} < \mathbf{K}$, $\mathbf{N} \in \mathcal{S}_1$, $\mathbf{K} \in \overline{\mathcal{S}}_1 \setminus \mathcal{S}_1$ i $\mathbf{K} = \bigcap\mathcal{D}_2$ za neki Dedekindov presek $(\mathcal{D}_1, \mathcal{D}_2)$, tada imamo u $\mathcal{S}_1$, pošto je $\overline{\mathcal{S}}_1$ bez maksimalnog elementa, neki term $\mathbf{L}$ za koji je $\mathbf{K} < \mathbf{L}$. Slično se tretiraju i ostali slučajevi, a lako se pokazuje i da je $\bigcup\overline{\mathcal{S}}_1 = \bigcup\mathcal{S}_1 (= \bigcup\overline{\mathcal{T}})$ kao i da je presek svakog nepraznog podsistema (sistema $\overline{\mathcal{S}}$) term u $\overline{\mathcal{S}}$.□

**Lema 47.3** *Skup skokova je gust u potpunom sistemu podgrupa.*

**Dokaz**. Ovo tvrđenje znači: između svaka dva različita terma potpunog sistema podgrupa $\mathcal{S}$ grupe $\mathbf{G}$ imamo terme koji obrazuju skok. Odista, ako $\mathbf{H}, \mathbf{K} \in \mathcal{S}$ i $\mathbf{H} < \mathbf{K}$, uzmimo bilo koji element $g$ iz $K \setminus H$. Onda su $\mathbf{N} = \bigcup\{\mathbf{L} \in \mathcal{S} \mid g \notin L\}$ i $\mathbf{P} = \bigcap\{\mathbf{M} \in \mathcal{S} \mid g \in M\}$ termi u $\mathcal{S}$ koji obrazuju skok i $\mathbf{H} \leq \mathbf{N} < \mathbf{P} \leq \mathbf{K}$.□

**Definicija 47.4** *Potpuni sistem* $\mathcal{S}$ *podgrupa grupe* $\mathbf{G}$ *je normalan sistem akko je za svaka dva terma* $\mathbf{H}$ *i* $\mathbf{K}$ *koji obrazuju skok* $\mathbf{H}$ *normalna podgrupa grupe* $\mathbf{K}$. *Odgovarajuće faktor grupe* $\mathbf{K}/\mathbf{H}$ *(za svaki skok) su faktori normalnog sistema.*

*Invarijantan sistem podgrupa grupe* $\mathbf{G}$ *je potpun sistem čiji su svi termi normalne podgrupe.*

*Normalan (invarijantan) sistem $\mathcal{S}$ koji je dobro uređen, tj. oblika $\{\mathbf{H}_\alpha \mid \alpha \leq \mu\}$, gde je $\mu$ ordinal, zove se rastući normalni (invarijantan) niz.*

*Analogno se definiše opadajući normalni (invarijantni) niz: $\{\mathbf{H}_\alpha \mid \alpha \leq \mu\}$, gde je sada $\mathbf{H}_0 = \mathbf{G}$, $\mathbf{H}_\mu = \mathbf{E}$ i $\mathbf{H}_\alpha > \mathbf{H}_\beta$ za $\alpha < \beta$ (indeksni skup je, smatramo, uređen inverznom relacijom "standardne" relacije dobrog uređenja).*

*Proširenje normalnog (invarijantnog) sistema definiše se kao i proširenje normalnog (invarijantnog) niza. Normalni sistem bez pravih proširenja zove se kompozicioni sistem, invarijantni sistem bez pravih proširenja zove se glavni sistem.*

*Dva normalna sistema grupe $\mathbf{G}$ su izomorfna akko se među njihovim faktorima može uspostaviti uzajamno jednoznačna korespondencija takva da su korespondentni faktori izomorfni.*

**Napomena**. Primetimo da se u definiciji izomorfnosti normalnih sistema ne zahteva da su sistemi u pitanju istog linearnog uređenja.

Normalni i invarijantni nizovi podgrupa su primeri normalnih i invarijantnih sistema, preciznije normalnih i invarijantnih rastućih, odnosno opadajućih nizova. Prirodno je da ako krećemo od cele grupe u formiranju niza, recimo izvodnog niza podgrupa, samu grupu, neka je to $\mathbf{G}$, obeležimo sa $\mathbf{G}^{(0)}$ (ili $\mathbf{G}_0$ ili $\mathbf{H}_0$), sledeću – $\mathbf{G}'$ – sa $\mathbf{G}^{(1)}$ (ili $\mathbf{G}_1$ ili $\mathbf{H}_1$) i tako dalje , kao što smo, s druge strane, imali u primeru višeg centralnog niza (46.23): $\mathbf{E} = \zeta_0\mathbf{G}$, $\mathbf{Z}(\mathbf{G}) = \zeta_1\mathbf{G}$, ....

Ako je potpun sistem $\mathcal{T}$ podgrupa grupe $\mathbf{G}$ proširenje potpunog sistema $\mathcal{S}$ i ako je $\mathbf{H} \in \mathcal{T} \setminus \mathcal{S}$, tada $\mathbf{H}$ "upada" u jedan skok sistema $\mathcal{S}$. Zaista, kako je sistem $\mathcal{S}$ potpun, to su i $\mathbf{M} = \bigcup\{\mathbf{K} \in \mathcal{S} \mid \mathbf{K} < \mathbf{H}\}$ i $\mathbf{N} = \bigcap\{\mathbf{L} \in \mathcal{S} \mid \mathbf{H} < \mathbf{L}\}$ njegovi termi koji, jasno, obrazuju skok u koji upada $\mathbf{H}$ $(\mathbf{M} < \mathbf{H} < \mathbf{N})$.

**Lema 47.5** (*a*) *Svaki normalni sistem se može proširiti do kompozicionog.*
(*b*) *Svaki invarijantni sistem se može proširiti do glavnog.*

**Dokaz.** (*a*) Neka je $\mathcal{S}$ normalni sistem grupe $\mathbf{G}$. Ako već nije kompozicioni, formiramo (transfinitnom rekurzijom) normalne sisteme podgrupa $\mathcal{S}_\alpha$ ($\alpha$ ordinal) na sledeći način: $\mathcal{S}_0 = \mathcal{S}$; $\mathcal{S}_{\alpha+1}$ je pravo normalno proširenje sistema $\mathcal{S}_\alpha$, ukoliko već ovaj nije kompozicioni – u suprotnom stajemo; za granični ordinal $\alpha$ je $\mathcal{S}_\alpha$ sistem nastao kompletiranjem sistema $\bigcup_{\beta<\alpha}\mathcal{S}_\beta$ na način opisan u lemi 47.2. Da je i u poslednjem slučaju u pitanju normalni sistem lako se proverava. Linearna uređenost (sistema) je očigledna, a ako je $(\mathcal{T}_1, \mathcal{T}_2)$ jedan njegov Dedekindov presek, onda su za svako $\beta < \alpha$, s obzirom na potpunost sistema $\mathcal{S}_\beta$, $\mathbf{H}_\beta = \bigcup\{\mathbf{H} \in \mathcal{S}_\beta \mid \mathbf{H} \leq \mathbf{M}$ za neki term $\mathbf{M} \in \mathcal{T}_1\}$ i $\mathbf{K}_\beta = \bigcap\{\mathbf{K} \in \mathcal{S}_\beta \mid \mathbf{N} \leq \mathbf{K}$ za neki term $\mathbf{N} \in \mathcal{T}_2\}$ termi sistema $\mathcal{S}_\beta$. No, $\bigcup\mathcal{T}_1 = \bigcup_{\beta<\alpha}\mathbf{H}_\beta$, $\bigcap\mathcal{T}_2 = \bigcap_{\beta<\alpha}\mathbf{K}_\beta$. Inkluzija $\bigcup_{\beta<\alpha}\mathbf{H}_\beta \leq \bigcup\mathcal{T}_1$ je jasna. Ako je, s druge strane, $g \in \bigcup\mathcal{T}_1$, recimo, $g \in D = \bigcap\mathcal{D}_2 \in \mathcal{S}_\alpha$, gde je $\mathcal{D}_2$ druga klasa Dedekindovog preseka $(\mathcal{D}_1, \mathcal{D}_2)$ uređenog sistema $\bigcup_{\beta<\alpha}\mathcal{S}_\beta$, tada je $\bigcap\mathcal{D}_2 < \mathbf{L}$ za neko $\mathbf{L} \in \mathcal{T}_1$ (pošto je klasa $\mathcal{T}_1$ bez maksimalnog elementa) i stoga je $\mathbf{D} \leq \mathbf{H} < \mathbf{L}$ za neko $\mathbf{H} \in \mathcal{D}_2$; dakle, ako je $\mathbf{H} \in \mathcal{S}_\gamma$, onda je $g \in \mathbf{H}_\gamma$. Diskusija u drugim slučajevima je još trivijalnija. Preostaje da se dokaže normalnost. Ako termi $\mathbf{M}$ i $\mathbf{N}$ sistema $\mathcal{S}_\alpha$ obrazuju skok, tada i za svako $\beta < \alpha$ termi $\mathbf{M}_\beta = \bigcup\{\mathbf{H} \in \mathcal{S}_\beta \mid \mathbf{H} \leq \mathbf{M}\}$ i $\mathbf{N}_\beta = \bigcap\{\mathbf{K} \in \mathcal{S}_\beta \mid \mathbf{N} \leq \mathbf{K}\}$ sistema $\mathcal{S}_\beta$ formiraju skok; znači, $\mathbf{M}_\beta$ je normalna podgrupa grupe $\mathbf{N}_\beta$. Trivijalno, za $\gamma < \beta$ $(< \alpha)$ je $\mathbf{M}_\gamma \leq \mathbf{M}_\beta$, $\mathbf{N}_\beta \leq \mathbf{N}_\gamma$, a važi i: $\bigcup_{\beta<\alpha}\mathbf{M}_\beta \lhd \bigcap_{\beta<\alpha}\mathbf{N}_\beta$, $\bigcup_{\beta<\alpha}\mathbf{M}_\beta = \mathbf{M}$, $\bigcap_{\beta<\alpha}\mathbf{N}_\beta = \mathbf{N}$. Ponovo je inkluzija $\bigcup_{\beta<\alpha}\mathbf{M}_\beta \leq \mathbf{M}$ očigledna, a $\mathbf{M}$, ukoliko već nije element sistema $\bigcup_{\beta<\alpha}\mathcal{S}_\beta$, ne može biti presek druge klase nekog Dedekindovog preseka (uređenog) sistema $\bigcup_{\beta<\alpha}\mathcal{S}_\beta$ (jer čini skok sa $\mathbf{N}$), pa inkluzija $\mathbf{M} \leq \bigcup_{\beta<\alpha}\mathbf{M}_\beta$ direktno sledi.

Konačno, proces formiranja normalnih sistema $\mathcal{S}_\alpha$ se završava sa nekim ordinalom $\mu$ $(\mathcal{S}_\mu = \mathcal{S}_{\mu+1} = \cdots)$, a sistem $\mathcal{S}_\mu$ je evidentno kompozicioni.□

Sledeći rezultat je uopštenje leme 46.11.

**Lema 47.6** *Neka je $\mathcal{S}$ normalni (invarijantni) sistem podgrupa grupe $\mathbf{G}$ i $\mathbf{A}$ jedna podgrupa grupe $\mathbf{G}$. Tada $\mathbf{A}$ ima normalni (invarijantni) sistem čiji su faktori izomorfni podgrupama različitih faktora sistema $\mathcal{S}$.*

**Dokaz.** Sistem $\mathcal{T} = \{\mathbf{A} \cap \mathbf{H} \mid \mathbf{H} \in \mathcal{S}\}$ je sigurno uređen sistem podgrupa grupe $\mathbf{A}$, moguće sa ponavljanjem, i za svaki presek $\mathcal{T} = \mathcal{T}_1 \cup \mathcal{T}_2$, gde su $\mathcal{T}_1, \mathcal{T}_2$ neprazne disjunktne familije i $\mathcal{T}_1$ je zatvorena naniže, važi jedno od:

(1) $\mathcal{T}_1$ ima maksimalan, $\mathcal{T}_2$ ima minimalni element;

(2) $\mathcal{T}_1$ ima maksimalni element koji je presek (podgrupa) klase $\mathcal{T}_2$;

(3) $\mathcal{T}_2$ ima minimalni element koji je unija (podgrupa) klase $\mathcal{T}_1$.

Zaista, pretpostavimo da ni $\mathcal{T}_1$ nema maksimalnog ni $\mathcal{T}_2$ minimalnog elementa. Ali tada su $\mathcal{S}_1 = \{\mathbf{H} \in \mathcal{S} \mid \mathbf{H} \cap \mathbf{A} \in \mathcal{T}_1\}$ i $\mathcal{S}_2 = \{\mathbf{K} \in \mathcal{S} \mid \mathbf{K} \cap \mathbf{A} \in \mathcal{T}_2\}$ neprazne disjunktne familije podgrupa (grupe $\mathbf{G}$), $\mathcal{S}_1 \cup \mathcal{S}_2 = \mathcal{S}$ i familija $\mathcal{S}_1$ je zatvorena naniže. Neka je $\mathbf{M} = \bigcup\mathcal{S}_1$, $\mathbf{N} = \bigcap\mathcal{S}_2$ (jasno, to su termi iz $\mathcal{S}$). Ako bi podgrupa $\mathbf{M} \cap \mathbf{A}$ bila u $\mathcal{T}_1$, bila bi i maksimalni element tog skupa ($\mathbf{H} \cap \mathbf{A} \in \mathcal{T}_1$ implicira redom: $\mathbf{H} \in \mathcal{S}_1$, $\mathbf{H} \leq \mathbf{M}$, $\mathbf{H} \cap \mathbf{A} \leq \mathbf{M} \cap \mathbf{A}$). Slično, $\mathbf{N} \cap \mathbf{A}$ ne može biti u klasi $\mathcal{T}_2$. Dakle, $\mathbf{M} \cap \mathbf{A} \in \mathcal{T}_2$, $\mathbf{N} \cap \mathbf{A} \in \mathcal{T}_1$, ali $\mathbf{M} \cap \mathbf{A} \leq \mathbf{N} \cap \mathbf{A}$ (jer je $\mathbf{M} \leq \mathbf{N}$ zbog linearne uređenosti sistema $\mathcal{S}$) i opet $\mathbf{M} \cap \mathbf{A} \in \mathcal{T}_1$, kontradikcija. Razmotrimo još slučaj: $\mathcal{T}_1$ ima maksimalni element – $\mathbf{L} \cap \mathbf{A}$, $\mathcal{T}_2$ nema minimalni. Tada je $\mathbf{P} = \bigcup\{\mathbf{K} \in \mathcal{S} \mid \mathbf{K} \cap \mathbf{A} = \mathbf{L} \cap \mathbf{A}\}$ maksimalni element klase $\mathcal{S}_1$, a $\bigcap\mathcal{T}_2 = \bigcap\mathcal{S}_2 \cap \mathbf{A} \geq \mathbf{P} \cap \mathbf{A}$: u stvari važi baš jednakost (iz $\mathbf{P} \cap \mathbf{A} < \bigcap\mathcal{S}_2 \cap \mathbf{A}$ sledilo bi $\mathbf{P} < \bigcap\mathcal{S}_2$ i klasa $\mathcal{T}_2$ bi imala minimalni element). Sada direktno sledi da je familija $\mathcal{T}$ zatvorena za unije i preseke.

Svakom skoku $\mathbf{H} \cap \mathbf{A}$, $\mathbf{K} \cap \mathbf{A}$ $(\mathbf{H}, \mathbf{K} \in \mathcal{S})$ odgovara jedan (jedini) skok u $\mathcal{S}$. Jer, neka je $\mathcal{D}_1 = \{\mathbf{M} \in \mathcal{S} \mid \mathbf{M} \cap \mathbf{A} = \mathbf{H} \cap \mathbf{A}\}$, $\mathcal{D}_2 = \{\mathbf{N} \in \mathcal{S} \mid \mathbf{N} \cap \mathbf{A} = \mathbf{K} \cap \mathbf{A}\}$,

$\mathbf{H}_1 = \bigcup \mathcal{D}_1$, $\mathbf{K}_1 = \bigcap \mathcal{D}_2$; onda je $\mathbf{H}_1 \cap \mathbf{A} = \mathbf{H} \cap \mathbf{A}$, $\mathbf{K}_1 \cap \mathbf{A} = \mathbf{K} \cap \mathbf{A}$ i $\mathbf{H}_1$, $\mathbf{K}_1$ čine skok u $\mathcal{S}$. Stoga je $\mathbf{H}_1$ normalna podgrupa grupe $\mathbf{K}_1$, te je i $\mathbf{H}_1 \cap \mathbf{A} = \mathbf{H}_1 \cap (\mathbf{K}_1 \cap \mathbf{A})$ normalna podgrupa grupe $\mathbf{K}_1 \cap \mathbf{A}$. Druga teorema o izomorfizmu nam daje:

$$(\mathbf{K} \cap \mathbf{A})/(\mathbf{H} \cap \mathbf{A}) = (\mathbf{K}_1 \cap \mathbf{A})/(\mathbf{H}_1 \cap \mathbf{A}) \cong (\mathbf{H}_1 \cdot (\mathbf{K}_1 \cap \mathbf{A})/\mathbf{H}_1 \leq \mathbf{K}_1/\mathbf{H}_1.$$

Na kraju, uzimajući po jednog reprezenta iz svake familije jednakih terma (upravo smo videli da zbog potpunosti sistema $\mathcal{S}$ svaka takva familija ima prvi i poslednji element – uređenje je, jasno: ako je $\mathbf{H} \cap \mathbf{A} = \mathbf{K} \cap \mathbf{A}$, $\mathbf{H}, \mathbf{K} \in \mathcal{S}$, i $\mathbf{H} < \mathbf{K}$, onda je $\mathbf{H} \cap \mathbf{A}$ "ispred" $\mathbf{K} \cap \mathbf{A}$) dobijamo, ne formirajući nove skokove, traženi normalni sistem podgrupe $\mathbf{A}$ – $\mathcal{S}_{\mathbf{A}}$.

Primetimo konačno: ako je $\mathcal{S}$ rastući normalni niz, onda je i $\mathcal{S}_{\mathbf{A}}$ rastući normalni niz podgrupa.□

Neka su $\mathcal{S} = \{\mathbf{H}_\alpha \mid \alpha \in \Delta\}$ i $\mathcal{T} = \{\mathbf{K}_\beta \mid \beta \in \Omega\}$ dva normalna sistema podgrupa grupe $\mathbf{G}$. Za svaki skok $\mathbf{H}_\alpha, \mathbf{H}_{\alpha+1}$ u $\mathcal{S}$ i svako $\beta \in \Omega$ neka je $\mathbf{H}_{\alpha,\beta} \stackrel{\text{def}}{=} \mathbf{H}_\alpha \cdot (\mathbf{H}_{\alpha+1} \cap \mathbf{K}_\beta)$; isto tako je, za svaki skok $\mathbf{K}_\beta, \mathbf{K}_{\beta+1}$ u $\mathcal{T}$ i svako $\alpha \in \Delta$, $\mathbf{K}_{\beta,\alpha} \stackrel{\text{def}}{=} \mathbf{K}_\beta \cdot (\mathbf{K}_{\beta+1} \cap \mathbf{H}_\alpha)$. Ako je $\alpha$ ($\in \Delta$) bez naslednika, pisaćemo: $\mathbf{H}_\alpha = \mathbf{H}_{\alpha,0}$; analogno je za $\beta$ ($\in \Omega$) bez naslednika: $\mathbf{K}_\beta = \mathbf{K}_{\beta,0}$ – u oba slučaja 0 je najmanji element skupova, respektivno, $\Delta$ i $\Omega$. Neka je $\overline{\mathcal{S}} = \{\mathbf{H}_{\alpha,0} \mid \alpha \in \Delta$ je bez naslednika $\} \cup \{\mathbf{H}_{\alpha,\beta} \mid \alpha \in \Delta$ ima naslednika, $\beta \in \Omega\}$, $\overline{\mathcal{T}} = \{\mathbf{K}_{\beta,0} \mid \beta \in \Omega$ je bez naslednika $\} \cup \{\mathbf{K}_{\beta,\alpha} \mid \beta \in \Omega$ ima naslednika, $\alpha \in \Delta\}$. Naravno, i ako $\alpha$ ($\beta$) ima naslednika, $\mathbf{H}_{\alpha,0}$ ($\mathbf{K}_{\beta,0}$) je baš $\mathbf{H}_\alpha$ ($\mathbf{K}_\beta$). Neko će stoga smatrati uputnijim da smo u prvom slučaju umesto najmanjih elemenata (označenih sa 0 u oba skupa) izabrali kakve druge, van skupova $\Delta$ i $\Omega$; to bi svakako imalo svojih prednosti kao što nas, s druge strane, naša notacija oslobađa dodatnih diskusija u razmatranjima koja slede. $\overline{\mathcal{S}}$ i $\overline{\mathcal{T}}$ su uređeni sistemi, moguće sa ponavljanjem; indeksni skup sistema $\overline{\mathcal{S}}$ – $\overline{\Delta} = \{(\alpha, 0) \mid \alpha \in \Delta$ je bez naslednika $\} \cup \{(\alpha, \beta) \mid \alpha \in \Delta$ ima naslednika, $\beta \in \Omega\}$ ($\mathbf{H}_{\alpha,\beta}$ stoji umesto $\mathbf{H}_{(\alpha,\beta)}$) – uređen je relacijom $<$ na sledeći način:

$$(\alpha, \beta) < (\alpha', \beta') \quad \text{akko} \quad \alpha < \alpha' \text{ ili } \alpha = \alpha' \text{ i } \beta < \beta';$$

radi se o takozvanom "leksikografskom" uređenju (jasno, relacije $<$ na desnoj strani ekvivalencije su uređenja skupova $\Delta$ i $\Omega$). No sada za $(\alpha, \beta) < (\alpha', \beta')$ nemamo nužno da je $\mathbf{H}_{\alpha,\beta}$ prava podgrupa grupe $\mathbf{H}_{\alpha',\beta'}$. Skokovi u skupu indeksa $\overline{\Delta}$ su oblika $(\alpha, \beta), (\alpha, \beta + 1)$, gde $\alpha$ ima naslednika. Evidentno, podgrupe $\mathbf{H}_{\alpha,\beta}, \mathbf{H}_{\alpha,\beta+1}$ ili čine skok ($\mathbf{H}_{\alpha,\beta}$ je prava podgrupa grupe $\mathbf{H}_{\alpha,\beta+1}$ i među njima nema drugih podgrupa sistema $\overline{\mathcal{S}}$) ili su jednake. Pitanje je, međutim, da li skokove u sistemu $\overline{\mathcal{S}}$ treba tražiti samo u parovima podgrupa $\mathbf{H}_{\alpha,\beta}, \mathbf{H}_{\alpha,\beta+1}$, $\alpha$ ima naslednika. Očigledno, ako je $\alpha$ bez naslednika i $\alpha' > \alpha$, onda $\mathbf{H}_{\alpha,0}$ i $\mathbf{H}_{\alpha',\beta}$, $\beta \in \Omega$ (ne ulazimo u to da li je $\alpha'$ sa ili bez naslednika) ne čine skok; za svako $\alpha'' \in \Delta$ koje je "između" $\alpha$ i $\alpha'$ – $\alpha < \alpha'' < \alpha'$



– imaćemo: $\mathbf{H}_{\alpha,0} < \mathbf{H}_{\alpha'',0} < \mathbf{H}_{\alpha',\beta}$. Stoga skokove mogu obrazovati samo podgrupe $\mathbf{H}_{\alpha,\beta}, \mathbf{H}_{\alpha,\gamma}$, $\alpha$ ima naslednika. Pretpostavimo da ga date podgrupe upravo čine i neka je $\Omega_1 = \{\beta' \in \Omega \mid \mathbf{H}_{\alpha,\beta'} \leq \mathbf{H}_{\alpha,\beta}\}$, $\Omega_2 = \{\gamma' \in \Omega \mid \mathbf{H}_{\alpha,\gamma'} \geq \mathbf{H}_{\alpha,\gamma}\}$. Ovim smo dobili presek skupa $\Omega$ ($\Omega = \Omega_1 \cup \Omega_2$, $\Omega_1 \cap \Omega_2 = \emptyset$ i $\Omega_i \neq \emptyset$, $i = 1, 2$). Primetimo da je (generalno): $\mathbf{H}_{\alpha,\beta} = \bigcup_{\beta' \in \Omega_1} \mathbf{H}_{\alpha,\beta'} = \bigcup_{\beta' \in \Omega_1} \mathbf{H}_\alpha \cdot (\mathbf{H}_{\alpha+1} \cap \mathbf{K}_{\beta'}) = \mathbf{H}_\alpha \cdot (\mathbf{H}_{\alpha+1} \cap \bigcup_{\beta' \in \Omega_1} \mathbf{K}_{\beta'})$, pa ako je $\bigcup_{\beta'} \mathbf{K}_{\beta' \in \Omega_1} = \mathbf{K}_\varepsilon$, onda je $\varepsilon$ najveći element u $\Omega_1$. S druge strane, nemamo uvek: $\mathbf{H}_\alpha \cdot (\mathbf{H}_{\alpha+1} \cap \bigcap_{\gamma' \in \Omega_2} \mathbf{K}_{\gamma'}) = \bigcap_{\gamma' \in \Omega_2} \mathbf{H}_\alpha \cdot (\mathbf{H}_{\alpha+1} \cap \mathbf{K}_{\gamma'})$ ($= \mathbf{H}_\alpha \cdot (\mathbf{H}_{\alpha+1} \cap \mathbf{K}_\gamma)$; inkluzija $\leq$ nam je, doduše, na raspolaganju, ali obrat već ne. Može se tako desiti da imamo strogu inkluziju, pa ako je $\bigcap_{\gamma' \in \Omega_2} \mathbf{K}_{\gamma'} = \mathbf{K}_\delta$, sledi $\delta = \varepsilon$ i $\varepsilon$ je bez naslednika. Ali tada nemamo ni garanciju da je $\mathbf{H}_{\alpha,\beta}$ normalna podgrupa grupe $\mathbf{H}_{\alpha,\gamma}$. Uopšte, sistemi $\overline{\mathcal{S}}$, $\overline{\mathcal{T}}$ su zatvoreni za unije prvih klasa preseka, ali ne nužno i za preseke drugih. Na primer, ako $\alpha$ ima naslednika i $\beta$ je iz $\Omega$, tada opet $\Omega_1 = \{\beta' \in \Omega \mid \mathbf{H}_{\alpha,\beta'} \leq \mathbf{H}_{\alpha,\beta}\}$ i $\Omega_2 = \{\gamma' \in \Omega \mid \mathbf{H}_{\alpha,\gamma} > \mathbf{H}_{\alpha,\beta}\}$ čine presek skupa $\Omega$, no $\bigcap_{\gamma' \in \Omega_2} \mathbf{H}_{\alpha,\gamma'}$ nije nužno element sistema $\overline{\mathcal{S}}$. U svakom slučaju, ako je za sve preseke $\Delta = \Delta_1 \cup \Delta_2$, $\Omega = \Omega_1 \cup \Omega_2$ ispunjeno: $\mathbf{H}_\alpha \cdot (\mathbf{H}_{\alpha+1} \cap \bigcap_{\gamma \in \Omega_2} \mathbf{K}_\gamma) = \bigcap_{\gamma \in \Omega_2} \mathbf{H}_\alpha \cdot (\mathbf{H}_{\alpha+1} \cap \mathbf{K}_\gamma)$ i $\mathbf{K}_\beta \cdot (\mathbf{K}_{\beta+1} \cap \bigcap_{\delta \in \Delta_2} \mathbf{H}_\delta) = \bigcap_{\delta \in \Delta_2} \mathbf{K}_\beta \cdot (\mathbf{K}_{\beta+1} \cap \mathbf{H}_\delta)$, skokovima u $\overline{\mathcal{S}}$, $\overline{\mathcal{T}}$ odgovaraće parovi elemenata i njihovih naslednika, a svaka familija jednakih terma sistema $\overline{\mathcal{S}}$, $\overline{\mathcal{T}}$ imaće, prema ranije rečenom, prvi i poslednji element; uzimanjem po jednog predstavnika iz svake takve familije dobijamo (od $\overline{\mathcal{S}}$, $\overline{\mathcal{T}}$) normalne sisteme bez ponavljanja $\widetilde{\mathcal{S}}$, $\widetilde{\mathcal{T}}$ (koji sadrže polazne $\mathcal{S}$, $\mathcal{T}$), pri čemu se ne stvaraju novi skokovi i ti sistemi su izomorfni (ako je, recimo, $\mathbf{H}_{\alpha,\beta} = \mathbf{H}_{\alpha,\beta+1}$, onda je $\mathbf{K}_{\beta,\alpha} = \mathbf{K}_{\beta,\alpha+1}$). Sledi

**Teorema 47.7** *Svaka dva normalna rastuća niza $\mathcal{S}$ i $\mathcal{T}$, ma koje grupe $\mathbf{G}$, imaju izomorfna proširenja koja su i sama rastući nizovi.*

*Ako postoji rastući kompozicioni niz, tada su svaka dva takva izomorfna.*

**Dokaz.** Koristimo notaciju iz prethodne diskusije. $\overline{\mathcal{S}}$ i $\overline{\mathcal{T}}$ su, jasno dobro uređeni, moguće s ponavljanjem, pa je trivijalno ispunjen i uslov zatvorenosti za preseke drugih klasa sistema $\overline{\mathcal{S}}$ i $\overline{\mathcal{T}}$ (u dobro uređenom skupu svaki neprazan podskup ima minimalni element). Sigurno, i $\widetilde{\mathcal{S}}$ i $\widetilde{\mathcal{T}}$ su dobro uređeni (kao podsistemi dobro uređenih sistema).■

**Lema 47.8** *Neka je $\mathcal{S}$ rastući invarijantni niz i $\mathcal{T}$ ma kakav invarijantni sistem podgrupa grupe $\mathbf{G}$. Tada postoje njihova invarijantna proširenja $\widetilde{\mathcal{S}}$ i $\widetilde{\mathcal{T}}$ takva da je skup faktora sistema $\widetilde{\mathcal{T}}$ podskup skupa faktora sistema $\widetilde{\mathcal{S}}$ (izjednačavamo izomorfne grupe).*

*Ako grupa $\mathbf{G}$ ima rastući glavni niz $\mathcal{P}$, onda je skup faktora svakog drugog glavnog sistema podskup skupa faktora niza $\mathcal{P}$.*

**Dokaz.** Ostajemo pri usvojenoj notaciji. S obzirom da je $\mathcal{S}$ rastući niz, $\overline{\mathcal{T}}$ je potpun sistem (skokovi sistema $\mathcal{T}$ su kompletirani rastućim dobro uređenim sistemom podgrupa). S druge strane, $\overline{\mathcal{S}}$ ne mora biti potpun sistem,

ali uključivanjem preseka drugih klasa svih preseka dobijamo (zahvaljujući i invarijantnosti sistema $\mathcal{S}$, $\mathcal{T}$) potpuno invarijantni sistem $\overline{\mathcal{S}}'$. Pri tom se mogu pojaviti i novi skokovi. Posao završavamo uzimanjem po jednog reprezenta iz svake familije jednakih terma i tako formiranjem sistema $\widetilde{\mathcal{S}}$ i $\widetilde{\mathcal{T}}$ (bez ponavljanja); pri tome se, rekli smo, ne dobijaju novi i ne gube stari skokovi – sem, uslovno rečeno, onih čiji su faktori jedinične grupe.□

Poseban slučaj prethodnog tvrđenja je

**Lema 47.9** *Ako grupa ima glavni rastući niz $\mathcal{S}$ oblika*

$$\mathbf{E} = \mathbf{H}_0 < \mathbf{H}_1 < \cdots < \mathbf{H}_n < \cdots < \mathbf{H}_\omega = \mathbf{G},$$

*tada su svi glavni sistemi izomorfni sa $\mathcal{S}$.*

**Dokaz.** Neka je $\mathcal{T} = \{\mathbf{K}_\alpha \mid \alpha < \mu\}$ (ma koji) glavni sistem i neka je $\overline{\mathcal{S}}$ već poznato proširenje, eventualno sa ponavljanjem, sistema $\mathcal{S}$. Kako je $\overline{\mathcal{S}}$ zatvoren za unije prvih klasa preseka, to za svaki prirodan broj $n$ postoji indeks $\alpha_n$ takav da je $\mathbf{H}_n = \mathbf{H}_{n,\alpha_n}$ $(= \mathbf{H}_n \cdot (\mathbf{H}_{n+1} \cap \mathbf{K}_{\alpha_n}))$, odnosno $\mathbf{H}_{n+1} \cap \mathbf{K}_{\alpha_n} \leq \mathbf{H}_n$, dok je $\mathbf{H}_{n+1} = \mathbf{H}_{n,\alpha}$ za $\alpha > \alpha_n$. Ako svaki od elemenata $\alpha_n$ ima naslednika $(\alpha_n + 1)$, onda je i $\overline{\mathcal{S}}$ potpun sistem i u prelazu na $\widetilde{\mathcal{S}}$, tj. u ovom slučaju na $\mathcal{S}$, ne dobijaju se novi skokovi, pa su sistemi $\mathcal{S}$ i $\mathcal{T}$ prema prethodnoj teoremi izomorfni. No, činjenica je, što ćemo i dokazati, da svako $\alpha_n$ ima naslednika. Uočimo prvo da važi:

*Ako za $\alpha', \alpha''$, $(0 \leq)\ \alpha' < \alpha''\ (\leq \mu)$, nijedan od indeksa $\alpha_i$, $i = 0, \ldots, n$, ne ispunjava uslov: $\alpha' \leq \alpha_i < \alpha''$, onda je $\mathbf{H}_{n+1} \cap \mathbf{K}_{\alpha'} = \mathbf{H}_{n+1} \cap \mathbf{K}_{\alpha''}$.*

Dokaz ovog tvrđenja je indukcijom po $n$. Za $n = 0$ je $\mathbf{H}_1 \cap \mathbf{K}_{\alpha_0} = \mathbf{E}\ (= \mathbf{H}_0)$ i $\mathbf{H}_1 \leq \mathbf{K}_\alpha$ za $\alpha > \alpha_0$ (jer je $\mathbf{H}_0 \cdot (\mathbf{H}_1 \cap \mathbf{K}_\alpha) = \mathbf{H}_1 \cap \mathbf{K}_\alpha = \mathbf{H}_1$). Prema tome je, za $\alpha'' < \alpha_0$, $\mathbf{H}_1 \cap \mathbf{K}_{\alpha'} = \mathbf{H}_1 \cap \mathbf{K}_{\alpha''} = \mathbf{E}$, a za $\alpha_0 < \alpha'$, $\mathbf{H}_1 \cap \mathbf{K}_{\alpha'} = \mathbf{H}_1 \cap \mathbf{K}_{\alpha''} = \mathbf{H}_1$. Pretpostavimo da je tvrđenje tačno za $n \geq 0$ i neka ni za jedno $\alpha_i$, $i = 0, 1, \ldots, n+1$, nije $\alpha' \leq \alpha_i < \alpha''$. Ako je $\alpha'' < \alpha_{n+1}$, tada je $\mathbf{H}_{n+2} \cap \mathbf{K}_{\alpha'} \leq \mathbf{H}_{n+1}$, $\mathbf{H}_{n+2} \cap \mathbf{K}_{\alpha''} \leq \mathbf{H}_{n+1}$, i odatle, prema induktivnoj pretpostavci, $\mathbf{H}_{n+2} \cap \mathbf{K}_{\alpha'} = \mathbf{H}_{n+1} \cap \mathbf{K}_{\alpha'} = \mathbf{H}_{n+1} \cap \mathbf{K}_{\alpha''} = \mathbf{H}_{n+2} \cap \mathbf{K}_{\alpha''}$. Neka je sada $\alpha_{n+1} < \alpha'$ i neka je $g \in H_{n+2} \cap K_{\alpha''} \leq H_{n+2} = H_{n+1} \cdot (H_{n+2} \cap K_{\alpha'})$ prozvod elemenata $a$ i $b$ $(g = ab)$, gde je $a \in H_{n+1}$, $b \in H_{n+2} \cap K_{\alpha'}$. Sledi (ponovo imamo u vidu induktivnu pretpostavku) $a = gb^{-1} \in H_{n+1} \cap K_{\alpha''} = H_{n+1} \cap K_{\alpha'}$; posebno, $a \in K_{\alpha'}$, te je $g \in H_{n+2} \cap K_{\alpha'}$.

Pretpostavimo dalje da neko $\alpha_n$ nema naslednika. Tada je $\mathbf{K}_{\alpha_n} = \bigcap_{\alpha > \alpha_n} \mathbf{K}_\alpha$ (ako bi $\mathbf{K}_{\alpha_n}$ bila prava podgrupa grupe $\bigcap_{\alpha > \alpha_n} \mathbf{K}_\alpha$, to bi značilo da se invarijantni sistem $\mathcal{T}$ može proširiti, kontradikcija). Ako je $\alpha_k$ najmanji među indeksima $\alpha_i$, $i > n$, koji je veći od $\alpha_n$, ukoliko takav postoji, onda je prema gornjem tvrđenju za svako $\alpha'$, $\alpha''$ između $\alpha_n$ i $\alpha_k$ $(\alpha_n < \alpha', \alpha'' < \alpha_k)$ $\mathbf{H}_{n+1} \cap \mathbf{K}_{\alpha'} = \mathbf{H}_{n+1} \cap \mathbf{K}_{\alpha''}$; ako nemamo $\alpha_k$ strogo veće od $\alpha_n$, tada je, naravno, za svako $\alpha', \alpha'' > \alpha_n$, $\mathbf{H}_{n+1} \cap \mathbf{K}_{\alpha'} = \mathbf{H}_{n+1} \cap \mathbf{K}_{\alpha''}$. Stoga je,



opet, za bilo koje $\beta$ veće od $\alpha_n$ i manje od $\alpha_k$ (ako postoji $\alpha_k$ veće od $\alpha_n$) $\mathbf{H}_{n+1} \cap \mathbf{K}_{\alpha_n} = \mathbf{H}_{n+1} \cap \bigcap_{\alpha > \alpha_n} \mathbf{K}_\alpha = \bigcap_{\alpha > \alpha_n} (\mathbf{H}_{n+1} \cap \mathbf{K}_\alpha) = \mathbf{H}_{n+1} \cap \mathbf{K}_\beta$, ali tada je $\mathbf{H}_{n+1} = \mathbf{H}_n \cdot (\mathbf{H}_{n+1} \cap \mathbf{K}_\beta) = \mathbf{H}_n \cdot (\mathbf{H}_{n+1} \cap \mathbf{K}_{\alpha_n}) = \mathbf{H}_{n,\alpha_n} = \mathbf{H}_n$, kontradikcija.□

## 48 Nilpotentne grupe

Klasa nilpotentnih grupa je, da tako kažemo, prva od ekstenzija klase Abelovih grupa, nastala slabljenjem (inače vrlo jakog) uslova komutativnosti (tako su Abelove grupe nilpotentne grupe klase nilpotentnosti 1). Nilpotentne grupe imaju netrivijalni centar, faktor grupa po centru opet ima netrivijalni centar i tako redom; idući po tim odgovarajućim podgrupama u konačno mnogo koraka stižemo do same grupe. No, počnimo formalno.

**Definicija 48.1** *Grupa je nilpotentna akko ima centralni niz.*

*Nilpotentna grupa čiji je najkraći centralni niz dužine $k$ je nilpotentna grupa klase $k$.*

Svaka Abelova grupa je, rekli smo, nilpotentna. Obrat ne važi; npr. grupa kvaterniona je nilpotentna: sa oznakama iz 5.7, $\mathbf{Q} > \langle A^2 \rangle > \mathbf{E}$ je centralni niz.

**Lema 48.2** *Sledeći uslovi su ekvivalentni za grupu $\mathbf{G}$:*

(1) $\mathbf{G}$ *je nilpotentna grupa;*

(2) $\mathbf{G}$ *ima niži centralni niz;*

(3) $\mathbf{G}$ *ima viši centralni niz.*

**Dokaz.** Neka je $\mathbf{G}$ nilpotentna grupa sa centralnim nizom $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{k-1} > \mathbf{G}_k = \mathbf{E}$. Indukcijom po $i$, $i = 1, 2, \ldots, k$, dokazujemo da je $\gamma_i \mathbf{G} \leq \mathbf{G}_i$. Kako je $\mathbf{G}/\mathbf{G}_1$ Abelova grupa, to je $\gamma_1 \mathbf{G} = [\gamma_0 \mathbf{G}, \mathbf{G}] = \mathbf{G}' \leq \mathbf{G}_1$ (6.8). Pretpostavimo da je tvrđenje tačno za svako $j \leq i$. Onda je prema induktivnoj hipotezi i lemi 46.21 $\gamma_{i+1} \mathbf{G} = [\gamma_i \mathbf{G}, \mathbf{G}] \leq [\mathbf{G}_i, \mathbf{G}] \leq \mathbf{G}_{i+1}$. Prema tome, $\gamma_k \mathbf{G} \leq \mathbf{G}_k = \mathbf{E}$.

S druge strane, niži centralni niz $\mathbf{G} = \gamma_0 \mathbf{G} > \gamma_1 \mathbf{G} = \mathbf{G}' > \cdots > \gamma_{n-1} \mathbf{G} > \gamma_n \mathbf{G} = \mathbf{E}$ je i centralni – 46.24 (ovde ne može biti ponavljanja, jer bi $\gamma_{j-1} \mathbf{G} = \gamma_j \mathbf{G} \neq \mathbf{E}$ impliciralo $\gamma_{j-1} \mathbf{G} = \gamma_{j+r} \mathbf{G}$ za svako $r \in \omega$).

Slično, indukcijom po $i$, $i = 0, 1, \ldots, k$, pokazujemo da je $\mathbf{G}_{k-i} \leq \zeta_i \mathbf{G}$. Za $i = 0$ to je očigledno, a za $i = 1$ je $\mathbf{G}_{k-1}/\mathbf{G}_k = \mathbf{G}_{k-1}/\mathbf{E} \leq \mathbf{Z}(\mathbf{G}/\mathbf{E})$, pa je $\mathbf{G}_{k-1} \leq \mathbf{Z}(\mathbf{G}) = \zeta_1 \mathbf{G}$. Neka je po induktivnoj pretpostavci, za svako $j \leq i < k$, $\mathbf{G}_{k-j} \leq \zeta_j \mathbf{G}$. Tada je $[\mathbf{G}_{k-(i+1)}, \mathbf{G}] \leq \mathbf{G}_{k-i} \leq \zeta_i \mathbf{G}$, te je, za prirodno homomorfno preslikavanje $\varphi : G \longrightarrow G/\zeta_i G$, $(\mathbf{G}_{k-(i+1)})\varphi \leq \mathbf{Z}(\mathbf{G}/\zeta_i \mathbf{G}) = \zeta_{i+1} \mathbf{G}/\zeta_i \mathbf{G}$ (za svako $a \in G_{k-(i+1)}$ i svako $g \in G$ je $[a, g] \in \zeta_i G$ i stoga je

$ag\,\zeta_iG = a\,\zeta_iG \cdot g\,\zeta_iG = g\,\zeta_iG \cdot a\,\zeta_iG = ga\,\zeta_iG$), a odatle je $\mathbf{G}_{k-(i+1)} \leq \zeta_{i+1}\mathbf{G}$ (za svako $a \in G_{k-(i+1)}$ postoji $b \in \zeta_{i+1}G$ takvo da je $a\,\zeta_iG = b\,\zeta_iG$, te je $a \in b\,\zeta_iG \subseteq \zeta_{i+1}G$).

Viši centralni niz je, po samoj definiciji, i centralni. U višem centralnom nizu $\mathbf{E} = \zeta_0\mathbf{G} < \zeta_1\mathbf{G} = \mathbf{Z}(\mathbf{G}) < \cdots < \zeta_{m-1}\mathbf{G} < \zeta_m\mathbf{G} = \mathbf{G}$ takođe ne može biti ponavljanja: iz $\zeta_j\mathbf{G} = \zeta_{j+1}\mathbf{G} \neq \mathbf{G}$ sledilo bi $\zeta_j\mathbf{G} = \zeta_{j+t}\mathbf{G}$, za svako $t \in \omega$.□

**Korolar 48.3** *U nilpotentnoj grupi* $\mathbf{G}$ *klase* $k$ *niži i viši centralni nizovi su iste dužine – $k$. Takođe, za svako $i$, $i = 0, \ldots, k$, važi:* $\gamma_i\mathbf{G} \leq \zeta_{k-i}\mathbf{G}$.

**Dokaz.** Iz dokaza prethodne leme sledi da su dužina nižeg i višeg centralnog niza manje ili jednake od dužine ma kog centralnog niza.

Imali smo takođe: $\gamma_i\mathbf{G} \leq \mathbf{G}_i = \mathbf{G}_{k-(k-i)} \leq \zeta_{k-i}\mathbf{G}$.□

**Lema 48.4** *Za svaka dva elementa $a, b$ nilpotentne grupe* $\mathbf{G}$ *klase najviše 2 i svako $z \in Z$ važi:*

$$(ab)^z = a^z b^z [b,a]^{\frac{1}{2}z(z-1)}.$$

**Dokaz.** Prema uslovu leme je $\gamma_2\mathbf{G} = [\gamma_1\mathbf{G}, \mathbf{G}] = [\mathbf{G}', \mathbf{G}] = \mathbf{E}$, što će reći: $\mathbf{G}' \leq \mathbf{Z}(\mathbf{G})$. Ostalo je već dokazano – 6.3($b$).□

**Lema 48.5** *Podgrupe i homomorfne slike nilpotentne grupe su nilpotentne grupe.*

**Dokaz.** Neka je $\mathbf{G}$ nilpotentna grupa i neka je $\mathbf{H}$ jedna njena podgrupa. Onda je, prema prethodnoj lemi, $\gamma_n\mathbf{G} = \mathbf{E}$ za neki prirodan broj $n$. No, trivijalno je, prema samoj definiciji nižeg centralnog niza, $\gamma_i\mathbf{H} \leq \gamma_i\mathbf{G}$ za svako $i$, $i = 0, 1, \ldots$.

Ako je pak $\mathbf{N}$ normalna podgrupa grupe $\mathbf{G}$, onda je prema 46.25(5)

$$\gamma_n(\mathbf{G}/\mathbf{N}) = (\gamma_n\mathbf{G} \cdot \mathbf{N})/\mathbf{N} = \overline{\mathbf{E}}.$$

Daćemo i naizgled drugi, "standardniji" dokaz koji polazi od ma kog centralnog niza grupe $\mathbf{G}$: $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{k-1} > \mathbf{G}_k = \mathbf{E}$. Posmatrajmo opadajući niz podgrupa podgrupe $\mathbf{H}$ (grupe $\mathbf{G}$): $\mathbf{H} = \mathbf{H}_0 = \mathbf{H} \cap \mathbf{G}_0 \geq \mathbf{H}_1 = \mathbf{H} \cap \mathbf{G}_1 \geq \cdots \geq \mathbf{H}_{k-1} = \mathbf{H} \cap \mathbf{G}_{k-1} \geq \mathbf{H}_k = \mathbf{H} \cap \mathbf{G}_k = \mathbf{E}$. Svi članovi niza su, prema 8.3, normalne podgrupe grupe $\mathbf{H}$. Osim toga, iz $\mathbf{H}_{i-1} \leq \mathbf{G}_{i-1}$ (i $\mathbf{H} \leq \mathbf{G}$) sledi $[\mathbf{H}_{i-1}, \mathbf{H}] \leq [\mathbf{G}_{i-1}, \mathbf{G}] \leq \mathbf{G}_i$, tj. $[\mathbf{H}_{i-1}, \mathbf{H}] \leq \mathbf{G}_i \cap \mathbf{H} = \mathbf{H}_i$. Eliminisanjem "viška" podgrupa (ukoliko se neke podgrupe ponavljaju) ostaje nam centralni niz grupe $\mathbf{H}$.

U faktor grupi $\mathbf{G}/\mathbf{N}$ posmatrajmo opadajući niz podgrupa: $\overline{\mathbf{G}}_0 = \mathbf{G}/\mathbf{N} = (\mathbf{G}_0 \cdot \mathbf{N})/\mathbf{N} \geq \overline{\mathbf{G}}_1 = (\mathbf{G}_1 \cdot \mathbf{N})/\mathbf{N} \geq \cdots \geq \overline{\mathbf{G}}_{k-1} = (\mathbf{G}_{k-1} \cdot \mathbf{N})/\mathbf{N} \geq \overline{\mathbf{G}}_k = (\mathbf{G}_k \cdot \mathbf{N})/\mathbf{N} = \mathbf{N}/\mathbf{N} = \overline{\mathbf{E}}$. Kako je proizvod normalnih podgrupa normalna



podgrupa, to su sve podgrupe $\overline{\mathbf{G}}_i$, $i = 0, 1, \ldots, k$, normalne podgrupe grupe $\overline{\mathbf{G}}$. Dalje, direktno proveravamo da je $[\overline{\mathbf{G}}_{i-1}, \overline{\mathbf{G}}] \leq \overline{\mathbf{G}}_i$. Neka je $a \in G_{i-1}$ i $g \in G$. Tada je $(aN)^{-1}(gN)^{-1}aN\,gN = [a,g]N \in (G_iN)/N = \overline{G}_i$. Ostaje, kao i obično, da se "eliminiše" višak u nizu.□

**Lema 48.6** ($a$) *Direktan proizvod konačno mnogo nilpotentnih grupa je nilpotentna grupa.*

($b$) *Ako je $\{\mathbf{G}_i \mid i \in I\}$ (neprazna) familija nilpotentnih grupa ograničenih klasa (postoji prirodan broj $n$ koji je veći ili jednak od klase svake nilpotentne grupe $\mathbf{G}_i$, $i \in I$), onda je $\prod_{i\in I}^{c}\mathbf{G}_i$ nilpotentna grupa (klase manje od ili jednake $n$).*

**Dokaz.** ($a$) Naravno, dovoljno je proveriti da je proizvod dve nilpotentne grupe nilpotentna grupa (ostalo je na indukciji). Neka su $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{k-1} > \mathbf{G}_k = \mathbf{E}$ i $\mathbf{H} = \mathbf{H}_0 > \mathbf{H}_1 > \cdots > \mathbf{H}_{l-1} > \mathbf{H}_l = \mathbf{E}$ centralni nizovi grupa, respektivno, $\mathbf{G}$ i $\mathbf{H}$, i neka je npr. $k < l$. Tada je $\mathbf{G} \times \mathbf{H} = \mathbf{G}_0 \times \mathbf{H}_0 > \mathbf{G}_1 \times \mathbf{H}_1 > \cdots > \mathbf{G}_{k-1} \times \mathbf{H}_{k-1} > \mathbf{E} \times \mathbf{H}_k > \cdots > \mathbf{E} \times \mathbf{H}_{l-1} > \mathbf{E} \times \mathbf{E}$ centralni niz grupe $\mathbf{G} \times \mathbf{H}$. Očigledno je invarijantan, a preslikavanje $\psi : (G \times H)/(G_i \times H_i) \longrightarrow G/G_i \times H/H_i$, gde je, za $a \in G$ i $b \in H$, $((a,b)(G_i \times H_i))\psi \stackrel{\text{def}}{=} (aG_i, bH_i)$, izomorfno je preslikavanje grupe $(\mathbf{G} \times \mathbf{H})/\mathbf{G}_i \times \mathbf{H}_i)$ na grupu $\mathbf{G}/\mathbf{G}_i \times \mathbf{H}/\mathbf{H}_i$ (10.3($b$)). Pri tome je $((\mathbf{G}_{i-1} \times \mathbf{H}_{i-1})/\mathbf{G}_i \times \mathbf{H}_i))\psi = \mathbf{G}_{i-1}/\mathbf{G}_i \times \mathbf{H}_{i-1}/\mathbf{H}_i \leq \mathbf{Z}(\mathbf{G}/\mathbf{G}_i) \times \mathbf{Z}(\mathbf{H}/\mathbf{H}_i) = \mathbf{Z}(\mathbf{G}/\mathbf{G}_i \times \mathbf{H}/\mathbf{H}_i)$ (10.3($d$)), pa je i $(\mathbf{G}_{i-1} \times \mathbf{H}_{i-1})/(\mathbf{G}_i \times \mathbf{H}_i) \leq \mathbf{Z}((\mathbf{G} \times \mathbf{H})/(\mathbf{G}_i \times \mathbf{H}_i))$.

Mogli smo i direktno proveriti:

$$[\mathbf{G}_{i-1} \times \mathbf{H}_{i-1}, \mathbf{G} \times \mathbf{H}] = [\mathbf{G}_{i-1}, \mathbf{G}] \times [\mathbf{H}_{i-1}, \mathbf{H}] \leq \mathbf{G}_i \times \mathbf{H}_i.$$

($b$) U osnovi nema razlike u odnosu na dokaz prethodne tačke. Naravno, kao podgrupa kartezijanskog proizvoda i $\prod_{i\in I}\mathbf{G}_i$ je nilpotentna grupa.□

**Korolar 48.7** *Familija (svih) nilpotentnih grupa klase manje od ili jednake nekom fiksnom broju je varijetet.*

**Dokaz.** Direktno, prema prethodnim dvema lemama i 24.21.□

**Korolar 48.8** *Neka su* $\mathbf{H}$ *i* $\mathbf{K}$ *normalne podgrupe grupe* $\mathbf{G}$. *Ako su faktor grupe* $\mathbf{G}/\mathbf{H}$ *i* $\mathbf{G}/\mathbf{K}$ *nilpotentne, onda je i faktor grupa* $\mathbf{G}/(\mathbf{H} \cap \mathbf{K})$ *nilpotentna.*

**Dokaz.** $\mathbf{G}/(\mathbf{H} \cap \mathbf{K})$ je, prema 10.15, izomorfna podgrupi nilpotentne grupe $\mathbf{G}/\mathbf{H} \times \mathbf{G}/\mathbf{K}$.

Jedan drugi dokaz ovog tvrđenja bi mogao izgledati ovako. Pošto je $\mathbf{G}/\mathbf{H}$ nilpotentna grupa, to je $\gamma_k(\mathbf{G}/\mathbf{H}) = \overline{\mathbf{E}}$ za neki prirodan broj $k$. No, prema 46.25(5) je $\gamma_k(\mathbf{G}/\mathbf{H}) = (\gamma_k\mathbf{G} \cdot \mathbf{H})/\mathbf{H}$, pa je $\gamma_k\mathbf{G} \leq \mathbf{H}$. Isto tako je $\gamma_m\mathbf{G} \leq \mathbf{K}$ za neko $m$, te ako je $n = max\,\{k, m\}$, sledi:

$$\gamma_n(\mathbf{G}/(\mathbf{H} \cap \mathbf{K})) = (\gamma_n\mathbf{G} \cdot (\mathbf{H} \cap \mathbf{K}))/(\mathbf{H} \cap \mathbf{K}) = \overline{\mathbf{E}}.$$□

**Primer 48.9** ($a$) *Konačne p-grupe su nilpotentne.*

**Dokaz.** Indukcijom po redu grupe. Grupa reda $p$ je ciklična, stoga i nilpotentna. Pretpostavimo da je tvrđenje tačno za sve grupe reda $p^k$, $k < n$ $(> 1)$, i neka je $\mathbf{G}$ neabelova grupa reda $p^n$ (ako je Abelova grupa, nemamo šta dokazivati). Prema 4.13 je $\mathbf{Z(G)} \neq \mathbf{E}$, a prema induktivnoj hipotezi je $\mathbf{G/Z(G)}$ nilpotentna grupa. Ako je $\mathbf{G/Z(G)} > \mathbf{G}_1\mathbf{/Z(G)} > \cdots > \mathbf{G}_{k-1}\mathbf{/Z(G)} > \overline{\mathbf{E}}$ centralni niz grupe $\mathbf{G/Z(G)}$, onda je $\mathbf{G} > \mathbf{G}_1 > \cdots > \mathbf{G}_{k-1} > \mathbf{G}_k = \mathbf{Z(G)} > \mathbf{G}_{k+1} = \mathbf{E}$ centralni niz grupe $\mathbf{G}$. Jer, za $i < k$, iz $(\mathbf{G}_{i-1}\mathbf{/Z(G)})/(\mathbf{G}_i\mathbf{/Z(G)}) \leq \mathbf{Z}((\mathbf{G/Z(G)})/(\mathbf{G}_i\mathbf{/Z(G)}))$, tj.

$$[\mathbf{G}_{i-1}\mathbf{/Z(G)}, \mathbf{G/Z(G)}] \leq \mathbf{G}_i\mathbf{/Z(G)}$$

sledi: za svako $a \in G_{i-1}$ i svako $g \in G$ važi $[aZ(\mathbf{G}), gZ(\mathbf{G})] = [a,g]Z(\mathbf{G}) \in G_i/Z(\mathbf{G})$, te je $[a,g] \in G_i$; dakle, $[\mathbf{G}_{i-1}, \mathbf{G}] \leq \mathbf{G}_i$, odnosno $\mathbf{G}_{i-1}/\mathbf{G}_i \leq \mathbf{Z(G/G}_i)$. I, jasno: $[\mathbf{Z(G)}, \mathbf{G}] = \mathbf{E}$, tj. $[\mathbf{G}_k, \mathbf{G}] \leq \mathbf{G}_{k+1}$.

Konstatujmo još da beskonačne $p$-grupe ne moraju biti nilpotentne – videti 14.4($a$).

($b$) *Ako je faktor grupa grupe* $\mathbf{G}$ – $\mathbf{G/H}$, *gde je* $\mathbf{H} \leq \mathbf{Z(G)}$, *nilpotentna grupa, onda je i* $\mathbf{G}$ *nilpotentna grupa.*

**Dokaz.** Videti dokaz prethodne tačke. Ili još jednostavnije: ako je $\gamma_n(\mathbf{G/H}) = (\gamma_n\mathbf{G}\cdot\mathbf{H})/\mathbf{H} = \overline{\mathbf{E}}$, onda je $\gamma_n\mathbf{G} \leq \mathbf{H}$ $(\leq \mathbf{Z(G)})$, pa je $\gamma_{n+1}\mathbf{G} = [\gamma_n\mathbf{G}, \mathbf{G}] = \mathbf{E}$.

($c$)$_1$ *Dijedarska grupa stepena* $2^n$, $n \geq 2$, *nilpotentna je grupa klase* $n$.

**Dokaz.** Nilpotentnost nam je već data (tačka ($a$)). U pitanju je, znači, samo klasa nilpotentnosti. Dokaz za nju je indukcijom po $n$ $(\geq 2)$. Centar dijedarske grupe $\mathbf{D}_4$ (slučaj $n = 2$) je reda $2$ – $\mathbf{Z}(\mathbf{D}_4) = \langle\{\imath, \rho^2\}, \circ\rangle$ (videti 3.4($e$)), i $\mathbf{E} = \zeta_0\mathbf{D}_4 < \mathbf{Z}(\mathbf{D}_4) = \zeta_1\mathbf{D}_4 < \mathbf{D}_4$ je viši centralni niz grupe $\mathbf{D}_4$ (dakle, $\mathbf{D}_{2^2}$ je klase 2). Pretpostavimo da je tvrđenje tačno za svaku dijedarsku grupu stepena $2^k$, $k \leq n$ $(> 2)$. Grupa $\mathbf{D}_{2^{n+1}}$ je, podsećamo, generisana elementima $\rho$ $(= \rho_{\frac{2\pi}{2^{n+1}}})$ i $\sigma$ $(= \sigma_y)$ za koje važi: $\rho^{2^{n+1}} = \sigma^2 = \imath$ i $\rho\sigma = \sigma\rho^{2^{n+1}-1}$. I centar ove grupe je dvoelementna podgrupa – $\langle\{\imath, \rho^{2^n}\}, \circ\rangle$; nijedan element oblika $\sigma\rho^i$, $0 < i < 2^{n+1}$, nije u centru, jer je:

$$\sigma\rho^i \circ \rho = \sigma\rho^{i+_{2^{n+1}}1} \neq \rho \circ \sigma\rho^i = \sigma\rho^{(2^{n+1}-1)+_{2^{n+1}}i}$$

(jasno, $i +_{2^{n+1}} 1 \neq (2^{n+1}-1) +_{2^{n+1}} i$). S druge strane, ako je $\rho^i \circ \sigma = \sigma \circ \rho^i$, $0 < i < 2^{n+1}$, odnosno, $\sigma\rho^{i\cdot_{2^{n+1}}(2^{n+1}-1)} = \sigma\rho^i$, onda je $i \cdot_{2^{n+1}} (2^{n+1}-1) = i$, a odatle sledi redom:

$$i(2^{n+1}-1) - [\tfrac{i(2^{n+1}-1)}{2^{n+1}}]2^{n+1} = i,$$
$$i2^{n+1} - i - i2^{n+1} - [\tfrac{-i}{2^{n+1}}]2^{n+1} = i,$$
$$2i = -[\tfrac{-i}{2^{n+1}}]2^{n+1} = 2^{n+1},$$
$$i = 2^n.$$



Grupa $\mathbf{D}_{2^{n+1}}/\mathbf{Z}(\mathbf{D}_{2^{n+1}})$ generisana je pak elementima $\rho Z, \sigma Z$ (stavili smo $Z = Z(\mathbf{D}_{2^{n+1}})$) i važi: $(\rho Z)^{2^n} = (\sigma Z)^2 = Z$ i $(\rho Z)(\sigma Z) = (\rho \circ \sigma)Z = (\sigma\rho^{2^n-1})Z = (\sigma Z)(\rho Z)^{2^n-1}$. Prema tome, $\mathbf{D}_{2^{n+1}}/\mathbf{Z}(\mathbf{D}_{2^{n+1}}) \cong \mathbf{D}_{2^n}$ i prema prethodnoj tački, induktivnoj hipotezi i dokazu prve tačke $\mathbf{D}_{2^{n+1}}$ je nilpotentna grupa klase $n+1$.

($c$)$_2$ *Dijedarske grupe čiji stepeni nisu stepeni broja* 2 *nisu nilpotentne.*

**Dokaz.** Ako je $n$ neparan broj, onda je, prema upravo izvedenom "računu", dijedarska grupa stepena $n$ bez centra. Ako je $n = 2^k m$, gde je $k \geq 1$ i $m$ neparan broj veći od 1, opet je centar dijedarske grupe $\mathbf{D}_n$ dvoelementna podgrupa $\langle\{\imath, \rho^{2^{k-1}m}\}, \circ\rangle$ i $\mathbf{D}_n/\mathbf{Z}(\mathbf{D}_n) \cong \mathbf{D}_{2^{k-1}m}$. Nastavljajući tako, formiranjem faktora novodobijenih grupa po njihovom centru, stigli bismo do grupe (izomorfne sa) $\mathbf{D}_m$. Proizilazi da grupa $\mathbf{D}_{2^k m}$ nije nilpotentna, jer ni njena homomorfna slika $(\mathbf{D}_m)$ nije nilpotentna.

($d$) *Generalna grupa kvaterniona reda* $2^{n+1}$, $n \geq 2$, – $\mathbf{Q}_{2^{n+1}}$, *je grupa sa prezentacijom* $(a, b; a^{2^n}, b^4, a^{2^{n-1}} \sim b^2, ba \sim a^{2^n-1}b)$; *jedna takva grupa je podgrupa multiplikativne grupe regularnih kompleksnih matrica formata* $2 \times 2$, *generisana matricama* $A = \begin{bmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{bmatrix}$, *gde je* $\xi$ *primitivni* $2^n$*-ti koren jedinice (na primer,* $\xi = e^{\frac{2\pi}{2^n}i}$*) i* $B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. *(Posebno, za* $n = 2$ *imamo poznatu grupu kvaterniona* – 5.7($a$).*) Ova grupa je nilpotentna grupa klase* $n$.

**Dokaz.** Opet se, kao i u prethodnoj tački, radi o 2-grupi, dakle i nilpotentnoj grupi i opet se indukcijom proverava klasa nilpotentnosti. Već smo konstatovali da je grupa kvaterniona $\mathbf{Q}$ $(= \mathbf{Q}_{2^2+1})$ klase 2. Stoga, neka je $n > 2$ i neka je tvrđenje tačno za sve generalne grupe kvaterniona reda $2^{k+1}$, $k < n$. Po treći put opet, centar grupe $\mathbf{Q}_{2^{n+1}}$ je reda $2$ – $\mathbf{Z}(\mathbf{Q}_{2^{n+1}}) = \langle\{e, a^{2^{n-1}}\}, \cdot\rangle$ (uzimamo da su elementi grupe: $e, a, a^2, \ldots, a^{2^n-1}, b, ab, a^2b, \ldots, a^{2^n-1}b$). Zaista,

$$b \cdot a^{2^{n-1}} = a^{(2^n-1)\cdot_{2^n}2^{n-1}}b = a^{2^{n-1}} \cdot b;$$

$(2^n-1)\cdot_{2^n}2^{n-1} = (2^n-1)2^{n-1} - [\frac{(2^n-1)2^{n-1}}{2^n}]2^n = 2^{2n-1} - 2^{n-1} - [\frac{2^n 2^{n-1} - 2^{n-1}}{2^n}]2^n = 2^{2n-1} - 2^{n-1} - 2^{2n-1} - [-\frac{2^{n-1}}{2^n}]2^n = 2^n - 2^{n-1} = 2^{n-1}$. S druge strane je, za svako $i$, $0 < i < 2^n$, $a^ib \cdot a \neq a \cdot a^ib$. Stavimo: $\mathbf{Z} = \mathbf{Z}(\mathbf{Q}_{2^{n+1}})$. Faktor grupa $\mathbf{Q}_{2^{n+1}}/\mathbf{Z}$ generisana je elementima $aZ$ i $bZ$, za koje važi:

$$(aZ)^{2^{n-1}} = (bZ)^2 = Z, \quad bZ \cdot aZ = (aZ)^{2^{n-1}-1} \cdot bZ.$$

Prema tome, $\mathbf{Q}_{2^{n+1}}/\mathbf{Z} \cong \mathbf{D}_{2^{n-1}}$, prema tački ($c$)$_1$ je $\mathbf{D}_{2^{n-1}}$ nilpotentna grupa klase $n-1$, pa zaključujemo, imajući u vidu tačku ($b$) i dokaz tačke ($a$), da je $\mathbf{Q}_{2^{n+1}}$ nilpotentna grupa klase $n$.

Prema dokazu takođe sledi da osim grupe kvaterniona nijedna druga generalna grupa kvaterniona nije Hamiltonova grupa; no, to sledi i prema 20.1.□

**Napomena**. Poslednje tačke primera i dokaz leme 48.5 nam kažu da, generalno, direktni proizvod beskonačno mnogo nilpotentnih grupa ne mora biti nilpotentna grupa. Npr. direktni proizvod $\prod_{n\geq 2}\mathbf{D}_{2^n}$ nije nilpotentna grupa; jer, ako bi bio nilpotentna grupa klase, recimo, $k$, sledilo bi da su i njegove dijedarske podgrupe $\mathbf{D}_{2^n}$, $n > k$ (preciznije, njegove podgrupe izomorfne pomenutim dijedarskim grupama) klase $\leq k < n$, kontradikcija.

Primetimo i da ekstenzija nilpotentne grupe nilpotentnom grupom nije nužno nilpotentna grupa. Tako je grupa $\mathbf{S}_3$ ekstenzija Abelove (dakle i nilpotentne) grupe $\mathbf{A}_3$ Abelovom grupom $\mathbf{C}_2$, ali nije nilpotentna – nejedinične grupe bez centra nisu nilpotentne (ako je $\mathbf{Z}(\mathbf{G}) = \mathbf{E}$, onda je $\zeta_n\mathbf{G} = \mathbf{E}$ za svako $n \in \omega$). Inače, ekstenzija nilpotentne grupe nilpotentnom grupom se zove *metanilpotentna grupa*. U vezi s tim navedimo bez dokaza sledeći stav P. Halla:

*Ako je* $\mathbf{H}$ *normalna nilpotentna podgrupa grupe* $\mathbf{G}$ *i ako je* $\mathbf{G}/\mathbf{H}'$ *nilpotentna grupa, tada je i* $\mathbf{G}$ *nilpotentna grupa.*

Tačka $(b)$ primera se može uopštiti.

**Korolar 48.10** *Ako je faktor grupa* $\mathbf{G}/\mathbf{H}$ *nilpotentna i ako je* $\mathbf{H} \leq \zeta_m\mathbf{G}$ *za neki prirodan broj* $m$*, onda je i* $\mathbf{G}$ *nilpotentna grupa.*

**Dokaz**. Kao homomorfna slika grupe $\mathbf{G}/\mathbf{H}$ i $\mathbf{G}/\zeta_m\mathbf{G}$ je nilpotentna. Neka je $\zeta_n(\mathbf{G}/\zeta_m\mathbf{G}) = \mathbf{G}/\zeta_m\mathbf{G}$. No, prema 46.25(4) je $\zeta_n(\mathbf{G}/\zeta_m\mathbf{G}) = \zeta_{m+n}\mathbf{G}/\zeta_m\mathbf{G}$, pa je $\zeta_{m+n}\mathbf{G} = \mathbf{G}$.□

**Lema 48.11** *Neka je, za ma koje polje* $\mathbf{F}$, $UT_n(\mathbf{F}) \stackrel{\text{def}}{=} \{A \mid A$ *je gornja trougaona matrica formata* $n \times n$ *sa elementima iz* $\mathbf{F}$ *čiji su svi dijagonalni elementi* $1\}$. $UT_n(\mathbf{F})$ *je domen nilpotentne grupe* – $\mathbf{UT}_n(\mathbf{F})$ – *klase nilpotentnosti* $n-1$.

**Dokaz**. Evidentno je da se radi o domenu podgrupe grupe $\mathbf{SL}_n(\mathbf{F})$ (19.36). Proizvod gornjih trougaonih matrica je gornja trougaona matrica, a ako je $A = [a_{ij}]$, $B = [b_{ij}] \in UT_n(\mathbf{F})$ i $AB = C = [c_{ij}]$, tada je $c_{ii} = \sum_{k=1}^{n} a_{ik}b_{ki} = \sum_{k=1}^{i-1} a_{ik}b_{ki} + a_{ii}b_{ii} + \sum_{k=i+1}^{n} a_{ik}b_{ki} = 0 + 1 + 0 = 1$. Isto tako, svako $A \in UT_n(\mathbf{F})$ se svodi na jediničnu množenjem s leva transvekcijama oblika $T_{ij}(a) = I + aI_{ij}$, $i < j$, $a \in F^*$ (videti dokaze leme 19.37 i korolara 19.38), te je $A^{-1}$ proizvod takvih transvekcija, prema tome i element skupa $UT_n(\mathbf{F})$. Sledi uopšte da je $\mathbf{UT}_n(\mathbf{F}) = \langle\{T_{ij}(a) \mid i < j, a \in F^*\}\rangle$. Neka je dalje, za $1 \leq r \leq n$, $UT_n^r(\mathbf{F}) = \{A \in UT_n(\mathbf{F}) \mid$ svi elementi prvih $r-1$ dijagonala iznad glavne su nula$\}$, posebno $UT_n^1(\mathbf{F}) = UT_n(\mathbf{F})$, $UT_n^n(\mathbf{F}) = \{I\}$. Pokazuje se, kao i gore, da je $UT_n^r(\mathbf{F})$ domen podgrupe generisane skupom $\{T_{ij}(a) \mid j-i \geq r, a \in F^*\}$. Odatle odmah proizilazi da je svaka podgrupa $\mathbf{UT}_n^r(\mathbf{F})$ normalna podgrupa grupe $\mathbf{UT}_n(\mathbf{F})$, a onda i da je $[\mathbf{UT}_n^r(\mathbf{F}), \mathbf{UT}_n^s(\mathbf{F})] = \mathbf{UT}_n^{r+s}$. Inkluzija $\leq$ se dokazuje dvostrukom indukcijom po broju transvekcija u proizvodu. Lako



se proverava da za $j - i \geq r$, $m - k \geq s$ i $a, b \in F^*$ važi $[T_{ij}(a), T_{km}(b)] \in UT_n^{r+s}(\mathbf{F})$. Za $m_1 - k_1$, $m_2 - k_2 \geq s$ imamo zbog normalnosti podgrupe $\mathbf{UT}_n^{r+s}(\mathbf{F})$ i prema 6.2$(e)$:

$$[T_{ij}(a),\, T_{k_1m_1}(b_1)T_{k_2m_2}(b_2)] =$$

$$[T_{ij}(a), T_{k_2m_2}(b_2)] \cdot T_{k_2m_2}(b_2)^{-1}[T_{ij}(a), T_{k_1m_1}(b_1)]T_{k_2m_2}(b_2) \in UT_n^{r+s}(\mathbf{F}).$$

Indukcijom se izvodi generalno: za svako $B \in UT_n^s(\mathbf{F})$ je $[T_{ij}(a), B] \in UT_n^{r+s}$. Ovo pak daje ($j_1 - i_1$, $j_2 - i_2 \geq r$)

$$[T_{i_1j_1}(a_1)T_{i_2j_2}(a_2), B] =$$

$$T_{i_2j_2}(a_2)^{-1}[T_{i_1j_1}(a_1), B]T_{i_2j_2}(a_2) \cdot [T_{i_2j_2}(a_2), B] \in UT_n^{r+s}(\mathbf{F}),$$

i uopšte: za svako $A \in UT_n^r(\mathbf{F})$ je $[A, B] \in UT_n^{r+s}(\mathbf{F})$. Suprotna inkluzija sledi iz već poznate relacije (videti komentar uz 6.1); npr. za $j - i \geq r + s$ i $a \in F^*$ je $T_{i,i+r}(a) \in UT_n^r(\mathbf{F})$, $T_{i+r,j}(1) \in UT_n^s(\mathbf{F})$ i $T_{ij}(a) = [T_{i,i+r}(-a), T_{i+r,j}(1)]$.

Zaključujemo da je

$$\mathbf{UT}_n(\mathbf{F}) = \mathbf{UT}_n^1(\mathbf{F}) > \mathbf{UT}_n^2(\mathbf{F}) > \cdots > \mathbf{UT}_n^{n-1}(\mathbf{F}) > \mathbf{UT}_n^n(\mathbf{F}) = \mathbf{E}$$

donji (ispostavlja se da je i gornji) centralni niz grupe $\mathbf{UT}_n(\mathbf{F})$.□

**Definicija 48.12** *Unipotentna matrica je kvadratna matrica čiji su svi karakteristični koreni* 1.

**Lema 48.13** *Ako je* $\mathbf{H}$ *nilpotentna podgrupa grupe* $\mathbf{GL}_n(\mathbf{Ra})$ *čiji su svi elementi unipotentne matrice, tada je* $\mathbf{H}$ *konjugovana podgrupi grupe* $\mathbf{UT}_n(\mathbf{Ra})$. *Posebno, ako je* $\mathbf{H}$ *i konačno generisana podgrupa, onda je konjugovana podgrupi grupe* $\mathbf{UT}_n(\mathbf{Z})$.

**Dokaz**. Koristićemo sledeće stavove iz linearne algebre (podrazumevajući njeno elementarno poznavanje):

$(a)$ *Ma koji skup uzajamno komutativnih linearnih transformacija vektorskog prostora* $\mathbf{F}^k$*, gde je* $\mathbf{F}$ *(ma koje) polje i* $k \in N$*, ima zajednički karakteristični vektor nad ekstenzijom polja* $\mathbf{F}$ *koja sadrži sve karakteristične korene tih transformacija;*

$(b)$ *Neka je* $\mathbf{U}$ *potprostor vektorskog prostora* $\mathbf{V}$ *invarijantan za linearnu transformaciju* $A$*. Preslikavanje* $A_1$ *faktor prostora* $\mathbf{V}/\mathbf{U}$ *definisano sa* $(v + U)A_1 = (v)A + U$ *linearna je transformacija čiji minimalni polinom deli minimalni polinom transformacije* $A$.

Stav $(b)$ je očigledan. Što se tiče stava $(a)$, pretpostavimo odmah da je polje $\mathbf{F}$ algebraski zatvoreno i neka je $\mathcal{S}$ data familija komutativnih linearnih transformacija. Slučaj kada su sve linearne transformacije skalarne

(dakle, za svaku datu linearnu transformaciju $A$ postoji skalar $\lambda_A$ takav da je $(\mathbf{v})A = \lambda_A\mathbf{v}$ za svaki vektor $\mathbf{v}$) je trivijalan. Uzmimo stoga da, recimo, linearna transformacija $A$ (sa odgovarajućom matricom – u oznaci opet $A$) nije skalarna. Neka je $\lambda$ jedan njen karakteristični koren (jedno rešenje jednačine $det(xI - A) = 0$) i neka je $\mathbf{W}_\lambda$ njemu odgovarajući invarijantan potprostor ($W_\lambda \stackrel{\text{def}}{=} \{\mathbf{v} \mid (\mathbf{v})A = \lambda\mathbf{v}\}$). Jasno, $dim(\mathbf{W}_\lambda) \leq k-1$ i $A|_{W_\lambda}$ je skalarna transformacija prostora $\mathbf{W}_\lambda$. Lako se pokazuje da je ovaj potprostor invarijantan za sve linearne transformacije komutativne sa $A$, dakle posebno, za sve transformacije familije $\mathcal{S}$; ako je $\mathbf{v} \in W_\lambda$ i $B \in \mathcal{S}$, onda je $((\mathbf{v})B)A = ((\mathbf{v})A)B = (\lambda\mathbf{v})B = \lambda(\mathbf{v})B$, pa je i $(\mathbf{v})B \in W_\lambda$. Posmatrajmo restrikcije svih linearnih transformacija iz $\mathcal{S}$ nad $W_\lambda$. Naravno, one su sve uzajamno komutativne i na neki način se vraćamo na polazni problem, s tim što je sada dimenzija prostora manja. Ako ni ove restrikcije nisu sve skalarne transformacije prostora $\mathbf{W}_\lambda$, odabiramo jednu, npr. $B|_{W_\lambda}$, $B \in \mathcal{S} \setminus \{A\}$ i ponavljamo "postupak". Dobijamo tako novi potprostor (prostora $\mathbf{W}_\lambda$) dimenzije manje od $dim(\mathbf{W}_\lambda)$; restrikcije od $A$ i $B$ nad tim potprostorom su skalarne, a ako to nije slučaj i sa ostalim transformacijama iz $\mathcal{S}$, produžavamo dalje. No evidentno, taj proces ne može ići u nedogled, te nakon konačno mnogo koraka dolazimo do nenula potprostora takvog da su restrikcije svih transformacija iz $\mathcal{S}$ nad njim skalarne. Svaki vektor tog prostora je onda zajednički karakteristični vektor svih transformacija iz $\mathcal{S}$.

Prelazimo na dokaz leme indukcijom po klasi nilpotentnosti grupe $\mathbf{H} - k$, uz napomenu da ćemo identifikovati linearne transformacije i njima odgovarajuće matrice.

Ako je $k = 1$, tj. $\mathbf{H}$ Abelova grupa, onda prema $(a)$ svi elementi iz $\mathbf{H}$ imaju zajednički karakteristični vektor, recimo $v_1$, pa je, s obzirom da su svi karakteristični koreni 1, $(v_1)A = v_1$ za svako $A$ iz $\mathbf{H}$. Neka je $\mathbf{V}_1$ invarijantan potprostor za sve transformacije iz $\mathbf{H}$ ($\forall A \in H \ (V_1)A \subseteq V_1$) prostora $\mathbf{Ra}^n$ generisan vektorom $v_1$. Tada prema $(a)$ i $(b)$ uzajamno permutabilne transformacije skupa $\{A_1 \mid A \in H\}$ vektorskog prostora $\mathbf{Ra}^n/\mathbf{V}_1$ imaju zajednički karakteristični vektor – $v_2 + V_1$, koji je za sve njih i fiksan: $\forall A_1 \ (v_2 + V_1)A_1 = (v_2)A + V_1 = v_2 + V_1$. Dakle, $(v_2)A = v_2 + \alpha_A v_1$ (gde je $\alpha_A$ skalar u funkciji transformacije $A$). Prostor $\mathbf{V}_2$ generisan vektorima $v_1$ i $v_2$ je, jasno, invarijantan za sve transformacije iz $\mathbf{H}$, te se priča ponavlja, ovog puta za faktor prostor $\mathbf{Ra}^n/\mathbf{V}_2$. Sada je, za neki vektor $v_3$ i svako $A$ iz $\mathbf{H}$: $(v_3)A = v_3 + \beta_A v_1 + \gamma_A v_2$ (gde su, treba li ponavljati? $\beta_A$ i $\gamma_A$ skalari u funkciji transformacije $A$). Konačno, sukcesivnim ponavljanjem postupka nalazimo bazu prostora $\mathbf{Ra}^n$ – $\{v_1, v_2, \ldots, v_n\}$ – u odnosu na koju su sve transformacije grupe $\mathbf{H}$ gornje trougaone matrice sa 1 na svim mestima glavne dijagonale. Drugim rečima, ako je $P$ matrica čije su vektor kolone elementi novodobijene baze, onda je, za svako $A \in H$, $P^{-1}AP$ jedna takva gornja trougaona matrica.



Pretpostavimo u nastavku da za svaku nilpotentnu grupu klase nilpotentnosti manje od ili jednake $k$ i sa unipotentnim matricama kao elementima postoji niz invarijantnih potprostora $\mathbf{Ra}^n = \mathbf{U}_0 > \mathbf{U}_1 > \cdots > \mathbf{U}_n = \mathbf{O}$ takav da su svi faktor prostori $\mathbf{U}_{i-1}/\mathbf{U}_i$, $i = 1, \ldots, n$, jednodimenzionalni i na svakom od tih prostora transformacije indukovane transformacijama grupe deluju trivijalno. Neka je $\mathbf{H}$ nilpotentna grupa klase $k+1$, čiji su svi elementi unipotentne matrice, a $\mathbf{Ra}^n = \mathbf{V}_m > \mathbf{V}_{m-1} > \cdots > \mathbf{V}_0 = \mathbf{O}$ niz invarijantnih potprostora za grupu $\mathbf{H}$ koji se ne može proširiti. Nađimo jednu bazu prostora $\mathbf{Ra}^n$ tako što ćemo (jednu) bazu prostora $\mathbf{V}_1$ proširiti do (jedne) baze prostora $\mathbf{V}_2$, ovu pak do baze prostora $\mathbf{V}_3$ i tako redom. Prema tome, odgovarajući podskupovi date baze su baze svakog od prostora $\mathbf{V}_i$, $i = 1, \ldots, m$. U odnosu na nju elementima iz $\mathbf{H}$ odgovaraju blok matrice (u smislu poslednje rečenice prethodnog paragrafa), gde su svi blokovi ispod, uslovno rečeno, glavne dijagonale nula blokovi, a $i$-tom dijagonalnom bloku odgovara dejstvo grupe $\mathbf{H}$ na faktor prostor $\mathbf{V}_i/\mathbf{V}_{i-1}$. Imamo u vidu: ako je npr. $\mathcal{B}_1 = \{v_1^1, \ldots, v_{i_1}^1\}$ baza prostora $\mathbf{V}_1$, $\mathcal{B}_2 = \mathcal{B}_1 \cup \{v_1^2, \ldots, v_{i_2}^2\}$ baza prostora $\mathbf{V}_2$ i, za $A \in H$, $(v_1^2)A = \alpha_1 v_1^1 + \cdots + \alpha_{i_1} v_{i_1}^1 + \beta_1 v_1^2 + \cdots + \beta_{i_2} v_{i_2}^2$, onda je $(v_1^2 + V_1)A_1 = (v_1^2)A + V_1 = (\alpha_1 v_1^1 + \cdots + \alpha_{i_1} v_{i_1}^1 + \beta_1 v_1^2 + \cdots + \beta_{i_2} v_{i_2}^2) + V_1 = (\beta_1 v_1^2 + \cdots + \beta_{i_2} v_{i_2}^2) + V_1 = \beta_1(v_1^2 + V_1) + \cdots + \beta_{i_2}(v_{i_2}^2 + V_1)$. Prema induktivnoj pretpostavci gornji niz potprostora se može proširiti do niza invarijantnih potprostora za podgrupu $\gamma_1\mathbf{H}$ čiji su svi faktor prostori jednodimenzionalni i na svaki od njih $\gamma_1\mathbf{H}$ deluje trivijalno (svaka linearna transformacija svakog faktor prostora indukovana bilo kojim elementom grupe $\gamma_1\mathbf{H}$ je identično preslikavanje). Pokazaćemo da $\mathbf{H}$ dejstvuje trivijalno na svaki prostor $\mathbf{V}_i/\mathbf{V}_{i-1}$, $i = 1, \ldots, m$. Fiksirajmo jedan: $\mathbf{W}_i = \mathbf{V}_i/\mathbf{V}_{i-1}$. Neka je $\overline{\mathbf{W}}_i$ (nenula) potprostor prostora $\mathbf{W}_i$ čiji je domen skup svih vektora koji ostaju fiksnim za svaku transformaciju iz $\gamma_1\mathbf{H}$ (znamo zasigurno da $\mathbf{W}_i$ sadrži jednodimenzionalni potprostor na koji $\gamma_1\mathbf{H}$ dejstvuje trivijalno). Ovaj potprostor je invarijantan za grupu $\mathbf{H}$: ako je $A \in H$, $B \in \gamma_1 H$ i $v + V_{i-1} \in \overline{W}_i$, onda je $((v+V_{i-1})A)B = ((v+V_{i-1})ABA^{-1})A = (v+V_{i-1})A$ (jer je $ABA^{-1} \in \gamma_1 H$). Pošto $\mathbf{W}_i$ nema netrivijalnih invarijantnih potprostora za grupu $\mathbf{H}$, sledi $\mathbf{W}_i = \overline{\mathbf{W}}_i$, što će reći da $\gamma_1\mathbf{H}$ deluje trivijalno na ceo prostor $\mathbf{W}_i$. Odatle dalje proizilazi da grupa $\mathbf{H}$ indukuje jednu Abelovu podgrupu linearnih transformacija prostora $\mathbf{W}_i$ – $\overline{\mathbf{H}}$. Prema već navedenom za Abelove grupe, transformacije iz $\overline{\mathbf{H}}$ imaju zajednički karakteristični vektor, recimo $v + V_{i-1}$, koji one ostavljaju i fiksnim (podsećamo, prema $(b)$ su svi karakteristični koreni tih transformacija 1). Na jednodimenzionalni potprostor prostora $\mathbf{W}_i$ generisanog tim vektorom $\overline{\mathbf{H}}$ deluje trivijalno, a potprostor generisan skupom $V_{i-1} \cup \{v\}$, u oznaci $\langle v, V_{i-1}\rangle$, je invarijantan za $\mathbf{H}$. Stoga je $\langle v, V_{i-1}\rangle = V_i$ i $\mathbf{V}_i/\mathbf{V}_{i-1} = \langle v + V_{i-1}\rangle$.

Preostaje da se dokaže poslednji deo tvrđenja. Neka je grupa $\mathbf{H}$ generisana skupom $\{A_1, \ldots, A_r\}$ i neka je, za $P \in GL_n(\mathbf{Ra})$, $P^{-1}\mathbf{H}P \leq \mathbf{UT}_n(\mathbf{Ra})$. Ako je $t$ najmanji zajednički sadržalac imenilaca svih elemenata matrica $A_1, \ldots, A_r$

i $Q = diag(1, t, t^2, \ldots, t^{n-1})$, tada je, što se neposredno proverava,

$$(PQ)^{-1}\mathbf{H}PQ \leq \mathbf{UT}_n(\mathbf{Z}).\square$$

**Teorema 48.14** *(Teorema Fittinga). Ako su* $\mathbf{M}$ *i* $\mathbf{N}$ *normalne nilpotentne podgrupe grupe* $\mathbf{G}$ *klasa, respektivno,* $m$ *i* $n$*, tada je* $\mathbf{MN}$ *nilpotentna grupa klase najviše* $m + n$*.*

**Dokaz**. Dokazujemo indukcijom po $i \geq 1$ da je $\gamma_i(\mathbf{MN})$ proizvod svih normalnih podgrupa oblika $[\mathbf{X}_1, \ldots, \mathbf{X}_{i+1}]$, gde je $\mathbf{X}_j$ $(j = 1, \ldots, i+1)$ ili $\mathbf{M}$ ili $\mathbf{N}$. U osnovi dokaza su tačke $(a)$ i $(c)$ leme 6.10. Za $i = 1$ imamo: $\gamma_1(\mathbf{MN}) = (\mathbf{MN})' = [\mathbf{MN}, \mathbf{MN}] = [\mathbf{M}, \mathbf{MN}] \cdot [\mathbf{N}, \mathbf{MN}] = [\mathbf{M}, \mathbf{M}] \cdot [\mathbf{M}, \mathbf{N}] \cdot [\mathbf{N}, \mathbf{M}] \cdot [\mathbf{N}, \mathbf{N}]$ $(= [\mathbf{M}, \mathbf{M}] \cdot [\mathbf{M}, \mathbf{N}] \cdot [\mathbf{N}, \mathbf{N}])$ (prema 6.10$(a)$ sve pomenute podgrupe su normalne, a prema tački $(c)$ je izvršeno "množenje"; koristili smo i poznatu, i trivijalnu, činjenicu: $[\mathbf{A}, \mathbf{B}] = [\mathbf{B}, \mathbf{A}]$). Pretpostavimo da je tvrđenje tačno za svako $k \leq i$. Onda je $\gamma_{i+1}(\mathbf{MN}) = [\gamma_i(\mathbf{MN}), \mathbf{MN}] = [\gamma_i(\mathbf{MN}), \mathbf{M}] \cdot [\gamma_i(\mathbf{MN}), \mathbf{N}]$ i prema induktivnoj hipotezi $\gamma_{i+1}(\mathbf{MN})$ je proizvod svih podgrupa $[\mathbf{X}_1, \ldots, \mathbf{X}_{i+2}]$, gde je, ponavljamo, $\mathbf{X}_j$ ili $\mathbf{M}$ ili $\mathbf{N}$. Primetimo dalje da ako se, recimo, $\mathbf{M}$ javlja u $[\mathbf{X}_1, \ldots, \mathbf{X}_k]$ $j+1$ puta, $1 \leq j+1 \leq k$, onda je $[\mathbf{X}_1, \ldots, \mathbf{X}_k] \leq \gamma_j\mathbf{M}$. U pitanju je direktna posledica tačke $(a)$ leme 6.10 i činjenice da je (za svako $l$) $\gamma_l\mathbf{M}$ normalna podgrupa grupe $\mathbf{G}$ (formalni dokaz je opet indukcijom). Kako se u (svakoj od grupa) $[\mathbf{X}_1, \ldots, \mathbf{X}_{m+n+1}]$ javlja ili $\mathbf{M}$ barem $m+1$ puta ili $\mathbf{N}$ barem $n+1$ puta, proizilazi da je $[\mathbf{X}_1, \ldots, \mathbf{X}_{m+n+1}] = \mathbf{E}$ (jer je $\gamma_m\mathbf{M} = \gamma_n\mathbf{N} = \mathbf{E}$), te je i $\gamma_{m+n}(\mathbf{MN}) = \mathbf{E}$.■

**Napomena**. Uslov iz prethodne teoreme da su obe podgrupe normalne ne može se oslabiti. Opet je tu kontraprimer grupa $\mathbf{S}_3$ sa svojim nilpotentnim podgrupama $\mathbf{A}_3$ i $\mathbf{H} = \langle(0\ 1)\rangle$ $(\mathbf{S}_3 = \mathbf{A}_3\mathbf{H})$.

**Lema 48.15** *Ako je* $\mathbf{N}$ *nejedinična normalna podgrupa nilpotentne grupe* $\mathbf{G}$*, onda je* $\mathbf{N} \cap \mathbf{Z}(\mathbf{G}) \neq \mathbf{E}$*.*

**Dokaz**. Neka je $\mathbf{E} = \zeta_0\mathbf{G} < \zeta_1\mathbf{G} < \cdots < \zeta_{k-1}\mathbf{G} < \zeta_k\mathbf{G} = \mathbf{G}$ viši centralni niz grupe $\mathbf{G}$ i neka je $i$ najmanji prirodan broj za koji je $\mathbf{N} \cap \zeta_i\mathbf{G} \neq \mathbf{E}$. Prema lemama 46.25(3) i 6.10$(a)$ je $[\mathbf{N} \cap \zeta_i\mathbf{G}, \mathbf{G}] \leq \mathbf{N} \cap \zeta_{i-1}\mathbf{G} = \mathbf{E}$ (dakle, elementi iz $\mathbf{N} \cap \zeta_i\mathbf{G}$ su permutabilni sa svim elementima iz $\mathbf{G}$). Stoga je $\mathbf{N} \cap \zeta_i\mathbf{G} \leq \mathbf{N} \cap \zeta_1\mathbf{G} = \mathbf{N} \cap \mathbf{Z}(\mathbf{G})$, pa je, zapravo, $i = 1$.□

**Korolar 48.16** *Minimalna normalna podgrupa nilpotentne grupe sadržana je u centru grupe i prostog je reda.*

**Dokaz**. Neka je $\mathbf{N}$ minimalna normalna podgrupa nilpotentne grupe $\mathbf{G}$. Prema prethodnoj lemi je $\mathbf{N} \cap \mathbf{Z}(\mathbf{G}) \neq \mathbf{E}$, te je $\mathbf{N} \cap \mathbf{Z}(\mathbf{G}) = \mathbf{N}$, odnosno $\mathbf{N} \leq \mathbf{Z}(\mathbf{G})$.□



**Korolar 48.17** *Ako je* $\mathbf{N}$ *normalna podgrupa reda* $p^m$ *(*$p$ *prost broj) nilpotentne grupe* $\mathbf{G}$*, tada je* $\mathbf{N} \leq \zeta_m\mathbf{G}$*.*

**Dokaz**. Prema 48.15 je, videli smo, $\mathbf{N} \cap \mathbf{Z}(\mathbf{G})$ $(= \mathbf{N} \cap \zeta_1\mathbf{G})$ nejedinična podgrupa (pod)grupe $\mathbf{N}$. Ako već nije $\mathbf{N} \leq \zeta_1\mathbf{G}$, onda je $(\mathbf{N}\zeta_1\mathbf{G})/\zeta_1\mathbf{G}$ nejedinična normalna podgrupa grupe $\mathbf{G}/\zeta_1\mathbf{G}$ pa je, opet prema 48.15 ali sada zajedno sa 5.27, $(\mathbf{N}\zeta_1\mathbf{G})/\zeta_1\mathbf{G} \cap \zeta_2\mathbf{G}/\zeta_1\mathbf{G} = (\mathbf{N}\zeta_1\mathbf{G} \cap \zeta_2\mathbf{G})/\zeta_1\mathbf{G} = ((\mathbf{N} \cap \zeta_2\mathbf{G})\zeta_1\mathbf{G})/\zeta_1\mathbf{G}$ nejedinična podgrupa, tj. $\mathbf{N} \cap \zeta_2\mathbf{G}$ nije podgrupa grupe $\zeta_1\mathbf{G}$, odnosno $\mathbf{N} \cap \zeta_1\mathbf{G}$ je prava podgrupa grupe $\mathbf{N} \cap \zeta_2\mathbf{G}$. Ukoliko nije ni $\mathbf{N} \leq \zeta_2\mathbf{G}$, postupak ponavljamo: $(\mathbf{N}\zeta_2\mathbf{G})/\zeta_2\mathbf{G}$ je normalna nejedinična podgrupa grupe $\mathbf{G}/\zeta_2\mathbf{G}$, ima netrivijalan presek sa njenim centrom $(\zeta_3\mathbf{G}/\zeta_2\mathbf{G})$ i ponovo će $\mathbf{N} \cap \zeta_2\mathbf{G}$ biti prava podgrupa grupe $\mathbf{N} \cap \zeta_3\mathbf{G}$. S obzirom na red grupe $\mathbf{N}$ jasno je da će u najviše $m$ koraka proces stati, drugim rečima, $\mathbf{N}$ je svakako podgrupa grupe $\zeta_m\mathbf{G}$.□

**Korolar 48.18** *Neka su* $\mathbf{H}$ *i* $\mathbf{K}$ *normalne podgrupe nilpotentne grupe* $\mathbf{G}$ *i neka je* $\mathbf{K}$ *prava podgrupa grupe* $\mathbf{H}$*. Tada postoji normalna podgrupa* $\mathbf{M}$ *grupe* $\mathbf{G}$ *koja strogo sadrži* $\mathbf{K}$*, sadržana je u* $\mathbf{H}$ *i faktor grupa* $\mathbf{M}/\mathbf{K}$ *je ciklična.*

**Dokaz**. Faktor grupa $\mathbf{G}/\mathbf{K}$ je nilpotentna, $\mathbf{H}/\mathbf{K}$ je njena nejedinična normalna podgrupa, te je $H/K \cap Z(\mathbf{G}/\mathbf{K}) \neq \{K\}$. Neka je $(K \neq)\, zK \in H/K \cap Z(\mathbf{G}/\mathbf{K})$. Onda je $\langle z, K\rangle/\mathbf{K}$ normalna podgrupa grupe $\mathbf{G}/\mathbf{K}$, pa je $\mathbf{M} = \langle z, K\rangle$ normalna podgrupa grupe $\mathbf{G}$ i, jasno, $\mathbf{M} \leq \mathbf{H}$ i $\mathbf{M}/\mathbf{K} = \langle zK\rangle$.□

**Korolar 48.19** *Neka nilpotentna grupa* $\mathbf{G}$ *ispunjava uslov maksimalnosti normalnih podgrupa (svaka neprazna familija normalnih podgrupa ima s obzirom na inkluziju maksimalni element). Tada važi:*

*(a) postoji invarijantni niz podgrupa* $\mathbf{E} = \mathbf{G}_0 < \mathbf{G}_1 < \cdots < \mathbf{G}_n = \mathbf{G}$ *takav da su grupe* $\mathbf{G}_{i+1}/\mathbf{G}_i$*,* $i = 0, \ldots, n-1$*, ciklične;*

*(b) svaka podgrupa grupe* $\mathbf{G}$ *je konačno generisana.*

**Dokaz**. $(a)$ Neposredna posledica prethodnog korolara. Za $\mathbf{G}_1$ uzimamo bilo koju nejediničnu normalnu cikličnu podgrupu grupe $\mathbf{G}$. Dalje, $\mathbf{G}_2$ je normalna podgrupa grupe $\mathbf{G}$ koja strogo sadrži $\mathbf{G}_1$ i čija je faktor grupa $\mathbf{G}_2/\mathbf{G}_1$ ciklična itd. Prema uslovu korolara rastući lanac normalnih podgrupa $\mathbf{E} < \mathbf{G}_1 < \mathbf{G}_2 < \cdots$ postaje posle konačno mnogo "koraka" stacionaran, dakle, za neko $n$ je $\mathbf{G}_n = \mathbf{G}_{n+1} = \cdots$. No jasno, prema samoj konstrukciji lanca je $\mathbf{G}_n = \mathbf{G}$.

$(b)$ Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$ i $\mathbf{E} = \mathbf{G}_0 < \mathbf{G}_1 < \cdots < \mathbf{G}_n = \mathbf{G}$ invarijantni niz grupe $\mathbf{G}$ iz prethodne tačke. Posmatrajmo rastući lanac normalnih podgrupa grupe $\mathbf{H}$: $\mathbf{E} = \mathbf{H}_0 = \mathbf{H} \cap \mathbf{G}_0 \leq \mathbf{H}_1 = \mathbf{H} \cap \mathbf{G}_1 \leq \cdots \leq \mathbf{H} = \mathbf{H}_n = \mathbf{H} \cap \mathbf{G}_n$ $(\mathbf{G}_i \lhd \mathbf{G}$ implicira $\mathbf{H}_i = \mathbf{H} \cap \mathbf{G}_i \lhd \mathbf{H})$. Prema drugoj teoremi o izomorfizmu za svako $i = 0, \ldots, n-1$ važi:

$$\mathbf{H}_{i+1}/\mathbf{H}_i = (\mathbf{H} \cap \mathbf{G}_{i+1})/((\mathbf{H} \cap \mathbf{G}_{i+1}) \cap \mathbf{G}_i) \cong$$

$$((\mathbf{H}\cap\mathbf{G}_{i+1})\cdot\mathbf{G}_i)/\mathbf{G}_i=(\mathbf{H}_{i+1}\cdot\mathbf{G}_i)/\mathbf{G}_i\leq\mathbf{G}_{i+1}/\mathbf{G}_i,$$

pa je $\mathbf{H}_{i+1}/\mathbf{H}_i$ ciklična grupa. Neka je za $h_{i+1}\in H_{i+1}$ $(i=0,\ldots,n-1)$ $\mathbf{H}_{i+1}/\mathbf{H}_i=\langle h_{i+1}H_i\rangle$. Tada je, očigledno, $\mathbf{H}=\langle h_1,\ldots,h_n\rangle$. U vezi ove tačke videti 5.15.□

**Lema 48.20** *Ako je* $\mathbf{A}$ *maksimalna normalna Abelova podgrupa nilpotentne grupe* $\mathbf{G}$ *(ovde dozvoljavamo mogućnost da je* $\mathbf{A}$ *baš cela grupa), tada je* $\mathbf{A}=\mathbf{C}(\mathbf{A})$. *Posebno, ako je* $\mathbf{A}$ *konačna grupa, onda je i* $\mathbf{G}$ *konačna grupa.*

**Dokaz.** $\mathbf{C}(\mathbf{A})$ je, podsećamo, centralizator podgrupe $\mathbf{A}$.

Pošto je $\mathbf{A}$ Abelova grupa, važi $\mathbf{A}\leq\mathbf{C}(\mathbf{A})$. Ako bi $\mathbf{A}$ bila prava podgrupa grupe $\mathbf{C}(\mathbf{A})$, onda bi $\mathbf{C}(\mathbf{A})/\mathbf{A}$ bila nejedinična normalna podgrupa nilpotentne grupe $\mathbf{G}/\mathbf{A}$ (jer je $\mathbf{C}(\mathbf{A})\lhd\mathbf{G}$), i prema prethodnoj lemi bi bilo $\mathbf{C}(\mathbf{A})/\mathbf{A}\cap\mathbf{Z}(\mathbf{G}/\mathbf{A})\neq\overline{\mathbf{E}}$ (jedinična podgrupa grupe $\mathbf{G}/\mathbf{A}$). No za $g$ takvo da je $(A\neq)\ gA\in C(\mathbf{A})/A\cap Z(\mathbf{G}/\mathbf{A})$ bila bi $\langle g,A\rangle$ Abelova normalna podgrupa grupe $\mathbf{G}$ koja strogo sadrži $\mathbf{A}$, kontradikcija (normalnost podgrupe $\langle g,A\rangle$ sledi iz normalnosti podgrupe $\langle g,A\rangle/\mathbf{A}$ faktor grupe $\mathbf{G}/\mathbf{A}$ - $\langle g,A\rangle/\mathbf{A}\leq\mathbf{Z}(\mathbf{G}/\mathbf{A})$).

Pretpostavimo sada da je $\mathbf{A}$ konačna grupa. No onda je i njen indeks $[\mathbf{G}:\mathbf{A}]$ konačan, dakle i $\mathbf{G}$ je konačna grupa. Jer, $\mathbf{Aut}(\mathbf{A})$ je konačna grupa, a ako je $\{g_\alpha\mid\alpha<[\mathbf{G}:\mathbf{A}]\}$ jedna desna transverzala podgrupe $\mathbf{A}$, onda je $\{u_{g_\alpha}|_A\mid\alpha<[\mathbf{G}:\mathbf{A}]\}$ skup različitih automorfizama podgrupe $\mathbf{A}$ (jasno, $u_g|_A=u_h|_A$ implicira $gh^{-1}\in C(\mathbf{A})=A$, tj. $Ag=Ah$).□

**Korolar 48.21** *Ako je* $\mathbf{A}$ *maksimalna normalna Abelova podgrupa nilpotentne grupe* $\mathbf{G}$, *onda je* $\mathbf{A}$ *i maksimalna Abelova podgrupa grupe* $\mathbf{G}$. *Grupa* $\mathbf{G}/\mathbf{A}$ *se utapa u grupu* $\mathbf{Aut}(\mathbf{A})$.

**Dokaz.** Utapanje je dato sa: $gA\longrightarrow u_g|_A$.□

**Lema 48.22** *Podgrupa konačno generisane nilpotentne grupe je konačno generisana; drugim rečima, konačno generisana nilpotentna grupa ispunjava uslov maksimalnosti podgrupa.*

**Dokaz.** Neka je $\mathbf{G}$ konačno generisana nilpotentna grupa sa nižim centralnim nizom $\mathbf{G}=\gamma_0\mathbf{G}>\gamma_1\mathbf{G}>\cdots>\gamma_{k-1}\mathbf{G}>\gamma_k\mathbf{G}=\mathbf{E}$ i neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$. Prema 48.5, opadajući niz podgrupa grupe $\mathbf{H}$ - $\mathbf{H}_0=\mathbf{H}\cap\gamma_0\mathbf{G}\geq\mathbf{H}_1=\mathbf{H}\cap\gamma_1\mathbf{G}\geq\cdots\geq\mathbf{H}_{k-1}=\mathbf{H}\cap\gamma_{k-1}\mathbf{G}\geq\mathbf{H}_k=\mathbf{H}\cap\gamma_k\mathbf{G}=\mathbf{E}$ je, kada se eliminiše eventualni "višak" podgrupa, centralni niz grupe $\mathbf{H}$. No to nam sada nije u prvom planu. Uočimo da je prema drugoj teoremi o izomorfizmu:

$$\mathbf{H}_{i-1}/\mathbf{H}_i=(\mathbf{H}\cap\gamma_{i-1}\mathbf{G})/(\mathbf{H}\cap\gamma_i\mathbf{G})=(\mathbf{H}\cap\gamma_{i-1}\mathbf{G})/((\mathbf{H}\cap\gamma_{i-1}\mathbf{G})\cap\gamma_i\mathbf{G})\cong$$

$$(\gamma_i\mathbf{G}\cdot(\mathbf{H}\cap\gamma_{i-1}\mathbf{G}))/\gamma_i\mathbf{G}\leq\gamma_{i-1}\mathbf{G}/\gamma_i\mathbf{G}.$$



Prema 46.29, $\gamma_{i-1}\mathbf{G}/\gamma_i\mathbf{G}$ je konačno generisana Abelova grupa, pa je i svaka njena podgrupa konačno generisana (32.7). Polazeći od očigledne činjenice:

*ako je* $\mathbf{N}$ *normalna podgrupa grupe* $\mathbf{K}$ *i ako su* $\mathbf{N}$ *i* $\mathbf{K}/\mathbf{N}$ *konačno generisane grupe, onda je i* $\mathbf{K}$ *konačno generisana grupa,*

izvodimo: $\mathbf{H}_{k-1}$ $(\cong\mathbf{H}_{k-1}/\mathbf{E})$ je konačno generisana, $\mathbf{H}_{k-2}$ je konačno generisana (jer su $\mathbf{H}_{k-1}$ i $\mathbf{H}_{k-2}/\mathbf{H}_{k-1}$ konačno generisane grupe), a onda redom i $\mathbf{H}_{k-3},\ldots,\mathbf{H}_1,\mathbf{H}_0=\mathbf{H}$.□

**Korolar 48.23** *Konačno generisana nilpotentna grupa ima centralni niz čiji su faktori ciklične grupe. Posebno, ako je grupa i torziono slobodna, onda ima centralni niz čiji su faktori beskonačne ciklične grupe.*

**Dokaz.** Direktno prema prethodnoj lemi, 46.31, 32.2 i očiglednoj činjenici da je proširenje centralnog niza centralni niz.□

**Lema 48.24** *Nilpotentna grupa generisana konačnim skupom elemenata konačnih redova je konačna.*

**Dokaz.** Neka je nilpotentna grupa $\mathbf{G}$ generisana skupom $\{g_1,\ldots,g_n\}$, gde je svaki element $g_j$ $(j=1,\ldots,n)$ konačnog reda - $n_j$, i neka je $\mathbf{G}=\gamma_0\mathbf{G}>\gamma_1\mathbf{G}>\cdots>\gamma_{k-1}\mathbf{G}>\gamma_k\mathbf{G}=\mathbf{E}$ njen niži centralni niz. Abelove grupe $\gamma_{i-1}\mathbf{G}/\gamma_i\mathbf{G}$ su, videli smo, konačno generisane, štaviše imaju konačni generatorni skup sa elementima konačnih redova, pa su konačne. Dokazaćemo to indukcijom po $i$ $(\geq1)$. Za $i=1$ imamo: grupa $\mathbf{G}/\gamma_1\mathbf{G}=\mathbf{G}/\mathbf{G}'$ je generisana skupom $\{g_1\mathbf{G}',\ldots,g_n\mathbf{G}'\}$. Pretpostavimo da je tvrđenje tačno za svako $j\leq i$ i neka je $\{a_1\,\gamma_iG,\ldots,a_m\,\gamma_iG\}$ generatorni skup grupe $\gamma_{i-1}\mathbf{G}/\gamma_i\mathbf{G}$, gde su svi elementi $a_l\,\gamma_iG$, $l=1,\ldots,m$, konačnog reda. Ali tada, prema dokazu leme 46.28, skup $\{[a_r,g_s]\gamma_{i+1}G\mid r=1,\ldots,m,\ s=1,\ldots,n\}$ generiše grupu $\gamma_i\mathbf{G}/\gamma_{i+1}\mathbf{G}$. $g_s^{n_s}=e$ i 6.2$(e)$ nam pak daju:

$$\gamma_{i+1}G=[a_r,g_s^{n_s}]\gamma_{i+1}G=([a_r,g_s^{n_s-1}]g_s^{-(n_s-1)}[a_r,g_s]g_s^{n_s-1})\gamma_{i+1}G=$$

$$([a_r,g_s^{n_s-1}]\,[a_r,g_s]\,[[a_r,g_s],g_s^{n_s-1}])\gamma_{i+1}G=[a_r,g_s^{n_s-1}]\gamma_{i+1}G\cdot[a_r,g_s]\gamma_{i+1}G=\cdots$$

(nastavljajući postupak)

$$=\underbrace{[a_r,g_s]\gamma_{i+1}G\cdots[a_r,g_s]\gamma_{i+1}G}_{n_s-puta}=([a_r,g_s]\gamma_{i+1}G)^{n_s}.$$

Prema tome, red elementa $[a_r,g_s]\gamma_{i+1}G$ (faktor grupe $\gamma_i\mathbf{G}/\gamma_{i+1}\mathbf{G}$) deli $n_s$. Iz konačnosti grupa $\gamma_{i-1}\mathbf{G}/\gamma_i\mathbf{G}$, $i=1,\ldots,k$, sledi konačnost grupe $\mathbf{G}$; ponavljamo se: $\gamma_{k-1}\mathbf{G}$ $(\cong\gamma_{k-1}\mathbf{G}/\mathbf{E})$ je konačna grupa (jer je $\gamma_{k-1}\mathbf{G}$ $(\leq\mathbf{Z}(\mathbf{G}))$ Abelova grupa - 48.3), $\gamma_{k-2}\mathbf{G}$ je konačna grupa jer su $\gamma_{k-1}\mathbf{G}$ i $\gamma_{k-2}\mathbf{G}/\gamma_{k-1}\mathbf{G}$ konačne grupe i tako dalje.□

**Lema 48.25** *Elementi konačnog reda (ma koje) nilpotentne grupe obrazuju potpuno invarijantnu podgrupu čija je faktor grupa, ukoliko grupa nije periodična, torziono slobodna.*

**Dokaz.** Neka je $\mathbf{G}$ nilpotentna mešovita grupa (trivijalni su slučajevi kada je $\mathbf{G}$ periodična ili torziono slobodna) i neka su $a$ i $b$ dva njena elementa konačnog reda. Onda je, prema prethodnoj lemi (i 48.5), podgrupa $\langle a, b\rangle$ konačna, pa je element $ab^{-1}$ konačnog reda. Stoga je $N = \{g \in G \mid g$ je konačnog reda $\}$ domen podgrupe i to potpuno invarijantne. Očigledno, $\mathbf{G/N}$ je torziono slobodna grupa: iz $(gN)^k = N$ sledi $g^k \in N$, a onda i $g \in N$.□

**Korolar 48.26** *Neka je $\mathbf{G}$ nilpotentna grupa. Tada važi:*

*(a) Ako je $\mathbf{G}$ klase nilpotentnosti $k$ i $m$ eksponent centra grupe, onda $\mathbf{G}$ ima eksponent koji deli $m^k$;*

*(b) Ako je $\mathbf{G}$ konačno generisana i beskonačna grupa, onda $\mathbf{Z(G)}$ ima element beskonačnog reda.*

**Dokaz.** $(a)$ Indukcijom po klasi nilpotentnosti $k$. Slučaj $k = 0$ $(\mathbf{G} = \mathbf{E})$ i $k = 1$ $(\mathbf{G} = \mathbf{Z(G)} \neq \mathbf{E})$ su trivijalni. Pretpostavimo da je tvrđenje tačno za sve nilpotentne grupe klase nilpotentnosti $l < k$ $(> 1)$ i neka je $\mathbf{G}$ klase nilpotentnosti $k$, $\mathbf{Z(G)}$ $(= \zeta_1\mathbf{G})$ eksponenta $m$ i $a \in \zeta_2 G$. Tada je, za svako $g \in G$, $[a, g] \in \zeta_1 G$, pa je prema 6.2$(h)$ $e = [a, g]^m = [a^m, g]$. Odatle, $a^m \in Z(\mathbf{G})$, tj. faktor grupa $\zeta_2\mathbf{G}/\zeta_1\mathbf{G}$ $(= \mathbf{Z(G}/\zeta_1\mathbf{G}))$ ima eksponent koji deli $m$. Prema induktivnoj pretpostavci nilpotentna grupa $\mathbf{G/Z(G)}$, klase nilpotentnosti $k - 1$, ima eksponent koji deli $m^{k-1}$, što će reći da $\mathbf{G}$ ima eksponent koji deli $m^k$ (za $g \in G$ je $g^{m^{k-1}} \in Z(\mathbf{G})$, te je $(g^{m^{k-1}})^m = g^{m^k} = e$).

$(b)$ Centar grupe je, prema 48.22, takođe konačno generisan. Pretpostavka i da je periodična grupa implicirala bi da je i konačna grupa (32.2), što bi opet impliciralo, prema tački $(a)$, da je $\mathbf{G}$ periodična grupa. Ali tada bi $\mathbf{G}$ bila konačna grupa (48.24), kontradikcija.□

**Definicija 48.27** *Grupa ispunjava uslov normalizatora akko je svaka prava podgrupa strogo sadržana u svom normalizatoru.*

*Grupa koja ispunjava uslov normalizatora kratko se naziva $N$-grupa.*

Sledeća teorema odnosi se na neke od mogućih karakterizacija konačnih nilpotentnih grupa.

**Teorema 48.28** *Za konačnu grupu $\mathbf{G}$ sledeći uslovi su ekvivalentni:*

(1) *$\mathbf{G}$ je nilpotentna grupa;*

(2) *Svaka podgrupa grupe $\mathbf{G}$ je dostižna;*

(3) *$\mathbf{G}$ je $N$-grupa;*



(4) *Svaka maksimalna podgrupa grupe $\mathbf{G}$ je normalna;*

(5) $\mathbf{G'} \leq \mathbf{Fr(G)}$;

(6) *$\mathbf{G}$ je direktni proizvod svojih Sylowih podgrupa, tj. $\mathbf{G}$ je $S$-grupa;*

(7) *Elementi grupe $\mathbf{G}$ uzajamno prostih redova su permutabilni.*

**Dokaz.** (1) $\Longrightarrow$ (2) Neka je $\mathbf{H}$ podgrupa nilpotentne grupe $\mathbf{G}$ sa višim centralnim nizom: $\mathbf{E} = \zeta_0\mathbf{G} < \zeta_1\mathbf{G} = \mathbf{Z(G)} < \cdots < \zeta_{n-1}\mathbf{G} < \zeta_n\mathbf{G} = \mathbf{G}$. Onda je za svako $j$ $(j = 0, 1, \ldots, n-1)$ $\mathbf{H}\,\zeta_j\mathbf{G}$ normalna podgrupa grupe $\mathbf{H}\,\zeta_{j+1}\mathbf{G}$. Jer, $\zeta_{j+1}\mathbf{G}/\zeta_j\mathbf{G} = \mathbf{Z(G}/\zeta_j\mathbf{G})$ i stoga je $(\mathbf{H}\,\zeta_j\mathbf{G})/\zeta_j\mathbf{G} \lhd (\mathbf{H}\,\zeta_{j+1}\mathbf{G})/\zeta_j\mathbf{G}$; zaista, za $a \in \zeta_{j+1}G$ i $h, h_1 \in H$ je $(ha)^{-1}\zeta_j G \cdot h_1\zeta_j G \cdot (ha)\zeta_j G = a^{-1}\zeta_j G \cdot h^{-1}\zeta_j G \cdot h_1\zeta_j G \cdot h\zeta_j G \cdot a\zeta_j G = a^{-1}\zeta_j G \cdot (h^{-1}h_1 h)\zeta_j G \cdot a\zeta_j G = (h^{-1}h_1 h)\zeta_j G \in (H\,\zeta_j G)/\zeta_j G$. Prema tome: $\mathbf{H} = \mathbf{H}\,\zeta_0\mathbf{G} \trianglelefteq \mathbf{H}\,\zeta_1\mathbf{G} \trianglelefteq \cdots \trianglelefteq \mathbf{H}\,\zeta_{n-1}\mathbf{G} \trianglelefteq \mathbf{H}\,\zeta_n\mathbf{G} = \mathbf{G}$ i $\mathbf{H}$ je dostižna (podnormalna) grupa.

(2) $\Longrightarrow$ (3) Neka je ispunjen uslov (2) i neka je $\mathbf{H}$ prava podgrupa grupe $\mathbf{G}$. Kako je $\mathbf{H}$ dostižna podgrupa, postoji niz $\mathbf{H} = \mathbf{H}_0 \lhd \mathbf{H}_1 \lhd \cdots \lhd \mathbf{H}_k = \mathbf{G}$, i tako je $\mathbf{H}$ prava podgrupa grupe $\mathbf{H}_1 \leq \mathbf{N(H)}$ $(\mathbf{H}_1 = \mathbf{G}$ je moguće, ako je $\mathbf{H}$ normalna podgrupa).

(3) $\Longrightarrow$ (4) Neka važi (3) i neka je $\mathbf{H}$ maksimalna podgrupa grupe $\mathbf{G}$. No, onda je $\mathbf{H}$ prava podgrupa svog normalizatora $\mathbf{N(H)}$, pa je $\mathbf{N(H)} = \mathbf{G}$.

(4) $\Longrightarrow$ (5) Ova implikacija je već (generalno) dokazana – 8.12.

(5) $\Longrightarrow$ (6) Neka je $\mathbf{G'} \leq \mathbf{Fr(G)}$ i neka je $\mathbf{P}$ Sylowa $p$-podgrupa grupe $\mathbf{G}$. Ako $\mathbf{P}$ ne bi bila normalna podgrupa, onda bi njen normalizator bio sadržan u nekoj maksimalnoj podgrupi, recimo $\mathbf{M}$. Pošto je $\mathbf{G'} \leq \mathbf{Fr(G)} \leq \mathbf{M}$, $\mathbf{M}$ bi bila normalna podgrupa, dok je prema 16.33 $\mathbf{M} = \mathbf{N(M)}$, kontradikcija. Dakle, sve Sylowe podgrupe su normalne, a njihov direktni proizvod je cela grupa (uslovi definicije 10.8 su ispunjeni – elementi različitih Sylowih podgrupa su uzajamno permutabilni, jer je presek tih podgrupa jedinična grupa, te je i presek bilo koje Sylowe podgrupe i podgrupe generisane unijom ostalih Sylowih podgrupa jedinična grupa; za uslov $(a)$ definicije videti i 4.3$(b)$).

(6) $\Longleftrightarrow$ (7) Trivijalno. U pravcu $(\Longleftarrow)$ koristiti: ako su $\mathbf{P}_1, \ldots, \mathbf{P}_i$ Sylowe podgrupe za različite proste brojeve, onda je $P_1 \ldots P_i$ domen podgrupe.

(6) $\Longrightarrow$ (1) Neka važi (6). Prema 48.9$(a)$, svaka Sylowa podgrupa je nilpotentna, pa je i grupa $\mathbf{G}$ (kao konačan direktan proizvod nilpotentnih grupa) nilpotentna.■

**Korolar 48.29** *Ako je $\mathbf{G}$ konačna nilpotentna grupa takva da je $\mathbf{G/G'}$ ciklična grupa, onda je i sama ciklična.*

**Dokaz.** Direktna posledica prethodne teoreme i korolara 5.11.□

**Korolar 48.30** *Za grupu $\mathbf{G}$ važi:*

(*a*) *Ako je* $\mathbf{Fr(G)} \leq \mathbf{H} \lhd \mathbf{G}$, $\mathbf{H}$ *konačna grupa i* $\mathbf{H/Fr(G)}$ *nilpotentna grupa, tada je* $\mathbf{H}$ *nilpotentna grupa;*

(*b*) *Ako je* $\mathbf{Fr(G)}$ *konačna podgrupa, onda je i nilpotetna;*

(*c*) *Ako je* $\mathbf{G}$ *konačna grupa,* $\mathbf{Fr(G)}$ *je nilpotentna grupa.*

**Dokaz.** (*a*) Neka je $\mathbf{P}$ Sylowa $p$-podgrupa grupe $\mathbf{H}$. Prema 16.43, $(\mathbf{Fr(G)} \cdot \mathbf{P})/\mathbf{Fr(G)}$ je Sylowa $p$-podgrupa (po uslovu) nilpotentne grupe $\mathbf{H/Fr(G)}$, stoga prema prethodnoj teoremi i karakteristična podgrupa, a jasno, $\mathbf{H/Fr(G)}$ je normalna podgrupa grupe $\mathbf{G/Fr(G)}$. Odatle, $\mathbf{Fr(G)} \cdot \mathbf{P}$ je normalna podgrupa grupe $\mathbf{G}$, pa je prema 16.30 i 5.10 $\mathbf{G} = \mathbf{Fr(G)} \cdot \mathbf{P} \cdot \mathbf{N_G(P)} = \mathbf{Fr(G)} \cdot \mathbf{N_G(P)} = \mathbf{N_G(P)}$. Prema tome, $\mathbf{P}$ je normalna podgrupa grupe $\mathbf{G}$ a onda i podgrupe $\mathbf{H}$; dakle, $\mathbf{H}$ je nilpotentna grupa.□

**Korolar 48.31** *Neka je* $\mathbf{H}$ *podgrupa konačne p-grupe* $\mathbf{G}$. *Tada važi:* $\mathbf{Fr(G)} \leq \mathbf{H}$ *akko je* $\mathbf{H}$ *normalna podgrupa grupe* $\mathbf{G}$ *i* $\mathbf{G/H}$ *je elementarna Abelova p-grupa.*

**Dokaz.** ($\Longrightarrow$) $\mathbf{G}$ je nilpotentna grupa, pa $\mathbf{G'} \leq \mathbf{Fr(G)} \leq \mathbf{H}$ implicira: $\mathbf{H} \lhd \mathbf{G}$ i $\mathbf{G/H}$ je Abelova grupa (6.8). Prema 16.16, maksimalne podgrupe grupe $\mathbf{G}$ su reda $p^{n-1}$, dakle indeksa $p$, pa ako je $\mathbf{K}$ jedna takva, onda je $g^p \in K$ za svako $g \in G$. Stoga je i $g^p \in Fr(\mathbf{G}) \subseteq H$, te je $\mathbf{G/H}$ elementarna Abelova $p$-grupa.

($\Longleftarrow$) Neka je $\overline{\mathbf{G}} = \mathbf{G/H}$ elementarna Abelova $p$-grupa. Tada je $\mathbf{Fr}(\overline{\mathbf{G}}) = \overline{\mathbf{E}}$ (10.35) i prema tome, ako je $\{\overline{\mathbf{K}_i} = \mathbf{K}_i/\mathbf{H} \mid i \in I\}$ skup svih maksimalnih podgrupa grupe $\overline{\mathbf{G}}$, onda je $\bigcap_{i\in I} \mathbf{K}_i = \mathbf{H}$, a $\{\mathbf{K}_i \mid i \in I\}$ je podskup skupa svih maksimalnih podgrupa grupe $\mathbf{G}$ (zapravo, skup svih maksimalnih podgrupa grupe $\mathbf{G}$ koje sadrže $\mathbf{H}$ – 8.7). Sledi: $\mathbf{Fr(G)} \leq \bigcap_{i\in I} \mathbf{K}_i = \mathbf{H}$.□

**Korolar 48.32** *U nilpotentnoj grupi su elementi uzajamno prostih redova permutabilni.*

**Dokaz.** Neka su $a$ i $b$ elementi uzajamno prostih redova ($(red(a), red(b)) = 1$) nilpotentne grupe $\mathbf{G}$. Tada je, prema 48.24, $\langle a, b\rangle$ konačna nilpotentna grupa i prema prethodnoj teoremi $a$ i $b$ su uzajamno permutabilni.□

**Korolar 48.33** *Za svaki prost broj p nilpotentna grupa sadrži jedinstvenu Sylowu p-podgrupu; drugim rečima: nilpotentna grupa je S-grupa.*

**Dokaz.** Neka je $\mathbf{G}$ nilpotentna grupa. Skup $H = \{g \in G \mid$ red elementa $g$ je stepen prostog broja $p\}$ je domen $p$-grupe periodičnog dela grupe $\mathbf{G}$; $H \neq \emptyset$ jer je barem $e \in H$, a ako su $a$ i $b$ elementi iz $H$, onda je prema 48.25 $\langle a, b\rangle$ konačna nilpotentna i to, očigledno, $p$-grupa – u suprotnom bi grupa $\langle a, b\rangle$ bila direktni proizvod različitih Sylowih podgrupa i pošto bi oba elementa bila



u Sylowoj $p$-podgrupi ne bi generisala celu grupu. Jasno, $\mathbf{H}$ je jedinstvena Sylowa $p$-podgrupa.

Ovo tvrđenje je posledica i leme 54.3, jer svaka nilpotentna grupa je $N$ grupa – videti donju napomenu.□

**Korolar 48.34** *Ako nilpotentna grupa ima element reda p, onda i njen centar ima element reda p.*

**Dokaz.** Direktna posledica prethodnog korolara i leme 48.15.□

**Korolar 48.35** (*a*) *Periodični deo nilpotentne grupe* $\mathbf{G}$ *je direktni proizvod svih Sylowih p-podgrupa grupe* $\mathbf{G}$;

(*b*) *Za svaki skup prostih brojeva* $\Pi$ *nilpotentna grupa ima jedinstvenu Sylowu* $\Pi$*-podgrupu.*

**Korolar 48.36** *Konačna grupa* $\mathbf{G}$ *sadrži nilpotentnu podgrupu* $\mathbf{H}$ *takvu da je* $[\mathbf{H}]_\mathbf{G} = \mathbf{G}$.

**Dokaz.** Indukcijom po redu grupe. Pretpostavimo da je tvrđenje tačno za sve grupe reda manjeg od $n$ ($> 1$) i neka je $\mathbf{G}$ reda $n$. Ako je $\mathbf{G}$ nilpotentna grupa, uzimamo jednostavno $\mathbf{H} = \mathbf{G}$. Ako $\mathbf{G}$ nije nilpotentna grupa, onda prema prethodnoj teoremi ((1) $\Longleftrightarrow$ (4)) sadrži i maksimalnu podgrupu $\mathbf{K}$ koja nije normalna. Prema induktivnoj pretpostavci $\mathbf{K}$ sadrži nilpotentnu podgrupu $\mathbf{H}$ takvu da je $[\mathbf{H}]_\mathbf{K} = \mathbf{K}$ ($[\mathbf{H}]_\mathbf{K}$ je, podsećamo, normalno zatvorenje podgrupe $\mathbf{H}$ u $\mathbf{K}$ – 5.16). No kako je $[\mathbf{H}]_\mathbf{K} = [\mathbf{K}, \mathbf{H}]\,\mathbf{H} = \mathbf{K} \leq [\mathbf{G}, \mathbf{H}]\,\mathbf{H} = [\mathbf{H}]_\mathbf{G}$ (6.16) i kako $\mathbf{K}$ nije normalna podgrupa, to je $[\mathbf{H}]_\mathbf{G} = \mathbf{G}$.□

**Napomena.** Primetimo da prema 8.12 i dokazu i numeraciji prethodne teoreme važi uopšte za svaku grupu $\mathbf{G}$:

$$(1) \Longrightarrow (2) \Longrightarrow (3) \Longrightarrow (4) \Longleftrightarrow (5).$$

Sam uslov, recimo, normalizatora, nije dovoljan za nilpotentnost (ma koje grupe); primer direktnog proizvoda $\prod_{n\geq 2} \mathbf{D}_{2^n}$ to potvrđuje. No, zajedno sa uslovom maksimalnosti podgrupa (5.14) implicira nilpotentnost (videti i 56.13).

Jedan poseban dokaz za (1) $\Longrightarrow$ (5) dat je u narednom stavu.

**Lema 48.37** *Ako za podgrupu* $\mathbf{H}$ *nilpotentne grupe* $\mathbf{G}$ *važi* $\mathbf{HG'} = \mathbf{G}$, *onda je* $\mathbf{H} = \mathbf{G}$. *Odatle,* $\mathbf{G'} \leq \mathbf{Fr(G)}$.

**Dokaz.** Pretpostavimo da je $\mathbf{HG'} = \mathbf{G}$, ali da je $\mathbf{H}$ prava podgrupa neabelove nilpotentne grupe $\mathbf{G}$ (u slučaju Abelovih grupa tvrđenje trivijalno sledi) sa višim centalnim nizom $\mathbf{E} = \zeta_0\mathbf{G} < \zeta_1\mathbf{G} < \cdots < \zeta_n\mathbf{G} = \mathbf{G}$. Obeležimo sa $\mathbf{H}_i$ podgrupu $\mathbf{H}\zeta_i\mathbf{G}$. Za svako $i$ ($< n$) je $\mathbf{H}_i$ normalna podgrupa grupe $\mathbf{H}_{i+1}$

(videti dokaz implikacije (1) $\Longrightarrow$ (2) u prethodnoj teoremi), a faktor grupa $\mathbf{H}_{i+1}/\mathbf{H}_i$ je Abelova; njeni koseti su oblika $a(H\zeta_i G) = a(\zeta_i GH)$, $a \in \zeta_{i+1}G$, pa je za $a, b \in \zeta_{i+1}G$: $a(\zeta_i GH)\cdot b(\zeta_i GH) = ab(\zeta_i GH) = (ab\zeta_i G)H = (ba\zeta_i G)H = ba(\zeta_i GH) = b(\zeta_i GH)\cdot a(\zeta_i GH)$. Neka je, dalje, $\mathbf{H}_k$ prava podgrupa, dok je $\mathbf{H}_{k+1} = \mathbf{G}$. S obzirom da je $\mathbf{G}/\mathbf{H}_k$ Abelova grupa, sledi $\mathbf{G}' \leq \mathbf{H}_k$ i dalje $\mathbf{G} = \mathbf{H}\mathbf{G}' \leq \mathbf{H}\mathbf{H}_k = \mathbf{H}_k$, kontradikcija.

Drugi deo tvrđenja je posledica leme 5.9. Neka je $[a, b]$ $(\neq e)$ element generatornog skupa $S$ grupe $\mathbf{G}$ ($|S| \geq 2$ jer je $\mathbf{G}$ nekomutativna grupa). No tada je $\mathbf{G} = \langle S \setminus \{[a,b]\}\rangle\mathbf{G}'$, te je $\mathbf{G} = \langle S \setminus \{[a,b]\}\rangle$. Prema tome, svaki komutator je u $\mathbf{Fr}(\mathbf{G})$, znači $\mathbf{G}' \leq \mathbf{Fr}(\mathbf{G})$.□

**Lema 48.38** *Neka je* $\mathbf{G}$ *grupa čija je svaka podgrupa dostižna. Ako je* $\mathbf{N}$ *normalna podgrupa grupe* $\mathbf{G}$ *takva da je* $\mathbf{G}/\mathbf{N}$ *ciklična grupa i* $\mathbf{Z}(\mathbf{N}) \neq \mathbf{E}$, *onda je i* $\mathbf{Z}(\mathbf{G}) \neq \mathbf{E}$.

**Dokaz.** Pretpostavićemo, jasno, da je $\mathbf{N}$ prava podgrupa. Kako je, za neko $g \in G$, $\mathbf{G}/\mathbf{N} = \langle gN\rangle$, to je $\mathbf{G} = \langle g, N\rangle$. Centar grupe $\mathbf{N}$ je pak normalna podgrupa grupe $\mathbf{G}$ (jer je karakteristična podgrupa grupe $\mathbf{N}$ – 4.34). Posmatrajmo podgrupu $\mathbf{H} = \langle g, Z(\mathbf{N})\rangle = \langle g\rangle\mathbf{Z}(\mathbf{N})$. Ciklična grupa $\langle g\rangle$ je kao dostižna podgrupa grupe $\mathbf{G}$ dostižna podgrupa i grupe $\mathbf{H}$ (jednostavno, ako je, generalno, za $\mathbf{K} \leq \mathbf{H}$: $\mathbf{K} = \mathbf{K}_0 \trianglelefteq \mathbf{K}_1 \trianglelefteq \cdots \trianglelefteq \mathbf{K}_m = \mathbf{G}$, onda je $\mathbf{K} = \mathbf{K}_0 \trianglelefteq \mathbf{K}_1 \cap \mathbf{H} \trianglelefteq \cdots \trianglelefteq \mathbf{K}_m \cap \mathbf{H} = \mathbf{H}$), pa je, za neko $z \in Z(\mathbf{N}) \setminus \langle g\rangle$, $z^{-1}\langle g\rangle z = \langle g\rangle$ (tj. $z \in N_{\mathbf{H}}(\langle g\rangle) \setminus \langle g\rangle$). Ako već $z$ nije u centru grupe $\mathbf{G}$, tada je $[z, g] \neq e$, $[z, g] = z^{-1}g^{-1}zg \in \langle g\rangle \cap Z(\mathbf{N})$ i stoga $[z, g] \in Z(\mathbf{G})$.□

**Korolar 48.39** *$N$-grupa koja ispunjava uslov maksimalnosti podgrupa je nilpotentna.*

**Dokaz.** Neka je $\mathbf{G}$ $N$-grupa koja ispunjava uslov maksimalnosti podgrupa. Pokazaćemo prvo da je $\mathbf{Z}(\mathbf{G}) \neq \mathbf{E}$. Neka je $a_0 \in G$ proizvoljno izabrani nejedinični element i $\mathbf{A}_0 = \langle a_0\rangle$. Formirajmo, dalje, rastući lanac podgrupa (grupe $\mathbf{G}$) na sledeći način: ako je već data podgrupa $\mathbf{A}_i$, onda je $\mathbf{A}_{i+1} = \langle a_{i+1}, A_i\rangle$, gde je $a_{i+1} \in N(\mathbf{A}_i) \setminus A_i$. Prema 5.15 i samom načinu formiranja lanca ovaj u konačno mnogo koraka stiže do $\mathbf{G} - \mathbf{A}_0 < \cdots < \mathbf{A}_i < \mathbf{A}_{i+1} < \cdots < \mathbf{A}_{m-1} < \mathbf{A}_m = \mathbf{G}$. Sledi, generalno, da je u $N$-grupi koja ispunjava uslov maksimalnosti podgrupa svaka podgrupa dostižna (s tim u vezi videti i 54.1), a ovo svojstvo, pokazali smo, prenosi se na podgrupe. Prema prethodnoj lemi, s obzirom da je $\mathbf{A}_0$ Abelova grupa i $\mathbf{A}_1/\mathbf{A}_0 = \langle a_1 A_0\rangle$, grupa $\mathbf{A}_1$ ima netrivijalni centar. Isto tako je $\mathbf{Z}(\mathbf{A}_2) \neq \mathbf{E}$ ($\mathbf{A}_1 \lhd \mathbf{A}_2$ i $\mathbf{A}_2/\mathbf{A}_1 = \langle a_2 A_1\rangle$) i, uopšte, izvodimo redom da je $\mathbf{Z}(\mathbf{A}_i) \neq \mathbf{E}$ za svako $i = 1, \ldots, m$. Prema 8.7 je i $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ $N$-grupa koja ispunjava uslov maksimalnosti podgrupa. Odatle, $\zeta_2\mathbf{G}/\zeta_1\mathbf{G} = \mathbf{Z}(\mathbf{G}/\mathbf{Z}(\mathbf{G})) \neq \overline{\mathbf{E}}$ (jedinična grupa faktor grupe $\mathbf{G}/\mathbf{Z}(\mathbf{G})$), tj. $\mathbf{E} < \mathbf{Z}(\mathbf{G}) = \zeta_1\mathbf{G} < \zeta_2\mathbf{G}$. Analogno, $\zeta_2\mathbf{G} < \zeta_3\mathbf{G}$ i tako dalje, a prema uslovu maksimalnosti podgrupa viši centralni lanac u konačno mnogo koraka stiže do $\mathbf{G}$.□



**Korolar 48.40** *Konačno generisana, torziono slobodna nilpotentna grupa je rezidualno konačna $p$-grupa za svaki prost broj $p$.*

**Dokaz.** Indukcijom po klasi nilpotentnosti ($k$) grupa sa datim svojstvima. U daljem, prost broj $p$ je fiksiran. Ako je $k = 1$ ($\zeta_1\mathbf{G} = \mathbf{G}$), $\mathbf{G}$ je (konačno generisana) slobodna Abelova grupa (32.2), pa je i rezidualno konačna $p$-grupa (31.21). Pretpostavimo da je tvrđenje tačno za sve grupe klase nilpotentnosti manje od $k$ ($> 1$) i neka je $\mathbf{G}$ konačno generisana torziono slobodna nilpotentna grupa klase $k$ i $g \in G \setminus \{e\}$. Ako $g \notin Z(\mathbf{G})$, tj. $gZ(\mathbf{G}) \neq Z(\mathbf{G})$, onda postoji normalna podgrupa $\mathbf{N}/\mathbf{Z}(\mathbf{G})$ konačno generisane, torziono slobodne nilpotentne grupe $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ takva da je $(\mathbf{G}/\mathbf{Z}(\mathbf{G}))/(\mathbf{N}/\mathbf{Z}(\mathbf{G}))$ ($\cong \mathbf{G}/\mathbf{N}$) konačna $p$-grupa i $gZ(\mathbf{G}) \notin N/Z(\mathbf{G})$ (imamo u vidu: $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ je torziono slobodna grupa prema 46.31 i 8.16). Razmotrimo sada slučaj: $g \in Z(\mathbf{G})$. Kako je centar, po uslovima leme, slobodna Abelova grupa (konačnog ranga), sledi: $\bigcap_{n\in\omega}(\mathbf{Z}(\mathbf{G}))^{p^n} = \mathbf{E}$ (ako je $\mathbf{Z}(\mathbf{G}) = \mathbf{H}_1 \times \cdots \times \mathbf{H}_r$, gde su $\mathbf{H}_i$, $i = 1, \ldots, r$, beskonačne ciklične grupe, tada je $(\mathbf{Z}(\mathbf{G}))^{p^n} = \mathbf{H}_1^{p^n} \times \cdots \times \mathbf{H}_r^{p^n}$, te su komponente elementa sadržanog u svakoj grupi $(\mathbf{Z}(\mathbf{G}))^{p^n}$ ($n \in \omega$) deljive sa svim stepenima broja $p$; ali u beskonačnoj cikličnoj grupi to važi samo za jedinični element). Prema tome, $g \notin (Z(\mathbf{G}))^{p^n}$ za neko $n \geq 1$. Neka je $\mathbf{H}$ maksimalna normalna podgrupa grupe $\mathbf{G}$ za koju je $(\mathbf{Z}(\mathbf{G}))^{p^n} \leq \mathbf{H}$ i $g \notin H$ (videti 4.38 – ovde je još uključena normalnost). Krenimo od hipoteze da je $\mathbf{G}/\mathbf{H}$ beskonačna grupa. Tada, prema tački ($b$) korolara 48.26, njen centar sadrži element beskonačnog reda, recimo $aH$. Podgrupa $\langle a, H\rangle$ je normalna podgrupa grupe $\mathbf{G}$ (8.7) koja strogo sadrži $\mathbf{H}$, znači $g \in \langle a, H\rangle$. Ako je, za $h \in H$ i neki ceo nenula broj $s$, $g = a^s h$, odnosno $a^s = gh^{-1} \in Z(\mathbf{G})H$, proizilazi: $a^{sp^n} = g^{p^n}h^{-p^n} \in (Z(\mathbf{G}))^{p^n}H = H$, kontradikcija. $\mathbf{G}/\mathbf{H}$ je, dakle, konačna grupa. $\mathbf{Z}(\mathbf{G}) \cap \mathbf{H}$ je prava podgrupa centra $\mathbf{Z}(\mathbf{G})$ i prema drugoj teoremi o izomorfizmu je $(\mathbf{Z}(\mathbf{G})\mathbf{H})/\mathbf{H} \cong \mathbf{Z}(\mathbf{G})/(\mathbf{Z}(\mathbf{G}) \cap \mathbf{H})$; odatle, $(1 \neq)$ $[\mathbf{Z}(\mathbf{G})\mathbf{H} : \mathbf{H}]$ deli $[\mathbf{Z}(\mathbf{G}) : (\mathbf{Z}(\mathbf{G}))^{p^n}] = [\mathbf{Z}(\mathbf{G}) : \mathbf{Z}(\mathbf{G})\cap\mathbf{H}]\cdot[\mathbf{Z}(\mathbf{G})\cap\mathbf{H} : (\mathbf{Z}(\mathbf{G}))^{p^n}]$ = neki stepen broja $p$ (ponavljamo: $\mathbf{Z}(\mathbf{G})$ je slobodna Abelova grupa konačnog ranga i prema već uvedenim oznakama je $\mathbf{Z}(\mathbf{G})/(\mathbf{Z}(\mathbf{G}))^{p^n} \cong \prod_{i=1}^r \mathbf{H}_i/\mathbf{H}_i^{p^n} \cong \prod_{i=1}^r \mathbf{C}_{p^n}$). Dobijamo da je jedinstvena Sylowa $p$-podgrupa $\mathbf{P}/\mathbf{H}$ grupe $\mathbf{G}/\mathbf{H}$ nejedinična. Ako bi i za neki drugi prost broj $q$ Sylowa $q$-podgrupa $\mathbf{Q}/\mathbf{H}$ bila nejedinična, onda $g \in P \cap Q = H$, kontradikcija. Elem, $\mathbf{G}/\mathbf{H}$ je $p$-grupa.□

**Lema 48.41** *U torziono slobodnoj nilpotentnoj grupi* $\mathbf{G}$ *nijedan nejedinični element nije konjugovan sa sebi inverznim elementom.*

**Dokaz.** Neka je $\mathbf{G} = \gamma_0\mathbf{G} > \gamma_1\mathbf{G} = \mathbf{G}' > \cdots > \gamma_{n-1}\mathbf{G} > \gamma_n\mathbf{G} = \mathbf{E}$ niži centralni niz grupe $\mathbf{G}$ i $n > 1$. Pretpostavimo da $\mathbf{G}$ ima nejedinični element $a$ koji je konjugovan sa sebi inverznim. Naravno, $a \notin \gamma_{n-1}G$ ($\subseteq Z(\mathbf{G})$). Neka je $a \in \gamma_k G$ za neko $k$ između 0 i $n-2$. No, ako je $g^{-1}ag = a^{-1}$ za neko $g \in G$, onda je $[a, g] = a^{-2} \in \gamma_{k+1}G$ i $g^{-1}a^2g = a^{-2}$. Prema

tome, našli smo i u $\gamma_{k+1}\mathbf{G}$ nejedinični element koji je konjugovan sa sebi inverznim. Analogno bismo dalje izveli: $[a^2, g] = a^{-4} \in \gamma_{k+2}G$ (i $g^{-1}a^4g = a^{-4}$), pa i $\gamma_{k+2}\mathbf{G}$ sadrži nejedinični element konjugovan sa sebi inverznim. Ponavljajući postupak konačno bismo dobili i u $\gamma_{n-1}\mathbf{G}$ nejedinični element $(a^{2^{n-(k+1)}})$ konjugovan sa sebi inverznim, kontradikcija.□

**Lema 48.42** *Torziono slobodna nilpotentna grupa je R-grupa.*

**Dokaz**. Indukcijom po klasi nilpotentnosti ($n$) torziono slobodnih nilpotentnih grupa.

Slučaj $n = 1$, tj. kada su u pitanju torziono slobodne Abelove grupe, je trivijalan (ova lema je upravo uopštenje tog očiglednog stava).

Pretpostavimo da je tvrđenje tačno za sve torziono slobodne nilpotentne grupe klase nilpotentnosti manje od ili jednake $n$. Neka je $\mathbf{E} = \zeta_0\mathbf{G} < \zeta_1\mathbf{G} < \cdots < \zeta_n\mathbf{G} < \zeta_{n+1}\mathbf{G} = \mathbf{G}$ viši centralni niz torziono slobodne grupe $\mathbf{G}$, a $a$ i $b$ njeni elementi za koje je, za neki prirodan broj $k$, $a^k = b^k$. Ako $a, b \in \zeta_nG$, onda je po induktivnoj pretpostavci $a = b$ ($\mathbf{E} < \zeta_1\mathbf{G} < \cdots < \zeta_{n-1}\mathbf{G} < \zeta_n\mathbf{G}$ je centralni niz grupe $\zeta_n\mathbf{G}$ – za svako $i = 0, \ldots, n-1$ je $[\zeta_{i+1}\mathbf{G}, \zeta_n\mathbf{G}] \leq [\zeta_{i+1}\mathbf{G}, \mathbf{G}] \leq \zeta_i\mathbf{G}$). Razmotrimo mogućnost: $a \notin \zeta_nG$. Tada je $\mathbf{H} = \langle a, \zeta_nG\rangle$ prava normalna podgrupa grupe $\mathbf{G}$; normalna, jer je $\mathbf{G}/\zeta_n\mathbf{G}$ Abelova grupa; prava, jer zbog 8.19 $\mathbf{G}/\zeta_n\mathbf{G} \cong (\mathbf{G}/\zeta_{n-1}\mathbf{G})/(\zeta_n\mathbf{G}/\zeta_{n-1}\mathbf{G}) = (\mathbf{G}/\zeta_{n-1}\mathbf{G})/\mathbf{Z}(\mathbf{G}/\zeta_{n-1}\mathbf{G})$ ne može biti ciklična grupa. $\mathbf{H}$ je nilpotentna grupa klase nilpotentnosti $\leq n$, pošto je $\mathbf{E} < \zeta_1\mathbf{G} < \cdots < \zeta_{n-1}\mathbf{G} < \mathbf{H}$ njen centralni niz. Zaista, za svako $i = 0, \ldots, n-1$ je $\zeta_{i+1}\mathbf{G}/\zeta_i\mathbf{G} = \mathbf{Z}(\mathbf{G}/\zeta_i\mathbf{G}) \leq \mathbf{Z}(\mathbf{H}/\zeta_i\mathbf{G})$, a $\mathbf{H}/\zeta_{n-1}\mathbf{G}$ je, opet prema 8.19, Abelova grupa. Kao i maločas, $\zeta_n\mathbf{G}/\zeta_{n-1}\mathbf{G} \leq \mathbf{Z}(\mathbf{H}/\zeta_{n-1}\mathbf{G})$, a $(\mathbf{H}/\zeta_{n-1}\mathbf{G})/(\zeta_n\mathbf{G}/\zeta_{n-1}\mathbf{G}) \cong \mathbf{H}/\zeta_n\mathbf{G}$ je ciklična grupa, pa je i $(\mathbf{H}/\zeta_{n-1}\mathbf{G})/\mathbf{Z}(\mathbf{H}/\zeta_{n-1}\mathbf{G})$ ciklična grupa. Prema induktivnoj hipotezi $\mathbf{H}$ je $R$-grupa, te je, zbog $a^k = b^{-1} \cdot b^k \cdot b = b^{-1} \cdot a^k \cdot b = (b^{-1}ab)^k \in H$, $a = b^{-1}ab$, tj. $ab = ba$ (a onda i $ab^{-1} = b^{-1}a$). Odatle, $e = a^kb^{-k} = (ab^{-1})^k$, pa je (s obzirom da se radi o torziono slobodnoj grupi) $ab^{-1} = e$ i $a = b$.□

**Teorema 48.43** *U nilpotentnoj torziono slobodnoj grupi normalizator izolovane podgrupe je izolovana podgrupa.*

**Dokaz**. Neka je $\mathbf{G}$ nilpotentna torziono slobodna grupa sa višim centralnim nizom $\mathbf{E} = \zeta_0\mathbf{G} < \zeta_1\mathbf{G} < \cdots < \zeta_n\mathbf{G} = \mathbf{G}$ i neka je $\mathbf{A}$ jedna njena izolovana podgrupa. Pretpostavimo da $\mathbf{N}(\mathbf{A})$ nije izolovana podgrupa, dakle za neko $g \in G$ i neko $m \geq 2$ važi: $g^m \in N(\mathbf{A})$ ali $g \notin N(\mathbf{A})$. Ne može biti $g^{-1}Ag \subset A$; to bi nam dalo $g^{-2}Ag^2 \subset g^{-1}Ag \subset A$ i, tako redom, konačno $g^{-m}Ag^m \subset A$, suprotno pretpostavci $g^m \in N(\mathbf{A})$. Za $a \in A$ takvo da $g^{-1}ag \notin A$ neka je $k_a$ najmanji indeks za koji je $a \in \zeta_{k_a+1}G \setminus \zeta_{k_a}G$ (naravno, $1 \leq k_a \leq n-1$). Ako je $k = min\{k_a \mid a \in A,\ g^{-1}ag \notin A\}$ ($\geq 1$), tada je $g^{-1}(A \cap \zeta_kG)g \subset A$. Možemo odmah pretpostaviti da je i $g(A \cap \zeta_kG)g^{-1} \subset A$; u suprotnom bismo, pošto je $(g^{-1})^m \in N(\mathbf{A})$ i $g^{-1} \notin N(\mathbf{A})$, ponovili priču sa $g^{-1}$ u glavnoj



ulozi, dobili odgovarajuće $l$ i onda uzeli $min\{k, l\}$. Definišimo za (ma koje) $a \in A \cap (\zeta_{k+1}G \setminus \zeta_kG)$ za koje $g^{-1}ag \notin A$: $b_1 = [a, g]$, $b_2 = [b_1, g]$ i, uopšte, $b_{n+1} = [b_n, g]$. Kako je $b_1 = a^{-1} \cdot g^{-1}ag \in [\zeta_{k+1}G, G] \subseteq \zeta_kG = \zeta_{(k+1)-1}G$, sledi: $b_2 = b_1^{-1} \cdot g^{-1}b_1g \in [\zeta_kG, \zeta_kG] \subseteq \zeta_{k-1}G = \zeta_{(k+1)-2}G$ i generalno, za $i \leq k+1$, $b_i \in \zeta_{(k+1)-i}G$. Posebno, $b_{k+1} \in \zeta_0G$, pa je

$$b_{k+1} = b_{k+2} = \cdots = e.$$

Iz $ab_1 = g^{-1}ag \notin A$ proizilazi $b_1 \notin A$, a $b_{i+1} = [b_i, g]$ nam daje $b_ib_{i+1} = g^{-1}b_ig$. Proizvod elemenata $b_i$ ćemo kraće obeležiti sa $c$, koristeći pri tom donje indekse; jasno, uvek je $c \in \zeta_kG$. Ako je $c = b_{j_1} \cdot \ldots \cdot b_{j_r}$, onda ćemo sa $c^{(1)}$ ili $c'$ označiti proizvod $b_{j_1+1} \cdot \ldots \cdot b_{j_r+1}$ (donji indeks svakog faktora je uvećan za 1). Stavljamo: $c^{(0)} = c$, $c^{(t+1)} = (c^{(t)})^{(1)}$. Pokazujemo u nastavku indukcijom: za svako $i \geq 1$ možemo naći element $c_i$ takav da je

$$g^{-i}ag^i = ac_i \quad \text{i, za } i > 1, \quad c_i = c_{i-1}b_1c_{i-1}^{(1)};$$

iz druge relacije sledi direktno: $c_i^{(s)} = c_{i-1}^{(s)}b_{s+1}c_{i-1}^{(s+1)}$ za svako $s \geq 0$, odnosno $c_{i-1}^{(s+1)} = b_{s+1}^{-1}(c_{i-1}^{(s)})^{-1}c_i^{(s)}$. Za $i = 1$ imamo, očigledno, $c_1 = b_1$. Ako je $i = 2$, onda je $g^{-2}ag^2 = g^{-1}(g^{-1}ag)g = g^{-1}ab_1g = g^{-1}ag \cdot g^{-1}b_1g = ab_1 \cdot b_1b_2$; prema tome, $c_2 = b_1b_1b_2 = c_1b_1c_1^{(1)}$. Pretpostavimo da smo već dobili sve elemente $c_i$, $i < j$. Znači, za $1 < i < j$ imamo: $ac_i = g^{-i}ag^i = g^{-1}(g^{-(i-1)}ag^{i-1})g = g^{-1} \cdot ac_{i-1} \cdot g = g^{-1}ag \cdot g^{-1}c_{i-1}g = ab_1 \cdot g^{-1}c_{i-1}g$, tj. $c_i = b_1 \cdot g^{-1}c_{i-1}g$, odnosno $g^{-1}c_{i-1}g = b_1^{-1}c_i$. Odatle, za $s \geq 1$ izvodimo, koristeći se već dobijenim relacijama i induktivnom pretpostavkom: $g^{-1}c_{i-1}^{(s)}g = b_{s+1}^{-1}c_i^{(s)}$. Tako je za $s = 1$:

$$g^{-1}c_{i-1}^{(1)}g = g^{-1}(b_1^{-1}c_{i-1}^{-1}c_i)g = (g^{-1}b_1g)^{-1} \cdot (g^{-1}c_{i-1}g)^{-1} \cdot g^{-1}c_ig =$$

$$(b_1b_2)^{-1} \cdot (b_1^{-1}c_i)^{-1} \cdot b_1^{-1}c_{i+1} = b_2^{-1} \cdot b_1^{-1}c_i^{-1}c_{i+1} = b_2^{-1} \cdot c_i^{(1)},$$

a ako je tvrđenje tačno za $s \geq 1$, onda je

$$c_{i-1}^{(s+1)} = (c_{i-1}^{(s)})^{(1)} = (b_{s+1}^{-1}(c_{i-1}^{(s-1)})^{-1}c_i^{(s-1)})^{(1)} = b_{s+1}^{-1} \cdot (c_{i-1}^{(s)})^{-1} \cdot c_i^{(s)}$$

(imamo u vidu očiglednu relaciju: $(c_i^{(s)})^{-1} = (c_i^{-1})^{(s)}$), pa je

$$g^{-1}c_{i-1}^{(s+1)}g = g^{-1}(b_{s+1}^{-1}(c_{i-1}^{(s)})^{-1}c_i^{(s)})g = (g^{-1}b_{s+1}g)^{-1} \cdot (g^{-1}c_{i-1}^{(s)}g)^{-1} \cdot g^{-1}c_i^{(s)}g =$$

$$(b_{s+1}b_{s+2})^{-1} \cdot (b_{s+1}^{-1}c_i^{(s)})^{-1} \cdot b_{s+1}^{-1}c_{i+1}^{(s)} = b_{s+2}^{-1} \cdot b_{s+1}^{-1}(c_i^{(s)})^{-1}c_{i+1}^{(s)} = b_{s+2}^{-1}c_i^{(s+1)}.$$

Proizilazi:

$$g^{-j}ag^j = g^{-1}(g^{-(j-1)}ag^{j-1})g = g^{-1} \cdot ac_{j-1} \cdot g = g^{-1}ag \cdot g^{-1}c_{j-1}g =$$

$$ab_1 \cdot g^{-1}(c_{j-2}b_1c_{j-2}^{(1)})g = ab_1 \cdot g^{-1}c_{j-2}g \cdot g^{-1}b_1g \cdot g^{-1}c_{j-2}^{(1)}g =$$

$$ab_1 \cdot b_1^{-1}c_{j-1} \cdot b_1b_2 \cdot b_2^{-1}c_{j-1}^{(1)} = ac_{j-1}b_1c_{j-1}^{(1)}$$

i $c_j = c_{j-1}b_1c_{j-1}^{(1)}$. Dalje, $g^m \in N(\mathbf{A})$, $b_1 \in \zeta_k G$ i $g^{-m}ag^m = ac_m$ daju: $c_m = c_{m-1}b_1c_{m-1}^{(1)} \in A \cap \zeta_k G$. Sledi:

$$g^{-1}(c_{m-1}b_1c_{m-1}^{(1)})g = g^{-1}c_{m-1}g \cdot g^{-1}b_1g \cdot g^{-1}c_{m-1}^{(1)}g = b_1^{-1}c_m \cdot b_1b_2 \cdot b_2^{-1}c_m^{(1)} =$$

$$b_1^{-1}c_mb_1c_m^{(1)} \in g^{-1}(A \cap \zeta_k G)g \subset A \cap \zeta_k G,$$

i odatle, zbog trivijalnog $a^{-1}(A \cap \zeta_k G)a$, $a(A \cap \zeta_k G)a^{-1} \subset A$,

$$b_1^{-1}(c_mb_1c_m^{(1)}b_1^{-1})b_1 = g^{-1}a^{-1}ga \cdot c_mb_1c_m^{(1)}b_1^{-1} \cdot a^{-1}g^{-1}ag$$

implicira $c_mb_1c_m^{(1)}b_1^{-1} \in A \cap \zeta_k G$. Ovo pak povlači, po istom rezonu, $c_m^{(1)} = c_{m-1}^{(1)}b_2c_{m-1}^{(2)} \in A \cap \zeta_k G$. Ponavljajući postupak dobijamo:

$$g^{-1}(c_{m-1}^{(1)}b_2c_{m-1}^{(2)})g = g^{-1}c_{m-1}^{(1)}g \cdot g^{-1}b_2g \cdot g^{-1}c_{m-1}^{(2)}g =$$

$$b_2^{-1}c_m^{(1)} \cdot b_2b_3 \cdot b_3^{-1}c_m^{(2)} = b_2^{-1}c_m^{(1)}b_2c_m^{(2)} \in A$$

i dalje, redom: $c_m^{(1)}b_2c_m^{(2)}b_2^{-1} \in A \cap \zeta_k G$,

$$b_2c_m^{(2)}b_2^{-1} = [b_1, g]c_m^{(2)}[g, b_1] = [a, g]^{-1}g^{-1}[a, g]g \cdot c_m^{(2)} \cdot g^{-1}[g, a]g[a, g] \in A \cap \zeta_k G.$$

Stoga je i $c_m^{(2)} \in A$. Analogno, $c_m^{(i)} \in A$, $i = 3, \ldots, k-1$. S obzirom da je $b_{k+1} = b_{k+2} = \cdots = e$, $c_m^{(k-1)}$ je stepen elementa $b_k$, te je $b_k \in A$. Sada indukcijom "naniže" pokazujemo da je $b_{k-i} \in A$ za svako $i = 0, \ldots, k-1$. Pretpostavimo: $b_k, b_{k-1}, \ldots, b_{i+1} \in A$. Pošto je $c_m^{(i-1)} = c_{m-1}^{(i-1)}b_ic_{m-1}^{(i)} \in A$ i zbog učinjene pretpostavke $c_{m-1}^{(i)} \in A$, to je i $c_{m-1}^{(i-1)}b_i \in A$, tj. $b_i^{-1}(b_ic_{m-1}^{(i-1)})b_i \in A$, što kao i ranije (ponovo zbog $g^{-1}(A \cap \zeta_k G)g$, $g(A \cap \zeta_k G)g^{-1} \subset A$) povlači $b_ic_{m-1}^{(i-1)} \in A$. Indukcijom dokazujemo da je $b_i^r c_{m-r}^{(i-1)} \in A$. Za $r = 1$ to smo upravo izveli, a ako je $b_i^r c_{m-r}^{(i-1)} \in A$, odnosno $b_i^r \cdot c_{m-r-1}^{(i-1)}b_ic_{m-r-1}^{(i)} \in A$, onda je $b_i^r c_{m-r-1}^{(i-1)}b_i = b_i^{-1}(b_i^{r+1}c_{m-(r+1)}^{(i-1)})b_i \in A$. Konkretno, za $r = m-1$ je $b_i^{m-1}c_1^{(i-1)} = b_1^{m-1}b_1^{(i-1)} = b_i^{m-1}b_i = b_i^m \in A$. Prema tome je i $b_i \in A$. Posebno, $b_1 \in A$, kontradikcija.■

**Definicija 48.44** *Fittingova (H. Fitting) ili nilradikalna (eng. nilradical) podgrupa grupe* $\mathbf{G}$*, u oznaci* $\mathbf{Fit}(\mathbf{G})$ *(koristi se i* $\mathbf{R}(\mathbf{G})$*), podgrupa je generisana unijom domena svih normalnih nilpotentnih podgrupa grupe* $\mathbf{G}$.



Ako npr. grupa $\mathbf{G}$ ispunjava uslov maksimalnosti normalnih podgrupa, onda je Fittingova podgrupa maksimalna normalna nilpotentna podgrupa grupe $\mathbf{G}$ (videti 48.14). Napomenimo da se u nekim knjigama pod Fittingovom podgrupom podrazumeva upravo maksimalna normalna nilpotentna podgrupa grupe $\mathbf{G}$, ukoliko takva postoji (u tom slučaju postoje grupe bez Fittingovih podgrupa). Generalno važi

**Lema 48.45** *Fittingova podgrupa ma koje grupe* $\mathbf{G}$ *je karakteristična, svaka njena konačno generisana podgrupa je nilpotentna i svi njeni elementi su nilelementi.*

**Dokaz.** Prvi deo tvrđenja je jasan; za svaki automorfizam grupe $\mathbf{G}$ slika normalne nilpotentne podgrupe je opet normalna nilpotentna podgrupa. Prema tome, ako je $\{\mathbf{N}_i \mid i \in I\}$ skup svih normalnih nilpotentnih podgrupa grupe $\mathbf{G}$, onda je, za $\varphi \in Aut(\mathbf{G})$, $\{\mathbf{N}_i \mid i \in I\} = \{(\mathbf{N}_i)\varphi \mid i \in I\}$.

Neka je $\mathbf{H} = \langle a_1, \ldots, a_k \rangle$, gde je $a_i \in Fit(\mathbf{G})$ za svako $i = 1, \ldots, k$. Ako je $a_i \in N_i$ (moguće je da je $\mathbf{N}_i = \mathbf{N}_j$ za različito $i, j$), onda je prema 48.14 $\mathbf{N} = \mathbf{N}_1 \cdot \ldots \cdot \mathbf{N}_k$ normalna nilpotentna podgrupa, pa je i $\mathbf{H}$ ($\leq \mathbf{N}$) nilpotentna podgrupa.

Konačno, neka je $a \in Fit(\mathbf{G})$. Tada je $[a, b] \in Fit(\mathbf{G})$ za svako $b \in G$, a podgrupa $\mathbf{K} = \langle a, [a, b] \rangle$ je, upravo smo konstatovali, nilpotentna podgrupa klase, recimo, $m$. Indukcijom po $i$, $i = 0, \ldots, m$, pokazujemo da je $[a, b]_{i+1} \in \gamma_i\mathbf{K}$. Za $i = 0$ već imamo $[a, b]_1 = [a, b] \in \gamma_0\mathbf{K} = \mathbf{K}$, a ako je tvrđenje tačno za svako $j \leq i < m$, onda je $[a, b]_{i+2} = [a, [a, b]_{i+1}] \in [K, \gamma_iK] = \gamma_{i+1}K$. Dakle, za $i = m$ je $[a, b]_{m+1} \in \gamma_mK = \{e\}$.□

**Lema 48.46** *Neka je* $\mathbf{G}$ *konačna grupa. Tada važi:*

(*a*) $\mathbf{Fr}(\mathbf{G}) \leq \mathbf{Fit}(\mathbf{G})$;

(*b*) *Ako je* $\mathbf{K}_p = \bigcap\{\mathbf{P} \mid \mathbf{P}$ *je Sylowa p-podgrupa grupe* $\mathbf{G}\}$, *onda je* $\mathbf{Fit}(\mathbf{G}) = \prod_{p \mid |G|} \mathbf{K}_p$.

**Dokaz.** (*a*) Prema 48.30(*c*) i 5.25 $\mathbf{Fr}(\mathbf{G})$ je nilpotentna normalna podgrupa grupe $\mathbf{G}$.

(*b*) Prema 4.8 i drugoj teoremi Sylowa (16.23(*b*)) svaka od podgrupa $\mathbf{K}_p$ je normalna i (kao $p$-grupa) nilpotentna. Stoga je $\prod_{p \mid |G|} \mathbf{K}_p \leq \mathbf{Fit}(\mathbf{G})$. S druge strane, jedinstvena Sylowa $p$-podgrupa grupe $\mathbf{Fit}(\mathbf{G})$ (48.28), neka je to $\mathbf{Q}_p$, sadržana je, prema 16.23(*a*), u nekoj Sylowoj $p$-podgrupi grupe $\mathbf{G}$, recimo $\mathbf{P}$. No, $\mathbf{Q}_p$ je kao karakteristična podgrupa grupe $\mathbf{Fit}(\mathbf{G})$ normalna podgrupa grupe $\mathbf{G}$ i, ponovo prema 4.8, $\mathbf{Q}_p \leq \mathbf{K}_p$. Dakle, $\mathbf{Q}_p = \mathbf{K}_p$, pa je $\mathbf{Fit}(\mathbf{G}) = \prod_{p \mid |G|} \mathbf{K}_p$.□

**Lema 48.47** *Ako je* $\mathbf{Fit}(\mathbf{G})$ *nilpotentna podrupa i* $\mathbf{N}$ *minimalna normalna podgrupa grupe* $\mathbf{G}$, *tada je* $\mathbf{Fit}(\mathbf{G}) \leq \mathbf{C}(\mathbf{N})$ *(centralizator podgrupe* $\mathbf{N}$ *u* $\mathbf{G}$*).*

**Dokaz.** Ako je $\mathbf{N} \cap \mathbf{Fit(G)} = \mathbf{E}$, onda je, za svako $a \in N$ i svako $b \in Fit(\mathbf{G})$, $[a,b] \in N \cap Fit(\mathbf{G}) = \{e\}$, pa je $ab = ba$. Ako je $\mathbf{N} \cap \mathbf{Fit(G)} \neq \mathbf{E}$, onda je, zbog minimalnosti podgrupe $\mathbf{N}$, $\mathbf{N} \leq \mathbf{Fit(G)}$, i prema 48.15 $\mathbf{E} \neq \mathbf{N} \cap \mathbf{Z(Fit(G))} \lhd \mathbf{G}$. Opet zbog minimalnosti podgrupe $\mathbf{N}$ sledi $\mathbf{N} \leq \mathbf{Z(Fit(G))}$, pa je $\mathbf{Fit(G)} \leq \mathbf{C(N)}$.□

**Lema 48.48** *Grupa $\mathbf{G}$ je rezidualno nilpotentna akko je $\gamma_\omega\mathbf{G}$ $(= \bigcap_{n\in\omega} \gamma_n\mathbf{G})$ jedinična podgrupa.*

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{G}$ rezidualno nilpotentna grupa; dakle, za svaki nejedinični element $g \in G$ postoji normalna podgrupa $\mathbf{N}_g$ takva da je $\mathbf{G}/\mathbf{N}_g$ nilpotentna grupa i $g \notin N_g$ (videti definiciju 5.19). Ako je $\gamma_n(\mathbf{G}/\mathbf{N}_g) = (\gamma_n\mathbf{G} \cdot \mathbf{N}_g)/\mathbf{N}_g = \overline{\mathbf{E}}$ (46.25(5)), tada je $\gamma_n\mathbf{G} \leq \mathbf{N}_g$, pa je $\bigcap_{k\in\omega} \gamma_k\mathbf{G} \leq \bigcap_{g\in G\setminus\{e\}} \mathbf{N}_g = \mathbf{E}$.

($\Longleftarrow$) Pretpostavimo odmah da je $\gamma_k\mathbf{G} \neq \mathbf{E}$ za svako $k$ $(\in \omega)$ (nilpotentna grupa je, trivijalno, rezidualno nilpotentna) i neka je $\bigcap_{k\in\omega} \gamma_k\mathbf{G} = \mathbf{E}$. Onda za svaki nejedinični element $g$ postoji $n \in \omega$ takvo da $g \notin \gamma_n G$, a $\mathbf{G}/\gamma_n\mathbf{G}$ je nilpotentna grupa (opet imamo u vidu 46.25(5)).□

**Korolar 48.49** *Grupa je rezidualno nilpotentna akko je podkartezijanski proizvod (kartezijanskog proizvoda) familije nilpotentnih grupa.*

**Dokaz.** Već dokazano: 10.21.□

**Primer 48.50** *Beskonačna dijedarska grupa je rezidualno nilpotentna.*

**Dokaz.** Prema tački $(o)$ primera 21.10 faktor grupa dijedarske grupe $\mathbf{D}_\infty$ (sa generatornim elementima $a$ i $b$, gde je $a^2 = (ab)^2 = e$ i $b$ beskonačnog reda – odatle i $ab^z a = b^{-z}$), po normalnoj podgrupi $\langle b^{2^n}\rangle$, $n \geq 2$, izomorfna je dijedarskoj grupi $\mathbf{D}_{2^n}$, a $\bigcap_{n\geq 2} \langle b^{2^n}\rangle = \mathbf{E}$.□

**Napomena.** Svaka dijedarska grupa je homomorfna slika beskonačne dijedarske grupe, a kako među njima ima i onih koje nisu nilpotentne, vidimo da homomorfna preslikavanja ne očuvavaju generalno svojstvo rezidualne nilpotentnosti; imamo u vidu i očiglednu činjenicu:

*Konačna grupa je rezidualno nilpotentna akko je nilpotentna.*

S druge strane važi

**Lema 48.51** $(a)$ *Podgrupa rezidualno nilpotentne grupe je rezidualno nilpotentna;*

$(b)$ *Kartezijanski i direktni proizvod rezidualno nilpotentnih grupa je rezidualno nilpotentna grupa.*



**Dokaz.** $(b)$ Direktna posledica tačke $(b)$ leme 10.3. Neka je $\{\mathbf{G}_i \mid i \in I\}$ $(|I| \geq \aleph_0)$ familija rezidualno nilpotentnih grupa i za $g \in \prod_{i\in I} G_i$ neka je $S(g) = \{i_1, \ldots, i_m\}$. Ako je $\mathbf{N}_{i_1}$ normalna podgrupa grupe $\mathbf{G}_{i_1}$ koja ne sadrži (nejedinični) element $(i_1)g$ i čija je faktor grupa $\mathbf{G}_{i_1}/\mathbf{N}_{i_1}$ nilpotentna, onda je $\mathbf{N} = \mathbf{N}_{i_1} \times \prod^c_{i\in I\setminus\{i_1\}} \mathbf{G}_i$ normalna podgrupa grupe $\mathbf{G} = \prod^c_{i\in I} \mathbf{G}_i$, $\mathbf{G}/\mathbf{N} \cong \mathbf{G}_{i_1}/\mathbf{N}_{i_1}$ i, naravno, $g \notin N$.□

**Teorema 48.52** *(Teorema Magnusa). Slobodne grupe su rezidualno nilpotentne.*

**Dokaz.** Opet nam je potrebno nešto priče o prstenima. Neka je $\mathbf{R} = \langle R, +, \cdot\rangle$ (ma koji) prsten. *Pridruženo množenje* (eng. *adjoint multiplication*) datog prstena je operacija, obeležimo je sa o, definisana sa: $a \circ b = a + b - a \cdot b$. Ona je asocijativna:

$$a \circ (b \circ c) = a \circ (b + c - bc) = a + (b + c - bc) - a \cdot (b + c - bc) =$$

$$a + b + c - (ab + ac + bc) + abc = (a + b - ab) + c - (a + b - ab) \cdot c =$$

$$(a + b - ab) \circ c = (a \circ b) \circ c,$$

a neutralni element prstena je njen jedinični element $(a \circ 0 = 0 \circ a = a)$. Element prstena se zove *radikal* akko ima inverzni s obzirom na pridruženo množenje, a grupa $\mathbf{G} = \langle \{a \in R \mid a \text{ je radikal }\}, \circ\rangle$ je tzv. *pridružena grupa* prstena $\mathbf{R}$ $(3.4(g))$.

Formiraćemo sada prsten čija će pridružena grupa biti slobodna grupa zadanog ranga $\lambda$ i preko koje ćemo dokazati teoremu. Neka je dat skup simbola $A = \{a_\alpha \mid \alpha < \lambda\}$. Pod *rečju* ćemo podrazumevati svaki konačni niz oblika $u \equiv a_{\alpha_1} \ldots a_{\alpha_{k-1}}$, gde je za svako $i$, $1 \leq i \leq k-1$, $\alpha_i \neq \alpha_{i+1}$. *Dužina reči* je, prema očekivanju, broj slova (simbola) u njoj. Posebno, ako je $k = 0$, imamo praznu reč, (ovog puta) u oznaci 0. Elementi prstena kojeg upravo pravimo biće, pored prazne reči, formalne sume oblika $k_1u_1 + \cdots + k_mu_m$, gde su $u_i$, $i = 1, \ldots, m$, neprazne reči, a $k_i$ nenula celi brojevi; podrazumevamo takođe da je $u_i \not\equiv u_j$ za $i \neq j$, kao i da je $k_1u_1 + \cdots + k_mu_m = l_1v_1 + \cdots + l_nv_n$ akko je $m = n$ i za neku permutaciju $\sigma$ skupa $\{1, \ldots, m\}$ i svako $i = 1, \ldots, m$, $k_i = l_{(i)\sigma}$ i $u_i \equiv v_{(i)\sigma}$. Korektnije bi bilo (ali i nepotrebno formalno) na skupu svih formalnih suma definisati relaciju ekvivalencije na gore opisan način i onda raditi sa klasama ekvivalencije. Operacija "sabiranja" (koristićemo oznaku $\oplus$) dve takve sume je opet suma dobijena "normalnim sabiranjem" celobrojnih koeficijenata uz iste reči; ako je njihov zbir nula, onda je u pitanju prazna reč (– neutralni element za sabiranje). Jasno, $\langle R, \oplus\rangle$ je Abelova grupa. "Proizvod" definišemo prvo za dve reči – pisaćemo: $u \bullet v$: ako je $u \equiv a_{\alpha_1} \ldots a_{\alpha_{k-1}}$ i $v \equiv a_{\beta_1} \ldots a_{\beta_{l-1}}$, tada je: $u \bullet v \overset{\text{def}}{=} \begin{cases} a_{\alpha_0} \ldots a_{\alpha_{k-1}} a_{\beta_0} \ldots a_{\beta_{l-1}} & \alpha_{k-1} \neq \beta_0 \\ 0 & \text{inače} \end{cases}$.

Proizvod prazne i bilo koje reči je prazna reč. Proizvod elemenata $u \equiv k_1u_1 + \cdots + k_mu_m$ i $v \equiv l_iv_1 + \cdots + l_nv_n$ je (formalna) suma dobijena množenjem svakog "sabirka" elementa $u$ sa svakim "sabirkom" elementa $v$, pri čemu se celobrojni koeficijenti množe "normalno" a reči na gore opisan način, i na kraju (uvedenim) sabiranjem "sličnih" sabiraka; tako je npr. uz pretpostavku da se radi o različitim indeksima: $[(-2)a_\alpha a_\beta + 5a_\alpha] \bullet [3a_\gamma + 6a_\beta a_\gamma] = 15a_\alpha a_\gamma + 24a_\alpha a_\beta a_\gamma$. Rutinska je provera da je operacija $\bullet$ asocijativna i distributivna u odnosu na operaciju $\oplus$, te je $\mathbf{R} = \langle R, \oplus, \bullet \rangle$, gde je $R$ skup svih formalnih suma, prsten. Neka je, dalje, $\mathbf{G} = \langle G\ (= \{u \in R \mid u$ je radikal $\}), \circ \rangle$ pridružena grupa prstena $\mathbf{R}$. Uočimo odmah da je $A \subseteq G$ $(a_\alpha \circ (-a_\alpha) = 0 = (-a_\alpha) \circ a)$. Skup $A$ je prema 23.8 slobodna baza podgrupe $\mathbf{F}$, grupe $\mathbf{G}$, koju generiše. Jer, $\underbrace{ka_\alpha \circ \cdots \circ ka_\alpha}_{m-puta} = (km)a_\alpha$, pa je potrebno i dovoljno da se dokaže da je (pridruženi) proizvod $k_1a_{\alpha_1} \circ \cdots \circ k_ma_{\alpha_m}$, gde su $k_1, \ldots, k_m$ proizvoljni nenula celi brojevi i $\alpha_i \neq \alpha_{i+1}$ za svako $i = 1, \ldots, m-1$, različit od jediničnog elementa – 0. Indukcijom po $m$ se pokazuje, što je i dovoljno, da svaki takav proizvod sadrži (u svom zbiru) jedan jedini term (sabirak) dužine $m - (k_1 \ldots k_m)a_{\alpha_1} \ldots a_{\alpha_m}$, dok su ostali termi "kraći". Za $m = 1$ to je jasno, a uz pretpostavku da je tvrđenje tačno za $m$ $(\geq 1)$, tačno je i za $m+1$; zaista, po definiciji je $(k_1a_{\alpha_1} \circ \cdots \circ k_ma_{\alpha_m}) \circ k_{m+1}a_{\alpha_{m+1}} = (k_1a_{\alpha_1} \circ \cdots \circ k_ma_{\alpha_m}) \oplus k_{m+1}a_{\alpha_{m+1}} \oplus (-((k_1a_{\alpha_1} \circ \cdots \circ k_ma_{\alpha_m}) \bullet k_{m+1}a_{\alpha_{m+1}}))$, u $(k_1a_{\alpha_1} \circ \cdots \circ k_ma_{\alpha_m})$ su svi sabirci dužine manje od $m+1$, a u proizvodu $(k_1a_{\alpha_1} \circ \cdots \circ k_ma_{\alpha_m}) \bullet k_{m+1}a_{\alpha_{m+1}}$ opet je samo jedan dužine $m + 1 - (k_1 \ldots k_m)a_{\alpha_1} \ldots a_{\alpha_m} \bullet k_{m+1}a_{\alpha_{m+1}} = (k_1 \ldots k_mk_{m+1})a_{\alpha_1} \ldots a_{\alpha_m}a_{\alpha_{m+1}}$ (zbog $\alpha_m \neq \alpha_{m+1}$). U nastavku definišemo *visinu* nenula elementa (prstena $\mathbf{R}$) $u \equiv k_1a_{\alpha_1} + \cdots + k_ma_{\alpha_m}$ kao dužinu njegovih najkraćih terma – u opštem može ih biti više, koje pak zovemo *najnižim termima* reči $u$. Visinu elementa $u$ ćemo označiti sa $h(u)$. Visina prazne reči biće $\infty$, gde se, naravno, podrazumeva da je $n < \infty$ i $n + \infty = \infty\ (= \infty + n)$ za svaki prirodan broj $n$. Dakle, visina prazne reči je strogo veća od visine svake druge reči. Prema samim definicijama množenja i sabiranja u prstenu važi: $h(u \oplus v) \geq min\{h(u), h(v)\}$, $h(u \bullet v) \geq h(u) + h(v)$ (proizvod dve reči je ili prazna reč ili reč čija je dužina jednaka zbiru njihovih dužina). Odatle, $h(u \circ v) = h(u \oplus v \oplus (-(u \bullet v)) \geq min\{h(u), h(v), h(-(u \bullet v))\} = min\{h(u), h(v)\}$. Uzajamno inverzni elementi grupe $\mathbf{G}$ su iste visine; za $u \neq 0$, iz $h(u \circ u^{-1}) = h(0) = \infty$ i činjenice da je $h(u \bullet u^{-1}) \geq h(u) + h(u^{-1}) > h(u), h(u^{-1})$ proizilazi da se najniži termi elemenata $u$ i $u^{-1}$ moraju "potirati" (što je opet moguće samo ako su iste dužine). Dalje je, za elemente $u, v$ grupe $\mathbf{G}$:

$$[u,v] = u^{-1} \circ v^{-1} \circ u \circ v = (u^{-1} \oplus v^{-1} \oplus (-(u^{-1} \bullet v^{-1})) \circ (u \oplus v \oplus (-(u \bullet v)) =$$

$$u^{-1} \oplus v^{-1} \oplus (-(u^{-1} \bullet v^{-1})) \oplus u \oplus v \oplus (-(u \bullet v)) \oplus (-(u^{-1} \bullet u)) \oplus (-(v^{-1} \bullet u)) \oplus$$

$$u^{-1} \bullet v^{-1} \bullet u \oplus (-(u^{-1} \bullet v)) \oplus (-(v^{-1} \bullet v)) \oplus u^{-1} \bullet v^{-1} \bullet v \oplus u^{-1} \bullet u \bullet v \oplus v^{-1} \bullet u \bullet v \oplus$$



$$(-(u^{-1} \bullet v^{-1} \bullet u \bullet v)) = (u^{-1} \circ u) \oplus (v^{-1} \circ v) \oplus (-((u^{-1} \circ u) \bullet v)) \oplus (-(u^{-1} \bullet v^{-1})) \oplus$$

$$(-(v^{-1} \bullet u)) \oplus u^{-1} \bullet v^{-1} \bullet u \oplus u^{-1} \bullet v^{-1} \bullet v \oplus (-(u^{-1} \bullet v^{-1} \bullet u \bullet v)) =$$

$$(-(u^{-1} \bullet v^{-1})) \oplus (-(v^{-1} \bullet u)) \oplus u^{-1} \bullet v^{-1} \bullet u \oplus u^{-1} \bullet v^{-1} \bullet v \oplus (-(u^{-1} \bullet v^{-1} \bullet u \bullet v)),$$

što nam, sa već konstatovanim, daje: $h([u,v]) > h(u), h(v)$ za $u, v \neq 0$. U nastavku dokazujemo indukcijom po $n$ da je visina svakog elementa iz $\gamma_n\mathbf{G}$ veća od ili jednaka $n + 1$. Za $n = 0$ to je očigledno. Pretpostavimo da tvrđenje važi za $n$ $(\geq 0)$. No, svaki element iz $\gamma_{n+1}\mathbf{G}$ $(= [\gamma_n\mathbf{G}, \mathbf{G}])$ je proizvod komutatora $[u,v]^k$, gde je $u \in \gamma_nG$, $v \in G$ i $k \in \{1, -1\}$, a prema upravo pokazanom je, za $u \neq 0$, $h([u,v]) > h(u) \geq n+1$, tj. $h([u,v]) \geq n+2$. Konačno zaključujemo: $\gamma_\omega\mathbf{G} = \bigcap_{n \in \omega} \gamma_n\mathbf{G} = \mathbf{E}\ (= \langle \{0\}, \circ \rangle)$; element iz preseka je visine veće od svakog prirodnog broja, a samo je jedan takav – 0.■

Paragraf završavamo s još nekim primerima klasa nilpotentnih grupa ([97]).

**Lema 48.53** *Grupa* $\mathbf{G}$ *je nilpotentna grupa klase najviše* 2
*akko je*
$\mathbf{G/Z(G)}$ *Abelova grupa*
*akko je*
$[[a,b],c] = [a,[b,c]]$ *za svako* $a, b, c \in G$
*akko je*
$[ab,c] = [a,c] \cdot [b,c]$ *i* $[a,bc] = [a,b] \cdot [a,c]$ *za svako* $a, b, c \in G$.

**Dokaz.** $\mathbf{G}$ je nilpotentna grupa klase 2 akko je $\gamma_2\mathbf{G} = [\gamma_1\mathbf{G}, \mathbf{G}] = [\mathbf{G}', \mathbf{G}] = \mathbf{E}$ akko je $\mathbf{G}' \leq \mathbf{Z(G)}$ akko je $\mathbf{G/Z(G)}$ Abelova grupa.

Ako je $\mathbf{G}' \leq \mathbf{Z(G)}$, onda je, trivijalno, $[[a,b],c] = [a,[b,c]] = e$ za svako $a, b, c \in G$, pa je, prema 6.3, $[ab,c] = [a,c] \cdot [b,c]$ i $[a,bc] = [a,c] \cdot [a,b] = [a,b] \cdot [a,c]$.

Pretpostavimo sada da je formiranje komutatora asocijativno:

$$\forall a, b, c\ [[a,b],c] = [a,[b,c]].$$

Onda je posebno, za $b = c$, $[[a,b],b] = [a,[b,b]] = [a,e] = e$ i odatle, redom:
$[a,b]^{-1}b^{-1}[a,b]b = e$,
$[a,b]^{-1} = b^{-1}[a,b]^{-1}b$,
$b[b,a]b^{-1} = [a,b]^{-1}$,
$[a,b^{-1}] = [a,b]^{-1}$.
Analogno, $[[a,a],b] = [a,[a,b]] = e$ implicira $[a,b]^{-1} = [a^{-1},b]$. Stoga: $[a,b] = ([a,b]^{-1})^{-1} = [a,b^{-1}]^{-1} = [a^{-1},b^{-1}]$ i
$[[a,b],c] = [[a,b]^{-1},c^{-1}] = [a,b]c[a,b]^{-1}c^{-1} = [a^{-1},b^{-1}]c[a^{-1},b]c^{-1}$,
$[a,[b,c]] = [a^{-1},[b,c]^{-1}] = a[b,c]a^{-1}[b,c]^{-1} = a[c,b]^{-1}a^{-1}[b,c^{-1}] =$
$a[c^{-1},b]a^{-1}[b,c^{-1}]$.
Polazeći od jednakosti $[a^{-1},b^{-1}]c[a^{-1},b]c^{-1} = a[c^{-1},b]a^{-1}[b,c^{-1}]$ izvodimo redom:

$aba^{-1}b^{-1}cab^{-1}a^{-1}bc^{-1} = acb^{-1}c^{-1}ba^{-1}b^{-1}cbc^{-1},$
$ba^{-1}b^{-1}cab^{-1}a^{-1}c^{-1}bab^{-1}cbc^{-1} = e,$
$c^{-1}ba^{-1}b^{-1}cab^{-1}a^{-1}c^{-1}bab^{-1}cb = c^{-1}c = e,$
$[b^{-1}c, a]b^{-1}[a, b^{-1}c]b = e,$
$[[a, b^{-1}c], b] = e.$

Prema tome je, s obzirom da su u pitanju proizvoljni elementi grupe, $\mathbf{G}' \leq \mathbf{Z}(\mathbf{G})$ i $\gamma_2\mathbf{G} = \mathbf{E}$.

Ako je pak $b^{-1}[a, c]b[b, c] = [ab, c] = [a, c] \cdot [b, c]$ za svako $a, b, c \in G$ (pozivamo se na 6.2($d$)), tada je $[a, c]b = b[a, c]$ i opet je $\mathbf{G}' \leq \mathbf{Z}(\mathbf{G})$.□

**Teorema 48.54** *Ako je $[a, b, b] = e$ za svaka dva elementa $a, b$ grupe $\mathbf{G}$, onda je $\mathbf{G}$ nilpotentna grupa klase najviše 3, $\gamma_1\mathbf{G} = \mathbf{G}'$ je Abelova grupa i $\gamma_2\mathbf{G}$, ako je nejedinična grupa, ima eksponent 3.*

**Dokaz.** U dokazu ćemo se stalno oslanjati na lemu 6.2. Da se ne bismo ponavljali, govorićemo samo o tačkama ove leme na koje se pozivamo.

Prema uslovu teoreme je $[a, bc, bc] = e$ za svako $a, b, c \in G$, a prema tački ($e$) (leme 6.2):

$$[a, bc, bc] = [[a, bc], bc] = [[a, bc], c]c^{-1}[[a, bc], b]c \tag{1}.$$

Prema istoj tački i uslovu teoreme važi:

$$[a, bc, c] = [[a, bc], c] = [[a, c]c^{-1}[a, b]c, c] =$$
$$c^{-1}[a, b]^{-1}c[a, c]^{-1} \cdot c^{-1} \cdot [a, c]c^{-1}[a, b]c \cdot c =$$
$$(c^{-1}[a, b]c)^{-1} \cdot ([a, c]^{-1}c^{-1}[a, c]c) \cdot (c^{-2}[a, b]c^2) =$$
$$(c^{-1}[a, b]c)^{-1} \cdot [a, c, c] \cdot (c^{-2}[a, b]c^2) = c^{-1} \cdot ([a, b]^{-1}c^{-1}[a, b]c) \cdot c =$$
$$c^{-1}[[a, b], c]c = [[a, b], c] = [a, b, c]$$

(u pretposlednjem koraku koristili smo, a to ćemo i ubuduće prećutno činiti, da je $[g, c] \cdot c = c \cdot [g, c]$ (za svako $g, c \in G$), što je ekvivalentno sa $[[g, c], c] = e$, tj. $[g, c, c] = e$; odatle je, uopšte (pošto je $c \cdot g^{-1}cg = g^{-1}cg \cdot c$) za svako $k, l \in Z$: $g_1^{-1}c^k g_1 \cdot g_2^{-1}c^l g_2 = g_2^{-1}c^l g_2 \cdot g_1^{-1}c^k g_1$ – videti i 6.21). Sumiramo:

$$[a, bc, c] = [a, b, c] \tag{2}.$$

Slično,

$$[a, bc, b] = [[a, bc], b] = [[a, c]c^{-1}[a, b]c, b] =$$
$$c^{-1}[a, b]^{-1}c[a, c]^{-1} \cdot b^{-1} \cdot [a, c]c^{-1}[a, b]c \cdot b =$$
$$(c^{-1}[a, b]c)^{-1} \cdot ([a, c]^{-1}b^{-1}[a, c]b) \cdot (b^{-1}c^{-1}[a, b]cb) =$$
$$(c^{-1}[a, b]c)^{-1} \cdot [[a, c], b] \cdot c^{-1}[a, b]c \cdot c^{-1}[a, b]^{-1}c \cdot b^{-1}c^{-1}[a, b]cb =$$



$$(c^{-1}[a, b]c)^{-1} \cdot [a, c, b] \cdot c^{-1}[a, b]c \cdot [c^{-1}[a, b]c, b].$$

No,

$$[c^{-1}[a, b]c, b] = [c^{-1}a^{-1}b^{-1}abc, b] = [(ac)^{-1}b^{-1}ac \cdot c^{-1}bc, b] =$$
$$(c^{-1}bc)^{-1} \cdot [(ac)^{-1}b^{-1}(ac), b] \cdot c^{-1}bc \cdot [c^{-1}bc, b] =$$

$(c^{-1}bc)^{-1} \cdot (ac)^{-1}b(ac) \cdot b^{-1} \cdot ((ac)^{-1}b(ac))^{-1} \cdot b \cdot c^{-1}bc \cdot (c^{-1}bc)^{-1} \cdot b^{-1} \cdot c^{-1}bc \cdot b = e,$

a $[a, c, b] = [a, c]^{-1}b^{-1}[a, c] \cdot b$ i $c^{-1}[a, b]c = c^{-1}a^{-1}b^{-1}abc = (ac)^{-1}b^{-1}ac \cdot c^{-1}bc$ su permutabilni kao proizvodi konjugata stepena elementa $b$. Na osnovu navedenog je

$$[a, bc, b] = [a, c, b] \tag{3}.$$

(1), (2) i (3) daju:

$$e = [a, bc, bc] = [a, bc, c] \cdot c^{-1} \cdot [a, bc, b] \cdot c =$$
$$[a, b, c] \cdot c^{-1} \cdot [a, c, b] \cdot c = c^{-1} \cdot [a, b, c] \cdot [a, c, b] \cdot c,$$

te je:

$$[a, b, c] \cdot [a, c, b] = e. \tag{4}.$$

Kako je $[a, b, c] = [[b, a]^{-1}, c] = [b, a] \cdot [[b, a], c]^{-1} \cdot [b, a]^{-1} = [b, a] \cdot [b, a, c]^{-1} \cdot [b, a]^{-1} = [b, a, c]^{-1}$ ($[b, a]$ i $[[b, a], c]$ su, prema ranijoj diskusiji, permutabilni), to je:

$$[a, b, c] = [b, a, c]^{-1} \tag{5},$$

i

$$[a, c, b] = [b, a, c] \tag{6}.$$

Po simetriji stvari je

$$[b, a, c] = [c, b, a] \tag{7}.$$

Takođe važi:

$$[a, c, a^{-1}ba] = [[a, c], b[b, a]] = [a, c]^{-1} \cdot [b, a]^{-1}b^{-1} \cdot [a, c] \cdot b[b, a] =$$
$$[a, c]^{-1}b^{-1}[a, c]b = [a, c, b] \tag{8}$$

(jer je $[b, a]$ permutabilno kako sa $b$ tako i sa $[a, c]$ – $[b, a] = b^{-1}a^{-1}b \cdot a$ i $[a, c] = a^{-1} \cdot c^{-1}ac$; radi se, dakle, o konjugatima stepena elementa $a$). Prema tački ($g$) i relacijama (6), (7) i (8) sledi:

$$[a, c, b]^3 = e \tag{9};$$

$e = [a, c, a^{-1}ba] \cdot [b, a, b^{-1}cb] \cdot [c, b, c^{-1}ac] = [a, c, b] \cdot [b, a, c] \cdot [c, b, a] = [a, c, b]^3$. Konačno izvodimo:

$$[a, b, c, d] = [[a, b], c, d] \overset{(4)}{=} [[a, b], d, c]^{-1} = [[a, b, d], c]^{-1} \overset{(6)}{=} [[d, a, b], c]^{-1} =$$

$$[[d,a],b,c]^{-1} \overset{(6)}{=} [c,[d,a],b]^{-1} \overset{(6)}{=} [b,c,[d,a]]^{-1} = [[b,c],[d,a]]^{-1} = [[d,a],[b,c]] =$$
$$[d,a,[bc]] \overset{(6)}{=} [[b,c],d,a] = [b,c,d,a] \overset{(4)}{=} [b,c,a,d]^{-1} = [[b,c,a],d]^{-1} \overset{(6)}{=}$$
$$[[a,b,c],d]^{-1} = [a,b,c,d]^{-1}.$$

Znači, za bilo koja četiri elementa $a,b,c,d$ grupe $\mathbf{G}$ je $[a,b,c,d]^2 = e$, dok je takođe, već smo pokazali: $[a,b,c,d]^3 = [[a,b],c,d]^3 = e$. Stoga je, prema "vezama" iz poslednjeg dokaza: $[a,b,c,d] = [[d,a],[b,c]] = e$, tj. $[d,a]\cdot[b,c] = [b,c]\cdot[d,a]$, što će reći da je $\gamma_1\mathbf{G} = \mathbf{G}'$ Abelova grupa. Grupa $\gamma_2\mathbf{G} = [\gamma_1\mathbf{G},\mathbf{G}] = [\mathbf{G}',\mathbf{G}]$ generisana je skupom $\{[[a,b],c]\ (=[a,b,c]) \mid a,b,c\in G\}$, te je $\gamma_2\mathbf{G} \le \mathbf{Z}(\mathbf{G})$ ($[a,b,c,d] = e$ povlači $[a,b,c]\cdot d = d\cdot[a,b,c]$), a onda je $\gamma_3\mathbf{G} = [\gamma_2\mathbf{G},\mathbf{G}] = \mathbf{E}$. Prema (9) (i zbog komutativnosti) grupa $\gamma_2\mathbf{G}$ ima eksponent 3.■

**Korolar 48.55** *Grupa $\mathbf{G}$ eksponenta 3 je nilpotentna grupa klase najviše 3 i $\mathbf{G}'$ je Abelova grupa.*

**Dokaz.** Prema 6.6 i prethodnoj teoremi.□

Drugi deo tvrđenja korolara specijalni je slučaj opštijeg stava.

**Lema 48.56** *Ako je $\mathbf{G}$ nilpotentna grupa klase $k$, onda je $\gamma_{[\frac{k}{2}]}\mathbf{G}$ Abelova grupa ($[\frac{k}{2}]$ - najveći ceo broja $\frac{k}{2}$).*

**Dokaz.** Prema 46.25(1) je $[\gamma_i\mathbf{G},\gamma_{k-i-1}\mathbf{G}] = \mathbf{E}$ za svako $i = 0,\dots,k-1$. Kako je $k-[\frac{k}{2}]-1 \le [\frac{k}{2}]$, sledi: $[\gamma_{[\frac{k}{2}]}\mathbf{G},\gamma_{[\frac{k}{2}]}\mathbf{G}] \le [\gamma_{[\frac{k}{2}]}\mathbf{G},\gamma_{k-[\frac{k}{2}]-1}\mathbf{G}] = \mathbf{E}$; znači, $\gamma_{[\frac{k}{2}]}\mathbf{G}$ je Abelova grupa.□

**Lema 48.57** *Neka je $\mathbf{G}$ grupa eksponenta 4, $\mathbf{B}$ njena konačna podgrupa i neka je, za neko $a\in G$, $\mathbf{G} = \langle a,B\rangle$ i $a^2\in B$. Tada je i $\mathbf{G}$ konačna grupa.*

**Dokaz.** Svaki element iz $\mathbf{G}$ se može, prema uslovima leme, predstaviti u obliku $b_0ab_1a\dots ab_{r+1}$, gde je $b_i\in B$, $i=0,\dots,r+1$. Pokazaćemo, a time i dokazati lemu, da zapravo postoji gornje ograničenje za "dužinu" proizvoda, tj. da postoji neko $n$ takvo da se svaki element može prestaviti u datoj formi, pri čemu je $r\le n$. Fiksirajmo jedan element $g\in G$ i neka je $b_0ab_1a\dots ab_{r+1}$ jedna njegova prezentacija sa minimalnim "$r$"; stoga je $b'_0ab'_1a\dots ab'_{s+1}\ne g$ čim je $s<r$, bez obzira na izbor elemenata $b'_j\in B$, $j=0,\dots,s+1$. Kako je $a^2\in B$, svaki od elemenata $b_1,\dots,b_r$ je različit od jediničnog. Za svako $i=1,\dots,r$ imamo $(ab_i)^4 = ab_i\cdot ab_i\cdot ab_i\cdot ab_i = e$, i odatle

$$ab_ia = b_i^{-1}a^{-1}b_i^{-1}a^{-1}b_i^{-1} = b_i^{-1}a^{-2}\cdot a\cdot b_i^{-1}a^{-2}\cdot a\cdot b_i^{-1} = c_iac_iab_i^{-1},$$

gde je $c_i = b_i^{-1}a^{-2}\in B$. Zamenom izraza $ab_ia$ u $b_0ab_1a\dots ab_ia\dots ab_{r+1}$ sa $c_iac_iab_i^{-1}$ ($i\in\{1,\dots,r\}$) dobijamo:

$$g = b_0a\dots b_{i-1}c_iac_iab_i^{-1}b_{i+1}a\dots ab_{r+1} = b_0a\dots b'_{i-1}ab'_iab'_{i+1}a\dots ab_{r+1},$$



gde je $b'_{i+1} = b_i^{-1}b_{i+1}\ne b_{i+1}$ (jer je $b_i\ne e$). Imajući u vidu navedeno, dajemo (induktivnu) metodu za dobijanje $i$ različitih predstavljanja elementa $g$ (u datoj formi) koja se razlikuju u "predstavniku" $b_i\in B$, dok su "predstavnici" $b_{i+1},\dots,b_{r+1}$ isti. Slučaj $i=1$ je (odviše) jasan. Pretpostavimo da je za $i = 1,\dots,r-1$ dato $i$ prezentacija elementa $g$ sa različitim $i$-tim predstavnicima (iz $\mathbf{G}$): $b_{i1},\dots,b_{ii}$, i istim $(i+1)$-vim, ..., $(r+1)$-vim predstavnikom. Ako u $j$-toj "verziji" zamenimo $ab_{ij}a$ sa $c_{ij}ac_{ij}ab_{ij}^{-1}$ nastaje izraz za $g$, gde je sada $b_{i+1,j} = b_{ij}^{-1}b_{i+1}$. Elementi $b_{i+1,j}$, $j=1,\dots,i$, međusobno su različiti i svi su različiti od $b_{i+1}$. Dobili smo, dakle, $i+1$ izraza za $g$ u kojima se $(i+1)$-va "komponenta" iz $B$ razlikuje (dok su one "iza" iste). Posebno, (za $i=r$) postoji $r$ različitih formi za $g$ sa različitim $r$-tim "komponentama". No, to su sve elementi iz $B$, i kako je $\mathbf{B}$ konačna grupa, mora biti $r\le|B|$.□

**Teorema 48.58** *Konačno generisana grupa $\mathbf{G}$ eksponenta 4 je nilpotentna.*

**Dokaz.** Dovoljno je da pokažemo da je $\mathbf{G}$ konačna grupa (u tom slučaju je nilpotentna kao 2-grupa - 48.9($a$)). Neka je $\mathbf{G}$ generisana skupom $\{g_1,\dots,g_n\}$ i neka je $\mathbf{G}_i = \langle g_1,\dots,g_i\rangle$ za $i=1,\dots,n$, i $\mathbf{H}_i = \langle G_i, g_{i+1}^2\rangle$ za $i=1,\dots,n-1$. Prema tome, $\mathbf{G}_{i+1} = \langle H_i, g_{i+1}\rangle$ za $i=1,\dots,n-1$. Indukcijom po $i$ ($=1,\dots,n-1$) pokazujemo simultano da su grupe $\mathbf{G}_i$, $\mathbf{H}_i$ konačne. Za $i=1$ je $\mathbf{G}_1 = \langle g_1\rangle$ i $g_1^4 = e$ (znači, $|G_1|\le 4$). Prema prethodnoj lemi je i $\mathbf{H}_1$ konačna grupa: $\mathbf{H}_1 = \langle G_1, g_2^2\rangle$ i $(g_2^2)^2 = e\in G_1$. Pretpostavimo da je tvrđenje tačno za svako $j\le i<n-1$. Onda iz $\mathbf{G}_{i+1} = \langle H_i, g_{i+1}\rangle$, $g_{i+1}^2\in H_i$ i $|H_i|<\infty$ sledi da je $\mathbf{G}_{i+1}$ konačna grupa, pa je i $\mathbf{H}_{i+1} = \langle G_{i+1}, g_{i+2}^2\rangle$ konačna grupa (ponovo je, zbog eksponenta grupe, $(g_{i+2}^2)^2 = e\in G_{i+1}$). No, kad je $\mathbf{H}_{n-1}$ konačna, konačna je i grupa $\mathbf{G} = \mathbf{G}_n = \langle H_{n-1}, g_n\rangle$.

Primetimo na kraju da se uslov konačne generisanosti ne može isključiti - postoje grupe eksponenta 4 koje nisu nilpotentne.■

Osnovu dokaza prethodne teoreme izdvajamo kao poseban stav.

**Lema 48.59** *Konačno generisana grupa eksponenta 4 je konačna.*

## 49 Rešive grupe

Rešive grupe su grupe nastale od Abelovih sukcesivnim formiranjem ekstenzija konačan broj puta (uporediti sa 46.7). Pojasnićemo to uz formalnu definiciju, no prvo

**Definicija 49.1** *Normalni niz je rešiv akko su svi njegovi faktori Abelove grupe.*

*Invarijantni niz je rešiv akko su svi njegovi faktori Abelove grupe.*

**Napomena.** Trivijalno, jedinična grupa ima rešiv niz - dužine 0. Ovo ćemo imati u vidu u narednim definicijama i tvrđenjima.

**Definicija 49.2** *Grupa je rešiva akko ima rešivi normalni niz.*

Ako je $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_k = \mathbf{E}$ rešivi normalni niz grupe $\mathbf{G}$, onda je $\mathbf{G}_{k-1}$ ($\cong \mathbf{G}_{k-1}/\mathbf{E}$) Abelova grupa, $\mathbf{G}_{k-2}$ je ekstenzija grupe $\mathbf{G}_{k-1}$ grupom $\mathbf{G}_{k-2}/\mathbf{G}_{k-1}$, ..., $\mathbf{G} = \mathbf{G}_0$ je ekstenzija grupe $\mathbf{G}_1$ grupom $\mathbf{G}/\mathbf{G}_1$.

**Lema 49.3** *Sledeći uslovi su ekvivalentni za grupu* $\mathbf{G}$*:*

(1) $\mathbf{G}$ *je rešiva grupa;*

(2) $\mathbf{G}$ *ima rešivi invarijantni niz;*

(3) *za neki prirodan broj* $n$ *je* $\mathbf{G}^{(n)} = \mathbf{E}$.

**Dokaz.** Pretpostavićemo da $\mathbf{G}$ nije jedinična grupa (taj slučaj je odveć trivijalan).

(1) $\Longrightarrow$ (3) Neka je $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_k = \mathbf{E}$ rešivi normalni niz grupe $\mathbf{G}$. Indukcijom po $i$ ($= 1, 2, \ldots$) dokazujemo da je $\mathbf{G}^{(i)} \leq \mathbf{G}_i$. $\mathbf{G}^{(1)} = \mathbf{G}' \leq \mathbf{G}_1$, jer je $\mathbf{G}/\mathbf{G}_1$ Abelova grupa (videti 6.8). Isto tako, iz $\mathbf{G}^{(i)} \leq \mathbf{G}_i$ sledi $\mathbf{G}^{(i+1)} = (\mathbf{G}^{(i)})' \leq \mathbf{G}_i' \leq \mathbf{G}_{i+1}$. Dakle, $\mathbf{G}^{(k)} \leq \mathbf{G}_k = \mathbf{E}$.

(3) $\Longrightarrow$ (2) Neka je $n$ najmanji prirodan broj za koji je $\mathbf{G}^{(n)} = \mathbf{E}$ i neka je $\mathbf{G} = \mathbf{G}^{(0)} \geq \mathbf{G}^{(1)} = \mathbf{G}' \geq \cdots \geq \mathbf{G}^{(n-1)} \geq \mathbf{G}^{(n)} = \mathbf{E}$ izvodni lanac grupe $\mathbf{G}$ - 6.1 ($\mathbf{G}^{(n+1)} = \mathbf{G}^{(n+2)} = \cdots = \mathbf{E}$). Svaka od grupa $\mathbf{G}^{(i)}$ je invarijantna podgrupa (6.7), a $\mathbf{G}^{(i)}/\mathbf{G}^{(i+1)}$ je Abelova grupa. Primetimo još da je (za $i = 1, \ldots, n$) $\mathbf{G}^{(i)}$ prava podgrupa grupe $\mathbf{G}^{(i-1)}$; pretpostavka $\mathbf{G}^{(k)} = \mathbf{G}^{(k-1)}$ za $k < n$ implicirala bi $\mathbf{G}^{(k-1)} = \mathbf{G}^{(k+j)}$ za svako $j \in N$ i izvodni lanac ne bi nikad "stigao" do jedinične grupe.

(2) $\Longrightarrow$ (1) Očigledno.□

**Napomena.** Iz dokaza prethodne leme sledi da je izvodni niz rešive grupe njen najkraći rešivi niz. Ako je, za grupu $\mathbf{G}$, $n$ najmanji prirodan broj za koji je $\mathbf{G}^{(n)} = \mathbf{E}$, grupu $\mathbf{G}$ ćemo zvati *rešivom grupom izvodne dužine* $n$ ili, kao u slučaju nilpotentnih grupa, *rešivom grupom klase* $n$.

**Lema 49.4** (*a*) *Proširenje rešivog normalnog niza je rešivi normalni niz;*

(*b*) *Svaki normalni niz rešive grupe ima rešivo normalno proširenje.*

**Dokaz.** (*a*) Neka je $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_k = \mathbf{E}$ rešivi normalni niz grupe $\mathbf{G}$, $\mathbf{G} = \mathbf{H}_0 > \mathbf{H}_1 > \cdots > \mathbf{H}_l = \mathbf{E}$ njegovo (normalno) proširenje i neka je za neko $i$, $1 \leq i \leq n$, $\mathbf{G}_{i-1} > \cdots > \mathbf{H}_{j-1} > \mathbf{H}_j > \cdots > \mathbf{G}_i$. Prema 6.8 je $\mathbf{H}_j$ normalna podgrupa grupe $\mathbf{G}_{i-1}$ i $\mathbf{G}_{i-1}/\mathbf{H}_j$ Abelova grupa ($\mathbf{G}_{i-1}' \leq \mathbf{G}_i < \mathbf{H}_j$), pa je i $\mathbf{H}_{j-1}/\mathbf{H}_j$ Abelova grupa.

(*b*) Direktna posledica teoreme Schreiera i prethodne tačke.□

**Korolar 49.5** (*a*) *Podgrupa rešive grupe klase* $n$ *je rešiva grupa klase najviše* $n$*;*

(*b*) *Homomorfna slika rešive grupe klase* $n$ *je rešiva grupa klase najviše* $n$.



**Dokaz.** (*a*) Direktna posledica leme 46.11, s tim što ćemo sada, naravno, poći od rešivog normalnog niza. Ili još jednostavnije: ako je $\mathbf{G}^{(n)} = \mathbf{E}$ i $\mathbf{H} \leq \mathbf{G}$, onda je, jasno, i $\mathbf{H}^{(n)} = \mathbf{E}$.

(*b*) Neka je $\mathbf{N}$ netrivijalna normalna podgrupa rešive grupe $\mathbf{G}$ i neka je $\mathbf{G} = \mathbf{G}_0 > \cdots > \mathbf{G}_k = \mathbf{N} > \cdots > \mathbf{G}_l = \mathbf{E}$ rešivi normalni niz (rešivo normalno proširenje normalnog niza $\mathbf{G} > \mathbf{N} > \mathbf{E}$). Tada je $\overline{\mathbf{G}} = \mathbf{G}/\mathbf{N} = \overline{\mathbf{G}_0} > \cdots > \overline{\mathbf{G}_{k-1}} = \mathbf{G}_{k-1}/\mathbf{N} > \overline{\mathbf{G}_k} = \overline{\mathbf{E}}$ rešivi normalni niz grupe $\overline{\mathbf{G}} = \mathbf{G}/\mathbf{N}$; jer, $\overline{\mathbf{G}_i} = \mathbf{G}_i/\mathbf{N}$ je, prema 8.7, normalna podgrupa grupe $\overline{\mathbf{G}}_{i-1} = \mathbf{G}_{i-1}/\mathbf{N}$ (za $i = 1, \ldots, k$) i $\overline{\mathbf{G}}_{i-1}/\overline{\mathbf{G}_i} = (\mathbf{G}_{i-1}/\mathbf{N})/(\mathbf{G}_i/\mathbf{N})$ ($\cong \mathbf{G}_{i-1}/\mathbf{G}_i$) je Abelova grupa.

Dokaz smo mogli dati i pozivajući se jednostavno na (očiglednu) činjenicu: ako je $\varphi$ homomorfno preslikavanje grupe $\mathbf{G}$ na grupu $\mathbf{H}$, onda je (za svaki prirodan broj $k$) $\mathbf{H}^{(k)} = (\mathbf{G}^{(k)})\varphi$; no već smo imali 6.22 - ako je $\mathbf{G}^{(n)} = \mathbf{E}$ i $\mathbf{N} \lhd \mathbf{G}$, tada je $(\mathbf{G}/\mathbf{N})^{(n)} = (\mathbf{G}^{(n)}\mathbf{N})/\mathbf{N} = \overline{\mathbf{E}}$.□

**Lema 49.6** *Ekstenzija rešive grupe rešivom grupom je rešiva grupa.*

**Dokaz.** Delom već dat. Ako su normalna podgrupa $\mathbf{N}$ grupe $\mathbf{G}$ i faktor grupa $\mathbf{G}/\mathbf{N}$ rešive i ako je $\mathbf{N}^{(r)} = \mathbf{E}$ i $(\mathbf{G}/\mathbf{N})^{(s)} = (\mathbf{G}^{(s)}\mathbf{N})/\mathbf{N} = \overline{\mathbf{E}}$, tada je $\mathbf{G}^{(s)} \leq \mathbf{N}$ i $(\mathbf{G}^{(s)})^{(r)} = \mathbf{G}^{(r+s)} \leq \mathbf{N}^{(r)}) = \mathbf{E}$.

Obično se, međutim, daje ovaj dokaz:

neka su $\mathbf{N}$ i $\mathbf{G}/\mathbf{N}$ rešive grupe sa rešivim nizovima, respektivno: $\mathbf{N} = \mathbf{N}_0 > \cdots > \mathbf{N}_l = \mathbf{E}$, $\mathbf{G}/\mathbf{N} = \overline{\mathbf{G}} = \overline{\mathbf{G}_0} > \overline{\mathbf{G}_1} = \mathbf{G}_1/\mathbf{N} > \cdots > \overline{\mathbf{G}_k} = \overline{\mathbf{E}}$. Onda je $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_k = \mathbf{N} > \cdots > \mathbf{N}_l = \mathbf{E}$ rešivi normalni niz grupe $\mathbf{G}$; opet je prema 8.7 $\mathbf{G}_i \lhd \mathbf{G}_{i-1}$, a $\mathbf{G}_{i-1}/\mathbf{G}_i \cong (\mathbf{G}_{i-1}/\mathbf{N})/(\mathbf{G}_i/\mathbf{N}) = \overline{\mathbf{G}}_{i-1}/\overline{\mathbf{G}_i}$ je Abelova grupa.□

**Korolar 49.7** *Direktni proizvod konačno mnogo rešivih grupa (klasa* $\leq n$*) je rešiva grupa (klase* $\leq n$*).*

**Dokaz.** Indukcijom po broju direktnih faktora - $n$. Za $n = 2$ imamo poseban slučaj prethodne leme i on ujedno, uz "asistenciju" 10.3($e$), objašnjava sve.

Ovo tvrđenje je, inače samo specijalan slučaj leme 49.10.□

**Lema 49.8** *Ako je* $\mathbf{A}$ *rešiva grupa izvodne dužine* $n$*, onda je* $\overline{\mathbf{G}} = \mathbf{A}\ Wr\ \mathbf{C}_2$ *rešiva grupa izvodne dužine* $n + 1$.

**Dokaz.** Koristimo notaciju iz paragrafa o spletenim proizvodima. Neka je $\mathbf{C}_2 = \langle\{\epsilon, \alpha\}, \cdot\rangle$, $\mathbf{B} = \mathbf{A}_\epsilon \times \mathbf{A}_\alpha$ ($\mathbf{A}_\epsilon = \mathbf{A}_\alpha = \mathbf{A}$) i $\Phi : C_2 \longrightarrow Aut(\mathbf{B})$, gde je $(\epsilon)\Phi = \imath_B$, $(\alpha)\Phi = \phi_\alpha$ i, za $(x, y) \in B$, $(x, y)\phi_\alpha = (y, x)$. Podsećamo: $\overline{\mathbf{G}} = \mathbf{A}\ Wr\ \mathbf{C}_2 = \mathbf{B} \times_\Phi \mathbf{C}_2$; prema tome, $\overline{\mathbf{B}} = \langle\{(\epsilon, f) \mid f \in B\}, \cdot\rangle$ je normalna i to rešiva podgrupa, izvodne dužine $n$, a zbog $\overline{\mathbf{G}}/\overline{\mathbf{B}} \cong \mathbf{C}_2$ je $\overline{\mathbf{G}}' \leq \overline{\mathbf{B}}$. Odatle, izvodna dužina grupe $\overline{\mathbf{G}}'$ je $\leq n$. S druge strane, ako je $\pi_\alpha$ projekcija grupe $\overline{\mathbf{B}}$ na $\overline{\mathbf{B}}_\alpha \overset{\text{def}}{=} \langle\{(\epsilon, (e, (\alpha)f)) \mid f \in \overline{B}\}, \cdot\rangle = \langle\{(\epsilon, (e, a)) \mid a \in A\}, \cdot\rangle$

(element $f \in \overline{B}$, gde je $(\epsilon)f = a$ i $(\alpha)f = b$, identifikujemo sa uređenim parom $(a,b)$ – dakle, $(\epsilon,(a,b))\pi_\alpha = (\epsilon,(e,b))$), onda je $\pi_\alpha|_{\overline{G}'}$ surjektivno homomorfno preslikavanje grupe $\overline{\mathbf{G}}'$ na $\overline{\mathbf{B}}_\alpha$. Zaista, ako je $a = c^{-1}d$, tada je

$$(\epsilon,(e,a)) = ([(\alpha,(e,e)),(\epsilon,(c,d))])\pi_\alpha;$$

imamo:

$$(\alpha,(e,e))^{-1}\cdot(\epsilon,(c,d))^{-1}\cdot(\alpha,(e,e))\cdot(\epsilon,(c,d)) =$$

$$(\alpha,(e,e))\cdot(\epsilon,(c^{-1},d^{-1}))\cdot(\alpha,(e,e))\cdot(\epsilon,(c,d)) = (\alpha,(c^{-1},d^{-1}))\cdot(\alpha,(c,d)) =$$

$$(\epsilon,(c^{-1},d^{-1})^\alpha\cdot(c,d)) = (\epsilon,(d^{-1},c^{-1})\cdot(c,d)) = (\epsilon,(d^{-1}c,c^{-1}d))$$

i $(\epsilon,(d^{-1}c,c^{-1}d))\pi_\alpha = (\epsilon,(e,a))$.

Primetimo da je uopšte za $0 \le i,j \le 1$:

$$[(\alpha^i,f),(\alpha^j,g)] = (\alpha^i,(f^{\alpha^i})^{-1})\cdot(\alpha^j,(g^{\alpha^j})^{-1})\cdot(\alpha^i,f)\cdot(\alpha^j,g) =$$

$$(\alpha^{i+2j},(f^{\alpha^{i+2j}})^{-1}\cdot(g^{\alpha^j})^{-1})\cdot(\alpha^{i+2j},f^{\alpha^j}\cdot g) = (\epsilon,f^{-1}\cdot(g^{\alpha^i})^{-1}\cdot f^{\alpha^j}\cdot g);$$

tako je npr.

$$((f^{\alpha^{i+2j}})^{-1})^{\alpha^{i+2j}} = ((f^{\alpha^{i+2j}})^{\alpha^{i+2j}})^{-1} = f^{\alpha^{i+2j}\cdot\alpha^{i+2j}} = (f^\epsilon)^{-1} = f^{-1}.$$

Mogli smo znači i tako dokazati da je $\overline{\mathbf{G}}' \le \overline{\mathbf{B}}$. Pošto je $\overline{\mathbf{B}}_\alpha \cong \mathbf{A}$, izvodna dužina podgrupe $\overline{\mathbf{G}}'$ je barem $n$ i stoga je, s obzirom na već pokazano, baš $n$.□

**Korolar 49.9** *Za svaki pozitivan prirodan broj n postoji rešiva grupa izvodne dužine n.*

**Dokaz.** Neka je $\mathbf{G}_1$ (ma koja) nejedinična Abelova grupa. Definišimo rekurzivno: $\mathbf{G}_2 = \mathbf{G}_1\ Wr\ \mathbf{C}_2$ i, generalno, $\mathbf{G}_{n+1} = \mathbf{G}_n\ Wr\ \mathbf{C}_2$. Indukcijom se lako proverava, pozivajući se na prethodnu lemu, da je (za svako pozitivno $n$) $\mathbf{G}_n$ rešiva grupa izvodne dužine $n$.□

**Napomena.** Kao i u slučaju nilpotentnih grupa, direktni proizvod (beskonačno mnogo) rešivih grupa ne mora biti rešiva grupa. Jedan takav (kontra)primer je grupa $\prod_{n\ge1}\mathbf{G}_n$, gde su $\mathbf{G}_n$, $n \ge 1$, grupe iz dokaza prethodnog korolara (ova grupa je, međutim, *lokalno rešiva*, tj. sve njene konačno generisane podgrupe su rešive); jasno, imamo u vidu i tačku $(a)$ korolara 49.5 na osnovu koje generalno izvodimo

**Lema 49.10** *Kartezijanski (direktni) proizvod rešivih grupa je rešiva grupa akko je skup izvodnih dužina direktnih faktora ograničen sa gornje strane.*

**Dokaz.** Direktno prema 10.3$(e)$ i prethodnoj napomeni.□



**Korolar 49.11** *Klasa rešivih grupa izvodnih dužina manjeg od ili jednakog nekom fiksnom prirodnom broju je varijetet.*

**Dokaz.** Prema 24.21, 49.5 i prethodnoj lemi.□

**Lema 49.12** *Neka su* $\mathbf{H}$ *i* $\mathbf{K}$ *normalne podgrupe grupe* $\mathbf{G}$. *Tada važi:*

$(a)$ *ako su* $\mathbf{H}$ *i* $\mathbf{K}$ *rešive (pod)grupe, onda je i* $\mathbf{H}\cdot\mathbf{K}$ *rešiva (pod)grupa;*

$(b)$ *ako su* $\mathbf{G}/\mathbf{H}$ *i* $\mathbf{G}/\mathbf{K}$ *rešive grupe, onda je i* $\mathbf{G}/(\mathbf{H}\cap\mathbf{K})$ *rešiva grupa.*

**Dokaz.** $(a)$ Neka su $\mathbf{H}$ i $\mathbf{K}$ rešive normalne podgrupe. Tada je, prema drugoj teoremi o izomorfizmu, $(\mathbf{H}\cdot\mathbf{K})/\mathbf{H} \cong \mathbf{K}/(\mathbf{H}\cap\mathbf{K})$, pa ostaje samo da se pozovemo na 49.6 (i 49.5$(b)$). Primetimo da je ovde uslov da su obe podgrupe normalne suvišan; dovoljno je pretpostaviti da je, recimo, samo $\mathbf{H}$ normalna podgrupa.

$(b)$ Možemo kao i slučaju nilpotentnih grupa (48.8) jednostavno krenuti od 10.15 i onda se pozvati na 49.5 i 49.7. Drugi dokaz koristi 49.6.

Neka su $\mathbf{G}/\mathbf{H}$ i $\mathbf{G}/\mathbf{K}$ rešive grupe. Opet se pozivamo na drugu teoremu o izomorfizmu: $\mathbf{H}/(\mathbf{H}\cap\mathbf{K}) \cong (\mathbf{H}\cdot\mathbf{K})/\mathbf{K} \le \mathbf{G}/\mathbf{K}$; dakle, $\mathbf{H}/(\mathbf{H}\cap\mathbf{K})$ je rešiva grupa, a prema trećoj teoremi o izomorfizmu je $\mathbf{G}/\mathbf{H} \cong (\mathbf{G}/(\mathbf{H}\cap\mathbf{K}))/(\mathbf{H}/(\mathbf{H}\cap\mathbf{K}))$. Dakle i grupa $\mathbf{G}/(\mathbf{H}\cap\mathbf{K})$ je rešiva grupa.□

**Korolar 49.13** *Konačna grupa ima jedinstvenu maksimalnu rešivu normalnu podgrupu (dozvoljavamo mogućnost da je to baš cela grupa).*

**Napomena.** Prethodni korolari se ne mogu generalisati. Direktni proizvod beskonačno mnogo rešivih grupa nije nužno rešiva grupa, a ako već nije, onda nema ni maksimalnu rešivu normalnu podgrupu.

**Lema 49.14** *Rešiva grupa sa kompozicionim nizom je konačna.*

**Dokaz.** Neka je $\mathbf{G}$ rešiva grupa sa kompozicionim nizom. Prema teoremi Schreiera i 49.4 svaki kompozicioni niz je rešiv. Fiksirajmo jedan. Njegovi faktori su proste Abelove grupe, dakle ciklične grupe prostog reda. Konačnost grupe $\mathbf{G}$ se onda pokazuje na način na koji smo pokazali da su Abelove grupe sa kompozicionim nizom konačne.□

**Lema 49.15** *Periodična, konačno generisana rešiva grupa je konačna.*

**Dokaz.** Indukcijom po dužini izvodnog niza $(n)$ grupa sa datim svojstvima (prema dokazu leme 49.3 izvodni niz je rešivi niz najkraće dužine). Ako je $n = 0$, grupa je jedinična. Pretpostavimo da je tvrđenje tačno za sve grupe sa datim svojstvima i izvodnim nizovima dužine manje od $n$ $(> 1)$ i neka je $\mathbf{G}$ periodična, konačno generisana rešiva grupa i $n$ najmanji broj za koji je $\mathbf{G}^{(n)} = \mathbf{E}$. Prema 6.22 i induktivnoj pretpostavci, $\mathbf{G}/\mathbf{G}^{(n-1)}$ je konačna grupa, $\mathbf{G}^{(n-1)}$ je pak Abelova periodična grupa, a prema 9.39 i konačno generisana, dakle, konačna. Sledi da je i $\mathbf{G}$ konačna grupa.□

**Korolar 49.16** *Konačna grupa je rešiva akko ima rešivi normalni niz čiji su faktori ciklične grupe prostog reda.*

*Kompozicioni faktori konačne rešive grupe su ciklične grupe prostog reda.*

**Korolar 49.17** *Faktori glavnog niza konačne rešive grupe su elementarne Abelove p-grupe.*

**Dokaz**. Neka je $\mathbf{G}$ konačna rešiva grupa i neka je $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{k-1} > \mathbf{G}_k = \mathbf{E}$ jedan njen glavni niz. Faktori su, znamo, Abelove grupe (49.3 i 49.4). Ako grupa $\mathbf{G}_{i-1}/\mathbf{G}_i$ ne bi bila $p$-grupa za neki prost broj $p$ (drugim rečima, ako bi red faktor grupe $\mathbf{G}_{i-1}/\mathbf{G}_i$ bio proizvod stepena više prostih brojeva), onda bi Sylowa $p$-podgrupa grupe $\mathbf{G}_{i-1}/\mathbf{G}_i$, neka je to $\overline{\mathbf{P}}$ (pretpostavljamo, jasno, da $p$ deli $|G_{i-1}/G_i|$), bila (prava) karakteristična podgrupa grupe $\mathbf{G}_{i-1}/\mathbf{G}_i$, stoga i normalna podgrupa grupe $\mathbf{G}/\mathbf{G}_i$ (4.34), i dati niz ne bi bio glavni; imali bismo $\mathbf{G}_{i-1} > \mathbf{P} > \mathbf{G}_i$, gde je $\overline{\mathbf{P}} = \mathbf{P}/\mathbf{G}_i$. Znači, $\mathbf{G}_{i-1}/\mathbf{G}_i$ jeste $p$-grupa. Grupa $p(\mathbf{G}_{i-1}/\mathbf{G}_i) = \mathbf{H}/\mathbf{G}_i$ je takođe karakteristična (šta više potpuno invarijantna) podgrupa grupe $\mathbf{G}_{i-1}/\mathbf{G}_i$, pa je $\mathbf{H} = \mathbf{G}_i$, tj. $p(\mathbf{G}_{i-1}/\mathbf{G}_i)$ je nula grupa i $\mathbf{G}_{i-1}/\mathbf{G}_i$ je elementarna Abelova $p$-grupa – svi nenula elementi su reda $p$; pretpostavka $p(\mathbf{G}_{i-1}/\mathbf{G}_i) = \mathbf{G}_{i-1}/\mathbf{G}_i$ (odnosno $\mathbf{H} = \mathbf{G}_{i-1}$) implicirala bi da je $\mathbf{G}_{i-1}/\mathbf{G}_i$ deljiva grupa (33.1), kontradikcija (konačna nenula grupa nije deljiva).□

**Korolar 49.18** *Minimalna normalna podgrupa konačne nejedinične rešive grupe $\mathbf{G}$ je elementarna Abelova p-grupa.*

**Dokaz**. Primetimo samo: minimalna normalna podgrupa grupe $\mathbf{G}$ je pretposlednji član nekog glavnog niza (grupe $\mathbf{G}$) – uporediti sa 48.16.□

**Lema 49.19** *Ako je nejedinična grupa rešiva, onda svaki njen nejedinični faktor sadrži nejediničnu normalnu Abelovu podgrupu. Za konačne grupe važi i obrat ovog tvrđenja.*

**Dokaz**. Neka je $\mathbf{G}$ nejedinična rešiva grupa i neka je $n$ najmanji prirodan broj za koji je $\mathbf{G}^{(n)} = \mathbf{E}$. Onda je $\mathbf{G}^{(n-1)}$ Abelova invarijantna (dakle i normalna) podgrupa grupe $\mathbf{G}$.

Neka je pak $\mathbf{G}$ konačna nejedinična grupa koja ispunjava uslov leme. Onda ona sadrži nejediničnu normalnu Abelovu podgrupu ($\mathbf{G} \cong \mathbf{G}/\mathbf{E}$) – neka je to $\mathbf{N}_1$. Ukoliko je $\mathbf{N}_1 \neq \mathbf{G}$, faktor grupa $\mathbf{G}/\mathbf{N}_1$ sadrži nejediničnu Abelovu normalnu podgrupu – $\mathbf{N}_2/\mathbf{N}_1$. Naravno, $\mathbf{N}_2 \lhd \mathbf{G}$. Ako je i $\mathbf{N}_2 \neq \mathbf{G}$, postupak nastavljamo. S obzirom na konačnost grupe $\mathbf{G}$ dobićemo (za neko $k$) $\mathbf{G} = \mathbf{N}_k$. Prema tome, $\mathbf{G}/\mathbf{N}_{k-1} = \mathbf{N}_k/\mathbf{N}_{k-1}$ je Abelova (nejedinična) grupa, a niz $\mathbf{G} = \mathbf{N}_k > \mathbf{N}_{k-1} > \cdots > \mathbf{N}_1 > \mathbf{E}$ je rešivi invarijantni niz.□



**Lema 49.20** *Neka je $\mathbf{G}$ rešiva grupa. Tada važi:*

*(a) $\mathbf{G}$ ispunjava uslov minimalnosti podgrupa akko su svi faktori nekog rešivog normalnog niza Abelove grupe koje ispunjavaju taj uslov;*

*(b) $\mathbf{G}$ ispunjava uslov maksimalnosti podgrupa akko su svi faktori nekog rešivog normalnog niza konačno generisane grupe.*

**Dokaz**. (*a*) Pravac ($\Longrightarrow$) je očigledan (videti 8.14 i komentar uz 5.22). Ako je pak $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{n-1} > \mathbf{G}_n = \mathbf{E}$ rešivi normalni niz (grupe $\mathbf{G}$) čiji faktori ispunjavaju uslov minimalnosti podgrupa, posebno ga ispunjava faktor $\mathbf{G}_{n-1}/\mathbf{G}_n$ ($\cong \mathbf{G}_{n-1}$), onda prema 8.15 taj uslov ispunjavaju i redom $\mathbf{G}_{n-2}, \ldots, \mathbf{G}_0 = \mathbf{G}$.

(*b*) Pravac ($\Longrightarrow$) je trivijalan; ako $\mathbf{G}$ ispunjava uslov maksimalnosti podgrupa, sve podgrupe su joj konačno generisane. Neka je, s druge strane, $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{n-1} > \mathbf{G}_n = \mathbf{E}$ rešivi normalni niz grupe $\mathbf{G}$ čiji su svi faktori konačno generisane Abelove grupe i $\mathbf{H}$ ma koja podgrupa. Prema 46.11 $\mathbf{H}$ ima normalni niz čiji su faktori izomorfni podgrupama nekih faktora datog normalnog niza, dakle i sami su konačno generisane Abelove grupe (32.7). Prema 8.15 je $\mathbf{H}$ konačno generisana grupa.□

**Korolar 49.21** *Rešiva grupa koja ispunjava uslov maksimalnosti normalnih podgrupa je konačno generisana.*

**Teorema 49.22** *(S. N. Černikov). Grupa je rešiva grupa koja ispunjava uslov minimalnosti podgrupa akko je ekstenzija direktnog proizvoda konačno mnogo Prüferovih grupa konačnom rešivom grupom.*

**Dokaz**. Pravac ($\Longleftarrow$) je neposredna posledica leme 13.3 i (njenog) korolara 13.4.

($\Longrightarrow$) Direktan proizvod nula Prüferovih grupa je, po konvenciji, jedinična grupa, pa je slučaj konačnih rešivih grupa trivijalan.

Neka je $\mathbf{G}$ beskonačna rešiva grupa koja ispunjava uslov minimalnosti podgrupa (dakle i periodična) i neka je $\mathbf{F}$ njen konačni ostatak (5.23). Ako je $\mathbf{F}$ Abelova grupa, onda je i deljiva. Jer, podsećamo – videti dokaz leme 33.35, za (bilo koji) prost broj $p$ je $[\mathbf{F} : \mathbf{F}^p] < \infty$ ($F^p \stackrel{\text{def}}{=} \{a^p \mid a \in F\}$), pa je $\mathbf{F}^p$ konačnog indeksa u $\mathbf{G}$ i odatle $\mathbf{F} = \mathbf{F}^p$, tj. $\mathbf{F}$ je deljiva grupa (33.1). Pošto $\mathbf{F}$ zadovoljava uslov minimalnosti podgrupa, u pitanju je direktni proizvod konačno mnogo Prüferovih grupa (33.19). Ali $\mathbf{F}$ i mora biti Abelova. Pretpostavimo, naime, suprotno i neka je $\mathbf{F}^{(k-1)}$ pretposlednji član njenog izvodnog niza ($\mathbf{F}^{(k)} = \mathbf{E}$). Kao Abelova grupa koja ispunjava uslov minimalnosti podgrupa $\mathbf{F}^{(k-1)}$ je direktni proizvod konačno mnogo Prüferovih i primarnih cikličnih grupa (33.35), dakle ima samo konačno mnogo elemenata datog reda. Proizilazi dalje da svaki element iz $\mathbf{F}^{(k-1)}$ ima samo konačno mnogo konjugata u $\mathbf{F}$ ($\mathbf{F}^{(k-1)}$ je potpuno invarijantna podgrupa grupe $\mathbf{F}$).

To će reći: za svako $a \in F^{(k-1)}$ je $[\mathbf{F} : \mathbf{C}_{\mathbf{F}}(a)] < \infty$, znači $\mathbf{F} = \mathbf{C}_{\mathbf{F}}(a)$, i stoga je $\mathbf{F}^{(k-1)} \leq \mathbf{Z}(\mathbf{F})$ $(= \zeta_1\mathbf{F})$. Odatle pak sledi da je $\mathbf{F}$ nilpotentna grupa. Naime, indukcijom po $i$ $(\geq 1)$ se pokazuje da je $\mathbf{F}^{(k-i)} \leq \zeta_i\mathbf{F}$. Ovo smo upravo dokazali za $i = 1$, a ako pođemo od rešive grupe $\mathbf{F}/\mathbf{F}^{(k-1)}$ klase $k-1$, dobijamo na analogan način da je $(\mathbf{F}/\mathbf{F}^{(k-1)})^{(k-2)} = \mathbf{F}^{(k-2)}/\mathbf{F}^{(k-1)} \leq \mathbf{Z}(\mathbf{F}/\mathbf{F}^{(k-1)})$, što implicira $\mathbf{F}^{(k-2)} \leq \zeta_2\mathbf{F}$. Koristimo da zbog $\zeta_2\mathbf{F}/\zeta_1\mathbf{F} = \mathbf{Z}(\mathbf{F}/\zeta_1\mathbf{F})$ važi:

$$(\zeta_2\mathbf{F}/\mathbf{F}^{(k-1)})/(\zeta_1\mathbf{F}/\mathbf{F}^{(k-1)}) = \mathbf{Z}((\mathbf{F}/\mathbf{F}^{(k-1)})/(\zeta_1\mathbf{F}/\mathbf{F}^{(k-1)})) \geq$$

$$(\mathbf{Z}(\mathbf{F}/\mathbf{F}^{(k-1)}) \cdot \zeta_1\mathbf{F}/\mathbf{F}^{(k-1)})/(\zeta_1\mathbf{F}/\mathbf{F}^{(k-1)}) \geq$$

$$((\mathbf{F}^{(k-2)}\zeta_1\mathbf{F})/\mathbf{F}^{(k-1)})/(\zeta_1\mathbf{F}/\mathbf{F}^{(k-1)});$$

uvek je, u stvari, za bilo koje normalne podgrupe $\mathbf{C}$, $\mathbf{D}$, gde je $\mathbf{C} \leq \mathbf{D}$, ma koje grupe $\mathbf{H}$:

$$(\mathbf{Z}(\mathbf{H}/\mathbf{C}) \cdot \mathbf{D}/\mathbf{C})/(\mathbf{D}/\mathbf{C}) \leq \mathbf{Z}((\mathbf{H}/\mathbf{C})/(\mathbf{D}/\mathbf{C})).$$

Ovo je ujedno "recept" za induktivni korak. Ako je $\mathbf{K}$ maksimalna normalna Abelova podgrupa grupe $\mathbf{F}$, prema 48.20 je $\mathbf{K} = \mathbf{C}_{\mathbf{F}}(\mathbf{K})$. S druge strane je $\mathbf{K} \leq \mathbf{Z}(\mathbf{F})$ $(< \mathbf{F})$ (priča se ponavlja: $\mathbf{K}$ je Abelova grupa koja ispunjava uslov minimalnosti podgrupa, dakle direktni proizvod konačno mnogo Prüferovih i primarnih cikličnih grupa, dakle sa konačno mnogo elemenata datog reda, a zbog njene normalnosti je za svaki njen element $a$ $[\mathbf{F} : \mathbf{C}_{\mathbf{F}}(a)] < \infty$ itd. itd.). Otuda, $\mathbf{F} = \mathbf{C}_{\mathbf{F}}(\mathbf{K})$, kontradikcija.■

**Napomena**. Generalno se grupa koja je konačna ekstenzija direktnog proizvoda konačno mnogo Prüferovih grupa zove *Černikova grupa*.

**Lema 49.23** *Ako je $\mathbf{G}$ nilpotentna grupa i $\mathbf{G}/\mathbf{G}'$ konačno generisana grupa, tada su svi faktori nižeg centralnog niza grupe $\mathbf{G}$ konačno generisani, a sama grupa $\mathbf{G}$ ispunjava uslov maksimalnosti podgrupa.*

**Dokaz**. Indukcijom po dužini nižeg centralnog niza, tj. po klasi nilpotentnosti grupe. Slučaj: $\mathbf{G}$ je Abelova grupa je već poznat – 32.8. Pretpostavimo da je tvrđenje tačno za sve nilpotentne grupe klase nilpotentnosti najviše $n$ $(\geq 1)$ i neka je

$$\mathbf{G} = \gamma_0\mathbf{G} > \gamma_1\mathbf{G} = \mathbf{G}' > \cdots > \gamma_n\mathbf{G} > \gamma_{n+1}\mathbf{G} = \mathbf{E}$$

niži centralni niz grupe $\mathbf{G}$ koja ispunjava uslove leme. Onda je

$$\mathbf{G}/\gamma_n\mathbf{G} > \gamma_1\mathbf{G}/\gamma_n\mathbf{G} > \cdots > \gamma_{n-1}\mathbf{G}/\gamma_n\mathbf{G} > \overline{\mathbf{E}}$$

niži centralni niz grupe $\mathbf{G}/\gamma_n\mathbf{G}$ (46.25(5)), koja takođe ispunjava uslove leme: $(\mathbf{G}/\gamma_n\mathbf{G})/\gamma_1(\mathbf{G}/\gamma_n\mathbf{G}) = (\mathbf{G}/\gamma_n\mathbf{G})/(\gamma_1\mathbf{G}/\gamma_n\mathbf{G}) \cong \mathbf{G}/\gamma_1\mathbf{G}$. Prema induktivnoj pretpostavci grupa $\mathbf{G}/\gamma_n\mathbf{G}$ ispunjava uslov maksimalnosti podgrupa, pa je sama kao i sve njene podgrupe konačno generisana. Samim tim su i svi



faktori nižeg centralnog niza grupe $\mathbf{G}$, osim eventualno poslednjeg, konačno generisani. Neka je grupa $\mathbf{G}/\gamma_n\mathbf{G}$ generisana skupom $\{a_1\gamma_nG, \ldots, a_k\gamma_nG\}$, a $\gamma_{n-1}\mathbf{G}/\gamma_n\mathbf{G}$ skupom $\{b_1\gamma_nG, \ldots, b_m\gamma_nG\}$. Prema 46.25(3) važi:

$$\gamma_n\mathbf{G} = [\gamma_{n-1}\mathbf{G}, \mathbf{G}] = [\gamma_{n-1}\mathbf{G}, \zeta_{n+1}\mathbf{G}] \leq \zeta_{(n+1)-((n-1)+1)}\mathbf{G} = \zeta_1\mathbf{G} = \mathbf{Z}(\mathbf{G}).$$

Svaki element iz $\mathbf{G}$ je pak proizvod nekog elementa $a$ podgrupe $\langle a_1, \ldots, a_k\rangle$ i nekog elementa $c$ iz $\gamma_nG$ (dakle, i iz centra grupe). Analogno, svaki element iz $\gamma_{n-1}\mathbf{G}$ je proizvod nekog elementa $b$ podgrupe $\langle b_1, \ldots, b_m\rangle$ i jednog elementa $d$ iz $\gamma_nG$. Jasno, $[ac, bd] = [a, b]$, no, $[a, b] \in \langle\{[a_i, b_j] \mid 1 \leq i \leq k, 1 \leq j \leq m\}\rangle$ – imamo u vidu tačke $(d)$ i $(e)$ leme 6.2 i, ponavljamo, činjenicu da je $\gamma_n\mathbf{G} \leq \mathbf{Z}(\mathbf{G})$. Kako je niži centralni niz ujedno i rešiv, prema tački $(b)$ prethodne leme $\mathbf{G}$ ispunjava uslov maksimalnosti podgrupa.□

O rešivim grupama koje ispunjavaju uslov maksimalnosti podgrupa videti i 51.4. Dokaz prethodne leme iskoristićemo u narednoj.

**Lema 49.24** *Neka je $\{a_1, \ldots, a_m\}$ generatorni skup nilpotentne grupe $\mathbf{G}$ i neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$ takva da je za svako $i = 1, \ldots, m$, $a_i^{m_i} \in H$ za neki pozitivan prirodan broj $m_i$. Tada je podgrupa $\mathbf{H}$ konačnog indeksa.*

**Dokaz**. Indukcijom po klasi nilpotentnosti $(k)$ grupe $\mathbf{G}$. Ako je $k = 1$, tj. ako je $\mathbf{G}$ Abelova grupa, slučaj je trivijalan; koseti podgrupe $\mathbf{H}$ su oblika $a_1^{r_1} \cdot \ldots \cdot a_m^{r_m}H$, gde je, za svako $i$, $0 \leq r_i < m_i$, i stoga ih je samo konačno mnogo. Pretpostavimo da je tvrđenje tačno za sve konačno generisane nilpotentne grupe klase nilpotentnosti najviše $k$ i neka je

$$\mathbf{G} = \gamma_0\mathbf{G} > \gamma_1\mathbf{G} > \cdots > \gamma_k\mathbf{G} > \gamma_{k+1}\mathbf{G} = \mathbf{E}$$

niži centralni niz grupe $\mathbf{G}$. Prema 48.22, svaka od podgrupa $\gamma_i\mathbf{G}$ je konačno generisana. Grupa $\mathbf{G}/\gamma_k\mathbf{G}$ je nilpotentna grupa klase nilpotentnosti najviše $k$, te je prema induktivnoj hipotezi, s obzirom da su ispunjeni uslovi leme za podgrupu $(\mathbf{H}\,\gamma_k\mathbf{G})/\gamma_k\mathbf{G}$, podgrupa $(\mathbf{H}\,\gamma_k\mathbf{G})/\gamma_k\mathbf{G}$ konačnog indeksa, a onda je i $[\mathbf{G} : \mathbf{H}\gamma_k\mathbf{G}] < \infty$. Grupa $\gamma_{k-1}\mathbf{G}/\gamma_k\mathbf{G}$ je pak generisana konačnim skupom elemenata $\{b_1\gamma_kG, \ldots, b_n\gamma_kG\}$, čiji (neki) pozitivni stepeni su u $(H\,\gamma_kG)/\gamma_kG$. Neka je $(b_j\gamma_kG)^{n_j} = b_j^{n_j}\gamma_kG \in (H\,\gamma_kG)/\gamma_kG$. Odatle je, za neko $h_j \in H$ i neko $c_j \in \gamma_kG \subseteq \zeta_1G = Z(\mathbf{G})$, $b_j^{n_j} = h_jc_j$. Prema prethodnoj lemi, skup $\{[a_i, b_j] \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ generiše Abelovu grupu $\gamma_k\mathbf{G}$. S druge strane, prema 6.2(d),(h) je $[a_i, b_j]^{m_i \cdot n_j} = [a_i^{m_i}, b_j^{n_j}] = [a_i^{m_i}, h_j^{n_j}c_j^{n_j}] = [a_i^{m_i}, h_j^{n_j}] \in H \cap \gamma_kG$. Proizilazi da je $\mathbf{H} \cap \gamma_k\mathbf{G}$ podgrupa konačnog indeksa grupe $\gamma_k\mathbf{G}$, a onda je prema drugoj teoremi o izomorfizmu $((\mathbf{H}\,\gamma_k\mathbf{G})/\mathbf{H} \cong \gamma_k\mathbf{G}/(\mathbf{H} \cap \gamma_k\mathbf{G}))$ i $\mathbf{H}$ podgrupa konačnog indeksa grupe $\mathbf{H}\gamma_k\mathbf{G}$ ($\mathbf{H}$ je normalna podgrupa grupe $\mathbf{H}\gamma_k\mathbf{G}$ jer je $\gamma_k\mathbf{G} \leq \mathbf{Z}(\mathbf{G})$). Sledi konačno:

$$[\mathbf{G} : \mathbf{H}] = [\mathbf{G} : \mathbf{H}\gamma_k\mathbf{G}] \cdot [\mathbf{H}\gamma_k\mathbf{G} : \mathbf{H}] < \infty.\square$$

Jedan od kriterijuma za rešivost konačnih grupa oslanja se na svojstvo skoro normalnosti.

**Definicija 49.25** *Podgrupa* $\mathbf{H}$ *grupe* $\mathbf{G}$ *je skoro normalna akko postoje normalne podgrupe* $\mathbf{N}$ *i* $\mathbf{N}_1$ *grupe* $\mathbf{G}$ *takve da je* $\mathbf{N}\cdot\mathbf{H}=\mathbf{G}$ *i* $\mathbf{N}\cap\mathbf{H}=\mathbf{N}_1$.

Svaka normalna podgrupa $\mathbf{H}$ grupe $\mathbf{G}$ je i skoro normalna; uzeti jednostavno: $\mathbf{N}=\mathbf{G}$ i $\mathbf{N}_1=\mathbf{H}$. Obrat, međutim, ne mora da važi. Na primer, u grupi $\mathbf{D}_n$ (videti 3.4($e$)), podgrupa $\langle\sigma\ (=\sigma_y)\rangle$ je skoro normalna ($\mathbf{N}=\langle\rho\ (=\rho_{\frac{2\pi}{n}})\rangle$, $\mathbf{N}_1=\mathbf{E}$). Slično, u grupi $\mathbf{S}_n$ je podgrupa $\langle(0\ 1)\rangle$ skoro normalna ($\mathbf{N}=\mathbf{A}_n$, $\mathbf{N}_1=\mathbf{E}$). Uopšte, u svakom poludirektnom proizvodu $\mathbf{G}=\mathbf{A}\rtimes\mathbf{B}$ je $\mathbf{B}$ skoro normalna ali ne i normalna podgrupa, ukoliko se baš ne radi o direktnom proizvodu.

**Teorema 49.26** *Konačna grupa* $\mathbf{G}$ *je rešiva akko ispunjava uslov, u* [92] *označen sa* $\mathcal{D}$*: ako su* $\mathbf{A}$ *i* $\mathbf{B}$ *podgrupe grupe* $\mathbf{G}$ *i ako je* $\mathbf{A}$ *maksimalna podgrupa grupe* $\mathbf{B}$*, tada je* $\mathbf{A}$ *skoro normalna u* $\mathbf{B}$.

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{G}$ rešiva grupa, $\mathbf{A}$ i $\mathbf{B}$ neke njene podgrupe i neka je $\mathbf{A}$ maksimalna (stoga i prava) podgrupa grupe $\mathbf{B}$. Neka je, dalje, $\mathbf{N}_1$ maksimalna normalna podgrupa grupe $\mathbf{B}$ sadržana u $\mathbf{A}$ (u pitanju je, recimo uzgred, jednoznačno određena grupa). Kako je $\mathbf{B}$ rešiva grupa, to je i $\mathbf{B}/\mathbf{N}_1$ rešiva grupa, pa prema 49.19 sadrži nejediničnu Abelovu normalnu podgrupu $\mathbf{N}/\mathbf{N}_1$. S obzirom na maksimalnost podgrupe $\mathbf{A}$ (i činjenicu da je $\mathbf{N}_1$ prava podgrupa grupe $\mathbf{N}$), važi: $\mathbf{B}=\mathbf{N}\cdot\mathbf{A}$. S druge strane, $\mathbf{N}_1\leq\mathbf{N}\cap\mathbf{A}\lhd\mathbf{A}$ i $(\mathbf{N}\cap\mathbf{A})/\mathbf{N}_1\lhd\mathbf{N}/\mathbf{N}_1$, te je $\mathbf{N}\cap\mathbf{A}$ normalna podgrupa i grupe $\mathbf{N}$, a onda i grupe $\mathbf{B}$ ($=\mathbf{N}\cdot\mathbf{A}$). Sledi: $\mathbf{N}\cap\mathbf{A}=\mathbf{N}_1$, znači, $\mathbf{A}$ je skoro normalna podgrupa grupe $\mathbf{B}$.

($\Longleftarrow$) Neka je $\mathbf{G}$ konačna grupa sa svojstvom $\mathcal{D}$. Očigledno i svaka podgrupa grupe $\mathbf{G}$ ima to svojstvo. No i faktor grupe grupe $\mathbf{G}$ imaju svojstvo $\mathcal{D}$. Jer, neka su $\mathbf{A}/\mathbf{N}$ i $\mathbf{B}/\mathbf{N}$ podgrupe grupe $\mathbf{G}/\mathbf{N}$ i neka je $\mathbf{A}/\mathbf{N}$ maksimalna podgrupa grupe $\mathbf{B}/\mathbf{N}$. Tada je $\mathbf{A}$ maksimalna podgrupa grupe $\mathbf{B}$ (8.7) i stoga je, za neke normalne podgrupe $\mathbf{N}_1$ i $\mathbf{N}_2$ grupe $\mathbf{B}$, $\mathbf{N}_1\cdot\mathbf{A}=\mathbf{B}$, $\mathbf{N}_1\cap\mathbf{A}=\mathbf{N}_2$. Ali tada je, za normalne podgrupe $(\mathbf{N}_2\cdot\mathbf{N})/\mathbf{N}$, $(\mathbf{N}_1\cdot\mathbf{N})/\mathbf{N}$: $(\mathbf{N}_1\cdot\mathbf{N})/\mathbf{N}\cdot\mathbf{A}/\mathbf{N}=\mathbf{B}/\mathbf{N}$ i $(\mathbf{N}_1\cdot\mathbf{N})/\mathbf{N}\cap\mathbf{A}/\mathbf{N}=(\mathbf{N}_2\cdot\mathbf{N})/\mathbf{N}$ (recimo, ako je $n_1N=aN\in(N_1\cdot N)/N\cap A/N$, onda je, za neko $n\in N$, $n_1=an\in N_1\cap A=N_2$ i $n_1N\in(N_2\cdot N)/N$). Neka je $\mathbf{G}=\mathbf{G}_0>\mathbf{G}_1>\cdots>\mathbf{G}_{k-1}>\mathbf{G}_k=\mathbf{E}$ kompozicioni niz grupe $\mathbf{G}$. Svi kompozicioni faktori imaju, pokazali smo, svojstvo $\mathcal{D}$, te su ciklične grupe prostog reda (u suprotnom bismo imali pravu podgrupu, no nijedna maksimalna podgrupa proste grupe nije skoro normalna).■

**Lema 49.27** *Ako je* $\mathbf{G}$ *direktni proizvod familije svojih podgrupa* $\{\mathbf{A}_i\mid i\in I\}$ *i ako je, za svako* $i\in I$, $\mathbf{A}_i$ *ili rešiva ili konačno generisana ili je* $\mathbf{Fr}(\mathbf{A}_i)$ *konačno generisana grupa, onda je* $\mathbf{Fr}(\mathbf{G})=\prod_{i\in I}\mathbf{Fr}(\mathbf{A}_i)$.



**Dokaz.** Dovoljno je da pokažemo da je $\mathbf{Fr}(\mathbf{G})\cap\mathbf{A}_i\geq\mathbf{Fr}(\mathbf{A}_i)$ za svako $i\in I$; to nam daje željenu inkluziju $\mathbf{Fr}(\mathbf{G})\geq\prod_{i\in I}\mathbf{Fr}(\mathbf{A}_i)$ (inkluzija $\leq$ nam je uvek data – 10.18). U nastavku ćemo, da bismo pojednostavili stvar, posmatrati samo direktni proizvod $\mathbf{G}=\mathbf{A}\times\mathbf{B}$, gde je $\mathbf{A}$ ili rešiva ili konačno generisana ili je $\mathbf{Fr}(\mathbf{A})$ konačno generisana grupa, i pokazati da je $\mathbf{Fr}(\mathbf{G})\cap\mathbf{A}\geq\mathbf{Fr}(\mathbf{A})$. Pretpostavimo suprotno: $\mathbf{Fr}(\mathbf{G})\cap\mathbf{A}<\mathbf{Fr}(\mathbf{A})$. Prema 10.20 postoji normalna podgrupa $\mathbf{C}$ grupe $\mathbf{A}$ takva da je $\mathbf{A}/\mathbf{C}$ beskonačna prosta grupa bez maksimalnih podgrupa. $\mathbf{A}$, jasno, ne može biti rešiva grupa, inače bi $\mathbf{A}>\mathbf{C}>\cdots$ bio deo rešivog niza (46.4) i $\mathbf{A}/\mathbf{C}$ bi bila beskonačna Abelova grupa. $\mathbf{A}$ nije ni konačno generisana. Jer, onda bi i $\mathbf{A}/\mathbf{C}$ bila konačno generisana podgrupa, ali takve su sa maksimalnim podgrupama; npr. ako bi $\{a_1C,\ldots,a_mC\}$ bio jedan ireducibilan generatorni sistem grupe $\mathbf{A}/\mathbf{C}$, a $\mathbf{D}/\mathbf{C}$ maksimalna podgrupa grupe $\mathbf{A}/\mathbf{C}$ koja ne sadrži element $a_1C$ a sadrži elemente $a_2C,\ldots,a_mC$ (4.38), tada bi ona ujedno bila i maksimalna podgrupa. Ostaje još mogućnost da je $\mathbf{Fr}(\mathbf{A})$ konačno generisana grupa. Neka je $\mathbf{M}$ maksimalna podgrupa grupe $\mathbf{G}$ koja ne sadrži $\mathbf{Fr}(\mathbf{A})$ ($\not\leq\mathbf{Fr}(\mathbf{G})$). Onda je $\mathbf{G}=\mathbf{Fr}(\mathbf{A})\cdot\mathbf{M}$ ($\mathbf{Fr}(\mathbf{A})$ je normalna podgrupa grupe $\mathbf{G}$ – 4.34), pa je $\mathbf{A}=\mathbf{Fr}(\mathbf{A})\cdot(\mathbf{A}\cap\mathbf{M})$, tj. prema 5.10, $\mathbf{A}=\mathbf{A}\cap\mathbf{M}$, dakle, $\mathbf{Fr}(\mathbf{A})\leq\mathbf{A}\leq\mathbf{M}$, kontradikcija.□

**Primer 49.28** ($a$) *Svaka nilpotentna grupa je rešiva. Posebno, konačne p-grupe su rešive.*

**Dokaz.** Očigledno, centralni niz je i rešiv niz.

($b$) *Grupe* $\mathbf{S}_n$, $\mathbf{A}_n$ *su rešive za* $n\leq4$, *za* $n>4$ *nisu.*

**Dokaz.** $\mathbf{S}_3$ ima rešivi normalni niz $\mathbf{S}_3>\mathbf{A}_3>\mathbf{E}$, $\mathbf{S}_4$ ima rešivi normalni niz $\mathbf{S}_4>\mathbf{A}_4>\langle\{(0\ 1)(2\ 3),(0\ 2)(1\ 3),(0\ 3)(1\ 2)\},\circ\rangle>\mathbf{E}$ (videti 9.23). Ako je $n>4$, onda je $\mathbf{S}_n'=\mathbf{A}_n=\mathbf{A}_n'$ i $\mathbf{S}_n$, $\mathbf{A}_n$ nisu rešive grupe (naravno, dovoljno je bilo posmatrati samo grupe $\mathbf{A}_n$, jer je $\mathbf{S}_n$ ekstenzija grupe $\mathbf{A}_n$ rešivom grupom – $\mathbf{C}_2$).

($c$) *Za različite proste brojeve* $p,q$ *i* $r$ *grupe reda* $p^mq$ ($m\geq1$), $p^2q^2$ *i* $pqr$ *su rešive.*

**Dokaz.** Pretpostavimo da za neke različite proste brojeve $p$ i $q$ postoji grupa reda $p^nq$ koja nije rešiva i neka je među takvima grupa $\mathbf{G}$ najmanjeg reda – $p^mq$. Naravno, $m>2$; postoje samo dve grupe reda $pq$ i nijedna od njih nije prosta – 16.53($a$); grupe reda $p^2q$ takođe nisu proste (16.53($b$)) – sigurno imamo normalnu podgrupu jednog od redova $p$, $p^2$, $q$, u svakom slučaju ta je rešiva, a rešiva je i njoj odgovarajuća faktor grupa – koja je onda reda, respektivno, $pq$, $q$, $p^2$. Grupa $\mathbf{G}$ je, jasno, prosta (svaka njena netrivijalna normalna podgrupa bi bila rešiva, bilo kao $p$- bilo kao $q$-grupa, bilo kao grupa reda $p^kq$, $k<m$, a rešiva bi bila i njoj odgovarajuća faktor grupa). Prema tome, $s_p=q$ ($s_p$ je, podsećamo, broj Sylowih $p$-podgrupa grupe $\mathbf{G}$); to smo, s obzirom na tačku ($a$), svakako mogli i odmah zaključiti. Neka su $\mathbf{P}_1$ i $\mathbf{P}_2$ neke dve različite Sylowe $p$-podgrupe grupe $\mathbf{G}$ čiji je presek najvećeg reda (ne može

presek svake dve Sylowe podgrupe biti jedinična grupa, jer bi u tom slučaju broj elemenata čiji je red stepen od $p$ bio $(p^m-1)q+1 = |G|-(q-1)$, pa bi postojala samo jedna, dakle i normalna, Sylowa $q$-podgrupa). Prema 48.28 (Sylowe podgrupe su konačne nilpotentne, stoga i $N$-grupe), $\mathbf{P}_1 \cap \mathbf{P}_2$ je prava normalna podgrupa svojih normalizatora u $\mathbf{P}_1$ i $\mathbf{P}_2$, i, naravno, $\mathbf{P}_1 \cap \mathbf{P}_2$ je normalna podgrupa i (pod)grupe $\mathbf{H} = \langle N_{\mathbf{P}_1}(\mathbf{P}_1 \cap \mathbf{P}_2), N_{\mathbf{P}_2}(\mathbf{P}_1 \cap \mathbf{P}_2)\rangle$. Ako bi $\mathbf{H}$ bila $p$-grupa, bila bi sadržana u nekoj Sylowoj $p$-podgrupi $\mathbf{P}_3$ (16.23), te bismo dobili: $\mathbf{P}_3 \cap \mathbf{P}_1 \geq \mathbf{H} \cap \mathbf{P}_1 \geq \mathbf{N}_{\mathbf{P}_1}(\mathbf{P}_1 \cap \mathbf{P}_2) > \mathbf{P}_1 \cap \mathbf{P}_2$, kontradikcija. Znači, $q$ deli $|H|$. Ako je $\mathbf{Q}$ Sylowa $q$-podgrupa grupe $\mathbf{H}$, imali bismo prema 3.21 $|QP_1| = p^m q$, tj. $G = QP_1$ i odatle: svako $g \in G$ je oblika $ab$, $a \in Q$, $b \in P_1$, pa je $g^{-1}(\mathbf{P}_1 \cap \mathbf{P}_2)g = (ab)^{-1}(\mathbf{P}_1 \cap \mathbf{P}_2)(ab) = b^{-1}(a^{-1}(\mathbf{P}_1 \cap \mathbf{P}_2)a)b = b^{-1}(\mathbf{P}_1 \cap \mathbf{P}_2)b \leq \mathbf{P}_1$ (jer je, ponavljamo, $\mathbf{P}_1 \cap \mathbf{P}_2 \lhd \mathbf{H}$). Analogno, $|QP_2| = p^m q = |G|$ i $g^{-1}(\mathbf{P}_1 \cap \mathbf{P}_2)g \leq \mathbf{P}_2$ za svako $g \in G$. Zaključujemo: za svako $g \in G$ je $g^{-1}(\mathbf{P}_1 \cap \mathbf{P}_2)g \leq \mathbf{P}_1 \cap \mathbf{P}_2$, tj. $\mathbf{P}_1 \cap \mathbf{P}_2$ je normalna netrivijalna podgrupa grupe $\mathbf{G}$, kontradikcija.

Što se tiče grupa reda $p^2q^2$ videti 16.53($c$) i iskoristiti prethodna razmatranja.

Konačno, neka je $\mathbf{G}$ grupa reda $pqr$ i neka je $r < q < p$. Tada je $s_p$ ili 1 ili $qr$. U prvom slučaju jedina Sylowa $p$-podgrupa je rešiva normalna podgrupa, a i njoj odgovarajuća faktor grupa je rešiva. Ako je $s_p = qr$, onda je $(p-1)qr = |G| - qr$ elemenata reda $p$. Iz pretpostavke da je npr. $s_q = p$ i $s_r = q$, sledilo bi da je u grupi $(q-1)p = qp-p$ elemenata reda $q$ i $(r-1)q = qr-q$ elemenata reda $r$. Ali onda je $(|G|-qr)+(qp-p)+(qr-q)+1 = |G|+(p-1)(q-1) > |G|$, kontradikcija.

Jedostavniji dokaz poslednjeg tvrđenja nam daje korolar 16.51. Uostalom on direktno implicira

*Grupa reda $p_1 \cdot \ldots \cdot p_n$, $n \geq 1$, gde su $p_1, \ldots, p_n$ različiti prosti brojevi, je rešiva.*

($d$) *Sve dijedarske grupe su rešive.*

**Dokaz.** Svaka od ovih grupa sadrži normalnu Abelovu (preciznije, cikličnu) podgrupu indeksa 2 (generisanu "osnovnom" rotacijom).

($e$) *Sve Hamiltonove grupe su rešive.*

**Dokaz.** Videti 20.1

($f$) *Sve grupe reda manjeg od ili jednakog* 200 *i različitog od* 60, 168 *i* 180 *su rešive.*

**Dokaz.** Prema tačkama ($a$) i ($c$) jedino su u pitanju grupe reda $72 = 2^3 \cdot 3^2$, $84 = 2^2 \cdot 3 \cdot 7$, $90 = 2 \cdot 3^2 \cdot 5$, $126 = 2 \cdot 3^2 \cdot 7$, $132 = 2^2 \cdot 3 \cdot 11$, $140 = 2^2 \cdot 5 \cdot 7$, $144 = 2^4 \cdot 3^2$, $150 = 2 \cdot 3 \cdot 5^2$, $156 = 2^2 \cdot 3 \cdot 13$, $198 = 2 \cdot 3^2 \cdot 11$ i $200 = 2^3 \cdot 5^2$. No, grupe reda 84, 126 i 140 imaju jedinstvene Sylowe 7-podgrupe (koje su rešive kao i njima odgovarajuće faktor grupe), grupe reda 156 imaju jedinstvenu



Sylowu 13-podgrupu, grupe reda 198 jedinstvenu Sylowu 11-podgrupu, grupe reda 200 samo jednu Sylowu 5-podgrupu.

Ako je $\mathbf{G}$ grupa reda $72 = 2^3 \cdot 3^2$ i $s_3 > 1$, onda je $s_3 = 4$ i prema 16.29 grupa $\mathbf{G}$ nije prosta. Opet su svaka njena netrivijalna normalna podgrupa i njoj odgovarajuća faktor grupa rešive grupe.

Neka je $\mathbf{G}$ grupa reda 90 i neka je $s_3 = 10$. Ako je presek bilo koje dve Sylowe 3-podgrupe jedinična podgrupa, onda unija svih Sylowih 3-podgrupa ima 81 element, pa je $s_5 = 1$ (naravno, $s_5 = 6$ nije moguće jer bi to dalo 24 nova elementa). Ako je pak za Sylowe 3-podgrupe $\mathbf{H}$ i $\mathbf{K}$ $|H \cap K| = 3$, onda je $HK$ podskup normalizatora podgrupe $\mathbf{H} \cap \mathbf{K}$, pa je $|N(\mathbf{H} \cap \mathbf{K})|$ ili 45 ili 90 ($|N(\mathbf{H} \cap \mathbf{K})|$ je deljivo sa 9). U prvom slučaju je $\mathbf{N}(\mathbf{H} \cap \mathbf{K})$ normalna podgrupa, u drugom $\mathbf{H} \cap \mathbf{K}$.

Ako je $|G| = 132$ i $s_{11} = 12$ a $s_3 = 4$ (ne može biti i $s_{11} = 12$ i $s_4 = 22$), onda je $s_2 = 1$.

Neka je sada $\mathbf{G}$ grupa reda $144 = 2^4 \cdot 3^2$. Ako je $s_3 = 4$, prema 16.29 $\mathbf{G}$ nije prosta grupa i ponovo su svaka netrivijalna normalna podgrupa i njoj odgovarajuća faktor grupa rešive grupe. Ako je $s_3 = 16$, onda prema 16.35 (pošto nije $16 \equiv 1 \pmod{3^2}$), postoje Sylowe 3-podgrupe $\mathbf{P}$ i $\mathbf{Q}$, gde je $|P \cap Q| = 3$ i prema istoj lemi (ili 16.16) je $\mathbf{P} \cap \mathbf{Q} \lhd \mathbf{P}$ i $\mathbf{P} \cap \mathbf{Q} \lhd \mathbf{Q}$. Prema tome, $PQ \subseteq N_{\mathbf{G}}(\mathbf{P} \cap \mathbf{Q})$, pa je $|N_{\mathbf{G}}(\mathbf{P} \cap \mathbf{Q})| \geq 27$. Ako je $\mathbf{P} \cap \mathbf{Q}$ baš normalna podgrupa, njena faktor grupa (reda $2^4 \cdot 3$) je rešiva. Ako je $|N_{\mathbf{G}}(\mathbf{P} \cap \mathbf{Q})|$ 36 ili 72, prema 9.36 grupa $\mathbf{G}$ ne može biti prosta i ponovo su svaka netrivijalna normalna podgrupa i njoj odgovarajuća faktor grupa rešive.

Kod grupa reda 150 je $s_5$ ili 1 ili 6, u svakom slučaju to nisu proste grupe i opet su netrivijalne normalne podgrupe i njima odgovarajuće faktor grupe rešive.

Ranije smo videli da je $\mathbf{A}_5$ (jedinstvena) neabelova prosta grupa reda 60 (9.23, 16.53($f$)) i kao takva nije rešiva. Naravno, onda ni grupe $\mathbf{A}_5 \times \mathbf{C}_2$ i $\mathbf{A}_5 \times \mathbf{C}_3$ redova, respektivno, 120 i 180 nisu rešive. Primer grupe reda 168 koja nije rešiva je $\mathbf{PSL}_2(7)$ – videti 19.45 (druga jedna prezentacija ove grupe je data u [70], str. 112, zadaci 15 – 20). Važi, recimo i to, da su primeri grupa reda 168 i 180 jedinstvene nerešive grupe datih redova, dok nerešivih grupa reda 120 ima tri – videti [113], paragraf 74.

Naravno, neko će uočiti i da su, redom, sve grupe reda 201, 202, 203, ... (do nekog broja $200 + k$ –ostavljamo čitaocu da odredi $k$) rešive.

($g$) *Konačna grupa $\mathbf{G}$ je rešiva akko je $\mathbf{G}/\mathbf{Fr}(\mathbf{G})$ rešiva grupa.*

**Dokaz.** Pravac ($\Longleftarrow$) je direktna posledica korolara 48.30 i leme 49.6.□

**Napomena.** Primer grupe $\mathbf{A}_5$ nam kazuje da uslov da su sve prave podgrupe date grupe rešive nije dovoljan da bi i sama grupa bila rešiva.

**Lema 49.29** *Neka je $\mathbf{G}$ konačna grupa čija je svaka maksimalna podgrupa nilpotentna dok ona sama nije nilpotentna. Tada važi:*

(1) **G** *je rešiva grupa;*

(2) **G** *je reda* $p^\alpha q^\beta$, $\alpha, \beta \geq 1$, *gde su* $p$ *i* $q$ *različiti prosti brojevi;*

(3) **G** *je proizvod dveju Sylowih podgrupa (za raličite proste brojeve), od kojih je jedna normalna a druga ciklična.*

**Dokaz.** (1) Pretpostavimo da tvrđenje nije tačno i neka je **G** grupa najmanjeg reda ($n$) za koju ono nije tačno. **G** je onda prosta grupa (složenog reda). Ako bi **N** bila netrivijalna normalna podgrupa, po učinjenoj pretpostavci bi i **N** i **G**/**N** bile rešive grupe, pa bi i grupa **G** bila rešiva; primetimo da su sve prave podgrupe grupe **G** nilpotentne (svaka je sadržana u nekoj maksimalnoj), a ako bi **K**/**N** bila maksimalna podgrupa grupe **G**/**N**, tada bi **K** bila maksimalna podgrupa grupe **G**, dakle nilpotentna, te bi i **K**/**N** bila nilpotentna grupa. U nastavku dokazujemo da postoje maksimalne podgrupe čiji je presek nejedinična grupa. Jer, pođimo od suprotne hipoteze i neka je **M** jedna maksimalna podgrupa grupe **G** reda $m$ ($\geq 2$). Prema pokazanom je $\mathbf{M} = \mathbf{N_G(M)}$, stoga postoji $\frac{n}{m}$ konjugata podgrupe **M**, koje zajedno sadrže $\frac{n}{m} \cdot (m-1) = n - \frac{n}{m}$ nejediničnih elemenata. Očigledno važi $\frac{n-1}{2} < \frac{n}{2} \leq n - \frac{n}{m} < n-2 < n-1$ i kako svaki nejedinični element pripada tačno jednoj maksimalnoj podgrupi, to je $n-1$ suma celih brojeva koji pokazuju koliko konjugati pojedinih maksimalnih podgrupa sadrže nejediničnih elemenata i koji su strogo veći od $\frac{n-1}{2}$ i strogo manji od $n-1$, što nije moguće. Neka su, dalje, **M** i **N** maksimalne podgrupe sa nejediničnim presekom **K** najvećeg reda. **K** je prema 48.28 prava podgrupa svog normalizatora u **M** – $\mathbf{N_G(K)} \cap \mathbf{M}$. Jasno, $\mathbf{N_G(K)} \neq \mathbf{G}$ (**K** nije normalna podgrupa) i ako je **L** maksimalna podgrupa koja sadrži $\mathbf{N_G(K)}$ sledi: $\mathbf{K} < \mathbf{N_G(K)} \cap \mathbf{M} \leq \mathbf{L} \cap \mathbf{M}$, znači $|K| < |L \cap M|$, kontradiktorno pretpostavci o redu podgrupe **K**. Iz svega navedenog proizilazi da nemamo kontraprimer za (1).

(2) Neka je $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, gde su $p_1, \dots, p_k$ različiti prosti brojevi, a $\alpha_1, \dots, \alpha_k$ pozitivni prirodni brojevi. Naravno, $k \geq 2$ jer **G** nije nilpotentna grupa (48.9($a$)). Pretpostavimo da je $k \geq 3$. Ako je **M** maksimalna normalna podgrupa grupe **G**, faktor grupa **G**/**M** je prema 49.16 ciklična grupa prostog reda, recimo $|G/M| = p_1$. Ako je $\mathbf{P}_i$ Sylowa $p_i$-podgrupa grupe **G**, onda je, za $i > 1$, $\mathbf{P}_i$ karakteristična podgrupa grupe **M** (48.28, (1) $\Longleftrightarrow$ (6) – **M** je nilpotentna grupa), dakle i normalna podgrupa grupe **G**. Naravno, $\mathbf{P_1 P}_i$ je prava podgrupa grupe **G** ($|P_1 P_i| = p_1^{\alpha_1} p_i^{\alpha_i}|$), prema tome i nilpotentna, što će reći: $\mathbf{P_1 P}_i = \mathbf{P}_1 \times \mathbf{P}_i$. Stoga je i $\mathbf{P}_1$ normalna podgrupa grupe **G**; $\mathbf{P}_1 \cap \mathbf{M}$ je Sylowa $p_1$-podgrupa grupe **M** (16.11, 16.23) i $\mathbf{M} = (\mathbf{P}_1 \cap \mathbf{M}) \times \mathbf{P}_2 \times \cdots \times \mathbf{P}_k$. Pozivajući se opet na 48.28, zaključujemo da je **G** nilpotentna grupa, suprotno uslovu leme. Znači, $k = 2$.

(3) Neka je $|G| = p^\alpha q^\beta$ i neka **G** ima maksimalnu normalnu podgrupu **M** indeksa $q$. Već smo konstatovali da je Sylowa $p$-podgrupa **P** grupe **M**, dakle i grupe **G**, normalna i da je $\mathbf{G} = \mathbf{PQ}$, gde je **Q** (neka) Sylowa $q$-podgrupa



(grupe **G**). Pretpostavimo da **Q** nije ciklična grupa i neka $e \neq a \in Q$. Tada je $\langle a, P\rangle \neq \mathbf{G}$; u suprotnom bismo imali: $\langle a, P\rangle/\mathbf{P} = \mathbf{G}/\mathbf{P} \cong \langle a\rangle/(\langle a\rangle \cap \mathbf{P}) \cong \langle a\rangle$ i $|\langle a\rangle| = |Q|$. Po uslovu leme je $\langle a, P\rangle$ nilpotentna grupa, te je $\langle a, P\rangle = \langle a\rangle \times \mathbf{P}$. Proizilazi da su elementi podgrupa **P** i **Q** uzajamno permutabilni, odnosno $\mathbf{G} = \mathbf{P} \times \mathbf{Q}$, i grupa **G** je nilpotentna, kontradikcija.□

**Korolar 49.30** *Konačna grupa čija je svaka podgrupa ili dostižna ili nilpotentna je rešiva.*

**Dokaz.** Indukcijom po redu grupa sa datim svojstvom. Pretpostavimo da je tvrđenje tačno za sve takve grupe reda manjeg od $n$ ($> 1$) i neka je **G** grupa s tim svojstvom reda $n$. Možemo odmah uzeti da je $n$ složen broj. Ako su sve maksimalne podgrupe grupe **G** nilpotentne, grupa **G** je prema prethodnoj lemi rešiva; primetimo da uslov leme da **G** nije nilpotentna grupa koristimo isključivo u dokazu njene druge i treće tačke, konkretno važi stav (koji se izvodi analogno, indukcijom po redu grupa):

*ako su sve maksimalne podgrupe konačne grupe nilpotentne, grupa je rešiva.*

Ako maksimalna podgrupa **H** grupe **G** nije nilpotentna, onda je **H**, prema uslovu korolara, normalna podgrupa, **G**/**H** je ciklična grupa prostog reda a sama grupa **H** takođe ispunjava uslove korolara; ukoliko neka njena podgrupa nije nilpotentna, budući da je dostižna u **G**, dostižna je i u **H**. Prema induktivnoj hipotezi **H** je rešiva grupa, a tada je i grupa **G** rešiva.□

Iskoristićemo prethodnu lemu i za naredni rezultat. No prvo

**Definicija 49.31** *Prirodan broj* $n$ *je cikličan (Abelov, nilpotentan) akko je svaka grupa reda* $n$ *ciklična (Abelova, nilpotentna).*

**Korolar 49.32** *Neka je* $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, *gde su, jasno,* $p_i$, $i = 1, \dots, k$, *različiti prosti brojevi i* $\alpha_i \geq 1$. *Tada važi:*

($a$) $n$ *je nilpotentan broj akko za svaka dva različita indeksa* $i, j$ ($1 \leq i, j \leq k$) *i svako* $\beta = 1, \dots, \alpha_i$ *važi* $p_i^\beta \not\equiv 1 \pmod{p_j}$;

($b$) $n$ *je Abelov (cikličan) broj akko je nilpotentan i za svako* $i = 1, \dots, k$ *važi* $\alpha_i \leq 2$ ($\alpha_i = 1$).

**Dokaz.** Ovde nudimo rešenje R. Bakića ([10]). Više o ovome (i drugome) videti u [131].

($a$) ($\Longleftarrow$) Indukcijom po $n$. Pretpostavimo da su sve grupe reda $m$ ($< n$), gde $m$ ispunjava postavljene uslove, nilpotentne i neka je **G** grupa reda $n$, gde $n$ takođe ispunjava zadate uslove. Pretpostavimo da **G** nije nilpotentna. Evidentno, po induktivnoj pretpostavci su sve njene maksimalne podgrupe nilpotentne, pa je prema poslednjoj lemi ona rešiva grupa reda $p^\alpha q^\beta$, gde su $p$ i $q$ različiti prosti brojevi i $\alpha, \beta \geq 1$. No, s obzirom na uslove, proizilazi $s_p =$

$s_q = 1$, dakle, $\mathbf{G}$ je direktan proizvod (normalnih) Sylowih $p$- i $q$-podgrupa koje su nilpotentne, pa je i $\mathbf{G}$ nilpotentna, kontradikcija.

($\Longrightarrow$) Pretpostavimo da $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ ne ispunjava uslove korolara. Recimo da je za neko $m$, $1 \leq m \leq \alpha_i$, $p_i^m \equiv 1 \ (mod\ p_j)$. Prema 10.46 je $|Aut(\underbrace{\mathbf{Z}_{p_i} \times \cdots \times \mathbf{Z}_{p_i}}_{m-puta})| = \prod_{r=0}^{m-1}(p_i^m - p_i^r)$. Prema tome, (ciklična) grupa $\mathbf{Z}_{p_j}$ se može utopiti u grupu $\mathbf{Aut}(\underbrace{\mathbf{Z}_{p_i} \times \cdots \times \mathbf{Z}_{p_i}}_{m-puta})$. Neka je $\theta$ jedno takvo utapanje. Prema 13.9 imamo poludirektni proizvod $\mathbf{G} = (\underbrace{\mathbf{Z}_{p_i} \times \cdots \times \mathbf{Z}_{p_i}}_{m-puta}) \times_\theta \mathbf{Z}_{p_j}$. Neka je $b$ nejedinični element grupe $\mathbf{Z}_{p_j}$. Tada $\varphi_b = (b)\theta$ nije identični automorfizam grupe $\underbrace{\mathbf{Z}_{p_i} \times \cdots \times \mathbf{Z}_{p_i}}_{m-puta}$ jer je $\theta$ utapanje (držimo se notacije iz 13.9), pa je, za neki element $\overline{a} = (a_1, \ldots, a_m)$, $\overline{a} \neq (\overline{a})\varphi_b$. Sa $\overline{0}$ ćemo obeležiti neutralni element grupe $\underbrace{\mathbf{Z}_{p_i} \times \cdots \times \mathbf{Z}_{p_i}}_{m-puta}$. Elementi $(0, \overline{a})$ i $(b, \overline{0})$ su uzajamno prostih redova ($p_i$ i $p_j$) i nisu komutativni – $(0,\overline{a}) * (b,\overline{0}) = (0 +_{p_j} b, (\overline{a})\varphi_b +_{p_i} \overline{0}) = (b, (\overline{a})\varphi_b) \neq (b, \overline{a}) = (b,\overline{0}) * (0,\overline{a})$. Prema 48.28, grupa $\mathbf{G}$ reda $p_i^m \cdot p_j$ nije nilpotentna, a onda ni grupa $\mathbf{G} \times \mathbf{Z}_{\frac{n}{p_i^m p_j}}$ reda $n$.□

**Lema 49.33** *Ako je indeks svake maksimalne podgrupe konačne grupe prost broj ili kvadrat prostog broja, ta grupa je rešiva.*

**Dokaz.** Indukcijom po redu grupa sa datim svojstvom. Neka je tvrđenje tačno za sve takve grupe reda manjeg od $n$ ($> 1$) i neka je $\mathbf{G}$ grupa sa tim svojstvom reda $n$. Neka je, dalje, $\mathbf{H}$ minimalna normalna podgrupa grupe $\mathbf{G}$ (podsećamo, moguće je da je $\mathbf{H} = \mathbf{G}$) i neka je $p$ najveći prost faktor reda podgrupe $\mathbf{H}$, a $\mathbf{P}$ Sylowa $p$-podgrupa grupe $\mathbf{H}$. Ako je $\mathbf{P}$ normalna podgrupa grupe $\mathbf{G}$, onda je $\mathbf{P} = \mathbf{H}$ i po induktivnoj pretpostavci, ukoliko već nije i $\mathbf{P} = \mathbf{G}$, što je trivijalni slučaj, $\mathbf{G/P}$ je rešiva grupa (indeksi maksimalnih normalnih podgrupa faktor grupe $\mathbf{G/P}$ su takođe prosti brojevi ili kvadrati prostih brojeva – 8.7), dok je $\mathbf{P}$ kao nilpotentna grupa i rešiva. Pretpostavimo sada da je $\mathbf{N_G(P)}$ ($= \mathbf{N(P)}$) prava podgrupa grupe $\mathbf{G}$ i neka je $\mathbf{M}$ maksimalna podgrupa grupe $\mathbf{G}$ koja sadrži $\mathbf{N(P)}$. Prema 16.30 (argument Frattinija), $\mathbf{G} = \mathbf{H} \cdot \mathbf{N(P)} = \mathbf{H} \cdot \mathbf{M}$, pa ako je $[\mathbf{G} : \mathbf{M}] = q$ ili $[\mathbf{G} : \mathbf{M}] = q^2$ za neki prost broj $q$, sledi da $q$ deli red podgrupe $\mathbf{H}$, dakle, $q \leq p$; iz $|G| = |HM| = \frac{|H| \cdot |M|}{|H \cap M|}$ (3.21) izvodimo: $[\mathbf{G} : \mathbf{M}] = [\mathbf{H} : \mathbf{H} \cap \mathbf{M}]$. Svi konjugati grupe $\mathbf{P}$ su u $\mathbf{H}$ i takvih je $[\mathbf{G} : \mathbf{N(P)}]$, i to su ujedno sve Sylowe $p$-podgrupe grupe $\mathbf{H}$; stoga je $[\mathbf{G} : \mathbf{N(P)}] \equiv 1 \ (mod\ p)$ (16.24). Slično, $\{a^{-1}\mathbf{P}a \mid a \in M\}$ je familija svih Sylowih $p$-podgrupa grupe $\mathbf{H} \cap \mathbf{M}$, kardinalnost te familije je $[\mathbf{M} : \mathbf{N_M(P)}] = [\mathbf{M} : \mathbf{N(P)}]$, te je i $[\mathbf{M} : \mathbf{N(P)}] \equiv 1 \ (mod\ p)$. Proizilazi da je i $[\mathbf{G} : \mathbf{M}] = \frac{[\mathbf{G}:\mathbf{N(P)}]}{[\mathbf{M}:\mathbf{N(P)}]}$ ($= [\mathbf{H} : \mathbf{H} \cap \mathbf{M}]$) kongruentno sa 1 po modulu $p$. Ne može,



znači, biti $[\mathbf{G} : \mathbf{M}] = q$ (jer je $q \leq p$). Preostaje $[\mathbf{G} : \mathbf{M}] = q^2 \equiv 1 \ (mod\ p)$, tj. $p$ deli $(q-1) \cdot (q+1)$. Ovo je moguće samo ako je $p = 3$ i $q = 2$. Prema 9.34, grupa $\mathbf{H/Core(H \cap M)}$ je izomorfna nejediničnoj podgrupi grupe $\mathbf{S_4}$, a svaka takva se razlikuje od svoje izvodne podgrupe (podgrupe i sa parnim i sa neparnim premutacijama imaju podgrupu indeksa 2, izvodna podgrupa grupe $\mathbf{A_4}$ je Kleinova grupa, prave podgrupe grupe $\mathbf{A_4}$ su Abelove – 9.21). Odatle je $\mathbf{H} \neq \mathbf{H'}$ ($\lhd \mathbf{G}$) (6.22), odnosno, s obzirom na izbor podgrupe $\mathbf{H}$, $\mathbf{H'} = \mathbf{E}$; drugim rečima, $\mathbf{H}$ je Abelova grupa. Pošto je prema induktivnoj hipotezi i $\mathbf{G/H}$ rešiva, to je i $\mathbf{G}$ rešiva grupa.□

**Lema 49.34** *Sledeći uslovi su ekvivalentni:*

(1) *Svaka grupa neparnog reda je rešiva;*

(2) *Svaka konačna neabelova prosta grupa je parnog reda.*

**Dokaz.** (1) $\Longrightarrow$ (2) Pretpostavimo da važi (1) i neka je $\mathbf{G}$ konačna neabelova prosta grupa. Ako bi grupa $\mathbf{G}$ bila neparnog reda, znači i rešiva, imala bi rešivi kompozicioni niz $\mathbf{G} = \mathbf{G_0} > \mathbf{G_1} > \cdots > \mathbf{G_k} = \mathbf{E}$ čiji su faktori ciklične grupe prostog reda. No, kako je $\mathbf{G}$ prosta grupa, moralo bi biti $k = 1$, pa bi $\mathbf{G} \cong \mathbf{G/E}$ bila ciklična grupa, kontradikcija.

(2) $\Longrightarrow$ (1) Neka važi (2). Indukcijom po redu grupa ($n$) neparnog reda pokazujemo da su sve grupe neparnog reda rešive. Ako je $n = 1$, trivijalno je jedinična grupa rešiva. Pretpostavimo da je tvrđenje tačno za sve grupe neparnog reda manjeg od ili jednakog $2k-1$ i neka je $|G| = 2k+1$. Ako je $\mathbf{G}$ Abelova grupa, onda je i rešiva. Ako nije Abelova, prema (2) ne može biti prosta, pa sadrži netrivijalnu normalnu podgrupu – neka je to $\mathbf{N}$. Po induktivnoj hipotezi su i $\mathbf{N}$ i $\mathbf{G/N}$ rešive, kao grupe neparnog reda manjeg od $2k+1$, te je i $\mathbf{G}$ rešiva grupa.□

**Napomena.** U svom čuvenom (i dugačkom) radu: "Solvability of groups of odd order" ([46]), W. Feit i J. G. Thompson su dokazali da, zapravo, ekvivalentni uslovi prethodne leme važe. Prema tome, izneti primeri rešivih grupa neparnog reda samo su posebni slučajevi opšteg stava:

**Teorema 49.35** *(Teorema Feit-Thompsona). Grupe neparnog reda su rešive.*

**Korolar 49.36** *Grupe reda $4n+2$ su rešive.*

**Dokaz.** Prema dokazu korolara 9.32 grupa reda $4n+2$ ima (normalnu) podgrupu indeksa 2, takva podgrupa je, dakle, neparnog reda, stoga i rešiva, pa je rešiva i sama grupa.□

Naredni rezultati se odnose na Sylowe $\Pi$-podgrupe, odnosno, kao što ćemo videti, na Hallove $\Pi$-podgrupe konačnih rešivih grupa. Hallova $\Pi$-podgrupa je, podsećamo, $\Pi$-podgrupa čiji su red i indeks uzajamno prosti brojevi.

**Definicija 49.37** *Neka je* $\Pi$ *neprazan podskup skupa prostih brojeva. Konačna grupa je* $\Pi$*-separabilna akko ima normalni niz takav da je red svakog njegovog faktora deljiv sa najviše jednim od prostih faktora iz* $\Pi$.

Prema 49.16, svaka konačna rešiva grupa je $\Pi$-separabilna za svaki neprazan skup prostih brojeva. Opet, ako $\Pi$ sadrži sve proste činioce reda grupe $\mathbf{G}$ i ako je $\mathbf{G}$ $\Pi$-separabilna, onda je i rešiva. Jer, neka je $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{k-1} > \mathbf{G}_k = \mathbf{E}$ njen normalni niz takav da je, za svako $i = 1, \ldots, k$, $|G_{i-1}/G_i|$ deljivo sa najviše jednim prostim brojem iz $\Pi$. No, $|G_{i-1}/G_i| = \frac{|G_{i-1}|}{|G_i|}$ je i delilac reda grupe, stoga su faktori $\mathbf{G}_{i-1}/\mathbf{G}_i$ $p$-grupe (za eventualno različite proste brojeve), pa je $\mathbf{G}$ rešiva grupa: $\mathbf{G}_{k-1}$ je rešiva grupa, $\mathbf{G}_{k-2}$ je rešiva grupa kao ekstenzija rešive grupe $\mathbf{G}_{k-1}$ rešivom grupom $\mathbf{G}_{k-2}/\mathbf{G}_{k-1}$ itd. Konačno, ako je $\Pi$ jednoelementni skup, svaka konačna grupa je, očigledno, $\Pi$-separabilna.

**Lema 49.38** *Podgrupa* $\Pi$*-separabilne grupe je* $\Pi$*-separabilna grupa.*

**Dokaz.** Direktno preme 46.11.□

**Definicija 49.39** *Neka je* $\mathbf{G}$ *konačna nejedinična grupa i neka je* $\Pi$ *neprazan podskup skupa svih prostih faktora reda grupe* $\mathbf{G}$. *Sylowa* $\Pi$*-baza grupe* $\mathbf{G}$ $(\mathcal{B})$ *je familija uzajamno permutabilnih Sylowih p-podgrupa grupe* $\mathbf{G}$, *po jedne za svaki prost broj iz* $\Pi$: $\mathcal{B} = \{\mathbf{P}_p \mid p \in \Pi,\ \mathbf{P}_p$ *je Sylowa p-podgrupa grupe* $\mathbf{G}$, *za svako* $p, q \in \Pi$ *je* $P_p \cdot P_q = P_q \cdot P_p\}$. *Ako je* $\Pi$ *baš skup svih prostih činilaca reda grupe* $\mathbf{G}$, *onda je* $\mathcal{B}$ *kompletna Sylowa baza grupe* $\mathbf{G}$.

*Dve Sylowe* $\Pi$*-baze grupe* $\mathbf{G}$, $\mathcal{B}_1$ *i* $\mathcal{B}_2$, *konjugovane su akko za neki element* $g$ $(\in G)$ *unutrašnji automorfizam* $u_g$ *preslikava Sylowe podgrupe baze* $\mathcal{B}_1$ *na (odgovarajuće) Sylowe podgrupe baze* $\mathcal{B}_2$; *prema tome, ako je* $\mathcal{B}_1 = \{\mathbf{P}_{p_1}, \ldots, \mathbf{P}_{p_k}\}$ *i* $\mathcal{B}_2 = \{\mathbf{S}_{p_1}, \ldots, \mathbf{S}_{p_k}\}$, *onda je za svako* $i = 1, \ldots, k$:

$$g^{-1}\mathbf{P}_{p_i}g = \mathbf{S}_{p_i}.$$

**Lema 49.40** *Skup* $\mathcal{B} = \{\mathbf{P}_i \mid p_i \in \Pi\}$ *Sylowih podgrupa konačne grupe* $\mathbf{G}$ *je Sylowa* $\Pi$*-baza akko za svaki podskup* $\mathcal{B}_1 = \{\mathbf{P}_{i_1}, \ldots, \mathbf{P}_{i_r}\} \subseteq \mathcal{B}$ *važi: red bilo kog elementa grupe* $\langle P_{i_1} \cup \ldots \cup P_{i_r}\rangle$ *je proizvod stepena prostih brojeva* $p_{i_1}, \cdots, p_{i_r}$.

**Dokaz.** Pravac $(\Longrightarrow)$ je jasan. Recimo, ako imamo samo dve uzajamno permutabilne Sylowe podgrupe – $\mathbf{P}_{i_1}$ i $\mathbf{P}_{i_2}$, onda je $\langle P_{i_1} \cup P_{i_2}\rangle$ grupa sa domenom $P_{i_1} \cdot P_{i_2}$, dakle reda $|P_{i_1}| \cdot |P_{i_2}|$ (3.21). Indukcija rešava opšti slučaj.

$(\Longleftarrow)$ Neka su $\mathbf{P} = \mathbf{P}_{i_m}$ i $\mathbf{Q} = \mathbf{P}_{i_n}$ iz $\mathcal{B}$. Onda $|P \cdot Q| = |P| \cdot |Q|$ deli red grupe $\langle P \cup Q\rangle$. S druge strane je baš $|\langle P \cup Q\rangle| = |P| \cdot |Q|$, jer je red svakog elementa iz $\langle P \cup Q\rangle$ proizvod stepena prostih brojeva $p_{i_m}$ i $p_{i_n}$ (prema tome,



red grupe $\langle P \cup Q\rangle$ je prema prvoj teoremi Sylowa proizvod stepena brojeva $p_{i_m}$ i $p_{i_n}$, a $|\langle P \cup Q\rangle|$ deli $|G|$; znači, $\langle P \cup Q\rangle = PQ = QP$).□

**Napomena.** Dogovorno ćemo, za datu grupu $\mathbf{G}$ reda $n$ $(> 1)$ i proizvoljan neprazan skup prostih brojeva $\Pi$, pod Sylowom $\Pi$-bazom grupe $\mathbf{G}$ podrazumevati Sylowu $\Pi_0$-bazu grupe $\mathbf{G}$, gde je $\Pi_0 = \{p \in \Pi \mid p$ deli $n\}$.

**Teorema 49.41** *(Gol'berg). Neka je* $\mathbf{G}$ *konačna* $\Pi$*-separabilna grupa i neka je* $\Pi_1 \subseteq \Pi$. *Tada* $\mathbf{G}$ *ima Sylowu* $\Pi_1$*-bazu i sve Sylowe* $\Pi_1$*-baze su (uzajamno) konjugovane.*

**Dokaz.** Pretpostavićemo odmah, što naravno ne utiče na opštost razmatranja (a isključuje trivijalan slučaj), da svi prosti brojevi iz $\Pi$ dele red grupe $\mathbf{G}$. Ukoliko polazni skup ne bi ispunjavao taj uslov, tj. ukoliko bismo imali prostih brojeva koji se ne javljaju kao delioci nijednog faktora datog normalnog niza, jednostavno bismo te brojeve eliminisali. Jasno, nije interesantno ni da nam tada ostane prazan skup. Stoga je, u daljem razmatranju, $\emptyset \neq \Pi_1 \subseteq \Pi$ i $p \mid |G|$ za svaki prost broj $p \in \Pi$. Neka je $\Pi_1 = \{p_1, \ldots, p_k\}$ ($p_i$ ovde ne znači da se radi baš o $i$-tom po redu prostom broju). Dokaz je indukcijom po redu grupe $\mathbf{G}$ $(|G| \geq 2)$. Slučaj $|G| = 2$ je trivijalan. Generalno, ako je $k = 1$, u pitanju je druga teorema Sylowa. Zato neka je $k > 1$ i $|G| > 2$. Zbog $k \geq 2$ grupa $\mathbf{G}$ ima normalnu podgrupu $\mathbf{H}$ takvu da je njen indeks $[\mathbf{G} : \mathbf{H}]$ deljiv sa najviše jednim prostim brojem iz $\Pi_1$. Ako nijedan prost broj iz $\Pi_1$ ne deli indeks grupe $\mathbf{H}$, onda je Sylowa $\Pi_1$-baza grupe $\mathbf{H}$, koja postoji po induktivnoj pretpostavci, ujedno Sylowa $\Pi_1$-baza i grupe $\mathbf{G}$. Takođe je svaka Sylowa $\Pi_1$-baza grupe $\mathbf{G}$ Sylowa $\Pi_1$-baza i podgrupe $\mathbf{H}$ (ako je $(p, [\mathbf{G} : \mathbf{H}]) = 1$, podgrupa $\mathbf{H}$ sadrži sve Sylowe $p$-podgrupe grupe $\mathbf{G}$, jer su sve one konjugovane i $\mathbf{H}$ je normalna podgrupa), pa su po induktivnoj hipotezi sve Sylowe $\Pi_1$-baze konjugovane u $\mathbf{H}$. Pretpostavimo u nastavku da neki prost broj $p_1$ iz $\Pi_1$ deli $[\mathbf{G} : \mathbf{H}]$. Neka su $p_1^{\alpha}$ i $p_1^{\alpha_1}$ najveći stepeni broja $p_1$ koji dele redove, respektivno, grupa $\mathbf{G}$ i $\mathbf{H}$ $(\alpha > \alpha_1 \geq 0)$. Prema induktivnoj hipotezi $\mathbf{H}$ ima Sylowu $\Pi_1$-bazu $\{\mathbf{P}_1', \mathbf{P}_2, \ldots, \mathbf{P}_k\}$ i sve njene Sylowe $\Pi_1$-baze su konjugovane. Za $i = 2, \ldots, k$ Sylowa $p_i$-podgrupa $\mathbf{P}_i$ je ujedno i Sylowa $p_i$-podgrupa grupe $\mathbf{G}$, dok je $|P_1'| = p_1^{\alpha_1}$. Neka je $P = P_1' \cup P_2 \cup \ldots \cup P_k$. Onda je, zbog normalnosti podgrupe $\mathbf{H}$ i konjugovanosti svih Sylowih $\Pi_1$-baza grupe $\mathbf{H}$, $[\mathbf{G} : \mathbf{N}_{\mathbf{G}}(P)] = [\mathbf{H} : \mathbf{N}_{\mathbf{H}}(P)]$. Podrobnije, neka je, recimo, $[\mathbf{G} : \mathbf{N}_{\mathbf{G}}(P)] = m$ i neka su $N_{\mathbf{G}}(P) = N_{\mathbf{G}}(P)g_0$, $N_{\mathbf{G}}(P)g_1$, ..., $N_{\mathbf{G}}(P)g_{m-1}$ svi desni koseti podgrupe $\mathbf{N}_{\mathbf{G}}(P)$. Tada su $g_i^{-1}Pg_i = g_i^{-1}P_1'g_i \cup g_i^{-1}P_2g_i \cup \ldots \cup g_i^{-1}P_kg_i$, $i = 0, 1, \ldots, m-1$, svi konjugati podskupa $P$, koji su zbog normalnosti podgrupe $\mathbf{H}$ sadržani u $H$, a zbog konjugovanosti svih Sylowih $\Pi_1$-baza u $\mathbf{H}$ imamo za svako $i = 0, 1, \ldots, m-1$ element $h_i$ u $H$ takav da je $g_i^{-1}Pg_i = h_i^{-1}Ph_i$ (jasno, $\{g_i^{-1}P_1'g_i, g_i^{-1}P_2g_i, \ldots, g_i^{-1}P_kg_i\}$ je Sylowa $\Pi_1$-baza grupe $\mathbf{H}$ – permutabilnost podgrupa je očigledno sačuvana). Neka je $p_1^{\beta}$ $(\beta \geq 0)$ najveći stepen (prostog) broja $p_1$ koji deli $m$ $(= [\mathbf{G} : \mathbf{N}_{\mathbf{G}}(P)] = [\mathbf{H} : \mathbf{N}_{\mathbf{H}}(P)])$. Presek $\mathbf{P}_1' \cap \mathbf{N}_{\mathbf{H}}(P)$ je

Sylowa $p_1$-podgrupa grupe $\mathbf{N_H}(P)$ reda $p_1^{\alpha_1-\beta}$ (svaka podgrupa grupe $\mathbf{N_H}(P)$ je permutabilna sa $\mathbf{P}_1'$, pa bi iz pretpostavke da $\mathbf{N_H}(P)$ sadrži Sylowu $p_1$-podgrupu, koja opet strogo sadrži podgrupu $\mathbf{P}_1' \cap \mathbf{N_H}(P)$, neka to bude $\mathbf{S}$, sledilo da $p_1$-podgrupa $\mathbf{P}_1' \cdot \mathbf{S}$ grupe $\mathbf{H}$ strogo sadrži njenu Sylowu $p_1$-podgrupu $\mathbf{P}_1'$). Kao $p_1$-podgrupa grupe $\mathbf{N_G}(P)$ ($N_{\mathbf{H}}(P) \subseteq N_{\mathbf{G}}(P)$), $\mathbf{P}_1' \cap \mathbf{N_H}(P)$ je podgrupa neke Sylowe $p_1$-podgrupe grupe $\mathbf{N_G}(P)$, neka je to $\mathbf{P}_1''$. Jasno, $|P_1''| = p_1^{\alpha-\beta}$. Kao i maločas, $P_1' \cdot P_1'' = P_1'' \cdot P_1'$, pa je $\mathbf{P}_1 = \mathbf{P}_1' \cdot \mathbf{P}_1''$ $p_1$-podgrupa grupe $\mathbf{G}$ reda $\frac{p_1^{\alpha_1} \cdot p_1^{\alpha-\beta}}{p_1^{\alpha_1-\beta}} = p_1^{\alpha}$ (naravno, $P_1' \cap N_{\mathbf{H}}(P) = P_1' \cap N_{\mathbf{G}}(P)$), dakle Sylowa $p_1$-podgrupa grupe $\mathbf{G}$. Očigledno, za svako $j = 2, \ldots, k$ važi $P_1 \cdot P_j = (P_1' \cdot P_1'') \cdot P_j = P_1' \cdot (P_1'' \cdot P_j) = P_1' \cdot (P_j \cdot P_1'')$ (jer je $P_1'' \subseteq N_{\mathbf{G}}(P)$ – konjugovanost očuvava red elementa) $= (P_1' \cdot P_j) \cdot P_1'' = P_j \cdot (P_1' \cdot P_1'') = P_j \cdot P_1$, te je $\{\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_k\}$ Sylowa $\Pi_1$-baza grupe $\mathbf{G}$.

Sada kada smo dokazali egzistenciju bar jedne Sylowe $\Pi_1$-baze, preostaje nam da dokažemo i da su bilo koje dve Sylowe $\Pi_1$-baze konjugovane. Posmatrajmo, uz već datu $\{\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_k\}$, i neku drugu (Sylowu $\Pi_1$-bazu) – $\{\mathbf{Q}_1, \mathbf{Q}_2, \ldots, \mathbf{Q}_k\}$. Prema 16.11 (i drugoj teoremi Sylowa) grupe $\mathbf{H} \cap \mathbf{P}_1$ i $\mathbf{H} \cap \mathbf{Q}_1$ su Sylowe $p_1$-podgrupe grupe $\mathbf{H}$, stoga su $\{\mathbf{P}_1 \cap \mathbf{H}, \mathbf{P}_2, \ldots, \mathbf{P}_k\}$ i $\{\mathbf{Q}_1 \cap \mathbf{H}, \mathbf{Q}_2, \ldots, \mathbf{Q}_k\}$ Sylowe $\Pi_1$-baze grupe $\mathbf{H}$ (podgrupa $\mathbf{H}$ je, ne zaboravimo, normalna). Neka je, za $h \in H$, $h^{-1}(\mathbf{Q}_1 \cap \mathbf{H})h = \mathbf{P}_1 \cap \mathbf{H}$, $h^{-1}\mathbf{Q}_1 h = \mathbf{R}_1$ (dakle, $\mathbf{R}_1 \cap \mathbf{H} = \mathbf{P}_1 \cap \mathbf{H}$) i $h^{-1}\mathbf{Q}_i h = \mathbf{P}_i$, $i = 2, \ldots, k$. Skup $\{\mathbf{R}_1, \mathbf{P}_2, \ldots, \mathbf{P}_k\}$ je Sylowa $\Pi_1$-baza grupe $\mathbf{G}$ (konjugovana sa bazom $\{\mathbf{Q}_1, \mathbf{Q}_2, \ldots, \mathbf{Q}_k\}$), pa nam je zbog tranzitivnosti relacije konjugovanosti baza dovoljno da dokažemo da su konjugovane baze $\{\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_k\}$ i $\{\mathbf{R}_1, \mathbf{P}_2, \ldots, \mathbf{P}_k\}$. Neka je $\mathbf{A} = \langle P_1, P_2, \ldots, P_k\rangle = \mathbf{P}_1 \cdot \mathbf{P}_2 \cdot \ldots \cdot \mathbf{P}_k$ i $\mathbf{B} = \langle R_1, P_2, \ldots, P_k\rangle = \mathbf{R}_1 \cdot \mathbf{P}_2 \cdot \ldots \cdot \mathbf{P}_k$ (videti 3.21($b$)). Pošto je $\mathbf{P}_i \leq \mathbf{H}$ za $i = 2, \ldots, k$ i $\mathbf{P}_1 \cap \mathbf{H} = \mathbf{R}_1 \cap \mathbf{H}$, to je $\mathbf{A} \cap \mathbf{H} = \mathbf{P}_1 \cdot (\mathbf{P}_2 \cdot \ldots \cdot \mathbf{P}_k) \cap \mathbf{H} = (\mathbf{P}_1 \cap \mathbf{H}) \cdot (\mathbf{P}_2 \cdot \ldots \mathbf{P}_k) = (\mathbf{R}_1 \cap \mathbf{H}) \cdot (\mathbf{P}_2 \cdot \ldots \cdot \mathbf{P}_k) = \mathbf{R}_1 \cdot (\mathbf{P}_2 \cdot \ldots \cdot \mathbf{P}_k) \cap \mathbf{H} = \mathbf{B} \cap \mathbf{H}$ (npr. ako je $a_1 b_1 \in H$, gde je $a_1 \in P_1$, $b_1 \in P_2 \cdot \ldots \cdot P_k \subseteq H$, onda je $a_1 \in P_1 \cap H = R_1 \cap H$ i $a_1 b_1 \in R_1 \cdot (P_2 \cdot \ldots \cdot P_k) \cap H$). Neka je $\mathbf{H}_1 = \mathbf{A} \cap \mathbf{H} = \mathbf{B} \cap \mathbf{H}$; $\mathbf{H}_1$ je normalna podgrupa grupa $\mathbf{A}$ i $\mathbf{B}$, stoga i grupe $\langle A, B\rangle$. Podgrupe $\mathbf{P}_1$ i $\mathbf{R}_1$ su kao Sylowe $p_1$-podgrupe (grupe $\langle A, B\rangle$) konjugovane u $\langle A, B\rangle$; odatle su i grupe $\mathbf{A} = \mathbf{H}_1 \cdot \mathbf{P}_1$ i $\mathbf{B} = \mathbf{H}_1 \cdot \mathbf{R}_1$ konjugovane (ako je, za $g \in \langle A, B\rangle$, $g^{-1}R_1 g = P_1$, onda je $g^{-1}Bg = g^{-1}(H_1 \cdot R_1)g = (g^{-1}H_1 g) \cdot (g^{-1}R_1 g) = H_1 \cdot P_1 = A$). Prema tome, (unutrašnji) automorfizam $u_g$ preslikava bazu $\{\mathbf{R}_1, \mathbf{P}_2, \ldots, \mathbf{P}_k\}$ grupe $\mathbf{B}$ u bazu $\{g^{-1}\mathbf{R}_1 g = \mathbf{P}_1, g^{-1}\mathbf{P}_2 g, \ldots, g^{-1}\mathbf{P}_k g\}$ grupe $\mathbf{A}$ i ukoliko je $\mathbf{A}$ prava podgrupa ta je, po induktivnoj pretpostavci, konjugovana sa polaznom bazom $\{\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_k\}$. Razmotrimo na kraju slučaj: $\mathbf{A} = \mathbf{G} = \mathbf{B}$; naravno, to je moguće ako i samo ako je $\Pi_1 = \Pi$ i $\Pi$ je skup svih prostih činilaca reda grupe $\mathbf{G}$. Neka je, za $i = 2, \ldots, k$, $\mathbf{A}_i = \langle P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_k\rangle = \mathbf{P}_1 \cdot (\mathbf{P}_2 \cdot \ldots \cdot \mathbf{P}_{i-1} \cdot \mathbf{P}_{i+1} \cdot \ldots \cdot \mathbf{P}_k)$ i $\mathbf{B}_i = \langle R_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_k\rangle = \mathbf{R}_1 \cdot (\mathbf{P}_2 \cdot \ldots \cdot \mathbf{P}_{i-1} \cdot \mathbf{P}_{i+1} \cdot \ldots \cdot \mathbf{P}_k)$. Prema navedenom, grupe $\mathbf{A}_i$ i $\mathbf{B}_i$ su konjugovane. Analogno se izvodi, da ne ponavljamo: grupa $\mathbf{H}_i = \mathbf{A}_i \cap \mathbf{H} = \mathbf{B}_i \cap \mathbf{H}$



je normalna podgrupa grupe $\langle A_i, B_i\rangle$, $\mathbf{P}_1$ i $\mathbf{R}_1$ su konjugovane Sylowe $p$-podgrupe grupe $\langle A_i, B_i\rangle$ i ako je $g_1^{-1}\mathbf{R}_1 g_1 = \mathbf{P}_1$ za $g_1 \in \langle A_i, B_i\rangle$, onda je $g_1^{-1}\mathbf{B}_i g_1 = g_1^{-1}(\mathbf{H}_i \cdot \mathbf{R}_1)g_1 = g_1^{-1}\mathbf{H}_i g_1 \cdot g_1^{-1}\mathbf{R}_1 g_1 = \mathbf{H}_i \cdot \mathbf{P}_1 = \mathbf{A}_i$. Pošto je $\mathbf{G} = \mathbf{B} = \mathbf{B}_i \cdot \mathbf{P}_i$, to je $x_i^{-1}\mathbf{B}_i x_i = \mathbf{A}_i$ za neki element $x_i \in P_i$. Fiksirajmo za svako $i = 2, \ldots, k$ jedan takav element. Važi, takođe, za svako $j \geq 2$, $j \neq i$, $x_i^{-1}\mathbf{P}_j x_i = \mathbf{P}_j$; jer, $x_i^{-1}\mathbf{P}_j x_i \leq \langle P_i, P_j\rangle \cap x_i^{-1}\mathbf{B}_i x_i = \mathbf{P}_i \cdot \mathbf{P}_j \cap \mathbf{A}_i = \mathbf{P}_j$. Dokazujemo, konačno, da unutrašnji automorfizam $u_{x_2 \ldots x_k}$ "prevodi" bazu $\{\mathbf{R}_1, \mathbf{P}_2, \ldots, \mathbf{P}_k\}$ u bazu $\{\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_k\}$. Za $j = 2, \ldots, k$, već smo pokazali: $(x_2 \cdot \ldots \cdot x_k)^{-1}\mathbf{P}_j(x_2 \cdot \ldots \cdot x_k) = \mathbf{P}_j$, a za svako $i = 2, \ldots, k$ imamo:

$$(x_2 x_3 \ldots x_k)^{-1} R_1 (x_2 x_3 \ldots x_k) =$$

$$\langle (x_2 \ldots x_{i-1}) x_i (x_{i+1} \ldots x_k)\rangle^{-1} R_1 (x_2 \ldots x_{i-1}) x_i (x_{i+1} \ldots x_k) =$$

$$(x_{i+1} \ldots x_k)^{-1} x_i^{-1} (x_2 \ldots x_{i-1})^{-1} R_1 (x_2 \ldots x_{i-1}) x_i (x_{i+1} \ldots x_k) \subset$$

$$(x_{i+1} \ldots x_k)^{-1} x_i^{-1} B_i x_i (x_{i+1} \ldots x_k) = (x_{i+1} \ldots x_k)^{-1} A_i (x_{i+1} \ldots x_k) = A_i.$$

Znači, $(x_2 \ldots x_k)^{-1}\mathbf{R}_1(x_2 \ldots x_k) \leq \mathbf{A}_2 \cap \ldots \cap \mathbf{A}_k = \mathbf{P}_1$, zapravo važi baš jednakost.■

**Korolar 49.42** *(Teorema Čunihina). Ako je* $\mathbf{G}$ *$\Pi$-separabilna grupa reda $n = kl$, gde je $(k, l) = 1$, i ako se svi prosti činioci broja $k$ nalaze u $\Pi$, onda* $\mathbf{G}$ *ima podgrupu reda $k$ i sve takve podgrupe su konjugovane.*

**Dokaz**. Neka su ispunjeni uslovi korolara i neka je $k, l > 1$ i $\Pi_1 = \{p \in \Pi \mid p \text{ deli } k\} = \{p_1, \ldots, p_r\}$. Prema prethodnoj teoremi $\mathbf{G}$ ima Sylowu $\Pi_1$-bazu, recimo $\mathcal{B} = \{\mathbf{P}_i \mid i = 1, \ldots, r\}$, gde je $\mathbf{P}_i$ Sylowa $p_i$-podgrupa reda $p_i^{\alpha_i}$ i $P_i \cdot P_j = P_j \cdot P_i$. No, onda je podgrupa $\langle P_1, \ldots, P_r\rangle = \mathbf{P}_1 \cdot \mathbf{P}_2 \cdot \ldots \cdot \mathbf{P}_r$ reda $p_1^{\alpha_1} \ldots p_r^{\alpha_r} = k$ ($k$ i $l$ su uzajamno prosti brojevi, pa iz činjenica da, za $i = 1, \ldots, k$, $p_i$ deli $k$ i $p_i^{\alpha_i}$ deli $n$ sledi: $p_i^{\alpha_i}$ deli $k$). Podgrupe pak $\mathbf{A}$ i $\mathbf{B}$ reda $k$ su $\Pi_1$ separabilne (46.11), pa imaju kompletne Sylowe baze koje su, kao Sylowe $\Pi_1$-baze grupe $\mathbf{G}$, konjugovane. Ali tada su i grupe $\mathbf{A}$ i $\mathbf{B}$, generisane podgrupama tih baza, konjugovane.■

**Korolar 49.43** *(Prva teorema Halla). Konačna rešiva grupa reda $n = kl$, gde je $(k, l) = 1$, ima podgrupu reda $k$, sve takve podgrupe su konjugovane i svaka podgrupa grupe* $\mathbf{G}$ *čiji red deli $k$ sadržana je u nekoj podgrupi reda $k$.*

**Dokaz**. Samo je poslednji deo korolara u pitanju (već smo rekli: konačna rešiva grupa je $\Pi$-separabilna za svaki skup prostih brojeva $\Pi$). Dokaz je indukcijom po redu grupe $\mathbf{G}$. Neka je, dakle, tvrđenje tačno za sve grupe reda manjeg od $n$ ($> 1$) i neka je $\mathbf{G}$ grupa reda $n = kl$, gde je $(k, l) = 1$ i $k, l > 1$ (izbegavamo trivijalne slučajeve), a $\mathbf{A}$ jedna podgrupa čiji red $k_0$ deli $k$. Pretpostavimo prvo da $\mathbf{G}$ ima netrivijalnu normalnu podgrupu $\mathbf{N}$ reda $n' = k'l'$, gde $k'$ deli $k$, $l'$ deli $l$ i $l'$ je manji od $l$. Red podgrupe

$(\mathbf{AN})/\mathbf{N}$ ($\cong \mathbf{A}/(\mathbf{A}\cap\mathbf{N})$) faktor grupe $\mathbf{G}/\mathbf{N}$ deli $\frac{k}{k'}$, te prema induktivnoj hipotezi postoji podgrupa grupe $\mathbf{G}/\mathbf{N}$ reda $\frac{k}{k'}$ koja sadrži $(\mathbf{AN})/\mathbf{N}$; neka je to $\mathbf{C}/\mathbf{N}$. Podgrupa $\mathbf{C}$ ($\geq \mathbf{AN}$) je reda $kl'$ ($< kl$) (znači, prava podgrupa grupe $\mathbf{G}$), pa opet prema induktivnoj hipotezi sadrži podgrupu $\mathbf{B}$ reda $k$ koja sadrži $\mathbf{A}$. Neka su sada, razmatramo preostalu mogućnost, redovi svih netrivijalnih normalnih podgrupa grupe $\mathbf{G}$ oblika $k'l$. Prema 49.18, minimalna normalna podgrupa grupe $\mathbf{G}$ je elementarna Abelova $q$-grupa ($q$ - prost broj). Fiksirajmo jednu, neka je to $\mathbf{H}$. Pošto $l$ ($> 1$) deli red grupe $\mathbf{H}$, sledi da je $|H| = l =$ stepen nekog prostog broja $p$. Podgrupa $\mathbf{AH}$ je reda $k_0 l$ ($|AH| = \frac{|A|\cdot|H|}{|A\cap H|} = |A|\cdot|H|$). Neka je $\mathbf{D}$ bilo koja podgrupa grupe $\mathbf{G}$ reda $k$. Kako je $\langle AH, D\rangle = \mathbf{HD} = \mathbf{G}$, imamo: $|(AH)D| = |A(HD)| = |G| = \frac{|AH|\cdot|D|}{|AH\cap D|}$ i $|AH\cap D| = k_0$. U grupi $\mathbf{AH}$ su podgrupe $\mathbf{A}$ i $\mathbf{A}_1 = \mathbf{AH}\cap\mathbf{D}$ konjugovane. Stoga je, za neko $g \in H$, $\mathbf{A} = g^{-1}\mathbf{A}_1 g \leq g^{-1}\mathbf{D}g$ i $g^{-1}\mathbf{D}g$ je podgrupa reda $k$ (grupe $\mathbf{G}$) koja sadrži $\mathbf{A}$.■

**Korolar 49.44** *(Druga teorema Halla). Svaka konačna rešiva grupa ima kompletnu Sylowu bazu i sve kompletne Sylowe baze su konjugovane.*

**Korolar 49.45** *Konačna rešiva grupa je proizvod međusobno permutabilnih nilpotentnih podgrupa.*

Na kraju dajemo i dopunu teoreme Schur-Zassenhausa (videti 16.49).

**Teorema 49.46** *(Zassenhaus). Svi komplementi normalne Hallove podgrupe su uzajamno konjugovani.*

**Dokaz.** Neka je $\mathbf{H}$ Hallova normalna podgrupa reda $m$ grupe $\mathbf{G}$ reda $n$ i neka su $\mathbf{K}$ i $\mathbf{K}^*$ dva njena komplementa.

Pretpostavimo prvo da je $\mathbf{H}$ Abelova grupa. Prema drugoj teoremi o izomorfizmu postoje kanonički izomorfizmi $\varphi$ i $\varphi^*$ grupe $\overline{\mathbf{G}} = \mathbf{G}/\mathbf{H} = (\mathbf{KH})/\mathbf{H} = (\mathbf{K}^*\mathbf{H})/\mathbf{H}$ na, redom, grupe $\mathbf{K}$ i $\mathbf{K}^*$; recimo, $(gH)\varphi = k$, gde je $g = kh$, $k \in K$, $h \in H$. Držeći se delimično notacije iz [140], elemente grupe $\overline{\mathbf{G}}$ ćemo obeležavati sa $\overline{g}$ ($= gH$), a slike elemenata $\overline{g}$ će biti: $(\overline{g})\varphi = s_{\overline{g}}$, $(\overline{g})\varphi^* = s^*_{\overline{g}}$. Jasno, $s^*_{\overline{g}} = s_{\overline{g}}\cdot h_{\overline{g}}$ za neko (jedinstveno) $h_{\overline{g}}$ podgrupe $\mathbf{H}$. Iz $s_{\overline{g_1}\cdot\overline{g_2}}\cdot h_{\overline{g_1}\cdot\overline{g_2}} = s^*_{\overline{g_1}\cdot\overline{g_2}} = s^*_{\overline{g_1}}\cdot s^*_{\overline{g_2}} = s_{\overline{g_1}}\cdot h_{\overline{g_1}}\cdot s_{\overline{g_2}}\cdot h_{\overline{g_2}} = s_{\overline{g_1}}\cdot s_{\overline{g_2}}\cdot(s^{-1}_{\overline{g_2}}\cdot h_{\overline{g_1}}\cdot s_{\overline{g_2}})\cdot h_{\overline{g_2}}$ sledi: $h_{\overline{g_1}\cdot\overline{g_2}} = (s^{-1}_{\overline{g_2}}\cdot h_{\overline{g_1}}\cdot s_{\overline{g_2}})\cdot h_{\overline{g_2}}$. Neka je $h = \prod_{\overline{g}\in\overline{G}} h_{\overline{g}}$. Tada je $h = \prod_{\overline{g_1}\in\overline{G}} h_{\overline{g_1}\cdot\overline{g_2}} = (\prod_{\overline{g_1}\in\overline{G}}(s^{-1}_{\overline{g_2}}\cdot h_{\overline{g_1}}\cdot s_{\overline{g_2}}))\cdot(h_{\overline{g_2}})^{\frac{n}{m}} = s^{-1}_{\overline{g_2}}\cdot(\prod_{\overline{g_1}\in\overline{G}} h_{\overline{g_1}})\cdot s_{\overline{g_2}}\cdot(h_{\overline{g_2}})^{\frac{n}{m}} = s^{-1}_{\overline{g_2}}\cdot h\cdot s_{\overline{g_2}}\cdot(h_{\overline{g_2}})^{\frac{n}{m}}$. Ako je, za cele brojeve $u$ i $v$, $um + v\frac{n}{m} = 1$ i $h_1 = h^v$, onda je $h = h_1^{\frac{n}{m}}$, pa je prema prethodnoj jednačini $h_1^{\frac{n}{m}} = (s^{-1}_{\overline{g_2}}\cdot h_1\cdot s_{\overline{g_2}}\cdot h_{\overline{g_2}})^{\frac{n}{m}}$, odnosno (ponovo zbog $(m, \frac{n}{m}) = 1$), $h_1 = s^{-1}_{\overline{g_2}}\cdot h_1 s_{\overline{g_2}}\cdot h_{\overline{g_2}}$, tj. $h_{\overline{g_2}} = s^{-1}_{\overline{g_2}}\cdot h_1^{-1}\cdot s_{\overline{g_2}}\cdot h_1$. Stoga je $s^*_{\overline{g_2}} = s_{\overline{g_2}}\cdot h_{\overline{g_2}} = h_1^{-1}\cdot s_{\overline{g_2}}\cdot h_1$, što će reći da je $\mathbf{K}^* = h_1^{-1}\mathbf{K}h_1$.



U opštem slučaju dokaz je indukcijom po redu grupe. Trivijalni su slučajevi ako je bilo $m = 1$ bilo $\frac{n}{m} = 1$. Pretpostavimo zato da tvrđenje važi za sve grupe (i njihove Hallove normalne podgrupe) reda manjeg od $n$ ($> 1$) i da je $1 < m < n$. Razlikovaćemo slučajeve: ($I$) $\mathbf{H}$ je rešiva grupa i ($II$) $\mathbf{G}/\mathbf{H}$ je rešiva grupa ($\mathbf{K}$ i $\mathbf{K}^*$ ostaju komplementi podgrupe $\mathbf{H}$). S obzirom da je $(m, \frac{n}{m}) = 1$, bar jedna od grupa $\mathbf{H}$, $\mathbf{G}/\mathbf{H}$ je neparnog reda, dakle, prema Feit-Thompsonovoj teoremi (49.35) i rešiva.

($I$) Neka je $\mathbf{H}$ rešiva ali ne i Abelova grupa (taj slučaj smo već razmotrili). Tada je $\mathbf{H}'$ njena prava nejedinična i potpuno invarijantna podgrupa (i kao takva ujedno i normalna podgrupa grupe $\mathbf{G}$). $\mathbf{H}/\mathbf{H}'$ je Hallova normalna podgrupa grupe $\mathbf{G}/\mathbf{H}'$, a $(\mathbf{KH}')/\mathbf{H}'$ i $(\mathbf{K}^*\mathbf{H}')/\mathbf{H}'$ su njeni komplementi. Pošto je $\mathbf{H}/\mathbf{H}'$ Abelova grupa, podgrupe $(\mathbf{KH}')/\mathbf{H}'$ i $(\mathbf{K}^*\mathbf{H}')/\mathbf{H}'$ su konjugovane u $\mathbf{G}/\mathbf{H}'$. Neka je $(\mathbf{K}^*\mathbf{H}')/\mathbf{H}' = (gH')^{-1}(\mathbf{KH}')/\mathbf{H}'gH' = ((g^{-1}\mathbf{K}g)\mathbf{H}')/\mathbf{H}'$, tj. $\mathbf{K}^*\mathbf{H}' = (g^{-1}\mathbf{K}g)\mathbf{H}'$. Dalje imamo da je $\mathbf{H}'$ Hallova normalna podgrupa grupe $\mathbf{K}^*\mathbf{H}'$ (jer red podgrupe $\mathbf{H}'$ deli $m$, a njen indeks je upravo red grupe $\mathbf{K}^*$ - $\frac{n}{m}$), a $\mathbf{K}^*$ i $g^{-1}\mathbf{K}g$ su njeni komplementi (u $\mathbf{K}^*\mathbf{H}'$). Prema induktivnoj pretpostavci ($|K^*H'| = |K^*|\cdot|H'| < |K^*|\cdot|H| = |G|$) $\mathbf{K}^*$ i $g^{-1}\mathbf{K}g$ su konjugovane podgrupe u $\mathbf{K}^*\mathbf{H}'$, znači i u grupi $\mathbf{G}$.

($II$) Neka je $\mathbf{M}/\mathbf{H}$ minimalna normalna podgrupa rešive grupe $\mathbf{G}/\mathbf{H}$. Prema 49.18 je $\mathbf{M}/\mathbf{H}$ elementarna Abelova $p$-grupa (za neki prost broj $p$). Iz $\mathbf{H} < \mathbf{M} \leq \mathbf{G} = \mathbf{HK}$ sledi prema Dedekindovom pravilu (videti kraj dokaza 11.1): $\mathbf{M} = \mathbf{M}\cap\mathbf{HK} = \mathbf{H}(\mathbf{M}\cap\mathbf{K})$. Po simetriji stvari je i $\mathbf{M} = \mathbf{H}(\mathbf{M}\cap\mathbf{K}^*)$. Naravno, $\mathbf{M}\cap\mathbf{K}$ i $\mathbf{M}\cap\mathbf{K}^*$ su Sylowe $p$-podgrupe grupe $\mathbf{M}$ ($p$ ne deli $m$ jer je prost faktor broja $\frac{n}{m}$ i ako je $|M/H| = p^k$, onda je $|M| = m\cdot p^k$ i $|M\cap K| = |M\cap K^*| = |M/H| = p^k$). Stoga je, za neko $a \in M$, $\mathbf{M}\cap\mathbf{K}^* = a^{-1}(\mathbf{M}\cap\mathbf{K})a$ i dalje, zbog $\mathbf{M}\cap\mathbf{K} \lhd \mathbf{K}$, $\mathbf{M}\cap\mathbf{K}^* = a^{-1}(\mathbf{M}\cap\mathbf{K})a \lhd \mathbf{K}^*\cap a^{-1}\mathbf{K}a$. Prema tome, ako je $\mathbf{N} = \mathbf{N}_{\mathbf{G}}(\mathbf{M}\cap\mathbf{K}^*)$, onda $a^{-1}\mathbf{K}a, \mathbf{K}^* \leq \mathbf{N}$ i $\mathbf{NH} = \mathbf{G}$. Prema drugoj teoremi o izomorfizmu je $\mathbf{G}/\mathbf{H} = (\mathbf{NH})/\mathbf{H} \cong \mathbf{N}/(\mathbf{N}\cap\mathbf{H})$, te je $\mathbf{N}/(\mathbf{N}\cap\mathbf{H})$ rešiva grupa i $\mathbf{N}\cap\mathbf{H}$ je Hallova normalna podgrupa grupe $\mathbf{N}$. Odatle sledi, s obzirom da je $(\mathbf{N}\cap\mathbf{H})\cdot(\mathbf{M}\cap\mathbf{K}^*) \lhd \mathbf{N}$, $((\mathbf{N}\cap\mathbf{H})\cdot(\mathbf{M}\cap\mathbf{K}^*))/(\mathbf{M}\cap\mathbf{K}^*) \cong (\mathbf{N}\cap\mathbf{H})/(\mathbf{N}\cap\mathbf{H}\cap\mathbf{M}\cap\mathbf{K}^*) \cong \mathbf{N}\cap\mathbf{H}$ i $(\mathbf{N}/(\mathbf{M}\cap\mathbf{K}^*))/(((\mathbf{N}\cap\mathbf{H})\cdot(\mathbf{M}\cap\mathbf{K}^*))/(\mathbf{M}\cap\mathbf{K}^*)) \cong \mathbf{N}/((\mathbf{N}\cap\mathbf{H})\cdot(\mathbf{M}\cap\mathbf{K}^*)) \cong (\mathbf{N}/(\mathbf{N}\cap\mathbf{H}))/(((\mathbf{N}\cap\mathbf{H})\cdot(\mathbf{M}\cap\mathbf{K}^*))/(\mathbf{N}\cap\mathbf{H}))$, da je $((\mathbf{N}\cap\mathbf{H})\cdot(\mathbf{M}\cap\mathbf{K}^*))/(\mathbf{M}\cap\mathbf{K}^*)$ Hallova normalna podgrupa grupe $\mathbf{N}/(\mathbf{M}\cap\mathbf{K}^*)$. Njeni komplementi su $\mathbf{K}^*/(\mathbf{M}\cap\mathbf{K}^*)$ i $a^{-1}\mathbf{K}a/(\mathbf{M}\cap\mathbf{K}^*)$; jer je npr. $|K^*/(M\cap K^*)| = \frac{|K^*|}{|M\cap K^*|} = \frac{[G:H]}{[M\cap K^*]} = \frac{[N:N\cap H]}{|M\cap K^*|} = |N/((N\cap H)\cdot(M\cap K^*))| = |(N/(M\cap K^*))/(((N\cap H)\cdot(M\cap K^*))/(M\cap K^*))|$. Kako je $\mathbf{M}\cap\mathbf{K}^*$ nejedinična podgrupa (jer je $\mathbf{H}$ prava podgrupa grupe $\mathbf{M}$), to je $|N/(M\cap K^*)| < |G|$, pa su po induktivnoj pretpostavci podgrupe $\mathbf{K}^*/(\mathbf{M}\cap\mathbf{K}^*)$ i $a^{-1}\mathbf{K}a/(\mathbf{M}\cap\mathbf{K}^*)$ konjugovane u $\mathbf{N}/(\mathbf{M}\cap\mathbf{K}^*)$, a onda su i $\mathbf{K}^*$ i $a^{-1}\mathbf{K}a$ konjugovane podgrupe u $\mathbf{N}$ (4.28($c$)), dakle i u $\mathbf{G}$.■

## 50 Superrešive grupe

Pooštrenjem uslova (2) iz 49.3 dobija se podklasa rešivih grupa koja u preseku sa klasom konačnih grupa daje klasu (konačnih) grupa čije su maksimalne podgrupe prostog indeksa.

**Definicija 50.1** *Invarijantni niz grupe je superrešiv akko su svi njegovi faktori ciklične grupe. Za superrešivi niz se koristi i (duži) termin – invarijantni ciklični niz.*

*Grupa* $\mathbf{G}$ *je superrešiva (eng. supersoluble ili supersolvable) akko ima superrešivi niz.*

*Ako su* $\mathbf{A}$ *i* $\mathbf{B}$ *normalne podgrupe grupe* $\mathbf{G}$ *i ako je* $\mathbf{A}$ *podgrupa grupe* $\mathbf{B}$, *superrešivi niz između* $\mathbf{A}$ *i* $\mathbf{B}$, *ili* $\mathbf{B}$ *i* $\mathbf{A}$ *(po želji), je niz podgrupa (oblika):*

$$\mathbf{B} = \mathbf{C}_0 > \mathbf{C}_1 > \cdots > \mathbf{C}_n = \mathbf{A},$$

*gde je, za svako* $i = 0, \ldots, n$, $\mathbf{C}_i$ *normalna podgrupa grupe* $\mathbf{G}$ *i, za* $j = 0, \ldots, n-1$, $\mathbf{C}_j/\mathbf{C}_{j+1}$ *ciklična grupa.*

Superrešive grupe dobijamo, dakle, od cikličnih grupa primenom konačno mnogo ekstenzija – prva ekstenzija je ekstenzija ciklične grupe cikličnom grupom. Stoga važi

**Korolar 50.2** *Superrešive grupe su prebrojive (konačne ili beskonačno prebrojive).*

Jasno, svaka superrešiva grupa je i rešiva. Obrat, međutim ne važi ni za prebrojive grupe. Grupa $\mathbf{A}_4$ je rešiva ali ne i superrešiva – već smo naveli njen jedini invarijantni niz (49.28($b$)) dužine 2 čiji je drugi faktor Kleinova grupa. Lako se proverava da je $\mathbf{A}_4$ i grupa najmanjeg reda među grupama koje su rešive ali ne i superrešive. Ovaj primer nam ujedno kazuje da ekstenzija superrešive grupe superrešivom grupom nije nužno superrešiva grupa.

**Lema 50.3** ($a$) *Podgrupe i homomorfne slike superrešive grupe su superrešive;*

($b$) *Direktni proizvod konačno mnogo superrešivih grupa je superrešiva grupa;*

($c$) *Grupa je superrešiva akko ima invarijantni niz čiji je svaki faktor ili ciklična grupa prostog reda ili beskonačna ciklična grupa;*

($d$) *Konačna grupa je superrešiva akko su faktori njenog glavnog niza ciklične grupe prostog reda;*

($e$) *Glavni niz konačne superrešive grupe je ujedno i kompozicioni niz.*



**Dokaz.** ($a$) Videti 46.11 (i treba li ponoviti: podgrupa ciklične grupe je ciklična).

($b$) Dovoljno je pokazati da je direktni proizvod dve superrešive grupe superrešiva grupa. Neka su, dakle, $\mathbf{G}$ i $\mathbf{H}$ superrešive grupe sa superrešivim nizovima $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{k-1} > \mathbf{G}_k = \mathbf{E}$ i $\mathbf{H} = \mathbf{H}_0 > \mathbf{H}_1 > \cdots > \mathbf{H}_{l-1} > \mathbf{H}_l = \mathbf{E}$. Onda je $\mathbf{G} \times \mathbf{H} > \mathbf{G}_1 \times \mathbf{H} > \cdots > \mathbf{G}_{k-1} \times \mathbf{H} > \mathbf{E} \times \mathbf{H} > \mathbf{E} \times \mathbf{H}_1 > \cdots > \mathbf{E} \times \mathbf{H}_{l-1} > \mathbf{E} \times \mathbf{E}$ superrešivi niz grupe $\mathbf{G} \times \mathbf{H}$ (videti 10.3($b$)).

($c$) Neka je $\mathbf{G}$ superrešiva grupa i $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{k-1} > \mathbf{G}_k = \mathbf{E}$ jedan njen superrešivi niz. Pretpostavimo da je za neko $i$, $1 \leq i \leq k$, $\mathbf{G}_{i-1}/\mathbf{G}_i$ konačna ciklična grupa složenog reda $n$, recimo $n = p_1 \ldots p_r$ (gde nisu nužno svi prosti brojevi $p_i$, $i = 1, \ldots, r$, različiti). Prema 7.2($g$), za svako $j = 1, \ldots, r-1$ ciklična grupa $\mathbf{G}_{i-1}/\mathbf{G}_i$ ima jedinstvenu, stoga i karakterističnu podgrupu (i inače znamo da su sve podgrupe ciklične grupe potpuno invarijantne – 7.2($b$)) reda $p_{j+1} \ldots p_r$ – neka je to $\mathbf{H}_j/\mathbf{G}_i$. Prema 4.34, $\mathbf{H}_j/\mathbf{G}_i$ je normalna podgrupa grupe $\mathbf{G}/\mathbf{G}_i$, pa je $\mathbf{H}_j$ normalna podgrupa grupe $\mathbf{G}$. Imamo sada proširenje polaznog niza: $\mathbf{G} = \mathbf{G}_0 > \cdots > \mathbf{G}_{i-1} > \mathbf{H}_1 > \cdots > \mathbf{H}_{r-1} > \mathbf{G}_i > \cdots > \mathbf{E}$, gde je $\mathbf{G}_{i-1}/\mathbf{H}_1$ ($\cong (\mathbf{G}_{i-1}/\mathbf{G}_i)/(\mathbf{H}_1/\mathbf{G}_i)$) ciklična grupa reda $p_1$ i uopšte, za $j = 2, \ldots, r-1$, $\mathbf{H}_{j-1}/\mathbf{H}_j$ ($\cong (\mathbf{H}_{j-1}/\mathbf{G}_i)/(\mathbf{H}_j/\mathbf{G}_i)$) ciklična grupa reda $p_j$ i, konačno, $\mathbf{H}_{r-1}/\mathbf{G}_i$ ciklična grupa reda $p_r$.

Tačke ($d$) i ($e$) su direktna posledica tačke ($c$).□

**Lema 50.4** ($a$) *Neka su* $\mathbf{A}$ *i* $\mathbf{B}$ *normalne podgrupe grupe* $\mathbf{G}$ *i neka su* $\mathbf{G}/\mathbf{A}$ *i* $\mathbf{G}/\mathbf{B}$ *superrešive grupe. Onda je i* $\mathbf{G}/(\mathbf{A} \cap \mathbf{B})$ *superrešiva grupa.*

($b$) *Neka je* $\mathbf{B} = \prod_{i \in I} \mathbf{A}_i$, $|I| < \infty$, *normalna podgrupa grupe* $\mathbf{G}$ *i neka je svaki "faktor"* $\mathbf{A}_i$ ($i \in I$) *takođe normalna podgrupa grupe* $\mathbf{G}$. *Ako je, za svako* $i \in I$, $\mathbf{B}_i \overset{\text{def}}{=} \prod_{i \neq j \in I} \mathbf{A}_j$ *i ako su sve faktor grupe* $\mathbf{G}/\mathbf{B}_i$ *superrešive, onda je i* $\mathbf{G}$ *superrešiva grupa.*

**Dokaz.** ($a$) Neka su $\mathbf{G}/\mathbf{A} = \mathbf{H}_0/\mathbf{A} > \mathbf{H}_1/\mathbf{A} > \cdots > \mathbf{H}_{m-1}/\mathbf{A} > \mathbf{H}_m/\mathbf{A} = \overline{\mathbf{E}}$ ($\mathbf{H}_m = \mathbf{A}$) i $\mathbf{G}/\mathbf{B} = \mathbf{K}_0/\mathbf{A} > \mathbf{K}_1/\mathbf{B} > \cdots > \mathbf{K}_{n-1}/\mathbf{B} > \mathbf{K}_n/\mathbf{B} = \overline{\mathbf{E}}$ ($\mathbf{K}_n = \mathbf{B}$) superrešivi nizovi grupa, respektivno, $\mathbf{G}/\mathbf{A}$ i $\mathbf{G}/\mathbf{B}$. Krenimo od segmenta budućeg superrešivog niza faktor grupe $\mathbf{G}/(\mathbf{A} \cap \mathbf{B})$: $\mathbf{G}/(\mathbf{A} \cap \mathbf{B}) > \mathbf{H}_1/(\mathbf{A} \cap \mathbf{B}) > \cdots > \mathbf{H}_{m-1}/(\mathbf{A} \cap \mathbf{B}) > \mathbf{H}_m/(\mathbf{A} \cap \mathbf{B}) = \mathbf{A}/(\mathbf{A} \cap \mathbf{B})$; svaka od podgrupa $\mathbf{H}_i$ je normalna i za $i = 0, \ldots, m-1$ je $(\mathbf{H}_i/(\mathbf{A} \cap \mathbf{B}))/(\mathbf{H}_{i+1}/(\mathbf{A} \cap \mathbf{B}))$ ($\cong \mathbf{H}_i/\mathbf{H}_{i+1} \cong (\mathbf{H}_i/\mathbf{A})/(\mathbf{H}_{i+1}/\mathbf{A})$) ciklična grupa. Prema drugoj teoremi o izomorfizmu je $\mathbf{A}/(\mathbf{A} \cap \mathbf{B}) \cong (\mathbf{AB})/\mathbf{B}$, a $(\mathbf{AB})/\mathbf{B}$ je pak kao podgrupa superrešive grupe i sama superrešiva. Prema 46.11 jedan njen superrešivi niz dobijamo uklanjanjem eventualnog "viška" iz niza: $(\mathbf{AB})/\mathbf{B} \geq (\mathbf{AB} \cap \mathbf{K}_1)/\mathbf{B} \geq \cdots \geq (\mathbf{AB} \cap \mathbf{K}_{n-1})/\mathbf{B} \geq (\mathbf{AB} \cap \mathbf{K}_n)/\mathbf{B} = \overline{\mathbf{E}}$. Preostaje da se ovaj niz iskoristi za dobijanje superrešivog niza grupe $\mathbf{A}/(\mathbf{A} \cap \mathbf{B})$. Primetimo samo: izomorfno preslikavanje $\varphi$ grupe $(\mathbf{AB})/\mathbf{B}$ na grupu $\mathbf{A}/(\mathbf{A} \cap \mathbf{B})$ dato je

sa $(aB)\varphi = a(A \cap B)$, pa je $((\mathbf{AB} \cap \mathbf{K}_1)/\mathbf{B})\varphi = \langle \{a(A \cap B) \mid a \in K_1 \cap A\}, \cdot \rangle$, što je, evidentno, zbog normalnosti podgrupe $\mathbf{K}_1$, normalna podgrupa grupe $\mathbf{G}/(\mathbf{A} \cap \mathbf{B})$.

Kraći dokaz nam daju (analogno slučaju nilpotentnih i rešivih grupa) 10.15 i tačke $(a)$ i $(b)$ prethodne leme.

$(b)$ Direktna posledica prethodne tačke. Demonstrirajmo to na slučaju $\mathbf{B} = \mathbf{A}_1 \times \mathbf{A}_2 \times \mathbf{A}_3$, gde su $\mathbf{A}_1$, $\mathbf{A}_2$ i $\mathbf{A}_3$ normalne podgrupe grupe $\mathbf{G}$. Po uslovu leme su $\mathbf{G}/(\mathbf{A}_1 \times \mathbf{A}_2)$, $\mathbf{G}/(\mathbf{A}_1 \times \mathbf{A}_3)$ i $\mathbf{G}/(\mathbf{A}_2 \times \mathbf{A}_3)$ superrešive grupe. Tada je i $\mathbf{G}/((\mathbf{A}_1 \times \mathbf{A}_2) \cap (\mathbf{A}_1 \times \mathbf{A}_3)) = \mathbf{G}/\mathbf{A}_1$ superrešiva grupa, a onda i $\mathbf{G}/(\mathbf{A}_1 \cap (\mathbf{A}_2 \times \mathbf{A}_3)) \cong \mathbf{G}$.

U opštem slučaju koristimo: $\mathbf{B}_i \cap \mathbf{B}_j = \prod_{k \in I \setminus \{i,j\}} \mathbf{A}_k$.□

**Lema 50.5** *Nilpotentna grupa je superrešiva akko ispunjava uslov maksimalnosti podgrupa.*

**Dokaz.** Svaka superrešiva grupa ispunjava uslov maksimalnosti podgrupa – 52.3.

Neka je $\mathbf{G}$ nilpotentna grupa sa višim centralnim nizom $\mathbf{E} = \zeta_0\mathbf{G} < \zeta_1\mathbf{G} < \cdots < \zeta_{n-1}\mathbf{G} < \zeta_n\mathbf{G} = \mathbf{G}$ i neka $\mathbf{G}$ ispunjava uslov maksimalnosti podgrupa. Taj uslov onda ispunjavaju i svi faktori centralnog niza (8.14), pa su to, prema 32.8, konačno generisane Abelove grupe, odnosno direktne sume (konačnog broja konačnih) nerazloživih cikličnih grupa. Prema tome, svaki faktor $\zeta_{i+1}\mathbf{G}/\zeta_i\mathbf{G}$, $0 \leq i \leq n-1$, ima invarijantni ciklični niz: $\mathbf{H}_{i0}/\zeta_i\mathbf{G}\ (= \zeta_i\mathbf{G}/\zeta_i\mathbf{G}) < \mathbf{H}_{i1}/\zeta_i\mathbf{G} < \cdots < \mathbf{H}_{im_i}/\zeta_i\mathbf{G}\ (= \zeta_{i+1}\mathbf{G}/\zeta_i\mathbf{G})$. Podgrupe $\mathbf{H}_{ij}$, $0 \leq j \leq m_i$, su normalne podgrupe grupe $\mathbf{G}$ (jer je $\mathbf{H}_{ij}/\zeta_i\mathbf{G} \leq \zeta_{i+1}\mathbf{G}/\zeta_i\mathbf{G} = \mathbf{Z}(\mathbf{G}/\zeta_i\mathbf{G})$, dakle $\mathbf{H}_{ij}/\zeta_i\mathbf{G} \lhd \mathbf{G}/\zeta_i\mathbf{G}$, dakle $\mathbf{H}_{ij} \lhd \mathbf{G}$ – 8.7). Grupa $\mathbf{G}$, znači, ima invarijantni ciklični niz, dato proširenje višeg centralnog niza, tj. superrešiva je $(\mathbf{H}_{i,k+1}/\mathbf{H}_{ik} \cong (\mathbf{H}_{i,k+1}/\zeta_i\mathbf{G})/(\mathbf{H}_{ik}/\zeta_i\mathbf{G})$ je ciklična grupa).□

**Korolar 50.6** $(a)$ *Konačno generisana nilpotentna grupa je superrešiva;*

$(b)$ *Konačna nilpotentna grupa je superrešiva.*

**Dokaz.** $(a)$ Prema prethodnoj lemi, 5.15 i 48.22.□

**Napomena.** U slučaju konačnih $p$-grupa svi kompozicioni nizovi su ujedno i glavni nizovi, dakle invarijantni ciklični nizovi čiji su faktori ciklične grupe reda $p$. Dokaz je u osnovi analogan dokazu prethodne leme; polazimo od višeg centralnog niza grupe i ma kog kompozicionog niza (čiji su faktori ciklične grupe reda $p$ – 16.16) i koristimo Schreierovu teoremu – adekvatno proširenje centralnog niza je invarijantni niz.

Već smo konstatovali da ekstenzija superrešive grupe superrešivom grupom ne mora biti superrešiva grupa. Važi međutim



**Lema 50.7** *Ako je* $\mathbf{H}$ *ciklična normalna podgrupa grupe* $\mathbf{G}$ *i ako je* $\mathbf{G}/\mathbf{H}$ *superrešiva grupa, onda je i* $\mathbf{G}$ *superrešiva grupa.*

**Dokaz.** Neka je $\varphi$ kanoničko homomorfno preslikavanje grupe $\mathbf{G}$ na faktor grupu $\overline{\mathbf{G}} = \mathbf{G}/\mathbf{H}$ i neka je

$$\overline{\mathbf{G}} = \overline{\mathbf{G}}_0 > \overline{\mathbf{G}}_1 = \mathbf{G}_1/\mathbf{H} > \cdots > \overline{\mathbf{G}}_{m-1} = \mathbf{G}_{m-1}/\mathbf{H} > \overline{\mathbf{G}}_m = \mathbf{H}/\mathbf{H}\ (= \overline{\mathbf{E}})$$

superrešivi niz grupe $\overline{\mathbf{G}}$. Tada je prema 8.7 i trećoj teoremi o izomorfizmu

$$\mathbf{G} > \mathbf{G}_1 > \cdots > \mathbf{G}_{m-1} > \mathbf{H} > \mathbf{E}$$

superrešivi niz grupe $\mathbf{G}$ (za $i = 0, \ldots, m$ je $\mathbf{G}_i = (\overline{\mathbf{G}}_i)\varphi^{-1}$ i za $1 \leq i \leq m$ je $\mathbf{G}_{i-1}/\mathbf{G}_i \cong \overline{\mathbf{G}}_{i-1}/\overline{\mathbf{G}}_i$).□

**Korolar 50.8** *Grupe reda* $2 \cdot p^n$, *gde je* $p$ *prost broj, su superrešive.*

**Dokaz.** Slučaj je trivijalan ako je $p = 2$ ili $n = 0$. Neka je stoga $p > 2$ i $n \geq 1$. Dokaz je indukcijom po $n$. Slučaj $n = 1$ je opet lak – videti 16.53$(a)$. Pretpostavimo da je tvrđenje tačno za sve grupe reda $2 \cdot p^k$, $k < n\ (> 1)$, i neka je $\mathbf{G}$ grupa reda $2 \cdot p^n$, $\mathbf{P}$ njena jedinstvena Sylowa $p$-podgrupa i $\mathbf{Q}$ (ne nužno jedinstvena) Sylowa 2-podgrupa. Neka je, dalje, $\mathbf{H}$ minimalna normalna podgrupa grupe $\mathbf{G}$. Ako je $\mathbf{H}$ prostog reda, znači reda 2 ili $p$, $\mathbf{G}$ je prema induktivnoj pretpostavci ($\mathbf{G}/\mathbf{H}$ je superrešiva grupa) i prethodnoj lemi superrešiva grupa. No, drugačije i ne može biti. Jer, kako je $\mathbf{G}$ u svakom slučaju rešiva grupa (49.28$(c)$), $\mathbf{H}$ je prema 49.18 elementarna Abelova grupa, dakle direktna suma cikličnih grupa prostog reda. Ako pretpostavimo da $\mathbf{H}$ nije reda 2 ili $p$, preostaje $|H| = p^r$, $1 < r \leq n$ (prema tome, $\mathbf{H} \leq \mathbf{P}$). Ali $\mathbf{P}$ je i nilpotentna grupa, te je prema 48.15 $\mathbf{E} \neq \mathbf{Z}(\mathbf{P}) \cap \mathbf{H}\ (\lhd \mathbf{G})$, pa je, zbog minimalnosti podgrupe $\mathbf{H}$, $\mathbf{H} \leq \mathbf{Z}(\mathbf{P})$. Ako je $\mathbf{HQ}$ prava podgrupa grupe $\mathbf{G}$, onda je prema induktivnoj hipotezi superrešiva. Jedan invarijantni niz grupe $\mathbf{HQ}$ je $\mathbf{HQ} > \mathbf{H} > \mathbf{E}$. Pošto su svi glavni nizovi grupe $\mathbf{HQ}$ izomorfni i pošto se svaki invarijantni niz može proširiti do glavnog (čiji su faktori ciklične grupe prostog reda – 50.3$(d)$), to $\mathbf{HQ}$ sadrži normalnu podgrupu $\mathbf{K}$ reda $p$, preciznije, imamo $\mathbf{K} < \mathbf{H}\ (\leq \mathbf{Z}(\mathbf{P}))$. Stoga je $\mathbf{N}(\mathbf{K}) \geq \mathbf{PQ} = \mathbf{G}$, protivno pretpostavci o minimalnosti normalne podgrupe $\mathbf{H}$. Mora, dakle, biti $\mathbf{HQ} = \mathbf{G}$ (tj. $\mathbf{H} = \mathbf{P}$, tj. $r = n$). Ali ako je $e \neq a \in P$ i $e \neq b \in Q\ (= \langle b \rangle)$ i $b^{-1}ab = bab \in \langle a \rangle$ ($b^2 = e$), tada je $\langle a \rangle \lhd \mathbf{G}$, kontradikcija ($\langle a \rangle$ je prava podgrupa grupe $\mathbf{P}$, koja nije ciklična). S druge strane, ako $b^{-1}ab \notin \langle a \rangle$ (svakako je $b^{-1}ab \in P$), onda je $b^{-1}ab \cdot a \neq e$, a $b^{-1}(b^{-1}ab \cdot a)b = abab = a \cdot b^{-1}ab = b^{-1}ab \cdot a$ i $\langle a \cdot b^{-1}ab \rangle$ je normalna podgrupa grupe $\mathbf{G}$ strogo sadržana u $\mathbf{P}$, kontradikcija opet.□

Prema korolaru 50.2 klasa Abelovih grupa nije sadržana u klasi superrešivih grupa. Nije to ni klasa prebrojivih Abelovih grupa (imati u vidu Prüferove grupe ili grupu $\mathbf{Ra}$). No, prema 32.2 klasa konačno generisanih Abelovih grupa

jeste. Grupe $S_3$ je pak "prvi" primer superrešive grupe koja nije nilpotentna (ali su joj zato sve prave podgrupe nilpotentne).

Zaključujemo: ako su $\mathcal{C}_k$, $\mathcal{A}_k$, $\mathcal{N}_k$, $\mathcal{R}_k$, $\mathcal{SR}_k$ klase konačnih, respektivno, cikličnih, Abelovih, nilpotentnih, rešivih i superrešivih grupa, onda imamo:

$$\mathcal{C}_k \subset \mathcal{A}_k \subset \mathcal{N}_k \subset \mathcal{SR}_k \subset \mathcal{R}_k.$$

**Lema 50.9** *Maksimalne podgrupe superrešive grupe su prostog indeksa.*

**Dokaz.** Neka je $\mathbf{H}$ maksimalna podgrupa superrešive grupe $\mathbf{G}$. Ako je $\mathbf{H}$ i normalna podgrupa, tvrđenje trivijalno sledi – $\mathbf{H}$ se javlja kao "drugi" član superrešivog niza (46.14), $\mathbf{G/H}$ je, dakle, ciklična grupa bez netrivijalnih podgrupa, stoga prostog reda. Ako $\mathbf{H}$ nije normalna podgrupa, onda je $\overline{\mathbf{H}} = \mathbf{H/Core(H)}$ maksimalna podgrupa superrešive (faktor) grupe $\overline{\mathbf{G}} = \mathbf{G/Core(H)}$. Prema tački $(c)$ leme 50.3 grupa $\overline{\mathbf{G}}$ ima normalnu cikličnu podgrupu $\overline{\mathbf{K}} = \mathbf{K/Core(H)}$ koja je ili beskonačna ili prostog reda (pretposlednji član invarijantnog niza čiji su faktori ili beskonačne ciklične ili ciklične grupe prostog reda). $\overline{\mathbf{H}} \cap \overline{\mathbf{K}} = \overline{\mathbf{E}}$, tj. $\mathbf{H} \cap \mathbf{K} = \mathbf{Core(H)}$, jer je svaka podgrupa grupe $\overline{\mathbf{K}}$ potpuno invarijantna (7.2$(b)$), znači i normalna podgrupa grupe $\overline{\mathbf{G}}$, pa je $\overline{\mathbf{H}} \cap \overline{\mathbf{K}}$ normalna podgrupa grupe $\overline{\mathbf{G}}$ sadržana u $\overline{\mathbf{H}}$ (no, $\mathbf{Core(H)}$ je maksimalna normalna podgrupa grupe $\mathbf{G}$ sadržana u $\mathbf{H}$ – 4.8; naravno, stalno nam je na umu i 8.7). Ako bi $\overline{\mathbf{K}}$ bila beskonačna ciklična grupa, tada bi za bilo koju njenu netrivijalnu podgrupu $\overline{\mathbf{K}}_1$ bilo: $\overline{\mathbf{H}} < \overline{\mathbf{H}} \cdot \overline{\mathbf{K}}_1 \ (= \overline{\mathbf{H}} \times \overline{\mathbf{K}}_1) < \overline{\mathbf{H}} \cdot \overline{\mathbf{K}} \ (= \overline{\mathbf{H}} \times \overline{\mathbf{K}})$, odnosno, $\mathbf{H} < \mathbf{H} \cdot \mathbf{K}_1 < \mathbf{H} \cdot \mathbf{K}$, kontradiktorno uslovu o maksimalnosti podgrupe $\mathbf{H}$. $\overline{\mathbf{K}}$ je, prema tome, ciklična grupa prostog reda, recimo $p$, i $\mathbf{H} < \mathbf{H} \cdot \mathbf{K} = \mathbf{G}$ (isto tako je $\overline{\mathbf{H}} < \overline{\mathbf{H}} \cdot \overline{\mathbf{K}} = \overline{\mathbf{G}}$), te je prema 3.17 i 8.7:

$$[\mathbf{G} : \mathbf{H}] = [\overline{\mathbf{G}} : \overline{\mathbf{H}}] = [\overline{\mathbf{H}} \cdot \overline{\mathbf{K}} : \overline{\mathbf{H}}] = [\overline{\mathbf{K}} : \overline{\mathbf{H}} \cap \overline{\mathbf{K}}] = |\overline{K}| = p.\square$$

Za konačne grupe važi i obrat prethodnog tvrđenja. Dokaz ćemo dati nešto kasnije.

**Lema 50.10** *Superrešiva grupa ima invarijantni ciklični niz čiji se beskonačni faktori, ukoliko ih ima, javljaju "na kraju".*

**Dokaz.** Neka je $\mathbf{G}$ beskonačna superrešiva grupa i neka je

$$\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_i > \mathbf{G}_{i+1} > \mathbf{G}_{i+2} > \cdots > \mathbf{G}_n = \mathbf{E}$$

jedan njen superrešivi niz. Pretpostavimo da je $\mathbf{G}_i/\mathbf{G}_{i+1}$ beskonačna ciklična, dok je $\mathbf{G}_{i+1}/\mathbf{G}_{i+2}$ konačna ciklična grupa. Polazeći od invarijantnog niza $\mathbf{G}/\mathbf{G}_{i+2} > \mathbf{G}_i/\mathbf{G}_{i+2} > \mathbf{G}_{i+1}/\mathbf{G}_{i+2} > \mathbf{G}_{i+2}/\mathbf{G}_{i+2}$ faktor grupe $\mathbf{G}/\mathbf{G}_{i+2}$, sledi prema 46.18$(a)$ egzistencija invarijantnog niza: $\mathbf{G}/\mathbf{G}_{i+2} > \mathbf{G}_i/\mathbf{G}_{i+2} > \mathbf{M}_1/\mathbf{G}_{i+2} > \mathbf{G}_{i+2}/\mathbf{G}_{i+2}$, gde je $\mathbf{M}_1/\mathbf{G}_{i+2}$ beskonačna ciklična grupa, dok je



$(\mathbf{G}_i/\mathbf{G}_{i+2})/(\mathbf{M}_1/\mathbf{G}_{i+2}) \cong \mathbf{G}_i/\mathbf{M}_1$ konačna grupa. Posmatrajmo dalje invarijantni niz grupe $\mathbf{G}$:

$$\mathbf{G} > \mathbf{G}_1 > \cdots > \mathbf{G}_{i-1} > \mathbf{G}_i > \mathbf{M}_1 > \mathbf{G}_{i+2} > \cdots > \mathbf{G}_n = \mathbf{E}.$$

Ukoliko je i $\mathbf{G}_{i-1}/\mathbf{G}_i$ beskonačna ciklična grupa, ponavljamo postupak na analogan način – sada bismo, naravno, krenuli od invarijantnog niza $\mathbf{G}/\mathbf{M}_1 > \mathbf{G}_{i-1}/\mathbf{M}_1 > \mathbf{G}_i/\mathbf{M}_1 > \mathbf{M}_1/\mathbf{M}_1$ i stigli do invarijantnog niza grupe $\mathbf{G}/\mathbf{M}_1$: $\mathbf{G}/\mathbf{M}_1 > \mathbf{G}_{i-1}/\mathbf{M}_1 > \mathbf{M}_2/\mathbf{M}_1 > \mathbf{M}_1/\mathbf{M}_1$, gde je $(\mathbf{G}_{i-1}/\mathbf{M}_1)/(\mathbf{M}_2/\mathbf{M}_1) \cong \mathbf{G}_{i-1}/\mathbf{M}_2$ konačna grupa i $\mathbf{M}_2/\mathbf{M}_1$ beskonačna ciklična grupa. Taj niz bi nam dao invarijantni niz grupe $\mathbf{G}$:

$$\mathbf{G} > \mathbf{G}_1 > \cdots > \mathbf{G}_{i-1} > \mathbf{M}_2 > \mathbf{M}_1 > \mathbf{G}_{i+2} > \cdots > \mathbf{G}_n = \mathbf{E}.$$

Očigledno, na ovaj način mogli bismo "transformisati" polazni invarijantni niz grupe $\mathbf{G}$ u invarijantni niz:

$$\mathbf{G} = \mathbf{H}_0 > \mathbf{H}_1 > \cdots > \mathbf{H}_j > \mathbf{H}_{j+1} > \cdots > \mathbf{H}_n = \mathbf{E},$$

čiji su faktori, redom, prvo konačne grupe npr. $\mathbf{G}/\mathbf{H}_1, \ldots, \mathbf{H}_{j-1}/\mathbf{H}_j$, a potom beskonačne ciklične grupe $\mathbf{H}_j/\mathbf{H}_{j+1}, \ldots, \mathbf{H}_{n-1}/\mathbf{H}_n \ (\cong \mathbf{H}_{n-1})$. $\mathbf{G}/\mathbf{H}_j$ je konačna superrešiva grupa, pa njen invarijantni niz

$$\mathbf{G}/\mathbf{H}_j > \mathbf{H}_1/\mathbf{H}_j > \cdots > \mathbf{H}_{j-1}/\mathbf{H}_j > \mathbf{H}_j/\mathbf{H}_j \ (= \overline{\mathbf{E}})$$

ima invarijantno ciklično proširenje (46.14) koje koristimo da bismo dobili invarijantno ciklično proširenje "segmenta" $\mathbf{G} > \mathbf{H}_1 > \cdots > \mathbf{H}_j$.$\square$

**Lema 50.11** *Konačna superrešiva grupa ima invarijantni ciklični niz čiji su faktori ciklične grupe prostog reda i redovi faktora čine neopadajući niz.*

**Dokaz.** Prvi deo tvrđenja nam je već poznat (50.3$(c)$). Drugi je direktna posledica leme 46.18$(b)$. Na primer, ako je

$$\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_i > \mathbf{G}_{i+1} > \mathbf{G}_{i+2} > \cdots > \mathbf{G}_n = \mathbf{E}$$

superrešivi niz čiji su faktori prostog reda i $|G_i/G_{i+1}| = p > q = |G_{i+1}/G_{i+2}|$, $p, q$ – prosti brojevi, tada niz $\mathbf{G}/\mathbf{G}_{i+2} > \mathbf{G}_i/\mathbf{G}_{i+2} > \mathbf{G}_{i+1}/\mathbf{G}_{i+2} > \mathbf{G}_{i+2}/\mathbf{G}_{i+2}$ $(= \overline{\mathbf{E}})$ ispunjava uslove tačke $(b)$ pomenute leme, pa postoji invarijantni niz $\mathbf{G}/\mathbf{G}_{i+2} > \mathbf{G}_i/\mathbf{G}_{i+2} > \mathbf{M}/\mathbf{G}_{i+2} > \overline{\mathbf{E}}$, gde je sada

$$|M/G_{i+2}| = p, \quad |(G_i/G_{i+2})/(M/G_{i+2})| = |G_i/M| = q.$$

Jasno, ovakvim postupkom možemo u datom invarijatnom nizu grupe $\mathbf{G}$ izvršiti nužne zamene pojedinih članova tako da redovi faktora novodobijenog invarijantnog niza čine neopadajući niz.$\square$

**Korolar 50.12** *Neka je* $\mathbf{G}$ *superrešiva grupa reda* $n = p_1^{k_1} \dots p_r^{k_r}$, *gde su* $p_i$, $i = 1, \dots, r$, *prosti brojevi i* $p_1 > \dots > p_r$, *i neka je, za svako* $i$, $\mathbf{P}_i$ *jedna Sylowa* $p_i$*-podgrupa grupe* $\mathbf{G}$. *Tada je* $\mathbf{P}_1 \dots \mathbf{P}_t$ *normalna podgrupa grupe* $\mathbf{G}$ *za svako* $t = 1, \dots, r$. *Posebno,* $\mathbf{P}_1$ *je jedinstvena Sylowa* $p_1$*-podgrupa.*

*Jednostavnije rečeno, konačna superrešiva grupa ima Sylow toranj* (16.45).

**Dokaz.** S obzirom na 50.9, dokaz je već dat – 16.46. Nudimo još jedan.

Prema prethodnoj lemi grupa $\mathbf{G}$ ima superrešivi niz

$$\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \dots > \mathbf{G}_i > \mathbf{G}_{i+1} > \dots > \mathbf{G}_m = \mathbf{E},$$

gde je $|G_i/G_{i+1}|$ prostog reda $q_i$ i $q_0 \leq q_1 \leq \dots \leq q_{m-1}$. Kako svako $q_j$ $(j = 0, \dots, m-1)$ deli red grupe, sledi: $m = \sum_{i=1}^{r} k_i$, $q_0 = \dots = q_{k_r-1} = p_r$, $q_{k_r} = \dots = q_{k_r+k_{r-1}-1} = p_{r-1}$, $\dots$, $q_{k_r+\dots+k_2} = \dots = q_{m-1} = p_1$. Prema tome: $|G_{m-1}| = p_1$, $|G_{m-2}| = p_1^2$, $\dots$, $|G_{m-k_1}| = p_1^{k_1}$ i $\mathbf{G}_{m-k_1}$ je normalna, stoga i jedinstvena, Sylowa $p_1$-podgrupa (dakle, $\mathbf{G}_{m-k_1} = \mathbf{P}_1$). Isto tako je $|G_{m-k_1-k_2}| = p_1^{k_1} p_2^{k_2}$, pa je $\mathbf{P}_2 \leq \mathbf{G}_{m-k_1-k_2}$ (zbog normalnosti podgrupe $\mathbf{G}_{m-k_1-k_2}$) i $\mathbf{G}_{m-k_1-k_2} = \mathbf{P}_1\mathbf{P}_2$. Generalno izvodimo (indukcijom):

$$\mathbf{G}_{m-k_1-\dots-k_t} = \mathbf{P}_1\mathbf{P}_2 \dots \mathbf{P}_t$$

(ako je $\mathbf{P}_1 \dots \mathbf{P}_{t-1}$ normalna podgrupa grupe $\mathbf{G}$, onda je $(\mathbf{P}_1 \dots \mathbf{P}_{t-1})\mathbf{P}_t$ podgrupa grupe $\mathbf{G}$, svaka podgrupa $\mathbf{P}_j$ $(j = 1, \dots, t)$ sadržana je u $\mathbf{G}_{m-k_1-\dots-k_t}$ i $|G_{m-k_1-\dots-k_t}| = |(P_1 \dots P_{t-1})P_t|$ – 3.21, 4.3).□

**Korolar 50.13** *Izvodna podgrupa superrešive grupe je nilpotentna.*

**Dokaz.** Neka je $\mathbf{G}$ superrešiva grupa sa invarijantnim cikličnim nizom $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \dots > \mathbf{G}_{i-1} > \mathbf{G}_i > \dots > \mathbf{G}_n = \mathbf{E}$ i neka je $\mathbf{G}' = \mathbf{H}_0 = \mathbf{G}' \cap \mathbf{G}_0 \geq \mathbf{H}_1 = \mathbf{G}' \cap \mathbf{G}_1 \geq \dots \geq \mathbf{H}_{i-1} = \mathbf{G}' \cap \mathbf{G}_{i-1} \geq \mathbf{H}_i = \mathbf{G}' \cap \mathbf{G}_i \geq \dots \geq \mathbf{H}_n = \mathbf{G}' \cap \mathbf{G}_n = \mathbf{E}$. Već znamo, faktori $\mathbf{H}_{j-1}/\mathbf{H}_j$, $j = 1, \dots, n$, su ciklične grupe (46.11). Pretpostavimo da je $\mathbf{H}_{i-1}/\mathbf{H}_i$ nejedinična grupa $(1 \leq i \leq n)$. Za svako $a \in G$ preslikavanje $\varphi_a : H_{i-1}/H_i \longrightarrow H_{i-1}/H_i$ dato sa (za $hH_i \in H_{i-1}/H_i$) $(hH_i)\varphi_a = (a^{-1}ha)H_i$ automorfizam je grupe $\mathbf{H}_{i-1}/\mathbf{H}_i$; dobra definisanost, injektivnost i surjektivnost su posledica normalnosti podgrupa $\mathbf{H}_{i-1}$ i $\mathbf{H}_i$, homomorfnost je očigledna. Kako važi i:

$$(hH_i)\varphi_{ab} = (ab)^{-1}h(ab)\,H_i = b^{-1}(a^{-1}ha)b\,H_i = (a^{-1}ha\,H_i)\varphi_b =$$

$$((hH_i)\varphi_a)\varphi_b = (hH_i)(\varphi_a \circ \varphi_b),$$

preslikavanje $\psi : G \longrightarrow Aut(\mathbf{H}_{i-1}/\mathbf{H}_i)$, gde je $(a)\psi = \varphi_a$, homomorfno je preslikavanje (grupe $\mathbf{G}$ u grupu $\mathbf{Aut}(\mathbf{H}_{i-1}/\mathbf{H}_i)$). Jasno, $\mathbf{Ker}(\psi) = \{a \in G \mid \forall h \in H_{i-1} \quad ah\,H_i = ha\,H_i\}$, $\mathbf{H}_i \leq \mathbf{Ker}(\psi)$ i $\mathbf{Ker}(\psi)/\mathbf{H}_i = \mathbf{C}_{\mathbf{G}/\mathbf{H}_i}(\mathbf{H}_{i-1}/\mathbf{H}_i)$. Pošto je $\mathbf{G}/\mathbf{Ker}(\psi)$ Abelova grupa (jer je $\mathbf{Aut}(\mathbf{H}_{i-1}/\mathbf{H}_i)$ Abelova grupa – 8.24, $\mathbf{Aut}(\mathbf{Z}) \cong \mathbf{Z}_2$), sledi: $\mathbf{G}' \leq \mathbf{Ker}(\psi)$, tj. $\mathbf{G}'/\mathbf{H}_i \leq \mathbf{Ker}(\psi)/\mathbf{H}_i$ $(= \mathbf{C}_{\mathbf{G}/\mathbf{H}_i}(\mathbf{H}_{i-1}/\mathbf{H}_i))$, i stoga je $\mathbf{H}_{i-1}/\mathbf{H}_i \leq \mathbf{Z}(\mathbf{G}'/\mathbf{H}_i)$. Zaključujemo: uklanjanjem eventualnog "viška" iz niza $\mathbf{G}' \geq \mathbf{H}_1 \geq \dots \geq \mathbf{H}_{i-1} \geq \mathbf{H}_i \geq \dots \geq \mathbf{E}$ ostaje nam centralni niz grupe $\mathbf{G}'$.□



**Teorema 50.14** *Konačna grupa čije su sve maksimalne podgrupe prostog indeksa je superrešiva.*

**Dokaz.** Pretpostavimo da tvrđenje ne važi i neka je konačna grupa $\mathbf{G}$ kontraprimer najmanjeg reda – $n$ $(> 1)$. Naravno, sve njene prave faktor grupe su superrešive, pa $\mathbf{G}$ ne može imati normalnu podgrupu prostog reda (50.7). Neka je $p$ najveći prost faktor broja $n$ i $\mathbf{P}$ Sylowa $p$-podgrupa grupe $\mathbf{G}$. Ako $\mathbf{P}$ ne bi bila normalna podgrupa, tj. ako bi bilo $\mathbf{N}(\mathbf{P}) \neq \mathbf{G}$, onda bismo za maksimalnu podgrupu $\mathbf{M}$ grupe $\mathbf{G}$ koja sadrži $\mathbf{N}(\mathbf{P})$ imali:

$$s_p = [\mathbf{G} : \mathbf{N}(\mathbf{P})] = [\mathbf{G} : \mathbf{M}] \cdot [\mathbf{M} : \mathbf{N}(\mathbf{P})] = [\mathbf{G} : \mathbf{M}] \cdot s_p^{\mathbf{M}},$$

gde je $s_p^{\mathbf{M}}$ broj Sylowih $p$-podgrupa grupe $\mathbf{M}$, te bi indeks podgrupe $\mathbf{M}$, koji je inače prost faktor reda grupe $\mathbf{G}$, bio kongruentan sa 1 po modulu $p$, kontradikcija. Razmotrimo prvo slučaj: $\mathbf{P}$ nije Abelova grupa. $\mathbf{Z}(\mathbf{P})$ je, znamo, nejedinična normalna podgrupa grupe $\mathbf{G}$, a $\mathbf{G}/\mathbf{Z}(\mathbf{P})$ je superrešiva grupa. Prema 50.11 ($p$ deli $|G/Z(\mathbf{P})|$) $\mathbf{G}/\mathbf{Z}(\mathbf{P})$ ima normalnu cikličnu podgrupu $\overline{\mathbf{H}} = \mathbf{H}/\mathbf{Z}(\mathbf{P})$ reda $p$. Jasno, $\overline{\mathbf{H}} \leq \mathbf{P}/\mathbf{Z}(\mathbf{P})$, jer je $\mathbf{P}/\mathbf{Z}(\mathbf{P})$ normalna Sylowa $p$-podgrupa grupe $\mathbf{G}/\mathbf{Z}(\mathbf{P})$, dakle, $\mathbf{H}$ je Abelova podgrupa grupe $\mathbf{P}$. Neka je $\mathbf{H} = \langle a, Z(\mathbf{P})\rangle$. $(\mathbf{H} \leq)$ $\mathbf{C}(\mathbf{H}) \cap \mathbf{P}$ je nejedinična normalna podgrupa grupe $\mathbf{G}$ $(4.4(g))$, naravno i prava podgrupa grupe $\mathbf{P}$ – u suprotnom bismo imali $\mathbf{P} \leq \mathbf{C}(\mathbf{H})$ i $\mathbf{H} \leq \mathbf{Z}(\mathbf{P})$. Opet, $\mathbf{G}/(\mathbf{C}(\mathbf{H}) \cap \mathbf{P})$ je superrešiva grupa, pa postoji normalna podgrupa $\mathbf{K}$ grupe $\mathbf{G}$ takva da je $\mathbf{K}/(\mathbf{C}(\mathbf{H}) \cap \mathbf{P})$ ciklična grupa reda $p$. Neka je $\mathbf{K} = \langle b, C(\mathbf{H}) \cap P\rangle$. Ponovo je $\mathbf{K} \leq \mathbf{P}$, a prema 16.22 ili 48.16 (po volji) je $\mathbf{H}/\mathbf{Z}(\mathbf{P}) \leq \mathbf{Z}(\mathbf{P}/\mathbf{Z}(\mathbf{P}))$, znači $\mathbf{H} \leq \zeta_2(\mathbf{P})$. Pošto je $[\mathbf{H}, \mathbf{K}] \leq [\zeta_2\mathbf{P}, \mathbf{P}] \leq \mathbf{Z}(\mathbf{P})$ (46.25(3)), prema 6.4 za $x \in Z(\mathbf{P})$ i $y \in C(\mathbf{H}) \cap P$ važi: $[a^i x, b^j y] = [a^i, b^j] = [a, b]^{ij}$, $[a, b]^p = [a^p, b] = e$ $(a^p \in Z(\mathbf{P}))$. Proizilazi da je normalna podgrupa $[\mathbf{H}, \mathbf{K}]$ reda $p$, protivurečno već konstatovanom. Prema tome, $\mathbf{P}$ je Abelova grupa. Minimalna normalna podgrupa grupe $\mathbf{G}$ sadržana u $\mathbf{P}$, recimo da je to $\mathbf{A}$, elementarna je Abelova $p$-grupa (10.43). Ako sama grupa $\mathbf{P}$ nije elementarna, tada postoji podgrupa $\mathbf{B}$ minimalna s obzirom na uslove da je normalna u $\mathbf{G}$ i neelementarna, da sadrži $\mathbf{A}$ i da je sadržana u $\mathbf{P}$. Kako je $\mathbf{G}/\mathbf{A}$ superrešiva grupa (što će reći da opet postoji normalna podgrupa $\mathbf{N}$ grupe $\mathbf{G}$ takva da je $\mathbf{N}/\mathbf{A} \leq \mathbf{P}/\mathbf{A} \leq \mathbf{G}/\mathbf{A}$ i $|N/A| = p$), $\mathbf{B}$ je izomorfna grupi oblika $\mathbf{Z}_{p^2} \oplus \mathbf{Z}_p \oplus \dots \oplus \mathbf{Z}_p$ (videti dokaz teoreme 32.10). Ali tada je $p\mathbf{B}$ normalna podgrupa grupe $\mathbf{G}$ (kao karakteristična podgrupa grupe $\mathbf{B}$) reda $p$, kontradikcija. Sledi da je $\mathbf{P}$ elementarna Abelova $p$-grupa i stoga je $\mathbf{P} = \mathbf{A} \times \mathbf{C}$ (za neku podgrupu $\mathbf{C}$). Prema 16.47 je za neku podgrupu

$\mathbf{R}$ (grupe $\mathbf{G}$) $\mathbf{G} = \mathbf{AR}$ i $\mathbf{A} \cap \mathbf{R} = \mathbf{E}$. Pošto je $[\mathbf{G} : \mathbf{R}] = |A| > p$, $\mathbf{R}$ nije maksimalna podgrupa. Ali, ako je $\mathbf{S}$ maksimalna podgrupa grupe $\mathbf{G}$ koja sadrži $\mathbf{R}$, onda je (zbog $\mathbf{A} \cap \mathbf{S} \lhd \mathbf{A}$, $\mathbf{A} \cap \mathbf{S} \lhd \mathbf{S}$) $\mathbf{A} \cap \mathbf{S}$ normalna podgrupa grupe $\mathbf{G}$ i prema tome, ili je $\mathbf{A} \cap \mathbf{S} = \mathbf{A}$ ili $\mathbf{A} \cap \mathbf{S} = \mathbf{E}$, kontradikcija u svakom slučaju ($\mathbf{A} \cap \mathbf{S} = \mathbf{A}$ daje $\mathbf{S} = \mathbf{G}$, $\mathbf{A} \cap \mathbf{S} = \mathbf{E}$ daje $\mathbf{G} = \mathbf{AR} < \mathbf{AS}$).■

**Korolar 50.15** *Konačna grupa $\mathbf{G}$ je superrešiva akko je $\mathbf{G}/\mathbf{Fr}(\mathbf{G})$ superrešiva grupa.*

Jedan drugi dokaz prethodne teoreme (videti [146], glava VII, paragraf 6) koristi naredne leme koje su i inače od šireg interesa.

**Definicija 50.16** *Neka su $\mathbf{H}$ i $\mathbf{K}$ normalne podgrupe grupe $\mathbf{G}$ i neka je $\mathbf{H} \leq \mathbf{K}$. Superrešivi niz između $\mathbf{K}$ i $\mathbf{H}$ je niz oblika $\mathbf{K} = \mathbf{K}_0 > \mathbf{K}_1 > \cdots > \mathbf{K}_m = \mathbf{H}$, gde su sve podgrupe $\mathbf{K}_i$, $i = 0, \ldots, m$, normalne u $\mathbf{G}$, a faktor grupe $\mathbf{K}_j/\mathbf{K}_{j+1}$, $j = 0, \ldots, m-1$, su ciklične.*

**Lema 50.17** *Neka je $\mathbf{H}$ normalna podgrupa grupe $\mathbf{G}$ i neka postoji superrešivi niz između $\mathbf{H}$ i $\mathbf{H}'$. Tada za svaki prirodan broj $k$ postoji superrešivi niz i između $\gamma_k\mathbf{H}$ i $\gamma_{k+1}\mathbf{H}$.*

**Dokaz.** Indukcijom po $k$. Za $k = 0$ imamo uslov leme. Neka je $(\gamma_0\mathbf{H} =)\ \mathbf{H} = \mathbf{K}_0 > \mathbf{K}_1 > \cdots > \mathbf{K}_{m-1} > \mathbf{K}_m = \mathbf{H}'\ (= \gamma_1\mathbf{H})$ jedan superrešivi niz između $\mathbf{H}$ i $\mathbf{H}'$. Pretpostavimo dalje da je tvrđenje tačno za sve prirodne brojeve manje od ili jednake $k$ i neka je $\gamma_k\mathbf{H} = \mathbf{M}_0 > \mathbf{M}_1 > \cdots > \mathbf{M}_{n-1} > \mathbf{M}_n = \gamma_{k+1}\mathbf{H}$ superrešivi niz između $\gamma_k\mathbf{H}$ i $\gamma_{k+1}\mathbf{H}$. Za svako $i = 0, 1, \ldots, m-1$ i svako $j = 0, 1, \ldots, n$ neka je

$$\mathbf{N}_{i,j} = \langle \gamma_{k+2}H \cup [K_i, M_j] \cup [K_{i+1}, \gamma_k H] \rangle = \gamma_{k+2}\mathbf{H} \cdot [\mathbf{K}_i, \mathbf{M}_j] \cdot [\mathbf{K}_{i+1}, \gamma_k\mathbf{H}]$$

i neka je $\mathbf{N}_{m,j} = \gamma_{k+2}\mathbf{H}$ – videti 46.25(1). Radi se, jasno, o normalnim podgrupama grupe $\mathbf{G}$. Za svako $\mathbf{N}_{i,j}$ je $\gamma_{k+1}\mathbf{H} \geq \mathbf{N}_{i,j} \geq \gamma_{k+2}\mathbf{H}$ ($\mathbf{N}_{0,0} = \gamma_{k+1}\mathbf{H}$, $\mathbf{N}_{m,n} = \gamma_{k+2}\mathbf{H}$), i za $i, i_1 \in \{0, \ldots, m\}$, $j, j_1 \in \{0, \ldots, n\}$ važi: $\mathbf{N}_{i,j} \geq \mathbf{N}_{i_1,j_1}$ ako je $\mathbf{K}_i > \mathbf{K}_{i_1}$ (tj. $i < i_1$) ili ako je $\mathbf{K}_i = \mathbf{K}_{i_1}$ ($i = i_1$) i $\mathbf{M}_j > \mathbf{M}_{j_1}$ ($j < j_1$). Imamo, znači, invarijantni niz između $\gamma_{k+2}\mathbf{H}$ i $\gamma_{k+1}\mathbf{H}$:

$$\gamma_{k+1}\mathbf{H} \geq \mathbf{N}_{0,1} \geq \cdots \geq \mathbf{N}_{0,n} \geq \mathbf{N}_{1,0} \geq \cdots \geq \mathbf{N}_{1,n} \geq \cdots \geq \mathbf{N}_{m,n} = \gamma_{k+2}\mathbf{H}.$$

Kako je, za svako $i = 0, \ldots, m-1$, $\mathbf{N}_{i,n} = \mathbf{N}_{i+1,0} = \gamma_{k+2}\mathbf{H} \cdot [\mathbf{K}_{i+1}, \gamma_k H]$ ($= \gamma_{k+2}\mathbf{H}$ ako je $i = m-1$), "prelaze" obrazuju parovi podgrupa, naravno ne nužno svi, $\mathbf{N}_{i,j}$, $\mathbf{N}_{i,j+1}$. Uzmimo da je upravo dat jedan takav. No onda, ako je $\mathbf{K}_i/\mathbf{K}_{i+1} = \langle aK_{i+1} \rangle$, tj. $\mathbf{K}_i = \langle a \rangle \cdot \mathbf{K}_{i+1}$ i $\mathbf{M}_j/\mathbf{M}_{j+1} = \langle bM_{j+1} \rangle$, odnosno $\mathbf{M}_j = \langle b \rangle \cdot \mathbf{M}_{j+1}$, sledi:

$$\mathbf{N}_{i,j}/\mathbf{N}_{i,j+1} =$$



$$([\mathbf{K}_i, \mathbf{M}_j] \cdot \gamma_{k+2}\mathbf{H} \cdot [\mathbf{K}_{i+1}, \gamma_k\mathbf{H}])/([\mathbf{K}_i, \mathbf{M}_{j+1}] \cdot \gamma_{k+2}\mathbf{H} \cdot [\mathbf{K}_{i+1}, \gamma_k\mathbf{H}]) =$$
$$\langle ([a, b])\, N_{i,j+1} \rangle.$$

Koristimo: ako je $x \in K_{i+1}$, $y \in M_{j+1}$, tada je prema 6.2 (tačke $(d)$, $(e)$):

$$[xa^m, yb^n]N_{i,j+1} = (a^{-m}[x, yb^n]a^m \cdot [a^m, yb^n])N_{i,j+1} = [a^m, yb^n]N_{i,j+1} =$$
$$([a^m, b^n] \cdot b^{-n}[a^m, y]b^n)N_{i,j+1} = [a^m, b^n]N_{i,j+1} = ([a, b]N_{i,j+1})^{mn};$$

druga jednakost važi jer je $[x, yb^n] \in [K_{i+1}, M_j] \subseteq [K_{i+1}, \gamma_k H]$ i $[\mathbf{K}_{i+1}, \mathbf{M}_j]$ je normalna podgrupa, četvrta jer je $[a^m, y] \in [K_i, M_{j+1}]$. Poslednja jednakost se dokazuje indukcijom, recimo prvo po $m$, a onda i po $n$. Ilustracije radi razmotrimo slučaj $m = 1$ (i $n \geq 1$) (opet nam treba lema 6.2 – konkretnije, njena tačka $(h)$):

$$[a, b^n]N_{i,j+1} = (\textstyle\prod_{s=0}^{n-1} b^{-s}[a, b]b^s)N_{i,j+1} = (\prod_{s=0}^{n-1}[a, b][[a, b], b^s])N_{i,j+1} =$$
$$([a, b]N_{i,j+1})^{1 \cdot n};$$

jer, $[a, b] \in [K_i, M_j] \subseteq [K_i, \gamma_k H] \subseteq \gamma_{k+1}H$ i zbog toga je $[[a, b], b^s] \in \gamma_{k+2}H \subseteq N_{i,j+1}$.□

**Lema 50.18** *Neka je $\mathbf{A}$ Abelova normalna podgrupa grupe $\mathbf{G}$ i neka za prost broj $p$ postoji superrešivi niz između $\mathbf{A}$ i $\mathbf{A}^p$ ($\mathbf{A}^p \stackrel{\text{def}}{=} \langle \{a^p \mid a \in A\}, \cdot \rangle$). Tada za svaki prirodan broj $k$ postoji superrešivi niz između $\mathbf{A}^{p^k}$ i $\mathbf{A}^{p^{k+1}}$.*

**Dokaz.** Ako je $\mathbf{A} = \mathbf{B}_0 > \mathbf{B}_1 > \cdots > \mathbf{B}_{n-1} > \mathbf{B}_n = \mathbf{A}^p$ superrešivi niz između $\mathbf{A}$ i $\mathbf{A}^p$, tada niz $\mathbf{A}^{p^k} = \mathbf{B}_0^{p^k} \geq \mathbf{B}_1^{p^k} \geq \cdots \geq \mathbf{B}_{n-1}^{p^k} \geq \mathbf{B}_n^{p^k} = \mathbf{A}^{p^{k+1}}$ daje, posle uklanjanja eventualnog "viška", superrešivi niz između $\mathbf{A}^{p^k}$ i $\mathbf{A}^{p^{k+1}}$ (ako je npr. $\mathbf{B}_i/\mathbf{B}_{i+1}$ ciklična grupa generisana elementom $cB_{i+1}$, onda je grupa $\mathbf{B}_i^{p^k}/\mathbf{B}_{i+1}^{p^{k+1}}$ generisana elementom $c^{p^k}B_{i+1}^{p^k}$).□

## 51 Policiklične grupe

Policiklične grupe su "najprirodnije" uopštenje superrešivih grupa.

**Definicija 51.1** *Policiklični niz je normalni niz čiji su svi faktori ciklične grupe.*

*Poli-beskonačno ciklični niz je normalni niz čiji su svi faktori beskonačne ciklične grupe.*

*Grupa je policiklična akko ima policiklični niz.*

*Grupa je poli-beskonačno ciklična akko ima poli-beskonačno ciklični niz.*

Opet je grupa $\mathbf{A}_4$ grupa najmanjeg reda koja je policiklična ali ne i superrešiva.

**Lema 51.2** (*a*) *Policiklične grupe su prebrojive;*

(*b*) *Podgrupe i homomorfne slike policiklične grupe su policiklične;*

(*c*) *Ekstenzija policiklične grupe policikličnom grupom je policiklična grupa;*

(*d*) *Direktni proizvod konačno mnogo policikličnih grupa je policiklična grupa;*

(*e*) *Policiklične grupe ispunjavaju uslov maksimalnosti podgrupa.*

**Dokaz**. (*b*) Prema lemi 46.11 je podgrupa policiklične grupe policiklična.

Ako je $\mathbf{N}$ normalna podgrupa policiklične grupe $\mathbf{G}$, onda postoji policiklični niz (grupe $\mathbf{G}$) koji "prolazi" kroz $\mathbf{N}$; jer, proširenje policikličnog niza je policiklični niz (naravno, u igri je i teorema Schreiera – 46.4). Preostaje nam još da se pozovemo, kao i u ostalim sličnim slučajevima, na 8.7.

(*c*) Dokaz je potpuno analogan drugom dokazu leme 49.6.

(*e*) Videti dokaz leme 52.3.□

**Korolar 51.3** *Ako su* $\mathbf{H}$ *i* $\mathbf{K}$ *normalne podgrupe grupe* $\mathbf{G}$ *i ako su* $\mathbf{G/H}$ *i* $\mathbf{G/K}$ *policiklične grupe, onda je i* $\mathbf{G/(H \cap K)}$ *policiklična grupa.*

**Dokaz**. Prema 10.15 i tačkama (*b*) i (*d*) prethodne leme.□

**Lema 51.4** *Grupa je policiklična akko je rešiva i ispunjava uslov maksimalnosti podgrupa.*

**Dokaz**. Pravac ($\Longrightarrow$) je već dokazan. Neka je pak $\mathbf{G}$ rešiva grupa koja ispunjava uslov maksimalnosti podgrupa. Onda su faktori izvodnog niza grupe $\mathbf{G}$ konačno generisane Abelove grupe. Recimo, $\mathbf{G/G'}$ je Abelova grupa koja, kao homomorfna slika grupe $\mathbf{G}$, ispunjava uslov maksimalnosti podgrupa (prema tome je i konačno generisana); iz istih razloga je i $\mathbf{G'/G''}$ Abelova konačno generisana grupa i tako dalje. No, konačno generisane Abelove grupe su direktne sume cikličnih grupa (32.4), pa se adekvatnim proširenjem izvodnog niza dobija policiklični niz.□

**Lema 51.5** *Svi policiklični nizovi (policiklične) grupe* $\mathbf{G}$ *imaju isti broj beskonačnih cikličnih grupa, tj. imaju istu tzv. Hirschovu dužinu (K. A. Hirsch).*

**Dokaz**. Videti dokaz leme 52.4.□

**Teorema 51.6** *Grupa* $\mathbf{G}$ *je policiklična akko ima karakteristični niz čiji je svaki faktor ili konačna elementarna Abelova grupa ili slobodna Abelova grupa konačnog ranga i pri tom možemo pretpostaviti da se beskonačni faktori, ukoliko ih ima, javljaju "na kraju".*



**Dokaz**. ($\Longleftarrow$) Slobodne Abelove grupe konačnog ranga (kao direktne sume konačno mnogo beskonačnih cikličnih grupa) i konačne elementarne Abelove grupe (kao direktne sume konačno mnogo cikličnih grupa prostog reda) su policiklične. Stoga, ako je dat karakteristični niz grupe $\mathbf{G}$ datih svojstava: $\mathbf{G} = \mathbf{G}_0 > \cdots > \mathbf{G}_i > \mathbf{G}_{i+1} > \cdots > \mathbf{G}_n = \mathbf{E}$, i ako je npr. $\overline{\mathbf{G}_i} = \mathbf{G}_i/\mathbf{G}_{i+1}$ konačna elementarna Abelova grupa, tada postoji policiklični niz (čiji su faktori cikличne grupe prostog reda): $\mathbf{G}_i/\mathbf{G}_{i+1} > \mathbf{H}_1/\mathbf{G}_{i+1} > \cdots > \mathbf{H}_m/\mathbf{G}_{i+1} = \overline{\mathbf{E}}$, te je $\mathbf{G}_i > \mathbf{H}_1 > \cdots > \mathbf{H}_{m-1} > \mathbf{H}_m = \mathbf{G}_{i+1}$ deo normalnog niza grupe $\mathbf{G}$ sa cikličnim faktorima.

($\Longrightarrow$) Indukcijom po dužini ($n$) najkraćeg policikličnog niza. Slučaj $n = 0$ ($\mathbf{G}$ je jedinična grupa) i $n = 1$ ($\mathbf{G}$ je ciklična grupa) su trivijalni; konačna ciklična grupa je direktna suma primarnih cikličnih grupa i tako, ako je $\mathbf{G} = \mathbf{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbf{Z}_{p_m^{k_m}}$, jedan karakteristični niz grupe "propisanih svojstava" je, recimo: $\mathbf{G} > p_1\mathbf{Z}_{p_1^{k_1}} \oplus (\mathbf{Z}_{p_2^{k_2}} \oplus \cdots \oplus \mathbf{Z}_{p_m^{k_m}}) > \cdots > p_1^{k_1-1}\mathbf{Z}_{p_1^{k_1}} \oplus (\mathbf{Z}_{p_2^{k_2}} \oplus \cdots \oplus \mathbf{Z}_{p_m^{k_m}}) > \mathbf{Z}_{p_2^{k_2}} \oplus \cdots \oplus \mathbf{Z}_{p_m^{k_m}} > \cdots > p_2^{k_2-1}\mathbf{Z}_{p_2^{k_2}} \oplus (\mathbf{Z}_{p_3^{k_3}} \oplus \cdots \oplus \mathbf{Z}_{p_m^{k_m}}) > \mathbf{Z}_{p_3^{k_3}} \oplus \cdots \oplus \mathbf{Z}_{p_m^{k_m}} > \cdots > \mathbf{E}$. Pretpostavimo da je tvrđenje tačno za sve grupe s policikličnim nizovima dužine manje od $n$ ($> 1$) i neka je $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \ldots > \mathbf{G}_n = \mathbf{E}$ najkraći policiklični niz grupe $\mathbf{G}$. Ako je $\mathbf{G/G}_1$ beskonačna ciklična grupa, onda je $\mathbf{G/Core}_k(\mathbf{G}_1)$, gde je $\mathbf{Core}_k(\mathbf{G}_1)$ karakteristično jezgro podgrupe $\mathbf{G}_1$ (4.33), slobodna Abelova grupa konačnog ranga. Zaista, $\mathbf{G}' \leq \mathbf{G}_1$ i za svako $\varphi \in Aut(\mathbf{G})$ je $\mathbf{G}' = (\mathbf{G}')\varphi \leq (\mathbf{G}_1)\varphi$, pa je $\mathbf{G}' \leq \bigcap_{\varphi \in Aut(\mathbf{G})}(\mathbf{G}_1)\varphi = \mathbf{Core}_k(\mathbf{G}_1)$; dakle, $\mathbf{G/Core}_k(\mathbf{G}_1)$ je konačno generisana Abelova grupa (sama grupa $\mathbf{G}$ je konačno generisana). Ali ona je i torziono slobodna. Jer, ako je $gCore_k(\mathbf{G}_1) \neq Core_k(\mathbf{G}_1)$, tada $g \notin (G_1)\psi$ za neki automorfizam $\psi$ grupe $\mathbf{G}$ i pošto je $\mathbf{G/G}_1 \cong \mathbf{G}/(\mathbf{G}_1)\psi$ ($\cong \mathbf{Z}$) (jedan automorfizam je dat sa: $aG_1 \longrightarrow (a)\psi(G_1)\psi$), $g^m \notin (G_1)\psi$, odnosno $g^m \notin Core_k(\mathbf{G}_1)$ za svaki pozitivan prirodan broj. Ako je $\mathbf{G/G}_1$ konačna ciklična grupa, $\mathbf{G/Core}_k(\mathbf{G}_1)$ je svejedno konačno generisana Abelova grupa, prema tome izomorfna grupi (oblika) $\sum_{i=1}^{r}\mathbf{Z}_i \oplus \sum_{j=1}^{t}\mathbf{Z}_{n_j}$; podrazumevamo da je za $r = 0$ ili $t = 0$ odgovarajući sumand nula grupa kao i da su brojevi $n_j$, $j = 1, \ldots, t$, stepeni prostih brojeva, ne nužno različiti za različite indekse. Stoga je, za neke podgrupe $\mathbf{H}$, $\mathbf{K}$ grupe $\mathbf{G}$, $\mathbf{G/Core}_k(\mathbf{G}_1) = \mathbf{H/Core}_k(\mathbf{G}_1) \times \mathbf{K/Core}(\mathbf{G}_1)$, gde je $\mathbf{H/Core}_k(\mathbf{G}_1)$ slobodna Abelova grupa ranga $r$ i $\mathbf{K/Core}_k(\mathbf{G}_1)$ direktna suma konačno mnogo primarnih cikličnih grupa. $\mathbf{K/Core}_k(\mathbf{G}_1)$ je, kao periodični deo, karakteristična podgrupa grupe $\mathbf{G/Core}_k(\mathbf{G}_1)$, pa je zbog karakterističnosti podgrupe $\mathbf{Core}_k(\mathbf{G}_1)$ i $\mathbf{K}$ karakteristična podgrupa (8.10). $\mathbf{G/K}$ ($\cong (\mathbf{G/Core}_k(\mathbf{G}_1))/(\mathbf{K/Core}_k(\mathbf{G}_1)) \cong \mathbf{H/Core}_k(\mathbf{G}_1)$) je slobodna Abelova grupa. Već smo pokazali (na neki način) kako ćemo između $\mathbf{K}$ i $\mathbf{Core}_k(\mathbf{G}_1)$ "ugraditi" karakteristični niz čiji su faktori konačne elementarne Abelove grupe. Dalje, $\mathbf{Core}_k(\mathbf{G}_1) \geq \mathbf{G}_2 \cap \mathbf{Core}_k(\mathbf{G}_1) \geq \cdots \geq \mathbf{G}_n \cap \mathbf{Core}_k(\mathbf{G}_1) = \mathbf{E}$ daje, posle uklanjanja eventualnog "viška", poli-

ciklični niz grupe $\mathbf{Core}_k(\mathbf{G}_1)$ dužine manje od $n$; na primer, ponavljamo se: $(\mathbf{G}_i \cap \mathbf{Core}_k(\mathbf{G}_1))/(\mathbf{G}_{i+1} \cap \mathbf{Core}_k(\mathbf{G}_1)) = (\mathbf{G}_i \cap \mathbf{Core}_k(\mathbf{G}_1))/(\mathbf{G}_{i+1} \cap (\mathbf{G}_i \cap \mathbf{Core}_k(\mathbf{G}_1))) \cong (\mathbf{G}_{i+1}(\mathbf{G}_i \cap \mathbf{Core}_k(\mathbf{G}_1)))/\mathbf{G}_{i+1} \leq \mathbf{G}_i/\mathbf{G}_{i+1}$. Prema induktivnoj hipotezi $\mathbf{Core}_k(\mathbf{G}_1)$ ima karakteristični niz čiji je svaki faktor ili konačna elementarna Abelova grupa ili slobodna Abelova grupa konačnog ranga, te ga zbog tranzitivnosti svojstva karakterističnosti ima i grupa $\mathbf{G}$. Konačno, 46.19 nam omogućuje eventualno potrebno "premeštanje" beskonačnih faktora na kraj niza. Neka je npr. za "propisni" karakteristični niz grupe $\mathbf{G} - \mathbf{G} = \mathbf{H}_0 > \cdots > \mathbf{H}_{i-1} > \mathbf{H}_i > \mathbf{H}_{i+1} > \cdots > \mathbf{E} - \mathbf{H}_{i-1}/\mathbf{H}_i$ slobodna Abelova grupa ranga $r$ i $\mathbf{H}_i/\mathbf{H}_{i+1}$ konačna elementarna Abelova grupa. Prema pomenutoj lemi grupa $\mathbf{H}_{i-1}/\mathbf{H}_{i+1}$ ima karakteristični niz čiji su faktori konačne elementarne Abelove grupe i slobodna Abelova grupa ranga $r$ koja dolazi "na kraj"; neka je to niz: $\mathbf{H}_{i-1}/\mathbf{H}_{i+1} = \mathbf{K}_0/\mathbf{H}_{i+1} > \mathbf{K}_1/\mathbf{H}_{i+1} > \cdots > \mathbf{K}_{s-1}/\mathbf{H}_{i+1} > \mathbf{K}_s/\mathbf{H}_{i+1} > \mathbf{K}_{s+1}/\mathbf{H}_{i+1} = \overline{\mathbf{E}}$. Ali, sve podgrupe $\mathbf{K}_1, \ldots, \mathbf{K}_s$ su karakteristične podgrupe grupe $\mathbf{H}_{i-1}$ $(= \mathbf{K}_0)$ (8.10), dakle i grupe $\mathbf{G}$, $\mathbf{K}_s/\mathbf{H}_{i+1}$ je slobodna Abelova grupa ranga $r$, a za $j = 0, \ldots, s-1$ je $\mathbf{K}_j/\mathbf{K}_{j+1} \cong (\mathbf{K}_j/\mathbf{H}_{i+1})/(\mathbf{K}_{j+1}/\mathbf{H}_{i+1})$ konačna elementarna Abelova grupa.■

**Korolar 51.7** (*a*) *Beskonačna policiklična grupa ima poli-beskonačnu cikličnu podgrupu konačnog indeksa;*

(*b*) *Beskonačna policiklična grupa sadrži kao karakterističnu podgrupu slobodnu Abelovu grupu konačnog ranga.*

**Teorema 51.8** *(A. I. Maljcev). Podgrupa* $\mathbf{H}$ *policiklične grupe* $\mathbf{G}$ *jednaka je preseku svih podgrupa konačnog indeksa (grupe* $\mathbf{G}$*) koje sadrže* $\mathbf{H}$.

**Dokaz**. Ako je $\mathbf{G}$ Abelova grupa, $\mathbf{H}$ je njena normalna podgrupa, $\mathbf{G}/\mathbf{H}$ je konačno generisana Abelova grupa, znači i rezidualno konačna (32.6), a u konačno rezidualnoj grupi je jedinična podgrupa presek normalnih podgrupa konačnog indeksa; za svaki nejedinični element $gH$ grupe $\mathbf{G}/\mathbf{H}$ postoji normalna podgrupa konačnog indeksa $\overline{\mathbf{N}}_{gH} = \mathbf{N}_{gH}/\mathbf{H}$ koja ne sadrži $gH$, pa je $\bigcap \{N_{gH} \mid gH \neq H\} = H$.

Generalno, dokaz dajemo indukcijom po Hirschovoj dužini – $l$. Ako je $l = 0$, grupa je konačna (i slučaj je trivijalan). Pretpostavimo da je tvrđenje tačno za sve policiklične grupe Hirschove dužine manje od $l$ $(> 0)$ i neka je $\mathbf{G}$ policiklična grupa Hirschove dužine $l$. Prema prethodnom korolaru (tačka $(b)$) $\mathbf{G}$ ima za karakterističnu podgrupu slobodnu Abelovu grupu konačnog ranga, neka je to $\mathbf{A}$, i pošto je $\mathbf{G}/\mathbf{A}$ policiklična grupa Hirschove dužine manje od $l$ za nju tvrđenje važi. U nastavku dokazujemo da za svaki element $g$ koji nije u $\mathbf{H}$ postoji podgrupa konačnog indeksa grupe $\mathbf{G}$ koja sadrži $\mathbf{H}$ i ne sadrži $g$ (što nam daje traženu relaciju: $\bigcap \{\mathbf{K} \leq \mathbf{G} \mid \mathbf{H} \leq \mathbf{K}, [\mathbf{G} : \mathbf{K}] < \infty\} = \mathbf{H}$). Ako $g \notin AH$, onda posebno, $gA \notin (AH)/A$ i u faktor grupi $\mathbf{G}/\mathbf{A}$ postoji podgrupa konačnog indeksa $\mathbf{K}/\mathbf{A}$ koja sadrži podgrupu $(\mathbf{AH})/\mathbf{A}$ i ne sadrži



element $gA$. Odatle, $\mathbf{H} \leq \mathbf{AH} \leq \mathbf{K}$, $g \notin K$ i $[\mathbf{G} : \mathbf{K}] = [\mathbf{G}/\mathbf{A} : \mathbf{K}/\mathbf{A}] < \infty$. Neka je sada $g \in AH$, dakle, $g = ah$ za neko $a \in A \setminus H$ i neko $h \in H$ $(a \in H$ bi dalo $g \in H)$. No, i $\mathbf{A}/(\mathbf{A} \cap \mathbf{H})$ je rezidualno konačna grupa (opet kao Abelova konačno generisana grupa), pa postoji neka njena podgrupa konačnog indeksa $\mathbf{B}/(\mathbf{A} \cap \mathbf{H})$ koja ne sadrži $a(A \cap H)$. Sledi da je $\mathbf{B}$ podgrupa konačnog indeksa grupe $\mathbf{A}$ koja sadrži $\mathbf{A} \cap \mathbf{H}$ i ne sadrži element $a$. Ako je $\mathbf{A} = \mathbf{A}_1 \times \cdots \times \mathbf{A}_m$, gde su $\mathbf{A}_i$, $i = 1, \ldots, m$, beskonačne ciklične grupe, onda je $\mathbf{B} = \mathbf{A}_1^{n_1} \times \cdots \times \mathbf{A}_m^{n_m}$ za neke pozitivne prirodne brojeve $n_1, \ldots, n_m$ (videti 32.10) i stoga je za neko $n$ (recimo $NZS(n_1, \ldots, n_m)$) $\mathbf{A}^n \leq \mathbf{B}$. Jasno, $\mathbf{A}^n$ je karakteristična (štaviše potpuno invarijantna) podgrupa (konačnog indeksa) grupe $\mathbf{A}$ i prema tome normalna podgrupa grupe $\mathbf{G}$. Ako $g \notin A^n H$, vraćamo se na prethodno razmatranje (s tim što sada koristimo induktivnu pretpostavku za faktor grupu $\mathbf{G}/\mathbf{A}^n$). Ali ni ne može biti $g \in A^n H$; ako bi za neko $a_1 \in A^n$ i neko $h_1 \in H$ bilo $g = a_1 h_1 = ah$, sledilo bi $a_1^{-1} a = h_1 h^{-1} \in A \cap H \subseteq B$, tj. $a \in a_1 B \subseteq B$, kontradikcija.■

Kao poseban slučaj prethodne teoreme $(\mathbf{H} = \mathbf{E})$ imamo (s obzirom na 4.19)

**Korolar 51.9** *Policiklične grupe su rezidualno konačne.*

**Teorema 51.10** *(K. Hirsch). Policiklična grupa koja nije nilpotentna ima za jednu homomorfnu sliku konačnu grupu koja nije nilpotentna.*

**Dokaz**. Pretpostavimo da tvrđenje ne važi i neka je $\mathbf{G}$ kontraprimer najkraće Hirschove dužine (jasno, $\mathbf{G}$ mora biti beskonačna grupa). Prema 51.7$(b)$ $\mathbf{G}$ sadrži, kao normalnu podgrupu, slobodnu Abelovu grupu konačnog ranga $(r)$ – $\mathbf{A}$. Za svaki prost broj $p$ je $\mathbf{G}/\mathbf{A}^p$ policiklična grupa Hirschove dužine manje od Hirschove dužine grupe $\mathbf{G}$, pa kako ne može imati za homomorfnu sliku konačnu nilpotentnu grupu (u suprotnom bi je i grupa $\mathbf{G}$ imala), to sama mora biti nilpotentna. $\mathbf{A}/\mathbf{A}^p$ je elementarna Abelova grupa reda $p^r$ (direktna suma $r$ cikličnih grupa reda $p$), normalna podgrupa grupe $\mathbf{G}/\mathbf{A}^p$, pa je prema 48.17 $\mathbf{A}/\mathbf{A}^p \leq \zeta_r(\mathbf{G}/\mathbf{A}^p)$, a onda je prema 46.27 i $[\mathbf{A}, \underbrace{\mathbf{G}, \ldots, \mathbf{G}}_{r-puta}] = \mathbf{A}^p$; koristimo: $[\mathbf{A}/\mathbf{A}^p, \underbrace{\mathbf{G}/\mathbf{A}^p, \ldots, \mathbf{G}/\mathbf{A}^p}_{r-puta}] = [\mathbf{A}, \underbrace{\mathbf{G}, \ldots, \mathbf{G}}_{r-puta}]/\mathbf{A}^p = \overline{\mathbf{E}}$. No, za skup (svih) prostih brojeva $P$ je $\bigcap_{p \in P} \mathbf{A}^p = \mathbf{E}$ ($\mathbf{A}^p$ je izomorfna grupi $\underbrace{p\mathbf{Z} \oplus \cdots \oplus p\mathbf{Z}}_{r-puta}$ i svaki element u preseku $\bigcap_{p \in P} \mathbf{A}^p$ je deljiv svim prostim brojevima, a samo je jedan takav – jedinični). Stoga je $[\mathbf{A}, \underbrace{\mathbf{G}, \ldots, \mathbf{G}}_{r-puta}] = \mathbf{E}$ i, ponovo prema 46.27, $\mathbf{A} \leq \zeta_r \mathbf{G}$. Ali tada je i grupa $\mathbf{G}/\zeta_r \mathbf{G}$ nilpotentna (kao homomorfna slika grupe $\mathbf{G}/\mathbf{A}^p$), onda i $\mathbf{G}$ (48.10), kontradikcija.■

**Korolar 51.11** *Frattinijeva podgrupa policiklične grupe* **G** *je nilpotentna.*

**Dokaz.** Pretpostavimo da $\mathbf{Fr(G)}$ nije nilpotentna grupa. Onda je prema prethodnoj teoremi, za neku njenu normalnu podgrupu $\mathbf{N}$, $\mathbf{Fr(G)/N}$ konačna grupa koja nije nilpotentna. Prema 9.41 $\mathbf{Fr(G)}$ sadrži karakterističnu podgrupu konačnog indeksa – $\mathbf{H}$ – koja je sadržana u $\mathbf{N}$. Opet $\mathbf{Fr(G)/H}$ nije nilpotentna grupa (ponavljamo: $\mathbf{Fr(G)/N}$ je njena homomorfna slika) i $\mathbf{H}$ je normalna podgrupa grupe $\mathbf{G}$. Ali $\mathbf{Fr(G/H)} = \mathbf{Fr(G)/H}$ (8.11), pa je prema 48.30($b$) $\mathbf{Fr(G)/H}$ nilpotentna grupa, kontradikcija.□

**Korolar 51.12** *Policiklična grupa* **G** *je nilpotentna akko je* $\mathbf{G'} \leq \mathbf{Fr(G)}$.

**Dokaz.** Pravac ($\Longrightarrow$) važi generalno (videti komentar posle korolara 48.36).

($\Longleftarrow$) Pretpostavimo da je $\mathbf{G'} \leq \mathbf{Fr(G)}$ ali da $\mathbf{G}$ nije nilpotentna grupa. Tada postoji neka njena konačna homomorfna slika $\mathbf{H}$ koja nije nilpotentna; neka je $\varphi$ surjektivno homomorfno preslikavanje grupe $\mathbf{G}$ na $\mathbf{H}$. No onda je $\mathbf{H'} = (\mathbf{G'})\varphi \leq (\mathbf{Fr(G)})\varphi = (\bigcap\{\mathbf{K} \mid \mathbf{K}$ je maksimalna podgrupa grupe $\mathbf{G}\})\varphi \leq \bigcap\{(\mathbf{K})\varphi \mid \mathbf{K}$ je maksimalna podgrupa grupe $\mathbf{G}\} \leq \mathbf{Fr(H)}$ (u opštem, homomorfna slika maksimalne podgrupe ne mora biti maksimalna podgrupa), te je prema teoremi 48.28 $\mathbf{H}$ nilpotentna grupa, kontradikcija.□

## 52 $M$-grupe

Jedna interesantna ekstenzija klase policikičnih grupa je klasa $M$-grupa.

**Definicija 52.1** *Normalni niz grupe* **G** *je normalni $M$-niz akko su njegovi faktori ili beskonačne ciklične grupe ili konačne grupe.*

*Grupa je $M$-grupa akko ima normalni $M$-niz.*

Naravno, svaka $M$-grupa je prebrojiva (konačna ili beskonačno prebrojiva). Opet, (prebrojiva) grupa $\mathbf{Ra}$ nije $M$-grupa (homomorfna slika deljive grupe je deljiva grupa); takođe, sve konačne grupe su $M$-grupe dok među njima ima onih koje nisu rešive (pa, dakle, ni policiklične).

**Lema 52.2** ($a$) *Podgrupe i homomorfne slike $M$-grupe su $M$-grupe;*

($b$) *Ako je* $\mathbf{N}$ *normalna podgrupa grupe* $\mathbf{G}$ *i ako su* $\mathbf{N}$ *i* $\mathbf{G/N}$ *$M$-grupe, onda je* $\mathbf{G}$ *$M$-grupa.*

($c$) *Ekstenzija $M$-grupe $M$-grupom je $M$-grupa;*

($d$) *Direktan proizvod konačno mnogo $M$-grupa je $M$-grupa.*

**Lema 52.3** *Svaka $M$-grupa ispunjava uslov maksimalnosti podgrupa.*



**Dokaz.** Neka je $\mathbf{G}$ $M$-grupa sa normalnim $M$-nizom $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_{k-1} > \mathbf{G}_k = \mathbf{E}$. Indukcijom po $i$ ($i = 1, \ldots, k$) pokazuje se da svaka podgrupa $\mathbf{G}_{k-i}$ ispunjava uslov maksimalnosti podgrupa. $\mathbf{G}_{k-1}$ ($\cong \mathbf{G}_{k-1}/\mathbf{G}_k$) je ili beskonačna ciklična grupa ili konačna grupa, u svakom slučaju ispunjava uslov maksimalnosti podgrupa (videti 5.15), i generalno, ako za $i < k$ grupa $\mathbf{G}_{k-i}$ ispunjava uslov maksimalnosti podgrupa, ispunjava ga, prema 13.3($d$), i $\mathbf{G}_{k-(i+1)}$.□

**Lema 52.4** *Normalni $M$-nizovi $M$-grupe imaju isti broj beskonačnih faktora.*

**Dokaz.** Neka je $\mathbf{G}$ $M$-grupa i neka su $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_k = \mathbf{E}$ i $\mathbf{G} = \mathbf{H}_0 > \mathbf{H}_1 > \cdots > \mathbf{H}_l = \mathbf{E}$ dva njena normalna $M$-niza. Prema Schreierovoj teoremi oni imaju izomorfna proširenja. Neka je $\mathbf{G} = \mathbf{K}_0 > \mathbf{K}_1 > \cdots > \mathbf{K}_m = \mathbf{E}$ odgovarajuće proširenje prvoga. Dovoljno je, jasno, da pokažemo da ta dva niza imaju isti broj beskonačnih faktora. Neka je za neko $i$, $1 \leq i \leq k$, $\mathbf{G}_{i-1} = \mathbf{K}_r > \mathbf{K}_{r+1} > \cdots > \mathbf{K}_{r+s} = \mathbf{G}_i$ "segment" datog proširenja. Ako je $\mathbf{G}_{i-1}/\mathbf{G}_i$ konačna grupa, onda su i svi faktori $\mathbf{K}_{r+t-1}/\mathbf{K}_{r+t}$, $1 \leq t \leq s$, konačni. Ako je pak $\mathbf{G}_{i-1}/\mathbf{G}_i$ beskonačna ciklična grupa, onda je $\mathbf{K}_{r+s-1}/\mathbf{K}_{r+s} = \mathbf{K}_{r+s-1}/\mathbf{G}_i$ takođe beskonačna ciklična grupa, dok su svi drugi faktori – $\mathbf{K}_{r+t-1}/\mathbf{K}_{r+t}$, $1 \leq t \leq s-1$, konačni; jer, $\mathbf{K}_{r+s-1}/\mathbf{G}_i$ je nejedinična podgrupa beskonačne ciklične grupe $\mathbf{G}_{i-1}/\mathbf{G}_i$, za $1 \leq t \leq s-1$ je $\mathbf{K}_{r+t-1}/\mathbf{K}_{r+t} \cong (\mathbf{K}_{r+t-1}/\mathbf{G}_i)/(\mathbf{K}_{r+t}/\mathbf{G}_i)$, a znamo da je faktor grupa beskonačne ciklične grupe za svaku nejediničnu podgrupu konačna grupa.□

**Korolar 52.5** *Invarijantni ciklični nizovi superrešive grupe imaju isti broj beskonačnih faktora.*

**Korolar 52.6** *Ako beskonačna $M$-grupa ima normalni $M$-niz dužine $m$, ima i normalni $M$-niz svake druge dužine $n > m$.*

**Dokaz.** Neka je $\mathbf{G}$ $M$-grupa sa normalnim $M$-nizom $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_m = \mathbf{E}$ i neka je $n = m + k$, $k \geq 1$. Bar jedan od faktora datog niza je beskonačna ciklična grupa (u suprotnom bi $\mathbf{G}$ bila konačna grupa). Izaberimo jedan takav; neka je to $\mathbf{G}_{i-1}/\mathbf{G}_i$, $1 \leq i \leq m$, i neka je $\mathbf{G}_{i-1}/\mathbf{G}_i = \langle aG_i \rangle$. Znači, $\mathbf{G}_{i-1} = \langle a, G_i \rangle$. Neka je, za $j = 0, \ldots, k$, $\mathbf{H}_j$ podgrupa grupe $\mathbf{G}_{i-1}$ generisana skupom $\{a^{2^j}, G_i\}$. Jasno, $\mathbf{H}_0 = \mathbf{G}_{i-1}$ i za svako $j = 0, \ldots, k$ je $\mathbf{H}_j/\mathbf{G}_i = \langle a^{2^j} G_i \rangle$. Prema tome, $\mathbf{H}_k/\mathbf{G}_i$ je beskonačna ciklična grupa, a za $1 \leq j \leq k$ je $\mathbf{H}_{j-1}/\mathbf{H}_j$ ($\cong (\mathbf{H}_{j-1}/\mathbf{G}_i)/(\mathbf{H}_j/\mathbf{G}_i)$) ciklična grupa reda 2, pa je $\mathbf{G} = \mathbf{G}_0 > \cdots > \mathbf{G}_{i-1} = \mathbf{H}_0 > \mathbf{H}_1 > \cdots > \mathbf{H}_k > \mathbf{G}_i > \cdots > \mathbf{G}_m = \mathbf{E}$ normalni $M$-niz grupe $\mathbf{G}$ dužine $m + k$.□

**Lema 52.7** *Grupa* **G** *je $M$-grupa akko ima karakteristični niz čiji je svaki faktor ili konačna grupa ili slobodna Abelova grupa konačnog ranga.*

**Dokaz**. Analogan dokazu teoreme 51.6 i jednostavniji utoliko što je u induktivnom koraku (pravca $\Longrightarrow$), u slučaju da je $\mathbf{G}/\mathbf{G}_1$ konačna grupa (zadržavamo notaciju iz pomenutog dokaza), dovoljno samo da se pozovemo na 9.41 – $\mathbf{G}_1$ sadrži karakterističnu podgrupu konačnog indeksa.□

**Korolar 52.8** *M-grupa ima karakteristični niz čiji je prvi faktor konačna grupa dok su ostali, ukoliko ih ima, slobodne Abelove grupe konačnog ranga.*

**Dokaz**. Opet imamo analogiju sa adekvatnim delom dokaza teoreme 51.6 i opet je situacija jednostavnija. Ponavljamo ga ukratko.

Neka je $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_n = \mathbf{E}$ ma koji karakteristični niz $M$-grupe $\mathbf{G}$, čiji su faktori ili konačne grupe ili slobodne Abelove grupe konačnog ranga. Pretpostavimo da je $\mathbf{G}_{i-1}/\mathbf{G}_i$ slobodna Abelova grupa konačnog ranga $r$, dok je $\mathbf{G}_i/\mathbf{G}_{i+1}$ konačna grupa. Dakle, u faktor grupi $\mathbf{G}_{i-1}/\mathbf{G}_{i+1}$ je $\mathbf{G}_i/\mathbf{G}_{i+1}$ konačna normalna podgrupa čija je faktor grupa (izomorfna grupi $\mathbf{G}_{i-1}/\mathbf{G}_i$)) slobodna Abelova grupa ranga $r$, pa prema 32.9 postoji karakteristična slobodna Abelova podgrupa ranga $r$ – $\mathbf{K}/\mathbf{G}_{i+1}$ (grupe $\mathbf{G}_{i-1}/\mathbf{G}_{i+1}$) čija je faktor grupa $(\mathbf{G}_{i-1}/\mathbf{G}_{i+1})/(\mathbf{K}/\mathbf{G}_{i+1})$ ($\cong \mathbf{G}_{i-1}/\mathbf{K}$) konačna. No, $\mathbf{K}$ je karakteristična podgrupa i grupe $\mathbf{G}$ (8.10). Jasno, sukcesivnim ponavljanjem ovog postupka potreban broj puta dobili bismo na kraju karakteristični niz kakav se traži.□

**Korolar 52.9** *Beskonačna M-grupa ima karakterističnu torziono slobodnu podgrupu konačnog indeksa.*

**Lema 52.10** *Ako M-grupa nije nilpotentna, onda ima za jednu homomorfnu sliku konačnu grupu koja nije nilpotentna.*

**Dokaz**. Videti (i kopirati) dokaz analognog tvrđenja za policiklične grupe – 51.10.□

**Korolar 52.11** *Za M-grupu* $\mathbf{G}$ *su sledeći uslovi ekvivalentni:*

(1) $\mathbf{G}$ *je nilpotentna;*

(2) $\mathbf{G}$ *je N-grupa;*

(3) *Svaka maksimalna podgrupa grupe* $\mathbf{G}$ *je normalna;*

(4) $\mathbf{G}' \leq \mathrm{Fr}(\mathbf{G})$.

**Dokaz**. Dovoljno je samo da dokažemo npr. (3) $\Longrightarrow$ (1). Pretpostavimo da važi (3) ali ne i (1). Tada je, za neku normalnu podgrupu $\mathbf{N}$ grupe $\mathbf{G}$, $\mathbf{G}/\mathbf{N}$ konačna grupa koja nije nilpotentna. Prema 48.28 neka maksimalna podgrupa grupe $\mathbf{G}/\mathbf{N}$ nije normalna – neka je to $\mathbf{K}/\mathbf{N}$. Ali onda je $\mathbf{K}$ maksimalna podgrupa grupe $\mathbf{G}$ koja nije normalna (8.7), kontradikcija.□



# 53 Konačne poluproste grupe

Konačnim rešivim grupama su, da tako kažemo, "suprotstavljene" konačne poluproste grupe.

**Definicija 53.1** *Grupa je poluprosta akko je jedinična podgrupa njena jedina rešiva normalna podgrupa.*

**Lema 53.2** *Grupa je poluprosta akko je jedinična podgrupa njena jedina Abelova normalna podgrupa.*

**Dokaz**. Direktna posledica leme 4.34 i činjenice da je u rešivoj grupi $\mathbf{G}$ čiji je izvodni lanac dužine $n$ ($\mathbf{G}^{(n)} = \mathbf{E}$ i $\mathbf{G}^{(n-1)} \neq \mathbf{E}$), podgrupa $\mathbf{G}^{(n-1)}$ Abelova karakteristična (štaviše potpuno invarijantna) podgrupa.□

**Lema 53.3** *Svaka konačna grupa je ekstenzija rešive grupe poluprostom grupom.*

**Dokaz**. Neka je $\mathbf{G}$ konačna grupa, a $\mathbf{H}$ njena jedinstvena maksimalna rešiva normalna podgrupa (49.12($a$)). Tada je $\mathbf{G}/\mathbf{H}$ poluprosta, jer ako bi $\mathbf{K}/\mathbf{H}$ bila njena nejedinična normalna rešiva podgrupa, onda bi prema 8.7 $\mathbf{K}$ bila normalna podgrupa grupe $\mathbf{G}$ koja strogo sadrži $\mathbf{H}$ i koja je još uz to rešiva (kao ekstenzija rešive grupe rešivom grupom – 49.6).□

Prethodna lema generalno važi za sve grupe koje imaju maksimalnu normalnu rešivu podgrupu (koja je onda i jedinstvena).

**Lema 53.4** *Konačna potpuno razloživa grupa bez centra je poluprosta.*

**Dokaz**. Neka je $\mathbf{G}$ konačna potpuno razloživa grupa bez centra. Pretpostavimo da je $\mathbf{H}$ njena nejedinična normalna rešiva podgrupa. $\mathbf{H}$ je prema 10.29 i sama potpuno razloživa grupa, pa je minimalna normalna podgrupa podgrupe $\mathbf{H}$, a to je neka elementarna Abelova $p$-grupa (49.18), direktni sumand podgrupe $\mathbf{H}$, dakle i grupe $\mathbf{G}$, protivno pretpostavci da je $\mathbf{Z}(\mathbf{G}) = \mathbf{E}$.□

**Lema 53.5** *Normalna podgrupa konačne poluproste grupe je i sama poluprosta.*

**Dokaz**. Direktna posledica leme 4.34 i korolara 49.13 (jasno, jedinstvena maksimalna rešiva normalna podgrupa je karakteristična).□

**Lema 53.6** *Neka je* $\mathbf{G}$ *konačna nejedinična poluprosta grupa. Tada važi:*

($a$) *Maksimalna potpuno razloživa normalna podgrupa* $\mathbf{H}$ *grupe* $\mathbf{G}$ *(dozvoljavamo mogućnost da je* $\mathbf{H}$ *baš* $\mathbf{G}$*) je nejedinična;*

($b$) $\mathbf{C}(\mathbf{H}) = \mathbf{E}$.

**Dokaz.** ($a$) Očigledno, $\mathbf{H}$ je bez centra (jer je $\mathbf{G}$ poluprosta grupa). Dokaz tvrđenja je indukcijom po redu grupe $\mathbf{G}$. Prema prethodnoj lemi, ako je $k$ ($> 1$) najmanji prirodan broj za koji postoji poluprosta (nejedinična) grupa reda $k$, onda je svaka poluprosta grupa reda $k$ i prosta, dakle jednaka svojoj maksimalnoj potpuno razloživoj normalnoj podgrupi. Pretpostavimo dalje da je tvrđenje tačno za sve (nejedinične) poluproste grupe reda manjeg od $|G| = n$ ($> k$). Ako je $\mathbf{G}$ prosta grupa, nema ničeg novog. Ako je pak $\mathbf{K}$ netrivijalna normalna podgrupa grupe $\mathbf{G}$, prema induktivnoj hipotezi je (s obzirom da je i $\mathbf{K}$ poluprosta) maksimalna potpuno razloživa normalna podgrupa grupe $\mathbf{K}$ različita od nejedinične. No, kao karakteristična podgrupa (pod)grupe $\mathbf{K}$ ona je i normalna podgrupa grupe $\mathbf{G}$.

($b$) Prema 4.10 je $\mathbf{C(H)}$ normalna podgrupa grupe $\mathbf{G}$, stoga i poluprosta. Jasno, $\mathbf{C(H)} \cap \mathbf{H} = \mathbf{Z(H)} = \mathbf{E}$, pa je $\mathbf{H} \cdot \mathbf{C(H)} = \mathbf{H} \times \mathbf{C(H)}$. Prema prethodnoj tački, ukoliko bi centralizator podgrupe $\mathbf{H}$ bio nejedinična grupa, njegova maksimalno potpuno razloživa normalna podgrupa, neka je to $\mathbf{N}$, bila bi normalna podgrupa grupe $\mathbf{G}$, suprotno pretpostavci da je $\mathbf{H}$ maksimalna potpuno razloživa normalna podgrupa grupe $\mathbf{G}$ ($\mathbf{H} < \mathbf{H} \times \mathbf{N}$ – 10.30, 11.10).□

U nastavku izvodimo karakterizaciju konačnih poluprostih grupa "do na konačne potpuno razložive grupe i njihove grupe automorfizama".

**Lema 53.7** *Neka je $\mathbf{G}$ konačna poluprosta grupa i $\mathbf{H}$ njena maksimalna potpuno razloživa normalna podgrupa. Tada je $\mathbf{H} \cong \mathbf{Inn(H)}$, a grupa $\mathbf{G}$ je izomorfna nekoj podgrupi grupe $\mathbf{Aut(H)}$ koja sadrži $\mathbf{Inn(H)}$.*

**Dokaz.** Kako je $\mathbf{H}$ bez centra, imamo: $\mathbf{Inn(H)} \cong \mathbf{H/Z(H)} \cong \mathbf{H}$ (8.21). Uopšte je preslikavanje $\varphi : G \longrightarrow Aut(\mathbf{H})$, gde je $(g)\varphi \stackrel{\text{def}}{=} u_g|_H$, utapanje grupe $\mathbf{G}$ u $\mathbf{Aut(H)}$; injektivnost je posledica tačke ($b$) prethodne leme: $u_a|_H = u_b|_H$ akko je $ba^{-1} \in C(\mathbf{H}) = \{e\}$.□

**Lema 53.8** *Neka je $\mathbf{H}$ konačna potpuno razloživa grupa bez centra. Tada je svaka podgrupa grupe $\mathbf{Aut(H)}$ koja sadrži $\mathbf{Inn(H)}$ poluprosta grupa, a $\mathbf{Inn(H)}$ je njena maksimalna potpuno razloživa normalna podgrupa.*

**Dokaz.** Uočimo prvo da je $\mathbf{C_{Aut(H)}(Inn(H))} = \mathbf{E}$. Zaista, ako je $\varphi$ ($\in Aut(\mathbf{H})$) element centralizatora podgrupe $\mathbf{Inn(H)}$, onda je $a^{-1} \cdot (b)\varphi \cdot a = ((a)\varphi)^{-1} \cdot (b)\varphi \cdot (a)\varphi$ za svako $a, b \in H$ (zbog $\varphi \circ u_a = u_a \circ \varphi$), pa je $(a)\varphi \cdot a^{-1} \in Z(\mathbf{H}) = \{e\}$ (za svako $a \in H$), dakle $\varphi = \imath$.

Neka je $\mathbf{\Gamma}$ podgrupa grupe $\mathbf{Aut(H)}$ koja sadrži $\mathbf{Inn(H)}$ i $\mathbf{\Delta}$ njena rešiva normalna podgrupa. Tada je $\mathbf{Inn(H)} \cap \mathbf{\Delta}$ rešiva normalna podgrupa grupe $\mathbf{Inn(H)}$ ($\cong \mathbf{H}$), znači jedinična podgrupa (53.4), pa je $\langle Inn(\mathbf{H}), \Delta \rangle = \mathbf{Inn(H)} \times \mathbf{\Delta}$ i $\mathbf{\Delta} \leq \mathbf{C_{Aut(H)}(Inn(H))} = \mathbf{E}$, tj. $\mathbf{\Delta} = \mathbf{E}$. Slično sledi i da je $\mathbf{Inn(H)}$ maksimalna potpuno razloživa normalna podgrupa grupe $\mathbf{\Gamma}$. Jer, ako bi bila strogo sadržana u nekoj potpuno razloživoj normalnoj podgrupi $\mathbf{\Lambda}$ grupe $\mathbf{\Gamma}$,



bila bi i njen netrivijalni direktni faktor; prema tome, centralizator podgrupe $\mathbf{Inn(H)}$ bi bio nejedinična grupa, kontradikcija.□

**Lema 53.9** *Neka je $\mathbf{H}$ konačna potpuno razloživa grupa bez centra. Tada su izomorfne podgrupe $\mathbf{\Gamma}$ i $\mathbf{\Delta}$ grupe $\mathbf{Aut(H)}$ koje sadrže $\mathbf{Inn(H)}$ i konjugovane.*

**Dokaz.** S obzirom da su $\mathbf{H}$ i $\mathbf{Inn(H)}$ izomorfne grupe, izomorfne su i grupe $\mathbf{Aut(H)}$ i $\mathbf{Aut(Inn(H))}$. Prema 2.10($e$), ako je $\Phi$ "prirodno" izomorfno preslikavanje grupe $\mathbf{H}$ na grupu $\mathbf{Inn(H)}$ ($(h)\Phi = u_h$), onda je $\overline{\Phi} : Aut(\mathbf{H}) \longrightarrow Aut(\mathbf{Inn(H)})$, gde je, za $\varphi \in Aut(\mathbf{H})$, $(\varphi)\overline{\Phi} = \Phi^{-1} \circ \varphi \circ \Phi$, izomorfno preslikavanje grupe $\mathbf{Aut(H)}$ na grupu $\mathbf{Aut(Inn(H))}$; primetimo da je

$$(u_h)((\varphi)\overline{\Phi}) = (u_h)(\Phi^{-1} \circ \varphi \circ \Phi) = u_{(h)\varphi} = \varphi^{-1} \circ u_h \circ \varphi \qquad (*);$$

za $a \in H$ je $(a)u_{(h)\varphi} = (h^{-1})\varphi \cdot a \cdot (h)\varphi = (h^{-1} \cdot (a)\varphi^{-1} \cdot h)\varphi = (((a)\varphi^{-1})u_h)\varphi = (a)(\varphi^{-1} \circ u_h \circ \varphi)$. Dalje, $\mathbf{Inn(H)}$ je prema prethodnoj lemi maksimalna potpuno razloživa normalna podgrupa svake od podgrupa $\mathbf{\Gamma}$, $\mathbf{\Delta}$, pa ako je $\Theta$ izomorfno preslikavanje podgrupe $\mathbf{\Gamma}$ na podgrupu $\mathbf{\Delta}$, tada je $\Theta_1 = \Theta|_{Inn(\mathbf{H})}$ automorfizam grupe $\mathbf{Inn(H)}$. Neka je $\overline{\mathbf{\Gamma}} = (\mathbf{\Gamma})\overline{\Phi}$, $\overline{\mathbf{\Delta}} = (\mathbf{\Delta})\overline{\Phi}$, $\overline{\mathbf{Inn(H)}} = (\mathbf{Inn(H)})\overline{\Phi}$. Preslikavanje $\overline{\Theta} : \overline{\mathbf{\Gamma}} \longrightarrow \overline{\mathbf{\Delta}}$ dato sa (za $\varphi \in \mathbf{\Gamma}$) $((\varphi)\overline{\Phi})\overline{\Theta} = ((\varphi)\Theta)\overline{\Phi}$ izomorfno je preslikavanje podgrupe $\overline{\mathbf{\Gamma}}$ na podgrupu $\overline{\mathbf{\Delta}}$ (grupe $\mathbf{Aut(Inn(H))}$). Pokazaćemo da je $\overline{\Theta}$ restrikcija unutrašnjeg automorfizma $u_{\Theta_1}$ ($\in Inn(\mathbf{Aut(Inn(H))})$) nad $\overline{\mathbf{\Gamma}}$, odnosno da su podgrupe $\overline{\mathbf{\Gamma}}$ i $\overline{\mathbf{\Delta}}$ konjugovane, a onda su konjugovane i podgrupe $\mathbf{\Gamma}$ i $\mathbf{\Delta}$ (grupe $\mathbf{Aut(H)}$). Neka je $h \in H$ i $\varphi \in \Gamma$. Tada je:

$$(u_h)(((\varphi)\overline{\Phi})\overline{\Theta}) = (u_h)(((\varphi)\Theta)\overline{\Phi}) \stackrel{(*)}{=} (\varphi^{-1})\Theta \circ u_h \circ (\varphi)\Theta$$

a i:

$$(u_h)(\Theta_1^{-1} \circ (\varphi)\overline{\Phi} \circ \Theta_1) = (((u_h)\Theta_1^{-1})(\varphi)\overline{\Phi})\Theta_1 \stackrel{(*)}{=}$$

$$(\varphi^{-1} \circ (u_h)\Theta_1^{-1} \circ \varphi)\Theta_1 = (\varphi^{-1} \circ (u_h)\Theta^{-1} \circ \varphi)\Theta = (\varphi^{-1})\Theta \circ u_h \circ (\varphi)\Theta;$$

(koristili smo: $\varphi^{-1} \circ (u_h)\Theta_1^{-1} \circ \varphi = \varphi^{-1} \circ (u_h)\Theta^{-1} \circ \varphi \in Inn(\mathbf{H}) \lhd Aut(\mathbf{H})$). Dakle, $((\varphi)\overline{\Phi})\overline{\Theta} = \Theta_1^{-1} \circ (\varphi)\overline{\Phi} \circ \Theta_1$.□

Naredna teorema je direktna posledica poslednjih triju lema.

**Teorema 53.10** *Sve konačne poluproste grupe (do na izomorfizam) dobiće se ako se iz svih familija konjugovanih podgrupa, svih grupa automorfizama svih konačnih potpuno razloživih grupa bez centra, koje sadrže odgovarajuće podgrupe unutrašnjih automorfizama, uzme po jedan predstavnik.*

**Napomena.** Ranije smo pokazali da je svaka potpuno razloživa grupa direktni proizvod familije normalnih, prostih podgrupa (10.30). Naravno, ako je ta familija konačna, grupa ima glavni niz. Posebno, svaka konačna potpuno razloživa grupa ima glavni niz, te su prema teoremi Krull-Schmidta (11.39) svake

dve dekompozicije sa nerazloživim faktorima takve grupe centralno izomorfne (11.7). Ako je grupa u pitanju i bez centra, proizilazi da ima samo jednu dekompoziciju sa nerazloživim faktorima. Pošto je poznat i metod kako se dobija grupa automorfizama konačne potpuno razložive grupe bez centra – $\mathbf{G} = \mathbf{G}_1 \times \cdots \times \mathbf{G}_n$, gde su $\mathbf{G}_i$, $i = 1, \ldots, n$, proste grupe, koristeći se grupama automorfizama grupa $\mathbf{G}_i$, istraživanje konačnih poluprostih grupa se prema prethodnoj teoremi svodi na istraživanje konačnih prostih grupa (i njihovih grupa automorfizama). Na tom planu su postignuti brojni vredni rezultati; najznačajniji je svakako 49.35. On se pak, kao i neki od narednih rezultata, bazira na teoriji reprezentacija i karaktera konačnih grupa o čemu u ovoj knjizi neće biti reči. Za dokaze videti: [22], paragrafi 241 i 244, [23], paragraf 27 ili [45], paragrafi 18 i 20, ili naznačeno tvrđenje.

*Grupa je rešiva ako je reda $p^m q^n$, gde su $p$ i $q$ prosti brojevi.*

*Konačna grupa je rešiva ako njen red nije deljiv ni sa trećim stepenom nijednog prostog broja ni sa* 12.

*Konačna grupa je rešiva ako njen red nije deljiv kvadratom nijednog prostog broja* (16.51).

*Konačna grupa nije prosta ako neka njena familija konjugovanih elemenata ima $p^n$ elemenata, $p$ prost broj.*

*Konačna grupa $\mathbf{G}$ nije prosta ako ima pravu podgrupu $\mathbf{H}$ jednaku svom normalizatoru i takvu da je $\mathbf{H} \cap g^{-1}\mathbf{H}g = \mathbf{E}$ za svako $g \in G \setminus H$.*

*Konačna grupa nije prosta ako za neki prost broj $p$ ima Sylowu $p$-podgrupu koja je sadržana u centru svog normalizatora.*

## 54 $N$- i $\widetilde{N}$-grupe

U napomeni uz 48.36 rekli smo da je grupa u kojoj je svaka podgrupa dostižna $N$-grupa. Važi, međutim, generalno

**Lema 54.1** *Grupa $\mathbf{G}$ je $N$-grupa akko je svaka njena podgrupa term nekog rastućeg normalnog niza.*

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{G}$ $N$-grupa i $\mathbf{H}$ njena prava podgrupa. Definišimo rastući normalni lanac podgrupa na sledeći način: $\mathbf{H}_0 = \mathbf{E}$, $\mathbf{H}_1 = \mathbf{H}$, $\mathbf{H}_2 = \mathbf{N}(\mathbf{H}_1)$, i uopšte, ako već imamo podgrupe $\mathbf{H}_\beta$, $\beta < \alpha$, onda je $\mathbf{H}_\alpha = \mathbf{N}(\mathbf{H}_{\alpha-1})$ ako je $\alpha$ naslednik ordinal, odnosno $\mathbf{H}_\alpha = \bigcup_{\beta<\alpha} \mathbf{H}_\beta$ ako je $\alpha$ granični ordinal. Očigledno, ovako ćemo stići do same grupe $\mathbf{G}$, dakle i dobiti rastući normalni niz čiji je jedan term podgrupa $\mathbf{H}$.

($\Longleftarrow$) Neka je $\mathbf{H}$ prava podgrupa grupe $\mathbf{G}$ i $\mathcal{S} = \{\mathbf{H}_\alpha \mid \alpha \leq \mu\}$, $\mu$ ordinal, rastući normalni niz čiji je jedan term $\mathbf{H}$, recimo $\mathbf{H} = \mathbf{H}_\beta$. Ali tada termi $\mathbf{H}_\beta, \mathbf{H}_{\beta+1}$ čine skok i $\mathbf{H}_\beta$ je prava normalna podgrupa grupe $\mathbf{H}_{\beta+1}$; dakle, $\mathbf{H} = \mathbf{H}_\beta < \mathbf{H}_{\beta+1} \leq \mathbf{N}(\mathbf{H})$.□



**Korolar 54.2** *Podgrupe i faktor grupe $N$-grupe $\mathbf{G}$ su takođe $N$-grupe.*

**Dokaz.** Neka je $\mathbf{H}$ podgrupa grupe $\mathbf{G}$ i neka je $\mathbf{K}$ prava podgrupa grupe $\mathbf{H}$. Prema prethodnoj lemi je $\mathbf{K}$ term nekog rastućeg normalnog niza grupe $\mathbf{G}$ – $\{\mathbf{K}_\alpha \mid \alpha \leq \mu\}$, a prema lemi 47.6 sistem $\{\mathbf{K}_\alpha \cap \mathbf{H} \mid \alpha \leq \mu\}$ je rastući normalni sistem grupe $\mathbf{H}$, doduše možda ne pravi jer su moguća ponavljanja. Eliminisanjem "viška" ostaje nam rastući "pravi" normalni niz grupe $\mathbf{H}$ čiji je jedan term $\mathbf{K}$ ($= \mathbf{K} \cap \mathbf{H}$).

Analogno rezonujemo u slučaju faktor grupa. Ako je $\mathbf{N}$ normalna podgrupa grupe $\mathbf{G}$ i ako je $\mathbf{K}/\mathbf{N}$ prava podgrupa faktor grupe $\mathbf{G}/\mathbf{N}$ a $\{\mathbf{K}_\alpha \mid \alpha \leq \mu\}$ rastući normalni niz grupe $\mathbf{G}$ čiji je jedan term $\mathbf{K}$, onda je $\{(\mathbf{K}_\alpha \cdot \mathbf{N})/\mathbf{N} \mid \alpha \leq \mu\}$ rastući normalni sistem, moguće sa ponavljanjem, grupe $\mathbf{G}/\mathbf{N}$. Svakom skoku ovog sistema odgovara (jedinstven) skok u nizu $\{\mathbf{K}_\alpha \mid \alpha \leq \mu\}$. Zaista, ako termi $\mathbf{L}/\mathbf{N}$ i $\mathbf{M}/\mathbf{N}$ (datog sistema) čine skok i ako je $\delta$ najmanji ordinal skupa $\{\gamma \mid (\mathbf{K}_\gamma \cdot \mathbf{N})/\mathbf{N} = \mathbf{M}/\mathbf{N}\}$, tada je $\delta$ naslednik ordinal, $\mathbf{M}/\mathbf{N} = (\mathbf{K}_\delta \cdot \mathbf{N})/\mathbf{N}$ i $\mathbf{L}/\mathbf{N} = (\mathbf{K}_{\delta-1} \cdot \mathbf{N})/\mathbf{N}$; imamo u vidu da je $\mathbf{L}/\mathbf{N} = \bigcup_{\alpha<\delta} (\mathbf{K}_\alpha \cdot \mathbf{N})/\mathbf{N} = (\bigcup_{\alpha<\delta} \mathbf{K}_\alpha \cdot \mathbf{N})/\mathbf{N}$. Ponovo preostaje samo da se ukloni višak podgrupa (što neće indukovati pojavu novih skokova – familije jednakih terma imaju prvi i poslednji element).□

**Lema 54.3** *Svaka $N$-grupa je $S$-grupa.*

**Dokaz.** Neka je, za prost broj $p$, $\mathbf{P}$ Sylowa $p$-podgrupa $N$-grupe $\mathbf{G}$. Iz pretpostavke da $\mathbf{P}$ nije normalna podgrupa grupe $\mathbf{G}$ sledilo bi da je $\mathbf{N}(\mathbf{P})$ prava podgrupa grupe $\mathbf{G}$, a onda, s obzirom da je $\mathbf{G}$ $N$-grupa, prava podgrupa i svog normalizatora – $\mathbf{N}(\mathbf{N}(\mathbf{P}))$, kontradiktorno sa 16.14.□

**Lema 54.4** *Neka je $\mathbf{H}$ normalna podgrupa $N$-grupe $\mathbf{G}$. Ako $\mathbf{H}$ ima netrivijalni centar i ako je $\mathbf{G}/\mathbf{H}$ ciklična grupa, onda i $\mathbf{G}$ ima netrivijalni centar.*

**Dokaz.** Neka je faktor grupa $\mathbf{G}/\mathbf{H}$ generisana elementom $aH$. Centar podgrupe $\mathbf{H}$ je normalna podgrupa grupe $\mathbf{G}$ (4.34), a $\mathbf{K} = \langle Z(\mathbf{H}) \cup \{a\}\rangle$ je, kao podgrupa $N$-grupe, $N$-grupa. Stoga, ili je $Z(\mathbf{H}) \subseteq \langle a\rangle$ (u kom slučaju je $\mathbf{K} = \langle a\rangle$) ili je $\langle a\rangle$ prava podgrupa svog normalizatora u $\mathbf{K}$ – $\mathbf{N}_\mathbf{K}(\langle a\rangle)$. Kako je $K = \{a^m b \mid b \in Z(\mathbf{H}), m \in Z\}$, proizilazi da je, nezavisno od slučaja, barem jedan nejedinični element iz $Z(\mathbf{H})$ u $\mathbf{N}_\mathbf{K}(\langle a\rangle)$; neka je to element $c$. Ako je $[c, a] = e$, tj. $ca = ac$, onda je $c \in Z(\mathbf{G})$ (elementi iz $\mathbf{G}$ su oblika $a^n h$, $h \in H$, $n \in Z$); ako je $e \neq [c, a] = c^{-1}a^{-1}ca \in Z(\mathbf{H}) \cap \langle a\rangle$, tada je $[c, a]$ nejedinični element centra grupe $\mathbf{G}$.□

**Lema 54.5** *Neka su $a$ i $b$ elementi $N$-grupe $\mathbf{G}$ i neka je $b_0 = b$, $b_1 = [b_0, a]$ ($= [b, a]$) i generalno (za svaki prirodan broj $k$) $b_{k+1} = [b_k, a] = [b, \underbrace{a, \ldots, a}_{k+1}]$. Tada je $b_n = e$ za neki prirodan broj $n$.*

**Dokaz**. Pretpostavimo suprotno i neka je $\mathbf{A}_0 = \mathbf{E}$, $\mathbf{A}_1 = \langle a \rangle$, ..., $\mathbf{A}_\alpha$, ..., $\mathbf{A}_\mu = \mathbf{G}$ rastući normalni niz grupe $\mathbf{G}$. Neka je dalje, za svako $k \in \omega$, $\mathbf{A}_{\alpha_k}$ prvi term niza čiji je element $b_k$. Jasno, $\alpha_k$ je nasledni ordinal veći od 1 ($b_k \in \langle a \rangle$ bi impliciralo: $b_{k+1} = [b_k, a] = e$). Prema tome, $a \in A_{\alpha_k - 1}$ i pošto je $\mathbf{A}_{\alpha_k - 1}$ normalna podgrupa grupe $\mathbf{A}_{\alpha_k}$, to je $b_{k+1} = b_k^{-1} a^{-1} b_k \cdot a \in A_{\alpha_k - 1}$; znači, $\alpha_k > \alpha_{k+1}$. Dobili smo, dakle, beskonačan opadajući niz ordinala, kontradikcija.□

**Definicija 54.6** *Grupa je $\tilde{N}$-grupa akko je svaka njena podgrupa term nekog normalnog sistema.*

**Lema 54.7** *$\tilde{N}$-grupa koja ispunjava uslov minimalnosti podgrupa je $N$-grupa.*

**Lema 54.8** *Podgrupe i faktor grupe $\tilde{N}$-grupe su takođe $\tilde{N}$-grupe.*

**Dokaz**. U osnovi je simulacija dokaza leme 54.2.□

**Lema 54.9** *Grupa $\mathbf{G}$ je $\tilde{N}$-grupa akko ispunjava uslov, označimo ga sa $\mathcal{D}'$: svaka maksimalna podgrupa (ma koje) podgrupe $\mathbf{A}$ grupe $\mathbf{G}$ je i normalna podgrupa grupe $\mathbf{A}$.*

**Dokaz**. ($\Longrightarrow$) Neka je $\mathbf{G}$ $\tilde{N}$-grupa, $\mathbf{A}$ podgrupa grupe $\mathbf{G}$, $\mathbf{B}$ maksimalna podgrupa grupe $\mathbf{A}$ i neka je $\{\mathbf{A}_\alpha \mid \alpha \in \Omega\}$ normalni sistem grupe $\mathbf{A}$ čiji je jedan term $\mathbf{B}$ (prema prethodnoj lemi je i $\mathbf{A}$ $\tilde{N}$-grupa). No, u tom sistemu $\mathbf{A}$ i $\mathbf{B}$ čine skok (jer među njima nema podgrupa), pa je $\mathbf{B}$ i normalna podgrupa grupe $\mathbf{A}$.

($\Longleftarrow$) Neka grupa $\mathbf{G}$ ispunjava uslov $\mathcal{D}'$ i neka je $\mathbf{A}$ njena prava nejedinična podgrupa. Ako je $\mathbf{A}$ i normalna podgrupa, onda je, trivijalno, term normalnog sistema $\mathbf{E} < \mathbf{A} < \mathbf{G}$. Ukoliko nije, formiramo potpuno proširenje prethodnog, sada samo uređenog sistema, koje opet nema pravih proširenja. Postupak je u osnovi analogan postupku dobijanja kompozicionog od normalnog sistema (47.5). Neka je $\mathcal{S}_0 = \{\mathbf{E}, \mathbf{A}, \mathbf{G}\}$. $\mathbf{A}$ nije maksimalna podgrupa grupe $\mathbf{G}$ (inače bismo imali $\mathbf{A} \lhd \mathbf{G}$), pa postoji uređeni sistem $\mathcal{S}_1$ koji je pravo proširenje sistema $\mathcal{S}_0$. Pretpostavimo da smo za sve ordinale $\beta < \alpha$ formirali uređene sisteme $\mathcal{S}_\beta$, gde je, za $\gamma < \beta\ (< \alpha)$, $\mathcal{S}_\gamma \subset \mathcal{S}_\beta$. Ako je $\alpha$ nasledni ordinal i $\mathcal{S}_{\alpha-1}$ nema pravih proširenje, postupak je završen; u suprotnom, $\mathcal{S}_\alpha$ je neko pravo proširenje uređenog sistema $\mathcal{S}_{\alpha-1}$, Ako je $\alpha$ granični ordinal, u kom slučaju podrazumevamo i da svaki sistem $\mathcal{S}_\beta$, $\beta < \alpha$, ima pravih proširenja (tj. drugim rečima, da lanac $\mathcal{S}_0 \subset \cdots \subset \mathcal{S}_\gamma \subset \cdots \subset \mathcal{S}_\beta \subset \cdots$ nije postao stacionaran), onda je $\mathcal{S}_\alpha = \bigcup_{\beta<\alpha} \mathcal{S}_\beta$. Konačno, za neki ordinal $\mu$ proces se završava: $\mathcal{S}_\mu = \mathcal{S}_{\mu+1} = \cdots$ i $\mathcal{S} = \mathcal{S}_\mu$ je uređeni sistem bez pravih proširenja. Evidentno, to je i potpun sistem, a ako njegovi termi $\mathbf{B}$, $\mathbf{C}$ čine skok, tada je $\mathbf{B}$ maksimalna podgrupa grupe $\mathbf{C}$, dakle, prema uslovu $\mathcal{D}'$ i normalna. U pitanju je, znači, normalan sistem (čiji je jedan term $\mathbf{A}$).□



**Lema 54.10** *Ako grupa $\mathbf{G}$ ima svojstvo $\tilde{N}$ lokalno (svaka konačno generisana podgrupa je $\tilde{N}$-grupa), onda je i $\tilde{N}$-grupa.*

**Dokaz**. Neka su $\mathbf{A}$ i $\mathbf{B}$ podgrupe grupe $\mathbf{G}$, koja ima svojstvo $\tilde{N}$ lokalno, i neka je $\mathbf{B}$ maksimalna podgrupa grupe $\mathbf{A}$. Pretpostavimo da $\mathbf{B}$ nije normalna podgrupa grupe $\mathbf{A}$. Tada, za neke elemente $a \in A \setminus B$ i $b \in B$, $c = a^{-1}ba \notin B$. Stoga je $\langle B \cup \{c\} \rangle = \mathbf{A}$, pa je, za neke elemente $b_1, \ldots, b_k \in B$, $a \in \langle b_1, \ldots, b_k, c \rangle = H$. Posebno, $a \in \langle H, b \rangle = K$ (ali $a \notin K \cap B$). Ako je $\mathbf{M}$ maksimalna podgrupa grupe $\mathbf{K}$ koja sadrži $\mathbf{K} \cap \mathbf{B}$ i ne sadrži element $a$, onda je, s obzirom da je $\mathbf{K}$ $\tilde{N}$-grupa, $\mathbf{M}$ normalna podgrupa grupe $\langle M, a \rangle$ ($\leq \mathbf{K}$). Prema tome, ($a^{-1}ba =$) $c \in M$, a tada i $a \in M$, kontradikcija.

Drugi dokaz ove leme je dat u 59.16.□

## 55 Generalno nilpotentne grupe

Neke od sistema podgrupa uvedenih u paragrafu 47 koristimo za definisanje novih klasa grupa.

**Definicija 55.1** *Invarijantni sistem podgrupa $\mathcal{S} = \{\mathbf{H}_\alpha \mid \alpha \in \Omega\}$ grupe $\mathbf{G}$ (47.4) je centralni sistem akko je za svaki par podgrupa $\mathbf{H}_\alpha$, $\mathbf{H}_{\alpha+1}$ koje formiraju skok $[\mathbf{H}_{\alpha+1}, \mathbf{G}] \leq \mathbf{H}_\alpha$ (tj. $\mathbf{H}_{\alpha+1}/\mathbf{H}_\alpha \leq \mathbf{Z}(\mathbf{G}/\mathbf{H}_\alpha)$).*

*Centralni dobro uređen sistem (sada je $\mathcal{S} = \{\mathbf{H}_\alpha \mid \alpha \leq \mu\}$, $\mu$ - ordinal) zove se rastući centralni niz.*

*Grupa koja ima bar jedan centralni sistem zove se $Z$-grupa. Grupa čiji je svaki glavni sistem centralni zove se $\overline{Z}$-grupa.*

*Grupa koja ima bar jedan rastući centralni niz zove se $ZA$-grupa. Grupa koja ima centralni sistem dobro uređen naniže zove se $ZD$-grupa.*

Jasno, za grupe koje ispunjavaju uslov minimalnosti podgrupa svojstva $Z$ i $ZA$ su ekvivalentna.

**Lema 55.2** *Konačna grupa je $Z$-, $\overline{Z}$-, $ZA$-, $ZD$-grupa akko je nilpotentna.*

**Dokaz**. Videti 48.2, a treba li reći, produženje centralnog niza je centralni niz: ako su podgrupe $\mathbf{K}$ i $\mathbf{M}$ novi termi produženog centralnog niza koji čine skok i koji su umetnuti između terma polaznog centralnog niza $\mathbf{H}_\alpha$ i $\mathbf{H}_{\alpha+1}$ tada imamo:

$$[\mathbf{M}, \mathbf{G}] \leq [\mathbf{H}_{\alpha+1}, \mathbf{G}] \leq \mathbf{H}_\alpha \leq \mathbf{K}.\square$$

**Lema 55.3** *Svaka podgrupa i svaka faktor grupa $ZA$-grupe je $ZA$-grupa;*

**Dokaz**. Neka je $\mathbf{K}$ prava podgrupa $ZA$-grupe $\mathbf{G}$ i neka je $\{\mathbf{H}_\alpha \mid \alpha \leq \mu\}$ rastući centralni niz grupe $\mathbf{G}$. Tada je $\{\mathbf{K}_\alpha\ (= \mathbf{K} \cap \mathbf{H}_\alpha) \mid \alpha \leq \mu\}$, uslovno rečeno, rastući centralni niz grupe $\mathbf{K}$, moguće s ponavljanjem. Svakom skoku

ovog niza odgovara (jedinstveni) skok u nizu $\{\mathbf{H}_\alpha \mid \alpha \leq \mu\}$. Jer, neka ga čine podgrupe $\mathbf{K}_\alpha$ i $\mathbf{K}_\beta$ i neka je $\delta$ najmanji element skupa ordinala $\{\gamma \leq \mu \mid \mathbf{K}_\beta = \mathbf{K}_\gamma\}$. Tada je $\delta$ nasledni ordinal i $\mathbf{K}_\alpha = \mathbf{K}_{\delta-1}$ (imamo u vidu: $\bigcup_{\varepsilon<\delta}(\mathbf{H}_\varepsilon \cap \mathbf{K}) = (\bigcup_{\varepsilon<\delta} \mathbf{H}_\varepsilon) \cap \mathbf{K}$). Kako je, dalje, $[\mathbf{H}_\delta, \mathbf{G}] \leq \mathbf{H}_{\delta-1}$, to je i $[\mathbf{K}_\delta, \mathbf{K}] \leq \mathbf{K}_{\delta-1}$ $(= \mathbf{K} \cap \mathbf{H}_{\delta-1})$. Eliminisanjem "viška" podgrupa, pri čemu se ne stvaraju novi skokovi, ostaje nam na raspolaganju rastući centralni niz grupe $\mathbf{K}$.

U slučaju faktor grupe $\mathbf{G}/\mathbf{N}$ krećemo od rastućeg normalnog niza, moguće s ponavljanjem (utoliko bi bilo bolje reći neopadajućeg niza) $\{(\mathbf{H}_\alpha\mathbf{N})/\mathbf{N} \mid \alpha \leq \mu\}$. Opet svakom skoku odgovara (jedinstven) skok u rastućem centralnom nizu $\{\mathbf{H}_\alpha \mid \alpha \leq \mu\}$ – rezonujemo kao i u prethodnom slučaju, s tim što sada koristimo: $\bigcup_{\varepsilon<\delta}(\mathbf{H}_\varepsilon \cdot \mathbf{N})/\mathbf{N} = (\bigcup_{\varepsilon<\delta} \mathbf{H}_\varepsilon \cdot \mathbf{N})/\mathbf{N}$.□

**Lema 55.4** *Grupa je $ZA$-grupa akko njen transfinitno produženi viši centralni lanac stiže do cele grupe.*

**Dokaz.** Pravac ($\Longleftarrow$) je (više nego) jasan; po samoj definiciji transfinitno produženje višeg centralnog lanca koje stiže do "cele" grupe postaje rastući centralni niz.

($\Longrightarrow$) Neka je $\{\mathbf{H}_\alpha \mid \alpha \leq \mu\}$ rastući centralni niz grupe $\mathbf{G}$ ($\mathbf{H}_0 = \mathbf{E}$, $\mathbf{H}_\mu = \mathbf{G}$, $[\mathbf{H}_{\alpha+1}, \mathbf{G}] \leq \mathbf{H}_\alpha$). Transfinitnom indukcijom se proverava da je $\mathbf{H}_\alpha \leq \zeta_\alpha\mathbf{G}$ za svako $\alpha \leq \mu$. Već imamo: $\mathbf{H}_0 = \zeta_0\mathbf{G} = \mathbf{E}$. Pretpostavimo da je tvrđenje tačno za sve ordinale $\gamma < \alpha$. Ako je $\alpha$ granični ordinal, slučaj je trivijalan, a ako je $\alpha$ nasledni ordinal, dokaz imamo u 48.2 ($(1) \Longrightarrow (3)$).□

**Lema 55.5** *(a) Svaka $Z$-grupa ima invarijantni sistem sa cikličnim faktorima;*

*(b) Svaka $ZA$-grupa ima rastući invarijantni niz sa cikličnim faktorima.*

**Dokaz.** U osnovi oba tvrđenja je očigledna činjenica da svaka Abelova grupa ima rastući invarijantni niz sa cikličnim faktorima. Neka je npr. $\{\mathbf{H}_\alpha \mid \alpha \in \Omega\}$ centralni sistem $Z$-grupe $\mathbf{G}$. Za svake dve podgrupe $\mathbf{H}_\beta$ i $\mathbf{H}_{\beta+1}$ koje čine skok postoji rastući ivarijantni niz sa cikličnim faktorima faktor grupe $\mathbf{H}_{\beta+1}/\mathbf{H}_\beta$, recimo $\{\mathbf{K}_{\beta,\gamma} \mid 0 \leq \gamma \leq \mu_\beta\}$, $\mu_\beta$ – ordinal. Sve podgrupe $\mathbf{K}_{\beta,\gamma}$ su normalne u grupi $\mathbf{G}$ (jer je $\mathbf{H}_{\beta+1}/\mathbf{H}_\beta \leq \mathbf{Z}(\mathbf{G}/\mathbf{H}_\beta)$) i, jasno, za svaki par susednih ordinala $\gamma, \gamma+1 \leq \mu_\beta$, faktor grupa $\mathbf{K}_{\beta,\gamma+1}/\mathbf{K}_{\beta,\gamma}$ je ciklična. Preostaje, znači, samo da se polazni sistem proširi umetanjem između svih podgrupa koje čine skok, $\mathbf{H}_\beta$, $\mathbf{H}_{\beta+1}$, rastući niz podgrupa $\mathbf{K}_{\beta,\gamma}$, $0 < \gamma < \mu_\beta$.□

Obrát ne važi. Najjednostavniji kontraprimer je grupa $\mathbf{S}_3$. U svakom slučaju imamo

**Lema 55.6** *Ako grupa $\mathbf{G}$ ima invarijantni sistem sa cikličnim faktorima, tada je njena izvodna podgrupa $Z$-grupa.*



**Dokaz.** Neka je $\mathcal{S} = \{\mathbf{H}_\alpha \mid \alpha \in \Omega\}$ invarijantni sistem grupe $\mathbf{G}$ sa cikličnim faktorima. Možemo odmah pretpostaviti da su svi faktori konačne ciklične grupe; u suprotnom bismo, ako je, recimo, $\mathbf{H}_{\alpha+1}/\mathbf{H}_\alpha$ beskonačna ciklična grupa, mogli između $\mathbf{H}_\alpha$ i $\mathbf{H}_{\alpha+1}$ umetnuti beskonačno mnogo invarijantnih podgrupa grupe $\mathbf{G}$, čiji je presek $\mathbf{H}_\alpha$, a koje daju konačne ciklične faktore (imamo u vidu npr. niz podgrupa: $\mathbf{Z} > n\mathbf{Z} > n^2\mathbf{Z} \cdots > n^k\mathbf{Z} > \cdots > \mathbf{O}$, gde je $n > 1$, $n^k\mathbf{Z}/n^{k+1}\mathbf{Z}$ ciklična grupa reda $n$ i $\bigcap_{k=1}^{\infty} n^k\mathbf{Z} = \mathbf{O}$). Prema 47.6 sistem $\mathcal{T}'$ nastao od $\mathcal{T} = \{\mathbf{K}_\alpha = \mathbf{G}' \cap \mathbf{H}_\alpha \mid \alpha \in \Omega\}$ uklanjanjem eventualnog "viška" je invarijantni sistem sa konačnim cikličnim faktorima (pod)grupe $\mathbf{G}'$. Neka podgrupe $\mathbf{K}_\alpha$ i $\mathbf{K}_{\alpha+1}$ sistema $\mathcal{T}'$ čine skok i neka je $\mathbf{K}_{\alpha+1}/\mathbf{K}_\alpha = \langle aK_\alpha \rangle$. Za svaki element $b$ grupe $\mathbf{G}$ postoji neki prirodan broj $m_b$ takav da je $bK_\alpha \cdot aK_\alpha \cdot (bK_\alpha)^{-1} = (bab^{-1})K_\alpha = a^{m_b}K_\alpha$ (jer je $bab^{-1} \in K_{\alpha+1}$). Stoga je za bilo koje elemente $b, c$ grupe $\mathbf{G}$:

$$(bc)K_\alpha \cdot aK_\alpha \cdot (bc)^{-1}K_\alpha = bK_\alpha \cdot (cK_\alpha \cdot aK_\alpha \cdot c^{-1}K_\alpha) \cdot b^{-1}K_\alpha =$$

$$bK_\alpha \cdot a^{m_c}K_\alpha \cdot b^{-1}K_\alpha = (bK_\alpha \cdot aK_\alpha \cdot b^{-1}K_\alpha)^{m_c} = (a^{m_b}K_\alpha)^{m_c} = (a^{m_c}K_\alpha)^{m_b} =$$

$$cK_\alpha \cdot a^{m_b}K_\alpha \cdot c^{-1}K_\alpha = cK_\alpha \cdot (bK_\alpha \cdot aK_\alpha \cdot b^{-1}K_\alpha) \cdot c^{-1}K_\alpha = (cb)K_\alpha \cdot aK_\alpha \cdot (cb)^{-1}K_\alpha,$$

pa je $[b, c]K_\alpha$ permutabilno sa $aK_\alpha$, dakle i sa svim elementima faktor grupe $\mathbf{K}_{\alpha+1}/\mathbf{K}_\alpha$. Prema tome, $\mathbf{K}_{\alpha+1}/\mathbf{K}_\alpha$ je podgrupa centra grupe $\mathbf{G}'/\mathbf{K}_\alpha$ i $\mathcal{T}'$ je centralni sistem grupe $\mathbf{G}'$.□

**Korolar 55.7** *(Teorema Wendta). Svaka konačna superrešiva grupa je meta-nilpotentna.*

**Lema 55.8** *Svaka $ZA$-grupa je $N$-grupa.*

**Dokaz.** Neka je $\mathbf{G}$ $ZA$-grupa sa rastućim centralnim nizom $\{\mathbf{H}_\alpha \mid \alpha \leq \mu\}$, $\mathbf{K}$ prava podgrupa grupe $\mathbf{G}$ i neka je $\delta$ najmanji ordinal u skupu $\{\beta \leq \mu \mid H_\beta \not\subseteq K\}$. Jasno, $\delta$ je nasledni ordinal i $\mathbf{H}_{\delta-1} \leq \mathbf{K}$. No tada je $[\mathbf{H}_\delta, \mathbf{K}] \leq [\mathbf{H}_\delta, \mathbf{G}] \leq \mathbf{H}_{\delta-1} \leq \mathbf{K}$ i $\mathbf{H}_\delta \leq \mathbf{N}(\mathbf{K})$ (za svako $a \in K$ i svako $b \in H_\delta$ je $a^{-1}b^{-1}ab \in K$, tj. $b^{-1}ab \in aK = K$).□

S druge strane imamo, recimo, ovakvu vezu

**Lema 55.9** *Ako je normalna podgrupa $\mathbf{H}$ $N$-grupe $\mathbf{G}$ $ZA$-grupa i ako je $\mathbf{G}/\mathbf{H}$ ciklična grupa, onda je i $\mathbf{G}$ $ZA$-grupa.*

**Dokaz.** Prema lemi 54.4 $\mathbf{G}$ ima netrivijalni centar. Pretpostavimo da smo dobili članove transfinitno produženog centralnog lanca $\zeta_\beta\mathbf{G}$ za sve ordinale $\beta < \alpha$. Ako je $\alpha$ granični ordinal, uzimamo, naravno, $\zeta_\alpha\mathbf{G} = \bigcup_{\beta<\alpha} \zeta_\beta\mathbf{G}$. Ako je $\alpha$ nasledni ordinal i $\zeta_{\alpha-1}\mathbf{G} \neq \mathbf{G}$, razmatramo slučajeve: (1) $\mathbf{H} \leq \zeta_{\alpha-1}\mathbf{G}$; (2) $\mathbf{H}$ nije podgrupa grupe $\zeta_{\alpha-1}\mathbf{G}$. U prvom slučaju je $\mathbf{G}/\zeta_{\alpha-1}\mathbf{G}$ $(\cong (\mathbf{G}/\mathbf{H})/(\zeta_{\alpha-1}\mathbf{G}/\mathbf{H}))$ ciklična grupa, pa je $\zeta_\alpha\mathbf{G} = \mathbf{G}$. U drugom imamo,

prema drugoj teoremi o izomorfizmu: $(\mathbf{H}\cdot\zeta_{\alpha-1}\mathbf{G})/\zeta_{\alpha-1}\mathbf{G} \cong \mathbf{H}/(\mathbf{H}\cap\zeta_{\alpha-1}\mathbf{G})$, a $\mathbf{H}/(\mathbf{H}\cap\zeta_{\alpha-1}\mathbf{G})$ je, prema 55.3, $ZA$-grupa. Stoga $(\mathbf{H}\cdot\zeta_{\alpha-1}\mathbf{G})/\zeta_{\alpha-1}\mathbf{G}$ ima netrivijalni centar. Osim toga je $(\mathbf{G}/\zeta_{\alpha-1}\mathbf{G})/((\mathbf{H}\cdot\zeta_{\alpha-1}\mathbf{G})/\zeta_{\alpha-1}\mathbf{G})$ ($\cong \mathbf{G}/(\mathbf{H}\cdot\zeta_{\alpha-1}\mathbf{G})$) ciklična grupa, a $\mathbf{G}/\zeta_{\alpha-1}\mathbf{G}$ $N$-grupa. Ponovo prema 54.4 $\mathbf{G}/\zeta_{\alpha-1}\mathbf{G}$ ima netrivijalni centar, te je $\zeta_\alpha\mathbf{G} = (\mathbf{Z}(\mathbf{G}/\zeta_{\alpha-1}\mathbf{G}))\varphi^{-1}$, gde je $\varphi$ kanoničko homomorfno preslikavanje grupe $\mathbf{G}$ na faktor grupe $\mathbf{G}/\zeta_{\alpha-1}\mathbf{G}$, prava ekstenzija podgrupe $\zeta_{\alpha-1}\mathbf{G}$. Zaključujemo: transfinitno produženi centralni lanac stiže do grupe $\mathbf{G}$.□

Za naredne karakterizacije $ZA$-grupa potrebna nam je sledeća

**Lema 55.10** *Neka je $\mathbf{G}$ grupa sa svojstvom $(*)$: za proizvoljni element $a$ i ma koji niz elemenata $b_1, b_2, \ldots$, postoji prirodan broj $n$ (koji je u funkciji izbora elemenata i niza) za koji je $c_n \stackrel{\text{def}}{=} [\ldots[[a,b_1],b_2],\ldots,b_n] = e$. Tada važi:*

*(a) svaka faktor grupa grupe $\mathbf{G}$ ima svojstvo $(*)$;*

*(b) $\mathbf{G}$ ima netrivijalni centar.*

**Dokaz.** (*a*) Neka je $\mathbf{H}$ normalna podgrupa grupe $\mathbf{G}$. Jasno:

$$[\ldots[[aH,b_1H],b_2H],\ldots,b_nH] = [\ldots[[a,b_1],b_2],\ldots,b_n]H\ (= c_nH);$$

(*b*) Neka je $a$ ma koji nejedinični element grupe $\mathbf{G}$. Ako je $a$ u centru grupe, tvrđenje je dokazano; u suprotnom, postoji element $b_1$ takav da je $c_1 = [a,b_1] \neq e$. Ako ni $c_1$ nije u centru, postoji element $b_2$ za koji je $c_2 = [c_1,b_2] = [[a,b_1],b_2] \neq e$. Po uslovu leme ovaj proces ne može ići u nedogled, drugim rečima u konačno mnogo koraka stići ćemo do nejediničnog elementa koji je iz centra grupe.□

**Korolar 55.11** *Grupa je $ZA$-grupa akko ima svojstvo $(*)$ iz prethodne leme.*

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{G}$ $ZA$-grupa, $\{\mathbf{H}_\alpha \mid \alpha \leq \mu\}$ njen rastući centralni niz, $a$ (njen) nejedinični element i $b_1, b_2, \ldots$ proizvoljan niz (elemenata grupe). Pretpostavimo da su svi elementi $c_n = [\ldots[[a,b_1],b_2],\ldots,b_n]$ nejedinični i neka je $\delta \leq \mu$ najmanji ordinal takav da $\mathbf{H}_\delta$ sadrži bar jedan element niza $c_1, c_2, \ldots$, recimo $c_n$. Naravno, $\delta$ je nasledni ordinal, a $c_{n+1} = [c_n, b_{n+1}] \in [H_\delta, G] \subseteq H_{\delta-1}$, kontradikcija.

($\Longleftarrow$) Svojstvo $(*)$ direktno implicira da transfinitno produženje višeg centralnog lanca stiže do grupe $\mathbf{G}$. Grupa ima netrivijalni centar, njena faktor grupa $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ takođe, dakle, $\mathbf{Z}(\mathbf{G}) = \zeta_1\mathbf{G}$ je prava podgrupa (pod)grupe $\zeta_2\mathbf{G}$. Analogno, $\zeta_2\mathbf{G}$ je prava podgrupa grupe $\zeta_3\mathbf{G}$ i uopšte je $\zeta_\alpha\mathbf{G}$, ukoliko već nismo stigli do grupe $\mathbf{G}$, prava podgrupa grupe $\zeta_{\alpha+1}\mathbf{G}$ ($\zeta_{\alpha+1}\mathbf{G}/\zeta_\alpha\mathbf{G} = \mathbf{Z}(\mathbf{G}/\zeta_\alpha\mathbf{G}) \neq \mathbf{E}$).□

**Korolar 55.12** *Grupa je $ZA$-grupa akko je svaka njena prebrojiva podgrupa $ZA$-grupa.*



**Dokaz.** Neka $\mathbf{G}$ nije $ZA$-grupa i neka je za element $a$ i niz elemenata $b_1, b_2, \ldots$, svaki od elemenata $c_n = [\ldots[[a,b_1],b_2],\ldots,b_n]$, $n \geq 1$, različit od jediničnog. Tada je podgrupa $\mathbf{H}$ generisana skupom $\{a\} \cup \{b_n \mid n \geq 1\}$ prebrojiva i nije $ZA$-grupa.□

## 56 Lokalno nilpotentne grupe

Prema 48.5 (i napomeni uz definiciju 17.1, koju smo uostalom imali u vidu i u slučaju $\widetilde{N}$-lokalnog svojstva) grupa $\mathbf{G}$ je lokalno nilpotentna akko je svaka njena konačno generisana podgrupa nilpotentna.

**Lema 56.1** *Podgrupe i faktor grupe lokalno nilpotentne grupe su lokalno nilpotentne.*

**Dokaz.** Slučaj podgrupa je jako trivijalan; slučaj faktor grupa je trivijalan. Neka je $\mathbf{N}$ normalna podgrupa lokalno nilpotentne grupe $\mathbf{G}$ i neka je $\overline{\mathbf{K}}$ podgrupa faktor grupe $\overline{\mathbf{G}} = \mathbf{G}/\mathbf{N}$ generisana skupom $\{g_1N, \ldots, g_kN\}$ (dakle, $\overline{\mathbf{K}} = (\langle g_1, \ldots, g_k\rangle \cdot \mathbf{N})/\mathbf{N}$). Podgrupa $\mathbf{H} = \langle g_1, \ldots, g_k\rangle$ grupe $\mathbf{G}$ je nilpotentna, pa ima centralni niz $\mathbf{H} = \mathbf{H}_0 > \mathbf{H}_1 > \cdots > \mathbf{H}_n = \mathbf{E}$ (gde je, podsećamo se, svaka podgrupa $\mathbf{H}_i$ normalna podgrupa grupe $\mathbf{H}$ i $\mathbf{H}_{i-1}/\mathbf{H}_i \leq \mathbf{Z}(\mathbf{H}/\mathbf{H}_i)$, tj. $[\mathbf{H}_{i-1}, \mathbf{H}] \leq \mathbf{H}_i$). No tada je $\overline{\mathbf{K}} = \overline{\mathbf{K}}_0 = (\mathbf{H}\cdot\mathbf{N})/\mathbf{N} \geq (\mathbf{H}_1\cdot\mathbf{N})/\mathbf{N} \geq \cdots \geq (\mathbf{H}_n\cdot\mathbf{N})/\mathbf{N} = \overline{\mathbf{E}}$, uslovno rečeno jer su moguća ponavljanja, centralni niz (grupe $\overline{\mathbf{K}}$). Višak je lako ukloniti, a ostalo se direktno se proverava. Očigledno, $(\mathbf{H}_i\cdot\mathbf{N})/\mathbf{N} \lhd (\mathbf{H}\cdot\mathbf{N})/\mathbf{N}$, a isto tako je i $[(\mathbf{H}_{i-1}\cdot\mathbf{N})/\mathbf{N}, (\mathbf{H}\cdot\mathbf{N})/\mathbf{N}] \leq (\mathbf{H}_i\cdot\mathbf{N})/\mathbf{N}$ (za $a \in H_{i-1}$ i $b \in H$ je $[a,b] \in H_i$, te je i $[aN, bN] = [a,b]N \in (H_i\cdot N)/N$).□

**Lema 56.2** *Unija lanca i presek familije lokalno nilpotentnih grupa je lokalno nilpotentna grupa.*

**Lema 56.3** *Periodična lokalno nilpotentna grupa je lokalno konačna.*

**Dokaz.** Direktno prema 48.24. Ovo tvrđenje je posledica i tačke (*b*) leme 58.11.□

**Lema 56.4** *Lokalno nilpotentna torziono slobodna grupa je $R$-grupa.*

**Dokaz.** Direktno prema 48.42.□

**Lema 56.5** *Maksimalna podgrupa lokalno nilpotentne grupe je normalna.*

**Dokaz.** Neka je $\mathbf{G}$ lokalno nilpotentna grupa i $\mathbf{H}$ (jedna) njena maksimalna podgrupa. Pretpostavimo da $\mathbf{H}$ nije normalna podgrupa. Onda, posebno, $G' \not\leq \mathbf{H}$. Neka je $g \in G' \setminus H$. Pošto je $\mathbf{H}$ maksimalna podgrupa, to je

$\mathbf{G} = \langle g, H\rangle$. Neka je $g = [a_1, b_1]\cdot\ldots\cdot[a_m, b_m]$. Svaki od elemenata $a_i, b_i$, $i = 1,\ldots,m$, može se predstaviti kao proizvod stepena nekih elemenata iz $\mathbf{H}$ i elementa $g$; drugim rečima, za svako $a_i$ ($b_i$) postoji konačan podskup $A_i$ ($B_i$) skupa $H$ takav da je $a_i \in \langle g, A_i\rangle$ ($b_i \in \langle g, B_i\rangle$). Neka je $C = \bigcup_{i=1}^m A_i \cup \bigcup_{i=1}^m B_i = \{h_1,\ldots,h_n\}$ i neka je $\mathbf{H}_1 = \langle C\rangle$, $\mathbf{G}_1 = \langle g, C\rangle$. Prema uslovu leme je $\mathbf{G}_1$ nilpotentna grupa, i jasno, $g \in G_1' \setminus H_1$. Prema tome, $\mathbf{H}_1$ je prava podgrupa grupe $\mathbf{G}_1$ i to dostižna (prema napomeni datoj posle 48.36). Dalje, prema 48.23 postoji normalni niz podgrupa grupe $\mathbf{G}_1$ - $\mathbf{G}_1 = \mathbf{K}_0 > \mathbf{K}_1 > \cdots > \mathbf{K}_{s-1} > \mathbf{K}_s = \mathbf{H}_1$ - čiji su svi faktori ciklične grupe. Odatle proizilazi da je $\mathbf{G}_1' \le \mathbf{K}_1$, dakle $g \in \mathbf{K}_1$, pa je $\mathbf{G}_1 = \mathbf{K}_1$, kontradikcija. Tu na kraju mogli smo i ovako rezonovati. Neka je $\mathbf{M}$ maksimalna podgrupa grupe $\mathbf{G}_1$ koja sadrži $\mathbf{H}_1$ i u kojoj nije $g$ (podsećamo, egzistenciju takve podgrupe obezbeđuje lema Zorna). No, $\mathbf{M}$ je i uopšte maksimalna podgrupa nilpotentne grupe $\mathbf{G}_1$ ($g$ je element svake podgrupe grupe $\mathbf{G}_1$ koja strogo sadrži $\mathbf{M}$, a $C \subseteq M$), te je $\mathbf{G}_1' \le \mathbf{Fr}(\mathbf{G}_1) \le \mathbf{M}$, ali i $g \in G_1'$, kontradikcija.□

**Korolar 56.6** *Ako je* $\mathbf{G}$ *lokalno nilpotentna grupa, onda je* $\mathbf{G}' \le \mathbf{Fr}(\mathbf{G})$.

**Dokaz.** Neka je $\mathbf{H}$ maksimalna podgrupa lokalno nilpotentne grupe $\mathbf{G}$. Prema prethodnoj lemi je $\mathbf{H}$ normalna podgrupa, a jasno, $\mathbf{G}/\mathbf{H}$ je ciklična grupa prostog reda, pa je $\mathbf{G}' \le \mathbf{H}$).□

**Lema 56.7** *Lokalno nilpotentna grupa koja ispunjava uslov maksimalnosti podgrupa je nilpotentna.*

**Dokaz.** Jasno; prema 5.15, uslov maksimalnosti podgrupa implicira konačnu generisanost grupe.□

**Lema 56.8** *Neka je* $\mathbf{A}$ *podgrupa lokalno nilpotentne torziono slobodne grupe* $\mathbf{G}$. *Tada je* $I(\mathbf{A}) = \{g \in G \mid g^n \in A$ *za neki pozitivan prirodan broj* $n$ $(= n(g))\}$ *(gde je, podsećamo,* $\mathbf{I}(\mathbf{A})$ *izolator podgrupe* $\mathbf{A}$*).*

**Dokaz.** Obeležimo skup na desnoj strani sa $D$. Inkluzija $D \subseteq I(\mathbf{A})$ je jasna (po samoj definiciji izolovane podgrupe i izolatora podgrupe - 4.41, 4.44). Stoga je dovoljno da pokažemo da je skup $D$ domen izolovane podgrupe. Neka je, za $b, c \in G$ i pozitivne prirodne brojeve $m, n$, $b^m, c^n \in A$. Podgrupa $\mathbf{H} = \langle a, b\rangle$ je konačno generisana nilpotentna grupa i kako $b^m, c^n \in A \cap H$ ($\subseteq H$), prema 49.24 $\mathbf{A}\cap\mathbf{H}$ je podgrupa konačnog indeksa u $\mathbf{H}$. Dakle, neki pozitivan stepen svakog elementa grupe $\mathbf{H}$ leži u $\mathbf{A}$, pa je $bc, b^{-1} \in D$. Konačno, ako je $g^m \in D$ za pozitivan prirodan broj $m$, onda je opet, za neko pozitivno $n$, $(g^m)^n = g^{mn} \in A$ i $g \in D$.□

**Teorema 56.9** *U lokalno nilpotentnoj torziono slobodnoj grupi normalizator izolovane podgrupe je izolovana podgrupa.*



**Dokaz.** Neka je $\mathbf{G}$ lokalno nilpotentna torziono slobodna grupa i $\mathbf{A}$ njena izolovana podgrupa, pa pretpostavimo opet, kao u 48.43, da $\mathbf{N}(\mathbf{A})$ nije izolovana podgrupa. Ako je, za neko $m$ veće od 1, $g^m \in N(\mathbf{A})$ i $g \notin N(\mathbf{A})$, onda prateći dokaz teoreme 48.43 nalazimo element $a \in A$ takav da $g^{-1}ag \notin A$. Podgrupa $\mathbf{H} = \langle a, g\rangle$ je nilpotentna, $\mathbf{A}\cap\mathbf{H}$ je očigledno njena izolovana podgrupa, te je i $\mathbf{N}_{\mathbf{H}}(\mathbf{A}\cap\mathbf{H})$ izolovana podgrupa u $\mathbf{H}$ (48.43). Jasno, $g \notin N_{\mathbf{H}}(\mathbf{A}\cap\mathbf{H})$, ali $g^{-m}(A\cap H)g^m = g^{-m}Ag^m \cap g^{-m}Hg^m = A\cap H$, dakle $g^m \in N_{\mathbf{H}}(\mathbf{A}\cap\mathbf{H})$, kontradikcija.■

**Korolar 56.10** *Neka su* $\mathbf{A}$ *i* $\mathbf{B}$ *podgrupe lokalno nilpotentne torziono slobodne grupe* $\mathbf{G}$. *Ako je* $\mathbf{A}$ *normalna podgrupa grupe* $\mathbf{B}$, *tada je izolator podgrupe* $\mathbf{A}$ *normalna podgrupa izolatora podgrupe* $\mathbf{B}$.

**Dokaz.** Očigledno, $I(\mathbf{A}) \subseteq I(\mathbf{B})$, a za $b \in B$ je, prema 4.48, $b^{-1}\mathbf{I}(\mathbf{A})b = \mathbf{I}(b^{-1}\mathbf{A}b) = \mathbf{I}(\mathbf{A})$. Prema tome, $\mathbf{B} \le \mathbf{N}(\mathbf{I}(\mathbf{A}))$. Kako je $\mathbf{N}(\mathbf{I}(\mathbf{A}))$ izolovana podgrupa, to je $\mathbf{I}(\mathbf{B}) \le \mathbf{N}(\mathbf{I}(\mathbf{A}))$ i $\mathbf{I}(\mathbf{A}) \lhd \mathbf{I}(\mathbf{B})$.□

**Teorema 56.11** *Svaka ZA-grupa je lokalno nilpotentna.*

**Dokaz.** Ako je $\{\mathbf{H}_\alpha \mid \alpha \le \mu\}$, $\mu$ ordinal, rastući centralni niz $ZA$-grupe $\mathbf{G}$, onda ćemo $\mu$ zvati njegovom dužinom. Dokaz teoreme je indukcijom po dužini centralnog niza (kojim grupa raspolaže). Ako je ta dužina 1 (ili 0, kada je u pitanju jedinična grupa) stvar je jasna; Abelove grupe su (lokalno) nilpotentne. Pretpostavimo da je tvrđenje tačno za sve $ZA$-grupe koje imaju centralni niz dužine manje od $\mu$ i vratimo se na našu grupu $\mathbf{G}$ sa datim centralnim nizom dužine $\mu$. Neka je $\mathbf{H}$ njena podgrupa generisana skupom elemenata $\{g_1,\ldots,g_k\}$. Ako je $\mu$ prirodan broj, $\mathbf{G}$ je nilpotentna grupa i slučaj je trivijalan. Ako je $\mu$ granični ordinal, tada je $\mathbf{H} \le \mathbf{H}_\beta$ za neko $\beta < \mu$, $\mathbf{H}_\beta$ ima centralni niz dužine $\beta$ i po induktivnoj pretpostavci je lokalno nilpotentna grupa, pa je $\mathbf{H}$ nilpotentna. Ako je, konačno, $\mu$ beskonačan nasledni ordinal, onda se na jedinstven način predstavlja kao ordinalna suma (jednog) graničnog ordinala, recimo $\beta$, i (jednog) pozitivnog prirodnog broja, recimo $n$; dakle, $\mu = \beta + n$, gde je $+$ ordinalno sabiranje. Komutatora, u širem smislu reči, $[g_{i_1},\ldots,g_{i_{n+1}}] = [\ldots[[g_{i_1}, g_{i_2}], g_{i_3}],\ldots,g_{i_{n+1}}] \in \gamma_n G$, $g_{i_j} \in \{g_i,\ldots,g_k\}$, ima konačno mnogo i svi oni leže u $\mathbf{H}_\beta$, štaviše, pošto je $\beta$ granični ordinal, u nekoj podgrupi $\mathbf{H}_\gamma$, $\gamma < \beta$. Zaista, indukcijom po $r = 1,\ldots,n$ pokazuje se da je $\gamma_r\mathbf{G} \le \mathbf{H}_{\beta+(n-r)}$; naravno, $\gamma_1\mathbf{G} = \mathbf{G}' \le \mathbf{H}_{\beta+(n-1)}$ ($\mathbf{H}_{\beta+n}/\mathbf{H}_{\beta+(n-1)} = \mathbf{G}/\mathbf{H}_{\beta+(n-1)}$ je Abelova grupa), a ako je $\gamma_r\mathbf{G} \le \mathbf{H}_{\beta+(n-r)}$ za $r < n$, tada je $\gamma_{r+1}\mathbf{G} = [\gamma_r\mathbf{G}, \mathbf{G}] \le [\mathbf{H}_{\beta+(n-r)}, \mathbf{G}] \le \mathbf{H}_{\beta+(n-(r+1))}$ (46.21). Grupa $\mathbf{K} = \langle H_\gamma, g_1,\ldots,g_k\rangle$ ima pak centralni niz dužine manje od ili jednake $\gamma + n$ ($< \beta < \beta + n = \mu$), te je prema induktivnoj hipotezi lokalno nilpotentna, a $\mathbf{H} = \langle g_1,\ldots,g_k\rangle$ je nilpotentna grupa. Jer, za početni segment jednog takvog centralnog niza uzimamo što nam je već dato: $\mathbf{K}_0 = \mathbf{H}_0 < \mathbf{K}_1 = \mathbf{H}_1 < \cdots < \mathbf{K}_\gamma = \mathbf{H}_\gamma$ (za $\alpha < \gamma$ je $[\mathbf{K}_{\alpha+1}, \mathbf{K}] \le [\mathbf{H}_{\alpha+1}, \mathbf{G}] \le$

$\mathbf{H}_\alpha = \mathbf{K}_\alpha$, znači i $\mathbf{K}_{\alpha+1}/\mathbf{K}_\alpha \leq \mathbf{Z}(\mathbf{K}/\mathbf{K}_\alpha)$). Dalje prirodno definišemo: $\mathbf{K}_{\gamma+1} = (\mathbf{Z}(\mathbf{K}/\mathbf{K}_\gamma))\varphi_\gamma^{-1}$, gde je $\varphi_\gamma$ kanoničko homomorfno preslikavanje grupe $\mathbf{K}$ na faktor grupu $\mathbf{K}/\mathbf{K}_\gamma$; $\mathbf{K}_{\gamma+2} = (\mathbf{Z}(\mathbf{K}/\mathbf{K}_{\gamma+1}))\varphi_{\gamma+1}^{-1}$ itd. Ne zamarajući se diskusijom da li neki od elememata $g_1, \ldots, g_k$ upadaju u $\mathbf{K}_\gamma$ ili u $\mathbf{K}_{\gamma+1}$ ili ... (ili su već svi u $\mathbf{K}$), dokazujemo generalno: za $s = 1, \ldots, n$ je $[g_{i_1}, \ldots, g_{i_s}] \in K_{\gamma+(n+1-s)}$ (to će reći: svi elementi $g_1, \ldots, g_k$ su sigurno u $\mathbf{K}_{\gamma+n}$ ili, drugim rečima, na opisani način ćemo u najviše $n$ "skokova" stići od $\mathbf{K}_\gamma$ do $\mathbf{K}$). Iz $[g_{i_1}, \ldots, g_{i_{n+1}}] = [[g_{i_1}, \ldots, g_{i_n}], g_{i_{n+1}}] \in K_\gamma$ proizilazi: element $[g_{i_1}, \ldots, g_{i_n}]K_\gamma$ je permutabilan sa elementima $g_1K_\gamma, \ldots, g_kK_\gamma$ ($g_{i_k}$ je ma koji od elemenata $g_1, \ldots g_k$) koji generišu grupu $\mathbf{K}/\mathbf{K}_\gamma$, dakle, $[g_{i_1}, \ldots, g_{i_n}]K_\gamma \in Z(\mathbf{K}/\mathbf{K}_\gamma)$, odnosno, $[g_{i_1}, \ldots, g_{i_n}] \in (Z(\mathbf{K}/\mathbf{K}_\gamma))\varphi_\gamma^{-1} = \mathbf{K}_{\gamma+1}$. Induktivni korak bi bio puko ponavljanje pa ga i ne dajemo.■

Prethodnu teoremu ćemo iskoristiti za dokaz da je svaka $N$-grupa lokalno nilpotentna. Nameće se, normalno, pitanje redosleda koraka; jer, već je pokazano da je svaka $ZA$-grupa $N$-grupa (55.8) i tako gledano bilo bi prirodnije da se prvo pokazalo da su $N$-grupe lokalno nilpotentne. Ispostavlja se ipak da je izabrani put lakši (što naravno ostaje u domenu subjektivne procene).

**Lema 56.12** *Ako je* $\mathbf{H}$ *lokalno nilpotentna, normalna podgrupa* $N$*-grupe* $\mathbf{G}$ *i ako je* $\mathbf{G}/\mathbf{H}$ *ciklična grupa, tada je i* $\mathbf{G}$ *lokalno nilpotentna grupa.*

**Dokaz.** Neka je grupa $\mathbf{G}/\mathbf{H}$ generisana elementom $aH$. S obzirom da je svaki element iz $\mathbf{G}$ oblika $a^k h$, $h \in H$, $k \in Z$, dovoljno je da pokažemo da su podgrupe grupe $\mathbf{G}$ generisane konačnim skupom $\{a, h_1, \ldots, h_n\}$, $h_i \in H$, $n \geq 1$, nilpotentne. Fiksirajmo $n$. Neka je, za $i = 1, \ldots, n$, $b_i^{(0)} = h_i$, $b_i^{(1)} = [b_i^{(0)}, a] = [h_i, a]$ i generalno, za $m \geq 1$, $b_i^{(m+1)} = [b_i^{(m)}, a] = [h_i, \underbrace{a, \ldots, a}_{m+1}]$. Sve su to elementi iz $\mathbf{H}$ ($\lhd \mathbf{G}$), pa je i podgrupa $\mathbf{K}$ generisana skupom $\{b_i^{(m)} \mid i = 1, \ldots, n, m \in \omega\}$ sadržana u $\mathbf{H}$. Kako je $\mathbf{H}$ i $N$-grupa (54.2), to je prema 54.5 samo konačno mnogo elemenata datog skupa različito od jediničnog. Stoga je $\mathbf{K}$ nilpotentna grupa, uz to i normalna podgrupa grupe $\overline{\mathbf{K}} = \langle a, h_1, \ldots, h_n \rangle$ ($= \langle a, b_1^{(0)}, \ldots, b_n^{(0)} \rangle$); iz $b_i^{(m+1)} = [b_i^{(m)}, a] = (b_i^{(m)})^{-1} a^{-1} b_i^{(m)} a$ sledi $a^{-1} b_i^{(m)} a = b_i^{(m)} b_i^{(m+1)}$ ($\in K$). Jasno, $\overline{\mathbf{K}}/\mathbf{K}$ je ciklična grupa, te je prema 55.9 $\overline{\mathbf{K}}$ konačno generisana $ZA$-grupa, dakle i nilpotentna grupa.□

**Korolar 56.13** *$N$-grupe su lokalno nilpotentne.*

**Dokaz.** Neka je $\mathbf{G}$ $N$-grupa. Formirajmo rastući normalni niz na sledeći način: $\mathbf{H}_0 = \mathbf{E}$; ako je $\alpha$ nasledni ordinal, $\mathbf{H}_\alpha = \langle H_{\alpha-1}, a_\alpha \rangle$, gde je $a_\alpha$ jedan od elemenata (nepraznog) skupa $N(H_{\alpha-1}) \setminus H_{\alpha-1}$ (izbor elementa $a_\alpha$ se može "regulisati" jednim dobrim uređenjem domena grupe); ako je $\alpha$ granični ordinal, $\mathbf{H}_\alpha = \bigcup_{\beta<\alpha} \mathbf{H}_\beta$. Pretpostavimo da $\mathbf{G}$ nije lokalno nilpotentna grupa



i neka je $\mathbf{H}_\alpha$ prva iz niza formiranih podgrupa koja nije lokalno nilpotentna. Naravno, $\alpha$ mora biti nasledni ordinal (iz istog razloga zbog kojeg i imamo podgrupe $\mathbf{H}_\beta$ koje nisu lokalno nilpotentne – 56.2). No, tada je $\mathbf{H}_{\alpha-1}$ lokalno nilpotentna, normalna podgrupa $N$-grupe $\mathbf{H}_\alpha$ i $\mathbf{H}_\alpha/\mathbf{H}_{\alpha-1}$ je ciklična grupa, a odatle je, prema prethodnoj lemi, i $\mathbf{H}_\alpha$ lokalno nilpotentna grupa, kontradikcija.□

**Lema 56.14** *Skup elemenata konačnog reda lokalno nilpotentne grupe* $\mathbf{G}$ *je domen potpuno invarijantne podgrupe* $t\mathbf{G}$ *(periodičnog dela grupe* $\mathbf{G}$ *– zadržavamo notaciju iz poglavlja o Abelovim grupama),* $\mathbf{G}/t\mathbf{G}$ *je torziono slobodna grupa i* $t(\mathbf{G})$ *je direktni proizvod p-grupa.*

**Dokaz.** Direktna posledica lema 48.25 (koja se pak oslanja na 48.24) i 48.28. Tako, na primer, ako su elementi $a$ i $b$ uzajamno prostih redova, onda su i permutabilni ($\langle a, b \rangle$ je konačna nilpotentna grupa), i stoga je $t(\mathbf{G})$ direktni proizvod $p$-grupa.□

**Teorema 56.15** *(Teorema Hirsch-Plotkina). Neka su* $\mathbf{H}$ *i* $\mathbf{K}$ *normalne, lokalno nilpotentne podgrupe grupe* $\mathbf{G}$*. Tada je i* $\mathbf{H} \cdot \mathbf{K}$ *normalna, lokalno nilpotentna podgrupa grupe* $\mathbf{G}$*.*

**Dokaz.** Neka je $\mathbf{L}$ podgrupa grupe $\mathbf{H} \cdot \mathbf{K}$ generisana konačnim skupom $\{a_1 b_1, \ldots, a_n b_n\}$, $a_i \in H$, $b_i \in K$, $\mathbf{A}$ podgrupa grupe $\mathbf{H}$ generisana skupom $\{a_1, \ldots, a_n\}$ i $\mathbf{B}$ podgrupa grupe $\mathbf{K}$ generisana skupom $\{b_1, \ldots, b_n\}$. Kako je $\mathbf{L}$ podgrupa grupe $\langle A, B \rangle$, dovoljno je da pokažemo da je $\langle A, B \rangle$ nilpotentna grupa. Neka je $C = \{[a_i, b_j] \mid 1 \leq i, j \leq n\}$. Jasno, zbog normalnosti podgrupa $\mathbf{H}$ i $\mathbf{K}$ je $C \subseteq H \cap K$. $\langle A, C \rangle$ je nilpotentna, konačno generisana podgrupa grupe $\mathbf{H}$, $\langle B, C \rangle$ je nilpotentna, konačno generisana podgrupa grupe $\mathbf{K}$. Podgrupa $C^{\mathbf{A}} = \langle \{a^{-1} c a \mid a \in A, c \in C\} \rangle$ je normalno zatvorenje skupa $C$ u $\langle A, C \rangle$ (5.16), dakle, konačno je generisana (48.22), a ujedno to je i podgrupa grupe $\mathbf{H} \cap \mathbf{K}$. Prema tome, $\langle C^A, B \rangle$ ($\leq \mathbf{K}$) je konačno generisana nilpotentna podgrupa. Prema 6.14($a$),($d$) je $[A, B] = [\{a_1, \ldots, a_n\}, \{b_1, \ldots, b_n\}]^{AB} = C^{AB}$, i dalje:

$$\langle B, C^A \rangle = \langle B, C^{AB} \rangle = \langle B, [A, B] \rangle = \mathbf{B}^{\mathbf{A}} \lhd \langle A, B \rangle.$$

Po simetriji stvari je $\langle A, C^B \rangle = \mathbf{A}^{\mathbf{B}} \lhd \langle A, B \rangle$, pa je prema teoremi Fittinga (48.14) $\langle A, B \rangle = \mathbf{A}^{\mathbf{B}} \cdot \mathbf{B}^{\mathbf{A}}$ nilpotentna grupa.■

**Korolar 56.16** *Svaka grupa ima jedinstvenu maksimalnu, normalnu i lokalno nilpotentnu podgrupu, tzv. Hirsch-Plotkinov (B. I. Plotkin) radikal.*

**Dokaz.** Neka je $\{\mathbf{H}_i \mid i \in I\}$ familija svih normalnih, lokalno nilpotentnih podgrupa grupe $\mathbf{G}$. Prema prethodnoj teoremi $\langle \{H_i \mid i \in I\} \rangle$ je opet normalna, lokalno nilpotentna podgrupa. Prema tome, familija $\{\mathbf{H}_i \mid i \in I\}$ ima jedinstven maksimalni tj. najveći element.

Jasno, Fittingova podgrupa je takođe sadržana u Hirsch-Plotkinovom radikalu.□

**Lema 56.17** *Svaka lokalno nilpotentna podgrupa grupe* $\mathbf{G}$ *koja je term nekog rastućeg normalnog niza sadržana je u Hirsch-Plotkinovom radikalu.*

**Dokaz.** Neka je $\mathbf{H}$ lokalno nilpotentna podgrupa grupe $\mathbf{G}$ i neka je $\mathbf{H} = \mathbf{H}_0 \leq \mathbf{H}_1 \leq \cdots \leq \mathbf{H}_\mu = \mathbf{G}$ deo rastućeg normalnog niza čiji je jedan term $\mathbf{H}$. Neka je dalje za $\alpha$, $1 \leq \alpha \leq \mu$: $\overline{\mathbf{H}}_\alpha = \mathbf{H}^{\mathbf{H}_\alpha}$ $(= \langle\{b^{-1}ab \mid a \in H, b \in H_\alpha\}\rangle)$. Tada je $\mathbf{H} = \overline{\mathbf{H}}_1 \leq \overline{\mathbf{H}}_2 \leq \cdots \leq \overline{\mathbf{H}}_\mu = \mathbf{H}^{\mathbf{G}}$ rastući normalni lanac podgrupa grupe $\mathbf{G}$. Svaka od podgrupa $\overline{\mathbf{H}}_\alpha$ je lokalno nilpotentna. Zaista, pretpostavimo da je $\gamma$ $((1 <)\ \gamma \leq \mu)$ najmanji ordinal za koji $\overline{\mathbf{H}}_\gamma$ nije lokalno nilpotentna podgrupa. Evidentno, $\gamma$ nije granični ordinal; u suprotnom bismo imali: $\overline{\mathbf{H}}_\gamma = \mathbf{H}^{\mathbf{H}_\gamma} = \langle\{b^{-1}ab \mid a \in H, b \in H_\gamma = \bigcup_{\beta<\gamma} H_\beta\}\rangle = \bigcup_{\beta<\gamma} \overline{\mathbf{H}}_\beta$, i pošto je po pretpostavci svaka od podgrupa $\overline{\mathbf{H}}_\beta$ lokalno nilpotentna, to bi i $\overline{\mathbf{H}}_\gamma$ bila lokalno nilpotentna grupa. S druge strane, kako je $(\overline{\mathbf{H}}_{\gamma-1})^{\mathbf{H}_\gamma} = (\mathbf{H}^{\mathbf{H}_{\gamma-1}})^{\mathbf{H}_\gamma} = \langle\{b^{-1}ab \mid a \in H, b \in H_{\gamma-1}\}\rangle^{\mathbf{H}_\gamma} = \langle\{c^{-1}ac \mid a \in H, c \in H_\gamma\}\rangle = \langle\bigcup_{c\in H_\gamma}(\overline{H}_{\gamma-1})u_c\rangle = \overline{\mathbf{H}}_\gamma$ i, za svako $c \in H_\gamma$, $(\overline{\mathbf{H}}_{\gamma-1})u_c$ normalna, lokalno nilpotentna podgrupa grupe $\overline{\mathbf{H}}_\gamma$, sledi prema prethodnoj teoremi da je i $\overline{\mathbf{H}}_\gamma$ lokalno nilpotentna podgrupa, kontradikcija. Stoga je $\overline{\mathbf{H}}_\mu = \mathbf{H}^{\mathbf{G}}$ normalna, lokalno nilpotentna podgrupa grupe $\mathbf{G}$, dakle i podgrupa njenog Hirsch-Plotkinovog radikala.□

## 57 Deljive nilpotentne grupe

Svaka konačno generisana torziono slobodna nilpotentna grupa se može utopiti, i to na jedan poseban način, u grupu tipa $\mathbf{UT}_n(\mathbf{Z})$. O tome i još ponečemu je reč u ovom paragrafu.

**Definicija 57.1** *Grupa* $\mathbf{G}$ *je deljiva u smislu Černikova ili Černikovski deljiva akko je* $\mathbf{G} = \langle\{g^n \mid g \in G\}\rangle$ *za svaki pozitivan prirodan broj* $n$.

Ovo je uopštenje pojma deljive grupe – očigledno, svaka deljiva grupa je i Černikovski deljiva. Evidentno, obrat važi za Abelove grupe, ali generalno ne. No imamo ga i u slučaju $ZA$-grupa. S dokazom upravo počinjemo.

**Lema 57.2** *$ZA$-grupa je Černikovski deljiva akko nema pravih podgrupa konačnog indeksa.*

**Dokaz.** ($\Longrightarrow$) Ovaj pravac važi za svaku grupu. Trivijalno, nijedna nejedinična konačna grupa ne može biti Černikovski deljiva, jednako trivijalno, homomorfna slika Černikovski deljive grupe je Černikovski deljiva, a setimo se (4.19, 9.35): ako grupa ima pravu podgrupu konačnog indeksa, onda ima i normalnu podgrupu konačnog indeksa.



($\Longleftarrow$) Neka je $\mathbf{G}$ $ZA$-grupa bez pravih podgrupa konačnog indeksa. Pretpostavimo da je, za neki pozitivan prirodan broj $n$, $\mathbf{H} = \langle\{g^n \mid g \in G\}\rangle$ prava podgrupa grupe $\mathbf{G}$. $ZA$-grupa $\mathbf{G}/\mathbf{H}$, ako već nije Abelova, može se netrivijalno homomorfno preslikati u svoj centar (8.18). Prema tome, jedna homomorfna slika grupe $\mathbf{G}$ je Abelova grupa čiji su elementi ograničenih redova (za svako $g \in G$ je $(gH)^n = H$) i koja je, prema 35.2, direktna suma konačnih cikličnih grupa. Ali svaka takva grupa ima pravu podgrupu konačnog indeksa, kojoj opet odgovara prava podgrupa konačnog indeksa grupe $\mathbf{G}$, kontradikcija.□

**Lema 57.3** *Periodični deo Černikovski deljive $ZA$-grupe* $\mathbf{G}$ $(t\mathbf{G})$ *sadržan je u centru grupe* $\mathbf{G}$.

**Dokaz.** Primetimo prvo: prema 48.25 i 56.11 je skup svih elemenata konačnog reda $ZA$-grupe odista domen podgrupe.

Neka je $\{\zeta_\alpha\mathbf{G} \mid 0 \leq \alpha \leq \mu\}$, $\mu$ – ordinal, viši centralni niz grupe $\mathbf{G}$, eventualno transfinitno produžen. Ako je $a \in tG \setminus \{e\}$ i $\alpha_a = min\{\beta \leq \mu \mid a \in \zeta_\beta G\}$, onda je, jasno, $\alpha_a$ nasledni ordinal. Transfinitnom indukcijom pokazujemo da ne može biti $2 \leq \alpha_a \leq \mu$ (znači, $a \in \zeta_1 G = Z(\mathbf{G})$). Pretpostavimo da je $\alpha_a = 2$ i neka je $red(a) = n$. Dokazaćemo da je $ab^n = b^n a$ za svako $b \in G$, samim tim i da je $a \in Z(\mathbf{G})$, kontradiktorno pretpostavci. Fiksirajmo element $b$. $\mathbf{H} = \langle a, b\rangle$ je nilpotentna podgrupa klase nilpotentnosti ne veće od 2. Jer, koristeći se tačkama $(b)$, $(c)$, $(d)$ i $(e)$ leme 6.2 i činjenicom da je, za svako $x \in G$ i svaki ceo broj $z$, $[a^z, x], [x, a^z] \in Z(\mathbf{G})$ (zbog: $[\zeta_2\mathbf{G}, \mathbf{G}] \leq \zeta_1\mathbf{G}$), izvodimo da je komutator svaka dva elementa $u, v$ iz $\mathbf{H}$ stepen komutatora $[a, b]$; zbog toga je i $[u, v] \in H \cap Z(\mathbf{G}) = Z(\mathbf{H})$. Prema tome, $\mathbf{H}' = \gamma_1\mathbf{H} \leq \mathbf{Z}(\mathbf{H})$ i $\gamma_2\mathbf{H} = [\gamma_1\mathbf{H}, \mathbf{H}] = \mathbf{E}$. Ako je $\mathbf{H}$ baš Abelova grupa, imamo odmah: $ab^n = b^n a$. U suprotnom, neka je $\mathbf{E} < \zeta_1\mathbf{H} = \mathbf{Z}(\mathbf{H}) < \zeta_2\mathbf{H} = \mathbf{H}$ viši centralni niz grupe $\mathbf{H}$. Abelova grupa $\langle Z(\mathbf{H}), b\rangle$ je normalna podgrupa grupe $\mathbf{H}$; njeni elementi su oblika $cb^z$, $c \in Z(\mathbf{H})$, $z$ – ceo broj, a $a \cdot cb^z = a \cdot cb^z \cdot a^{-1} \cdot (cb^z)^{-1} \cdot cb^z \cdot a = [a^{-1}, (cb^z)^{-1}]cb^z \cdot a \in \langle Z(\mathbf{H}), b\rangle a$; slično se proverava: $\langle Z(\mathbf{H}), b\rangle a \subseteq a\langle Z(\mathbf{H}), b\rangle$. Jednostavniji dokaz koristi 8.7 – $\mathbf{H}/\mathbf{Z}(\mathbf{H})$ je Abelova grupa. Sledi da je element $b$ permutabilan sa svim svojim konjugatima u $\mathbf{H}$. Zato je:

$$b^n \cdot [b, a] \cdot [b, a^2] \cdot \ldots \cdot [b, a^{n-1}] =$$

$$b^n \cdot (b^{-1} \cdot a^{-1}ba) \cdot (b^{-1} \cdot a^{-2}ba^2) \cdot \ldots \cdot (b^{-1} \cdot a^{-(n-1)}ba^{n-1}) =$$

$$b^n \cdot b^{-(n-1)} \cdot (a^{-1}ba) \cdot (a^{-2}ba^2) \cdot \ldots \cdot (a^{-(n-1)}ba^{n-1}) =$$

$$b \cdot (a^{-1}ba) \cdot (a^{-2}ba^2) \cdot \ldots \cdot (a^{-(n-1)}ba^{n-1}).$$

Kako je, zbog $a^n = e$,

$$a^{-1} \cdot (b \cdot (a^{-1}ba) \cdot (a^{-2}ba^2) \cdot \ldots \cdot (a^{-(n-1)}ba^{n-1}) \cdot a =$$

$$a^{-1}ba \cdot a^{-2}ba^2 \cdot \ldots \cdot a^{-(n-1)}ba^{n-1} \cdot b =$$
$$b \cdot a^{-1}ba \cdot a^{-2}ba^2 \cdot \ldots \cdot a^{-(n-1)}ba^{n-1},$$

element $b \cdot a^{-1}ba \cdot a^{-2}ba^2 \cdot \ldots \cdot a^{-(n-1)}ba^{n-1}$ je komutativan sa $a$, jasno, i sa $b$, pa pripada centru podgrupe $\mathbf{H}$. S druge strane, elementi $[b,a],\ldots,[b,a^{n-1}]$ su, već smo rekli, takođe u centru, te je i $b^n$ element centra. Odatle, $ab^n = b^n a$.

Pretpostavimo u nastavku da ni za jedan nejedinični element $x$ iz $tG$ nije $2 \leq \alpha_x < \alpha$ $(> 2)$ (dakle, ako je $\alpha_x < \alpha$, tada je $\alpha_x = 1$). Neka je, za "naše" $a$, $\alpha_a = \alpha$. Tada je, za svako $b \in G$, $[a,b] = a^{-1} \cdot b^{-1}ab \in [\zeta_\alpha G, G] \cap tG \subseteq \zeta_{\alpha-1}G \cap tG$, pa je po induktivnoj pretpostavci $[a,b] \in \zeta_1 G$. Sledi: $a\zeta_1 G \cdot b\zeta_1 G = b\zeta_1 G \cdot a\zeta_1 G$ i $a \in \zeta_2 G$ (podsećamo: $\zeta_2\mathbf{G}/\zeta_1\mathbf{G} = \mathbf{Z}(\mathbf{G}/\zeta_1\mathbf{G})$, kontradikcija.□

**Korolar 57.4** *Černikovski deljiva periodična grupa je Abelova.*

**Lema 57.5** *Ako je periodični deo Černikovski deljive ZA-grupe* $\mathbf{G}$ *konačan, onda je baš jedinična podgrupa, a grupa* $\mathbf{G}$ *ima rastući centralni niz čiji su svi faktori Abelove deljive torziono slobodne grupe, po želji ranga* 1.

**Dokaz.** Prema prethodnoj lemi je $t\mathbf{G} \leq \mathbf{Z}(\mathbf{G})$. Ako je $\mathbf{G}$ Abelova grupa, izomorfna je direktnoj sumi kopija aditivne grupe racionalnih brojeva (jer periodični deo Abelove deljive grupe je ili jedinična ili beskonačna podgrupa – 33.19) i taj slučaj je trivijalan. U suprotnom, prema 8.18 postoji netrivijalno homomorfno preslikavanje $\varphi$ grupe $\mathbf{G}$ u njen centar. $(\mathbf{G})\varphi$ je Abelova deljiva grupa, pa dakle, prema upravo rečenom i torziono slobodna $((\mathbf{G})\varphi \cap t\mathbf{G} = \mathbf{E})$. Neka je $\mathbf{H}_1$ jedna Abelova deljiva torziono slobodna podgrupa grupe $\mathbf{Z}(\mathbf{G})$, po želji ranga 1. Tada je $t(\mathbf{G}/\mathbf{H}_1) = (t\mathbf{G} \cdot \mathbf{H}_1)/\mathbf{H}_1$. Inkluzija $\geq$ je očigledna, a ako je $(aH_1)^m = a^m H_1 = H_1$, tj. $a^m \in H_1$, onda je, za neko $b \in H_1$, $a^m = b^m$. Prema tome, $a^m b^{-m} = (ab^{-1})^m = e$, $ab^{-1} \in tG$ i $aH_1 = (ab^{-1})H_1 \in (tG \cdot H_1)/H_1$. Pretpostavimo dalje da je formiran invarijantan strogo rastući lanac podgrupa grupe $\mathbf{G}$:

$$\mathbf{H}_1 < \mathbf{H}_2 < \cdots < \mathbf{H}_\alpha < \cdots, \quad \alpha < \beta,$$

pri čemu je, za svako $\alpha < \beta$, $\mathbf{H}_\alpha \cap t\mathbf{G} = \mathbf{E}$, $t(\mathbf{G}/\mathbf{H}_\alpha) = (t\mathbf{G} \cdot \mathbf{H}_\alpha)/\mathbf{H}_\alpha$ i za $\alpha + 1 < \beta$ je $\mathbf{H}_{\alpha+1}/\mathbf{H}_\alpha$ Abelova deljiva torziono slobodna grupa (ranga 1) sadržana u centru grupe $\mathbf{G}/\mathbf{H}_\alpha$. Ako je $\beta$ granični ordinal, uzimamo jednostavno: $\mathbf{H}_\beta = \bigcup_{\alpha<\beta} \mathbf{H}_\alpha$. Očigledno, $\mathbf{H}_\beta \lhd \mathbf{G}$ i $\mathbf{H}_\beta \cap t\mathbf{G} = \bigcup_{\alpha<\beta}(\mathbf{H}_\alpha \cap t\mathbf{G}) = \mathbf{E}$. Ako je pak $(aH_\beta)^m = H_\beta$, onda je $a^m \in H_\alpha$ za neko $\alpha < \beta$. Stoga je $aH_\alpha \in t(G/H_\alpha) = (tG \cdot H_\alpha)/H_\alpha$, te je, za neko $b \in tG$, $aH_\alpha = bH_\alpha$, onda i $aH_\beta = bH_\beta \in (tG \cdot H_\beta)/H_\beta$. Ako je $\beta$ nasledni ordinal, ponavlja se priča s početka dokaza. Faktor grupa $\mathbf{G}/\mathbf{H}_{\beta-1}$ ispunjava uslove leme i njen centar sadrži Abelovu deljivu torziono slobodnu grupu (po želji ranga 1) – $\mathbf{H}_\beta/\mathbf{H}_{\beta-1}$ – koja sa $t(\mathbf{G}/\mathbf{H}_{\beta-1}) = (t\mathbf{G} \cdot \mathbf{H}_{\beta-1})/\mathbf{H}_{\beta-1}$ ima trivijalni presek. I tako:



$\mathbf{H}_\beta \cap t\mathbf{G} \cdot \mathbf{H}_{\beta-1} = \mathbf{H}_{\beta-1}$, što zajedno sa $t\mathbf{G} \cap \mathbf{H}_{\beta-1} = \mathbf{E}$ povlači $\mathbf{H}_\beta \cap t\mathbf{G} = \mathbf{E}$ (ako je $x \in H_\beta \cap tG$, onda je $x \in H_\beta \cap tG \cdot H_{\beta-1}$ i $x \in tG \cap H_{\beta-1}$). Dalje, $t((\mathbf{G}/\mathbf{H}_{\beta-1})/(\mathbf{H}_\beta/\mathbf{H}_{\beta-1})) = ((t\mathbf{G} \cdot \mathbf{H}_\beta)/\mathbf{H}_{\beta-1})/(\mathbf{H}_\beta/\mathbf{H}_{\beta-1})$. Inkluzija $\geq$ ostaje očigledna, a ako je, za $c \in G$, $(cH_{\beta-1}H_\beta/H_{\beta-1})^m = H_\beta/H_{\beta-1}$, tj. $c^m H_{\beta-1} \in H_\beta/H_{\beta-1}$, tada je, kao i maločas, za neko $d \in H_\beta$, $c^m H_{\beta-1} = d^m H_{\beta-1}$, što implicira redom: $(cd^{-1})^m H_{\beta-1} = H_{\beta-1}$ (jer je $\mathbf{H}_\beta/\mathbf{H}_{\beta-1} \leq \mathbf{Z}(\mathbf{G}/\mathbf{H}_{\beta-1})$), $(cd^{-1})H_{\beta-1} \in t(G/H_{\beta-1}) = (tG \cdot H_{\beta-1})/H_{\beta-1}$, $cH_{\beta-1} \in (tG \cdot H_{\beta-1})/H_{\beta-1}\, dH_{\beta-1} \subseteq (tG \cdot H_\beta)/H_{\beta-1}$. Odatle je, prema trećoj teoremi o izomorfizmu: $t(\mathbf{G}/\mathbf{H}_\beta) = (t\mathbf{G} \cdot \mathbf{H}_\beta)/\mathbf{H}_\beta$. Ovaj postupak se može nastaviti sve dok se za neki ordinal $\gamma$ ne dobije $\mathbf{H}_\gamma = \mathbf{G}$. No kako je $\mathbf{H}_\gamma \cap t\mathbf{G} = \mathbf{E}$, to je $t\mathbf{G}$ jedinična podgrupa, a niz

$$\mathbf{E} < \mathbf{H}_1 < \cdots < \mathbf{H}_\gamma = \mathbf{G}$$

je, prema samoj konstrukciji, rastući centralni niz grupe $\mathbf{G}$ čiji su faktori torziono slobodne Abelove deljive grupe (po želji ranga 1).□

**Lema 57.6** *Periodični deo Černikovski deljive ZA-grupe* $\mathbf{G}$ *i sam je Černikovski deljiv.*

**Dokaz.** Prema 57.3 je $t\mathbf{G}$ Abelova grupa. Ako bismo pretpostavili da sadrži pravu podgrupu konačnog indeksa – $\mathbf{H}$, onda bi faktor grupa $\mathbf{G}/\mathbf{H}$ bila Černikovski deljiva $ZA$-grupa sa konačnim periodičnim delom: $t(\mathbf{G}/\mathbf{H}) = t\mathbf{G}/\mathbf{H}$. Prema prethodnoj lemi sledilo bi $t\mathbf{G} = \mathbf{H}$, kontradikcija. Stoga je, prema 33.7, $t\mathbf{G}$ Abelova deljiva, dakle i Černikovski deljiva grupa.□

**Lema 57.7** *Černikovski deljiva ZA-grupa ima rastući centralni niz*

$$\mathbf{E} = \mathbf{H}_0 \leq \mathbf{H}_1 < \mathbf{H}_2 < \cdots < \mathbf{H}_\alpha < \cdots < \mathbf{H}_\mu = \mathbf{G},$$

*gde je* $\mathbf{H}_1$ *periodična deljiva grupa, eventualno jedinična, dok su svi ostali faktori torziono slobodne Abelove deljive grupe, po želji ranga* 1.

**Dokaz.** Direktna posledica prethodnih dveju lema. Stavljamo: $\mathbf{H}_1 = t\mathbf{G}$. $\mathbf{G}/t\mathbf{G}$ je torziono slobodna Černikovski deljiva $ZA$-grupa, koja ima rastući centralni niz

$$\overline{\mathbf{E}} < \mathbf{H}_2/\mathbf{H}_1 < \cdots < \mathbf{H}_\alpha/\mathbf{H}_1 < \cdots < \mathbf{H}_\mu/\mathbf{H}_1 = \mathbf{G}/\mathbf{H}_1$$

čiji su faktori torziono slobodne Abelove deljive grupe, po želji ranga 1. No, onda je

$$\mathbf{E} \leq \mathbf{H}_1 < \mathbf{H}_2 < \cdots < \mathbf{H}_\alpha < \cdots < \mathbf{H}_\mu = \mathbf{G}$$

traženi rastući centralni niz grupe $\mathbf{G}$: $\mathbf{H}_{\alpha+1}/\mathbf{H}_\alpha \cong (\mathbf{H}_{\alpha+1}/\mathbf{H}_1)/(\mathbf{H}_\alpha/\mathbf{H}_1)$ i kako je $(\mathbf{H}_{\alpha+1}/\mathbf{H}_1)/(\mathbf{H}_\alpha/\mathbf{H}_1) \leq \mathbf{Z}((\mathbf{G}/\mathbf{H}_1)/(\mathbf{H}_\alpha/\mathbf{H}_1))$, to je i $\mathbf{H}_{\alpha+1}/\mathbf{H}_\alpha \leq \mathbf{Z}(\mathbf{G}/\mathbf{H}_\alpha)$.□

**Teorema 57.8** *ZA-grupa je Černikovski deljiva akko je deljiva.*

**Dokaz.** Neka je $\mathbf{G}$ Černikovski deljiva $ZA$-grupa. Naravno, ničeg interesantnog ako je $\mathbf{G}$ Abelova grupa. Stoga neka je $\mathbf{G}$ neabelova grupa. Fiksirajmo nejedinični element $a_0$ i pozitivan prirodan broj $n$ i pokažimo da jednačina $a_0 = x^n$ ima rešenje. Neka je

$$\mathbf{E} \leq \mathbf{H}_1 = t\mathbf{G} < \mathbf{H}_2 < \cdots < \mathbf{H}_\mu = \mathbf{G}$$

rastući centralni niz iz prethodne leme i neka je, kao ranije, $\alpha_{a_0} = min\{\beta \leq \mu \mid a_0 \in H_\beta\}$. Onda $a_0 \notin H_{\alpha_{a_0}-1}$, i pošto je $\mathbf{H}_{\alpha_{a_0}}/\mathbf{H}_{\alpha_{a_0}-1}$ deljiva Abelova grupa, postoji element $b_1 \in H_{\alpha_{a_0}}$ takav da je $a_0 H_{\alpha_{a_0}-1} = b_1^n H_{\alpha_{a_0}-1}$, te je $a_0 = b_1^n a_1$ za neko $a_1 \in H_{\alpha_{a_0}-1}$. Sigurno, $\alpha_{a_1} < \alpha_{a_0}$. U $\mathbf{H}_{\alpha_{a_1}}$ postoji element $b_2$ za koji je $a_1 H_{\alpha_{a_1}-1} = (b_2 H_{\alpha_{a_1}-1})^n$. Odatle, $a_0 H_{\alpha_{a_1}-1} = (b_1^n a_1) H_{\alpha_{a_1}-1} = (b_1 H_{\alpha_{a_1}-1})^n \cdot a_1 H_{\alpha_{a_1}-1} = (b_1 H_{\alpha_{a_1}-1})^n \cdot (b_2 H_{\alpha_{a_1}-1})^n = (b_1 b_2)^n H_{\alpha_{a_1}-1}$, i stoga je, za neko $a_2 \in H_{\alpha_{a_1}-1}$, $a = (b_1 b_2)^n a_2$. Ako je već dobijen opadajući niz indeksa $\alpha_{a_0} > \alpha_{a_1} > \cdots > \alpha_{a_{k-1}}$, gde je, za neke elemente $b_i \in H_{\alpha_{a_{i-1}}}$, $1 \leq i \leq k$, i neko $a_k \in H_{\alpha_{a_{k-1}}-1}$, $a_0 = (b_1 \cdot \ldots \cdot b_k)^n a_k$, činimo korak dalje i na već opisan način dobijamo indeks $\alpha_{a_k}$ $(= min\{\beta \mid a_k \in H_\beta\})$ i elemente $b_{k+1} \in H_{\alpha_{a_k}}$ i $a_{k+1} \in H_{\alpha_{a_k}-1}$ za koje je $a_0 = (b_1 \cdot \ldots \cdot b_k \cdot b_{k+1})^n a_{k+1}$. Naravno, ovaj proces ne može ići u nedogled. Za neko $m$ će biti $a_0 = (b_1 \cdot \ldots \cdot b_m)^n a_m$, gde je $a_m \in H_1$ $(= tG)$ ili, u slučaju da je $t\mathbf{G} = \mathbf{E}$, $a_m \in H_2$. Kako bilo, $a_m$ je element Abelove deljive grupe koja je sadržana u centru, te je $a_m = b_{m+1}^n$ za neko $b_{m+1} \in Z(\mathbf{G})$, a tada je i $a_0 = (b_1 \cdot \ldots \cdot b_m \cdot b_{m+1})^n$.■

Naredna teorema daje potpunu karakterizaciju deljivih $ZA$-grupa.

**Teorema 57.9** *Grupa $\mathbf{G}$ je deljiva $ZA$-grupa akko postoji sistem njenih podgrupa $\{\mathbf{A}_\alpha \mid 0 \leq \alpha < \mu\}$ za koje važi:*

(1) *svaka podgrupa $\mathbf{A}_\alpha$ je izomorfna ili nekoj Prüferovoj $p$-grupi ili aditivnoj grupi racionalnih brojeva;*

(2) *za svako $\beta$, $1 \leq \beta \leq \mu$, je $\mathbf{B}_\beta \stackrel{\text{def}}{=} \langle \bigcup_{\alpha<\beta} A_\alpha \rangle$ normalna podgrupa grupe $\mathbf{G}$;*

(3) *za svako $\beta$, $0 < \beta < \mu$ je $\mathbf{A}_\beta \cap \mathbf{B}_\beta = \mathbf{E}$;*

*i*

(4) $\mathbf{B}_\mu = \mathbf{G}$.

**Dokaz.** ($\Longrightarrow$) Neka je $\mathbf{G}$ deljiva $ZA$-grupa sa rastućim centralnim nizom iz prethodne leme

$$\mathbf{E} = \mathbf{H}_0 \leq \mathbf{H}_1 < \mathbf{H}_2 < \cdots < \mathbf{H}_\mu = \mathbf{G},$$

s tim što sada uzimamo da je za $\alpha \geq 1$ faktor grupa $\mathbf{H}_{\alpha+1}/\mathbf{H}_\alpha$ baš ranga 1. Ovaj niz će nam dati traženi sistem podgrupa. Pretpostavimo da je $\mathbf{H}_1$ nejedinična grupa. Kao periodična deljiva Abelova grupa ona je izomorfna direktnoj sumi Prüferovih $p$-grupa. Neka je $\mathbf{H}_1 = \prod_{\alpha<\delta+1} \mathbf{A}_\alpha$, $\delta$ – ordinal, gde su podgrupe $\mathbf{A}_\alpha$ izomorfne Prüferovim grupama. Evidentno, uslov (3) je ispunjen za svako $0 < \beta < \delta + 1$, takođe i uslov (2) (ne zaboravimo da je $\mathbf{H}_1 \leq \mathbf{Z}(\mathbf{G})$). Dalje je, za svako $\alpha \geq 1$, $\mathbf{H}_{\alpha+1}/\mathbf{H}_\alpha \cong \mathbf{Ra}$. Pokazaćemo da je $\mathbf{H}_{\alpha+1}$ tzv. *rastavljajuća ekstenzija* (eng. *splitting extension*), tj. da postoji transverzala podgrupe $\mathbf{H}_\alpha$, $\{a^{\delta+\alpha} \mid a \in Ra\}$, takva da je $a^{\delta+\alpha} \cdot b^{\delta+\alpha} = (a+b)^{\delta+\alpha}$. Takva transverzala je, očigledno, domen podgrupe izomorfne grupi $\mathbf{Ra}$, a važi i $\mathbf{H}_{\alpha+1} = \mathbf{H}_\alpha \rtimes \langle \{a^{\delta+\alpha} \mid a \in Ra\}, \cdot \rangle$. Neka je $h_1^{\delta+\alpha}$ ma koji element iz $H_{\alpha+1} \setminus H_\alpha$. Formirajmo niz elemenata:

$$h_1^{\delta+\alpha}, h_2^{\delta+\alpha}, \ldots, h_n^{\delta+\alpha}, \ldots$$

na sledeći način: $h_2^{\delta+\alpha}$ je (jedno) rešenje jednačine $h_1^{\delta+\alpha} = x^2$, i, generalno, za već dobijeno $h_n^{\delta+\alpha}$, $h_{n+1}^{\delta+\alpha}$ je (jedno) rešenje jednačine $h_n^{\delta+\alpha} = x^{n+1}$. Takva rešenja postoje pošto je $\mathbf{G}$ deljiva grupa. Osim toga, sva ona su u $H_{\alpha+1}$ $(\setminus H_\alpha)$. Jer, pretpostavimo npr. da je, za rešenje $g$ jednačine $h_1^{\delta+\alpha} = x^2$, $\alpha_g = min\{\beta \mid g \in H_\beta\} > \alpha + 1$. No, $\mathbf{H}_{\alpha_g}/\mathbf{H}_{\alpha_g-1}$ je torziono slobodna grupa, pa nijedan nenula stepen elementa $g$ nije u $\mathbf{H}_{\alpha_g-1} \geq \mathbf{H}_{\alpha+1}$, kontradikcija. Podgrupa $\mathbf{A}_{\delta+\alpha} = \langle \{h_n^{\delta+\alpha} \mid n \geq 1\} \rangle$ grupe $\mathbf{H}_{\alpha+1}$ izomorfna je grupi $\mathbf{Ra}$ ($h_1^{\delta+\alpha}$ je, jasno, beskonačnog reda – videti 21.10($p$)) i ima trivijalan presek sa $\mathbf{H}_\alpha$ (jer je, za svako pozitivno $n$, $\mathbf{H}_\alpha \cap \langle h_n^{\delta+\alpha} \rangle = \mathbf{E}$; koristimo: $h_1^{\delta+\alpha} = (h_n^{\delta+\alpha})^{n!}$ i $\langle h_1^{\delta+\alpha} \rangle \cap \mathbf{H}_\alpha = \mathbf{E}$). Kako je element $h_1^{\delta+\alpha} H_\alpha$ beskonačnog reda i, trivijalno, $h_n^{\delta+\alpha} H_\alpha = (h_{n+1}^{\delta+\alpha} H_\alpha)^{n+1}$ za svako $n$, elementi $h_1^{\delta+\alpha} H_\alpha, h_2^{\delta+\alpha} H_\alpha, \ldots, h_n^{\delta+\alpha} H_\alpha, \ldots$ generišu isto tako podgrupu grupe $\mathbf{H}_{\alpha+1}/\mathbf{H}_\alpha$ izomorfnu grupi $\mathbf{Ra}$. Ali, $\mathbf{H}_{\alpha+1}/\mathbf{H}_\alpha$ je i sama takva, i kako grupa $\mathbf{Ra}$ nema pravih nenula deljivih podgrupa, to je baš $\langle \{h_n^{\delta+\alpha} H_\alpha \mid n \geq 1\} \rangle = \mathbf{H}_{\alpha+1}/\mathbf{H}_\alpha$. Odatle: $\mathbf{H}_\alpha \mathbf{A}_{\delta+\alpha} = \mathbf{H}_{\alpha+1}$ i $\mathbf{H}_{\alpha+1} = \mathbf{H}_\alpha \rtimes \mathbf{A}_{\delta+\alpha}$.

Traženi sistem podgrupa je $\{\mathbf{A}_\alpha \mid 0 \leq \alpha < \delta + \mu\}$. Već smo videli: za svako $\beta \leq \delta + 1$ je $\langle \bigcup_{\alpha<\beta} A_\alpha \rangle = \mathbf{B}_\beta \leq \mathbf{H}_1 \leq \mathbf{Z}(\mathbf{G})$, i zato je $\mathbf{B}_\beta \lhd \mathbf{G}$. Za svako $\beta = \delta + \gamma$ je pak $\mathbf{B}_\beta = \mathbf{H}_\gamma$, znači normalna podgrupa grupe $\mathbf{G}$. Zaista, pretpostavimo da je to tvrđenje tačno za svako $\delta + \epsilon < \delta + \gamma = \beta$. Ako je $\gamma$ granični ordinal, onda je $\mathbf{B}_\beta = \langle \bigcup_{\alpha<\beta} A_\alpha \rangle = \langle \bigcup_{\epsilon<\gamma} H_\epsilon \rangle = \mathbf{H}_\gamma$; ako je $\gamma$ sledbeni ordinal, onda je $\mathbf{B}_\beta = \langle \bigcup_{\alpha<\delta+(\gamma-1)} A_\alpha \cup A_{\delta+(\gamma-1)} \rangle = \langle H_{\gamma-1} \cup A_{\delta+(\gamma-1)} \rangle = \mathbf{H}_\gamma$. Prema samoj konstrukciji i već konstatovanom, sledi direktno i: $\langle \bigcup_{\alpha<\beta} A_\alpha \rangle \cap \mathbf{A}_\beta = \mathbf{E}$ kao i $\langle \bigcup_{\alpha<\delta+\mu} A_\alpha \rangle = \mathbf{G}$.

($\Longleftarrow$) Neka je $\mathbf{G}$ neabelova grupa sa sistemom podgrupa $\{\mathbf{A}_\alpha \mid 0 \leq \alpha < \mu\}$, koje ispunjavaju uslove (1) – (4). Dokazaćemo još da je $\mathbf{G}$ bez pravih podgrupa konačnog indeksa što će nam, zajedno sa 57.2 i prethodnom teoremom, dati da je $\mathbf{G}$ i deljiva grupa. Jer, rastući invarijantni niz podgrupa:

$$\mathbf{E} < \mathbf{B}_1 < \cdots < \mathbf{B}_\mu = \mathbf{G}$$

će biti (rastući) centralni niz grupe $\mathbf{G}$. Zaista, $\mathbf{B}_1 = \mathbf{A}_0$ je normalna deljiva podgrupa grupe $\mathbf{G}$, izomorfna ili grupi $\mathbf{Ra}$ ili nekoj Prüferovoj grupi, te je

prema 35.9 $\mathbf{B}_1 \leq \mathbf{Z}(\mathbf{G})$. Iz istog razloga je za $\beta \geq 1$ grupa $\mathbf{B}_{\beta+1}/\mathbf{B}_\beta$ ($\cong \mathbf{A}_\beta$) podgrupa centra grupe $\mathbf{G}/\mathbf{B}_\beta$.

Transfinitnom indukcijom pokazujemo da nijedna od podgrupa $\mathbf{B}_\beta$, $1 \leq \beta \leq \mu$ nema pravu podgrupu konačnog indeksa. Za $\mathbf{B}_1$ to je jasno. Pretpostavimo da tvrđenje važi za sve podgrupe $\mathbf{B}_\gamma$, $1 \leq \gamma < \beta$. Neka je $\beta$ granični ordinal i $\mathbf{K}$ prava podgrupa konačnog indeksa grupe $\mathbf{B}_\beta = \bigcup_{\gamma<\beta} \mathbf{B}_\gamma$. Ako je, za $\alpha < \beta$, $\mathbf{K} \cap \mathbf{B}_\alpha < \mathbf{B}_\alpha$ (primetimo da se $\mathbf{K}$ ne može sadržati ni u jednoj od podgrupa $\mathbf{B}_\gamma$ ($\gamma < \beta$), jer su $\mathbf{B}_{\gamma+1}/\mathbf{B}_\gamma$ beskonačne grupe, a jasno, ne može ni sadržati sve podgrupe $\mathbf{B}_\gamma$), tada je $\mathbf{K} \cap \mathbf{B}_\alpha$ prava podgrupa konačnog indeksa grupe $\mathbf{B}_\alpha$ (za svako $x, y \in B_\alpha$ je $x(K \cap B_\alpha) = y(K \cap B_\alpha)$ akko je $xK = yK$), kontradikcija. Ako je $\beta$ nasledni ordinal, iz pretpostavke da je $\mathbf{M}$ prava podgrupa konačnog indeksa grupe $\mathbf{B}_\beta$ sledilo bi: $\mathbf{B}_{\beta-1} \leq \mathbf{M} < \mathbf{B}_\beta$. ($\mathbf{B}_{\beta-1} \cap \mathbf{M} < \mathbf{B}_{\beta-1}$ bi značilo da je $\mathbf{M} \cap \mathbf{B}_{\beta-1}$ prava podgrupa konačnog indeksa grupe $\mathbf{B}_{\beta-1}$). No, tada je $\mathbf{M}/\mathbf{B}_{\beta-1}$ prava podgrupa konačnog indeksa grupe $\mathbf{B}_\beta/\mathbf{B}_{\beta-1}$, izomorfne deljivoj grupi $\mathbf{A}_{\beta-1}$, kontradikcija.■

**Napomena.** Karakterizacija Abelovih deljivih grupa (33.19) je specijalan slučaj prethodne teoreme; primetimo samo, zadržavajući notaciju iz teoreme: za svako $\beta < \mu$ je $\mathbf{B}_{\beta+1}$ baš direktni priozvod podgrupa $\mathbf{B}_\beta$ i $\mathbf{A}_\beta$ (koja je trivijalno normalna).

Dokaz naredne leme je manje-više već sadržan u prethodnim razmatranjima.

**Lema 57.10** *Neka je* $\mathbf{G}$ *torziono slobodna lokalno nilpotentna deljiva grupa. Tada važi:*

(*a*) *Presek familije deljivih podgrupa grupe* $\mathbf{G}$ *je i sama deljiva podgrupa;*

(*b*) *Normalizator deljive podgrupe je deljiva podgrupa;*

(*c*) *Svi elementi višeg centralnog lanca grupe* $\mathbf{G}$ ($\zeta_\alpha \mathbf{G}$) *su deljive podgrupe, a faktori tog lanca* ($\zeta_\alpha \mathbf{G}/\zeta_{\alpha+1}\mathbf{G}$) *su torziono slobodne deljive grupe.*

**Dokaz.** (*a*) je trivijalno, (*b*) je direktna posledica teoreme 48.43 (deljiva podgrupa je u ovom slučaju i izolovana podgrupa, kao što je i izolovana podgrupa deljiva, jer je $\mathbf{G}$ deljiva $R$-grupa – 56.4). (*c*) sledi iz 46.32 i očigledne činjenice da je homomorfna slika deljive grupe deljiva grupa.□

U 14.9 i 28.10 je pokazano da se svaka grupa može utopiti u deljivu grupu. U opštem, za datu grupu njena deljiva ekstenzija nije jednoznačno određena. Abelova grupa se može utopiti u Abelovu (33.4), ali i u neabelovu deljivu grupu. U tom smislu može se postaviti pitanje: da li se svaka nilpotentna (lokalno nilpotentna) grupa može utopiti u deljivu nilpotentnu (lokalno nilpotentnu) grupu. Odgovor nije uvek pozitivan. Recimo, neabelova periodična nilpotentna grupa nema deljivu nilpotentnu ekstenziju – kod deljivih nilpotentnih grupa periodični deo podgrupe je podgrupa njenog centra (57.3). U nastavku pokazujemo da se svaka torziono slobodna (lokalno) nilpotentna



grupa može utopiti u torziono slobodnu (lokalno) nilpotentnu deljivu grupu. Počinjemo sa dokazom.

**Definicija 57.11** *Neka je* $G$ *neprazan skup. Konačan niz funkcija* $(t_0, \ldots, t_{s-1})$, *gde je* $t_i : G \longrightarrow Z$, $i = 0, \ldots, s-1$, *koordinatni je sistem za* $G$ *akko je preslikavanje* $t : G \longrightarrow Z^s$ *dato sa* $t(g) = (t_0(g), \ldots, t_{s-1}(g))$ *injektivno (ovde iznimno originale pišemo s desne strane funkcijskog znaka).*

*Preslikavanje* $\phi : Z^s \longrightarrow Z^r$ *je polinomno preslikavanje akko postoje polinomi* $p_0(x_0, \ldots, x_{s-1}), \ldots, p_{r-1}(x_0, \ldots, x_{s-1}) \in Ra[x_0, \ldots, x_{s-1}]$ *(- skup polinoma sa racionalnim koeficijentima po* $s$ *promenljivih) takvi da je, za* $\overline{a} = (a_0, \ldots, a_{s-1}) \in Z^s$, $(\overline{a})\phi = (p_0(\overline{a}), \ldots, p_{r-1}(\overline{a}))$. *Ako su svi polinomi* $p_0, \ldots, p_{r-1}$ *prvog stepena,* $\phi$ *je linearno (polinomno) preslikavanje.*

Ako je $\mathbf{G}$ konačno generisana torziono slobodna nilpotentna grupa, onda prema 48.23 ima centralni niz $\mathbf{G} = \mathbf{G}_0 > \mathbf{G}_1 > \cdots > \mathbf{G}_s = \mathbf{E}$ čiji su svi faktori beskonačne ciklične grupe. Neka je $\mathbf{G}_i/\mathbf{G}_{i+1} = \langle a_i G_{i+1} \rangle$, $i = 0, \ldots, s-1$. Tada je $\mathbf{G} = \langle a_0, \ldots, a_{s-1} \rangle$ i, očigledno, svaki element $g$ iz $\mathbf{G}$ se može na jedinstven način predstaviti u obliku $g = a_0^{t_0(g)} \cdot \ldots \cdot a_{s-1}^{t_{s-1}(g)}$, gde $t_i(g) \in Z$, $i = 0, \ldots, s-1$. Stoga je $s$-torka $(t_0, \ldots, t_{s-1})$ koordinatni sistem za $G$ (kazaćemo i za grupu $\mathbf{G}$), $s$-torka $(a_0, \ldots, a_{s-1})$ je tzv. baza Maljceva (reda $s$) grupe $\mathbf{G}$, dok su $t_0(g), \ldots, t_{s-1}(g)$ koordinate Maljceva elementa $g$ s obzirom na bazu $(a_0, \ldots, a_{s-1})$. .

**Teorema 57.12** *Neka je* $\mathbf{G}$ *konačno generisana torziono slobodna nilpotentna grupa sa koordinatnim sistemom* $(t_0, \ldots, t_{s-1})$ *i bazom Maljceva* $(a_0, \ldots, a_{s-1})$. *Tada postoji prirodan broj* $n = n(\mathbf{G})$ *i utapanje* $\phi$ *grupe* $\mathbf{G}$ *u* $\mathbf{UT}_n(\mathbf{Z})$, *koje je polinomno, dok je inverzno preslikavanje* $\phi^{-1}$ *na* $(\mathbf{G})\phi$ *linearno; ovde identifikujemo* $G$ *sa* $Z^s$ *a* $UT_n(\mathbf{Z})$ *sa podskupom skupa* $Z^{n^2}$. *Osim toga, operacije množenja i stepenovanja u* $\mathbf{G}$ *mogu se opisati polinomima sa Maljcevskim koordinatama, konkretnije, za* $g, h \in G$ *i* $0 \leq i \leq s-1$ *važi:*

$$t_i(gh) = \text{polinom nad poljem } \mathbf{Ra} \text{ po } \{t_j(g), t_j(h) \mid j < i\} + t_i(g) + t_i(h) \quad (1);$$

$$t_i(g^m) = \text{polinom nad poljem } \mathbf{Ra} \text{ po } m \text{ i } \{t_j(g) \mid j < i\} + mt_i(g) \quad (2).$$

**Dokaz.** Držali smo se notacije a i pratimo dokaz iz [78].

Pokazujemo prvo da su (1) i (2) posledice prvog dela tvrđenja. Pretpostavimo stoga da on važi. Ako je $A \in UT_n(\mathbf{Z})$ i $m \in Z$, onda je prema binomnoj formuli i teoremi Cayley-Hamiltona (*svaka matrica* $A$ *je nula svog karakterističnog polinoma* $p(\lambda) = det(\lambda I - A) - p(A) = O$ *- nula matrica*; u našem slučaju sve matrice, elementi grupe $\mathbf{UT}_n(\mathbf{Z})$, imaju isti karakteristični polinom: $(\lambda - 1)^n$):

$$A^m = \sum_{i=0}^{n-1} \binom{m}{i} (A - I)^i;$$

za pozitivno $m$ imamo jednostavno: $A^m = (I+(A-I))^m = \sum_{k=0}^{m} \binom{m}{k} (A-I)^k = \sum_{k=0}^{n-1} \binom{m}{k} (A-I)^k$ (zbog $(A-I)^n = O$), a pošto je $\sum_{k=0}^{n-1} \binom{m}{k} (A-I)^k \cdot \sum_{r=0}^{n-1} \binom{-m}{r} (A-I)^r = \sum_{t=0}^{n-1} (\sum_{k+r=t} \binom{m}{k} \cdot \binom{-m}{r}) \cdot (A-I)^t = I$, tvrđenje sledi i za $-m$. Prema tome, elementi matrice $A^m$ su polinomi po $m$ i elementima matrice $A$. Prema osnovnom delu teoreme $t_i(gh)$, $t_i(g^m)$ su linearni polinomi po elementima matrica $(gh)\phi$, $(g^m)\phi$, a ovi su opet polinomi po $m$ i elementima matrica $(g)\phi$, $(h)\phi$. Konačno, ponovo prema osnovnom delu, elementi matrica $(g)\phi$, $(h)\phi$ su polinomi po $t_i(g)$, $t_j(h)$. Činjenica da su $t_i(gh)$ i $t_i(g^m)$ baš datog oblika proizilazi iz same definicije centralnog niza i koordinata Maljceva. Priča koja sledi će to još pojasniti.

Prelazimo sada na glavni deo teoreme. Zapravo pokazaćemo, što je prema 48.13 i dovoljno, da postoji polinomno utapanje $\psi$ grupe $\mathbf{G}$ u grupu $\mathbf{GL}_n(\mathbf{Z})$ takvo da je $\psi^{-1}$ linearno i $(g)\psi$ unipotentna matrica za svako $g \in G$. Dokaz je indukcijom po redu baze Maljceva – $s$. Ako je $s = 0$, $\mathbf{G}$ je jedinična grupa i sve je trivijalno. Pretpostavimo da tvrđenje važi za sve grupe sa bazama Maljceva reda manjeg od $s$ ($> 0$); dakle, prema konstatovanom i 48.13 imamo da kompletna teorema važi za sve takve grupe. Neka je $(a_0, \dots, a_{s-1})$ baza Maljceva grupe $\mathbf{G}$. U cilju iznalaženja preslikavanja $\psi$ dokazujemo prvo da je, za svako $g, h \in G$, $t_i(gh)$ polinom navedene forme. $t_i(g)$ obeležavamo sa $\xi_i$, $t_i(h)$ sa $\eta_i$, pa je:

$$gh = a_0^{\xi_0} \dots a_{s-1}^{\xi_{s-1}} \cdot a_0^{\eta_0} \dots a_{s-1}^{\eta_{s-1}} =$$

$$a_0^{\xi_0+\eta_0} \cdot (a_0^{-\eta_0} a_1^{-1} a_0^{\eta_0})^{-\xi_1} \cdot (a_0^{-\eta_0} a_2^{-1} a_0^{\eta_0})^{-\xi_2} \cdot \dots \cdot (a_0^{-\eta_0} a_{s-1}^{-1} a_0^{\eta_0})^{-\xi_{s-1}} \cdot a_1^{\eta_1} \dots a_{s-1}^{\eta_{s-1}} =$$

$$a_0^{\xi_0+\eta_0} ([a_0^{\eta_0}, a_1] \cdot a_1^{-1})^{-\xi_1} \cdot ([a_0^{\eta_0}, a_2] \cdot a_2^{-1})^{-\xi_2} \dots ([a_0^{\eta_0}, a_{s-1}] \cdot a_{s-1}^{-1})^{-\xi_{s-1}} \cdot a_1^{\eta_1} \dots a_{s-1}^{\eta_{s-1}}.$$

Prema induktivnoj hipotezi dovoljno je pokazati da su koordinate elementa $[a_0^{\eta_0}, a_i]$ s obzirom na bazu Maljceva $(a_1, \dots, a_{s-1})$ polinomi po $\eta_0$ (naravno, $[a_0^{\eta_0}, a_i] \in G_{i+1}$). Kako je $[a_0^{\eta_0}, a_i] = a_0^{-\eta_0} (a_i^{-1} a_0 a_i)^{\eta_0}$ i $a_i^{-1} a_0 a_i = a_0 \cdot [a_0, a_i] = a_0 a_{i+1}^{c_{i,i+1}} \dots a_{s-1}^{c_{i,s-1}}$, $c_{i,j} \in Z$, u grupi $\langle a_0, a_{i+1}, \dots, a_{s-1} \rangle$ sa centralnim nizom $\langle a_0, G_{i+1} \rangle > \mathbf{G}_{i+1} > \dots > \mathbf{G}_{s-1} > \mathbf{G}_s = \mathbf{E}$ i bazom Maljceva $(a_0, a_{i+1}, \dots, a_{s-1})$ važi:

$$(a_i^{-1} a_0 a_i)^{\eta_0} = a_0^{\eta_0} a_{i+1}^{\zeta_{i,i+1}} \dots a_{s-1}^{\zeta_{i,s-1}},$$

gde su $\zeta_{i,j}$, $j = i+1, \dots, s-1$, polinomi po $\eta_0$. Stoga je

$$[a_0^{\eta_0}, a_i] = a_0^{-\eta_0} \cdot (a_i^{-1} a_0 a_i)^{\eta_0} = a_{i+1}^{\zeta_{i,i+1}} \dots a_{s-1}^{\zeta_{i,s-1}},$$

te je formula (1) tačna za grupu $\mathbf{G}$. Primetimo samo:

$$gh = a_0^{\xi_0+\eta_0} a_1^{\xi_1} (a_2^{\zeta_{1,2}} \dots a_{s-1}^{\zeta_{1,s-1}})^{-\xi_1} \cdot a_2^{\xi_2} \cdot (a_3^{\zeta_{2,3}} \dots a_{s-1}^{\zeta_{2,s-1}})^{-\xi_2} \cdot \dots \cdot a_{s-1}^{\xi_{s-1}} \cdot a_1^{\eta_1} \dots a_{s-1}^{\eta_{s-1}},$$



a tvrđenje je po hipotezi tačno za grupu $\mathbf{G}_1$ sa bazom Maljceva $(a_1, \dots a_{s-1})$.

Konstruišimo na kraju funkciju $\psi$. Neka je $\mathbf{Ra}[t_0, \dots, t_{s-1}] = \mathbf{Ra}[\bar{t}]$ prsten polinoma nad poljem $\mathbf{Ra} = \langle Ra, +, \cdot \rangle$ (ovom prilikom koristimo oznaku koju smo inače rezervisali za aditivnu grupu racionalnih brojeva i za polje racionalnih brojeva) po funkcijama $t_0, \dots, t_{s-1}$ (gde se funkcije sabiraju i množe po indeksima). Za $g \in G$ i $p \in Ra[t_0, \dots, t_{s-1}]$, $p(g)$ će biti kraći zapis za $p(t_0(g), \dots, t_{s-1}(g))$. Za $a \in G$ neka je $p^a(g) \stackrel{\text{def}}{=} p(ag)$. Ovim je definisano dejstvo grupe $\mathbf{G}$ na skup $Ra[t_0, \dots, t_{s-1}]$: $\phi : G \longrightarrow S_{Ra[t_0,\dots,t_{s-1}]}$, gde je $(a)\phi = \widehat{a}$ i $(p)\widehat{a} = p^a$. Imamo u vidu: polinom $p(x_0, \dots, x_{s-1}) \in Ra[x_0, \dots, x_{s-1}]$ koji se anulira za sve $n$-torke celih brojeva je nula polinom; odatle sledi i: $p = q \iff p^a = q^a$, $(p+q)^a = p^a + q^a$, $(p \cdot q)^a = p^a \cdot q^a$, kao i $(p^a)^b = p^{ab}$. Dakle, $\widehat{a}$ je automorfizam prstena $\mathbf{Ra}[t_0, \dots, t_{s-1}]$ (jasno, $p = (p^{a^{-1}})\widehat{a}$), a $\phi$ je utapanje grupe $\mathbf{G}$ u grupu $\mathbf{Aut}(\mathbf{Ra}[t_0, \dots, t_{s-1}])$. Zaista, ako je $\widehat{a}$ identično preslikavanje, onda je $a = e$. Pretpostavimo suprotno; neka je $a = a_0^{\alpha_0} \dots a_{s-1}^{\alpha_{s-1}} \neq e$ i neka je $i$ prvi indeks za koji je $\alpha_i \neq 0$. No tada je $1 = t_i(a_i) = t_i^a(a_i) = t_i(aa_i) = t_i(a_i^{\alpha_i} \dots a_{s-1}^{\alpha_{s-1}} \cdot a_i) = t_i(a_i^{\alpha_i} a_i \cdot a_i^{-1}(a_{i+1}^{\alpha_{i+1}} \dots a_{s-1}^{\alpha_{s-1}}) a_i) = \alpha_i + 1$, kontradikcija.

Prema (1) je, posebno:

$$t_i^a = t_i + \sum_j p_{ij}(a) M_j(\bar{t}) \tag{3},$$

gde su $p_{ij}(a)$ polinomi nad $\mathbf{Ra}$ po koordinatama Maljceva elementa $a$, a *monomi* (*jednočlani*) $M_j(\bar{t})$, tj. polinomi oblika $t_0^{m_0} \cdot \dots \cdot t_{s-1}^{m_{s-1}}$, koji se javljaju s nenula koeficijentima ne sadrže $t_i, t_{i+1}, \dots, t_{s-1}$. Primetimo, ako je uopšte potrebno: $t_i^b = t_i + \sum_j p_{ij}(b) M_j(\bar{t})$, tj. polinomi $p_{ij}(\bar{x})$ su fiksni, a menjaju se samo, u zavisnosti od elementa, koordinate.

Na skupu monoma definišimo relaciju $<$ sa: $a_0^{m_0} \dots a_{s-1}^{m_{s-1}} < a_0^{n_0} \dots a_{s-1}^{n_{s-1}}$ akko je za neko $k$ $(0 \leq k \leq s-1)$ za svako $l > k$ $m_l = n_l$ i $m_k < n_k$. Za monom $M(\bar{t})$ je, prema (3), $(M(\bar{t}))(\widehat{a} - \widehat{e})$ ($\widehat{a} - \widehat{e}$ je, jasno, endomorfizam prstena $\mathbf{Ra}[\bar{t}]$) ili nula polinom ili linearna kombinacija monoma manjih (s obzirom na uvedeno uređenje) od $M(\bar{t})$. Prema tome, $(\widehat{a} - \widehat{e})^m$ je nula endomorfizam za neki dovoljno velik prirodan broj $m = m(a, M(\bar{t}))$.

Neka je $\mathbf{H}$ aditivna podgrupa grupe $\langle Ra[\bar{t}], + \rangle$ generisana skupom $\{t_i^g \ (= (t_i)\widehat{g}) \mid 0 \leq i \leq s-1, g \in G\}$. Prema (3) postoji pozitivan prirodan broj $K$ takav da je grupa $\mathbf{H}$ sadržana u torziono slobodnoj Abelovoj grupi generisanoj elementima $t_i$, $\frac{1}{K} M_j(\bar{t})$, $0 \leq i \leq s-1$, pa je i $\mathbf{H}$ konačno generisana slobodna Abelova grupa (32.7, 32.2). Neka je njena baza, recimo, $h_1, \dots, h_n$ i za $g \in G$ neka je

$$h_k^g = \sum_{l=1}^{n} \psi_{kl}(g) h_l \tag{4}.$$

Tada je $[\psi_{kl}(g)]_{1 \leq k,l \leq n}$ matrica restrikcije preslikavanja $\widehat{g}$ na $H$ (s obzirom na datu bazu), a preslikavanje $\psi : G \longrightarrow GL_n(\mathbf{Z})$ dato sa $(g)\psi = [\psi_{kl}(g)]_{1 \leq k,l \leq n}$ je utapanje grupe $\mathbf{G}$ u grupu $\mathbf{GL}_n(\mathbf{Z})$. Ako je, za $a, b \in G$, $(a)\psi = (b)\psi$, onda je $\widehat{a}|_H = \widehat{b}|_H$ i kako je $t_i \in H$ za svako $i = 0, \dots, s-1$, to je $a = b$.

$(G)\psi$ se, očigledno, sastoji od unipotentnih matrica (za svako $a \in G$ postoji, videli smo, prirodan broj $m$ takav da je $(\widehat{a} - \widehat{e})^m$ nula endomorfizam, dakle, karakteristični polinom matrice $(a)\psi$ deli $(\lambda - 1)^m$ i svi karakteristični koreni su 1). Preslikavanje $\psi^{-1}$ je linearno na $(G)\psi$ - $(g =)$ $(t_0(g), \ldots, t_{s-1}(g)) = ([\psi_{kl}(g)]_{1 \leq k,l \leq n})\psi^{-1}$; svako $t_i(g)$ je linearna kombinacija elemenata $h_k(g)$, $k = 1, \ldots, n$, dok je $h_k(g)$ linearna kombinacija elemenata $\psi_{kl}(g)$; iz (4) sledi

$$h_k^g(e) = h_k(g) = \sum_l h_l(e)\psi_{kl}(g).$$

Preostalo je da se pokaže da je $\psi$ polinomno, drugim rečima da je $\psi_{kl}$ restrikcija nekih polinoma nad $\mathbf{Ra}$ na $G$ (koje identifikujemo sa $Z^s$). Fiksirajmo $a \in G$. Svako $h_k$ je linearna kombinacija nekih $t_i^g$ ($\mathbf{H}$ je, podsećamo, generisana skupom $\{t_i^g \mid 0 \leq i \leq s-1, g \in G\}$). Neka je $T$ (konačan podskup skupa $G$) skup elemenata grupe koji se javljaju u prezentaciji elemenata $h_k$, $k = 1, \ldots, n$. Prema (3) je $h_k^a$ linearna kombinacija polinoma $t_i^{ga} = t_i + \sum_j c_{ij}(ga)M_j(t_0, \ldots, t_{s-1})$, $g \in T$, $i = 0, \ldots, s-1$. Postoje stoga polinomi $P_{kl}$ nad $\mathbf{Ra}$ za koje je

$$h_k^a = \sum_j P_{kj}(a)M_j(t_0, \ldots, t_{s-1}) \tag{5}$$

i posebno:

$$h_k = h_k^e = \sum_j P_{kj}(e)M_j(t_0, \ldots, t_{s-1}) \tag{6}.$$

Kako su $h_1, \ldots, h_n$ linearno nezavisni elementi, nezavisni su i vektori kolone matrice $[P_{kj}(e)]$. Prema (4) i (6) sledi:

$$\sum_j P_{kj}(a)M_j(\bar{t}) = h_k^a = \sum_l \psi_{kl}h_l = \sum_l \psi_{kl}(a)\sum_j P_{lj}(e)M_j(\bar{t}),$$

što daje, s obzirom na linearnu nezavisnost skupa monoma $\{M_j(\bar{t}) \mid j$ "ide" nekim skupom indeksa$\}$, sistem linearnih jednačina

$$P_{kj}(a) = \sum_l \psi_{kl}(a)P_{lj}(e),$$

a odatle pak trivijalno proizilazi da je $\psi_{kl}$ restrikcija nekog racionalnog polinoma na $G$.■

**Definicija 57.13** *Neka je* $\mathbf{H}$ *torziono slobodna (lokalno) nilpotentna grupa. Deljiva torziono slobodna (lokalno) nilpotentna grupa koja sadrži* $\mathbf{H}$ *i čija nijedna prava deljiva podgrupa ne sadrži* $\mathbf{H}$ *zove se (lokalno) nilpotentno deljivo zatvorenje grupe* $\mathbf{H}$.

**Napomena.** Obično se prefiks *(lokalno) nilpotentna* u definiciji deljivog zatvorenja izostavlja, pa se jednostavno govori o deljivom zatvorenju.



**Lema 57.14** *Neka je* $\mathbf{H}$ *podgrupa deljive torziono slobodne nilpotentne grupe* $\mathbf{G}$. *Skup* $\{g \in G \mid g^m \in H$ *za neki pozitivan prirodan broj* $m = m(g)\}$, *u oznaci* $\sqrt{H}$, *domen je podgrupe* $(\sqrt{\mathbf{H}})$ *koja je deljivo zatvorenje grupe* $\mathbf{H}$. *Osim toga važi:*

$$\zeta_i\sqrt{\mathbf{H}} = \sqrt{\zeta_i\mathbf{H}}, \quad \zeta_i\mathbf{H} = \mathbf{H} \cap \sqrt{\zeta_i\mathbf{H}}.$$

**Dokaz.** Neka $a, b \in \sqrt{H}$, $\mathbf{A} = \langle a, b\rangle$ i $\mathbf{B} = \mathbf{A} \cap \mathbf{H}$. Pokazujemo da je $\mathbf{B}$ podgrupa konačnog indeksa grupe $\mathbf{A}$ (onda direktno sledi da je $(ab)^r \in B \subseteq H$ za neki pozitivan prirodan broj $r$, odnosno da je $ab \in \sqrt{H}$). Neka je $\mathbf{A}$ klase nilpotentnosti $k$. Kako je $[\mathbf{A} : \mathbf{B}] = [\mathbf{B}\,\gamma_0\mathbf{A} : \mathbf{B}\,\gamma_1\mathbf{A}] \cdot [\mathbf{B}\,\gamma_1\mathbf{A} : \mathbf{B}\,\gamma_2\mathbf{A}] \cdot \ldots \cdot [\mathbf{B}\,\gamma_{k-1}\mathbf{A} : \mathbf{B}\,\gamma_k\mathbf{A}]$, dovoljno je da dokažemo da je za svako $i$, $i = 0, \ldots, k-1$, $[\mathbf{B}\,\gamma_i\mathbf{A} : \mathbf{B}\,\gamma_{i+1}\mathbf{A}]$ konačno. U nizu $\mathbf{A} = \mathbf{B}\,\gamma_0\mathbf{A} \geq \mathbf{B}\,\gamma_1\mathbf{A} \geq \cdots \geq \mathbf{B}\,\gamma_{k-1}\mathbf{A} \geq \mathbf{B}\,\gamma_k\mathbf{A} = \mathbf{B}$ svaka od podgrupa je normalna u prethodnoj, a faktor grupe su Abelove grupe; jer, prema 6.2 imamo za $x, y \in B$ i $u, v \in \gamma_i A$:

$$[xu, vy] = [xu, y]y^{-1}[xu, v]y = u^{-1}[x, y]u[u, y] \cdot y^{-1} \cdot u^{-1}[x, v]u[u, v] \cdot y =$$

$$[x, y] \cdot [[x, y], u] \cdot [u, y] \cdot (uy)^{-1}[x, v]uy \cdot y^{-1}[u, v]y \in B\gamma_{i+1}A.$$

Prema 49.24 je $\mathbf{A}/(\mathbf{B}\,\gamma_1\mathbf{A}) = (\mathbf{B}\,\gamma_0\mathbf{A})/(\mathbf{B}\,\gamma_1\mathbf{A})$ konačna grupa, recimo eksponenta $m$. Pretpostavimo da je tvrđenje tačno za svako $j \leq i$ kao i da je faktor grupa $(\mathbf{B}\,\gamma_{j-1}\mathbf{A})/(\mathbf{B}\,\gamma_j\mathbf{A})$ (konačna grupa) eksponenta $m^j$ $(j = 1, \ldots, i)$. $(\mathbf{B}\gamma_i\mathbf{A})/(\mathbf{B}\gamma_{i+1}\mathbf{A})$ je prema 48.22 konačno generisana grupa. Uočimo dalje da je zbog komutativnosti grupe dovoljno da se proveri da je za svako $[u, x]$, $u \in \gamma_{i-1}A$, $x \in A$, $[u, x]^{m^{i+1}} \in B\,\gamma_{i+1}A$ (koristeći se induktivnom pretpostavkom $u^{m^i} \in B\,\gamma_i A \cap \gamma_{i-1}A = (B \cap \gamma_{i-1}A)\gamma_i A$ i dokazanim $x^m \in B\,\gamma_1 A$). Ako je i $v \in \gamma_{i-1}A$, tada je

$$[uv, x]\gamma_{i+1}A = (v^{-1}[u, x]v[v, x])\gamma_{i+1}A = ([u, x] \cdot [[u, x], v] \cdot [v, x])\gamma_{i+1}A =$$

$$[u, x]\gamma_{i+1}A \cdot [v, x]\gamma_{i+1}A.$$

Isto tako je za $y \in A$:

$$[u, xy]\gamma_{i+1}A = ([u, y]y^{-1}[u, x]y)\gamma_{i+1}A = ([u, y] \cdot [u, x] \cdot [[u, x], y])\gamma_{i+1}A =$$

$$[u, y]\gamma_{i+1}A \cdot [u, x]\gamma_{i+1}A = [u, x]\gamma_{i+1}A \cdot [u, y]\gamma_{i+1}A.$$

Neka je $u^{m^i} = b_1a_1$, $b_1 \in B \cap \gamma_{i-1}A$, $a_1 \in \gamma_i A$, $x^m = b_2a_2$, $b_2 \in B$, $a_2 \in \gamma_1 A$. Onda je

$$[u, x]^{m^{i+1}}B\gamma_{i+1}A = [u^{m^i}, x^m]B\gamma_{i+1}A = [b_1a_1, b_2a_2]B\gamma_{i+1}A =$$

$$[b_1, b_2]B\gamma_{i+1}A \cdot [b_1, a_2]B\gamma_{i+1}A \cdot [a_1, b_2]B\gamma_{i+1}A \cdot [a_1, a_2]B\gamma_{i+1}A = B\gamma_{i+1}A;$$

$[b_1, a_2], [a_1, a_2] \in \gamma_{i+1}A$ prema 46.25(1).

Drugi deo tvrđenja, oba dela, dokazujemo simultano indukcijom po $i$, $i = 0, \ldots, k$. Za $i = 0$ sve je trivijalno. Pretpostavimo da je tačno za $i$ i neka je

$x \in \zeta_{i+1}\sqrt{H}$ i $x^n \in H$ za neki pozitivan prirodan broj $n$. Onda je, prema induktivnoj hipotezi i zbog $[\zeta_{i+1}\sqrt{\mathbf{H}}, \sqrt{\mathbf{H}}] \leq \zeta_i\sqrt{\mathbf{H}}$, za svako $h \in H$: $[x^n, h] \in H \cap \zeta_i\sqrt{H} = H \cap \sqrt{\zeta_i H} = \zeta_i H$, i odatle $x^n \in \zeta_{i+1}H$, tj. $x \in \sqrt{\zeta_{i+1}H}$. Druga inkluzija, $\sqrt{\zeta_{i+1}\mathbf{H}} \leq \zeta_{i+1}\sqrt{\mathbf{H}}$, je, znamo, ekvivalentna sa $[\sqrt{\zeta_{i+1}\mathbf{H}}, \sqrt{\mathbf{H}}] \leq \zeta_i\sqrt{\mathbf{H}}$. Neka je $x \in \sqrt{\zeta_{i+1}H}$, $y \in \sqrt{H}$, $x^m \in \zeta_{i+1}H$, $y^n \in H$. Tada je, zbog $[\zeta_{i+1}\mathbf{H}, \mathbf{H}] \leq \zeta_i\mathbf{H} \leq \sqrt{\zeta_i\mathbf{H}}$, $[x^m, y^n] \in \sqrt{\zeta_i H}$, tj. $x^m y^n \sqrt{\zeta_1 H} = y^n x^m \sqrt{\zeta_i H}$. Prema 46.31 i 48.42 je $\sqrt{\mathbf{H}}/\sqrt{\zeta_i\mathbf{H}}$ torziono slobodna $R$-grupa, te je $xy\sqrt{\zeta_i H} = yx\sqrt{\zeta_i H}$ (4.46 i 56.4).

Očigledno, $\zeta_{i+1}\mathbf{H} \leq \mathbf{H} \cap \sqrt{\zeta_{i+1}\mathbf{H}}$. Neka je $x \in H \cap \sqrt{\zeta_{i+1}H}$ i $x^m \in \zeta_{i+1}H$. Onda je, za svako $h \in H$, $[x^m, h] \in \zeta_i H$ i (kao maločas) $[x, h] \in \zeta_i H$, dakle $x \in \zeta_{i+1}H$.□

**Lema 57.15** *Grupa* $\mathbf{UT}_n(\mathbf{Ra})$ *je deljiva nilpotentna torziono slobodna grupa.*

**Dokaz.** Definišimo (proširujući formulu iz 57.12 na sve racionalne brojeve) za $A \in UT_n(\mathbf{Ra})$ i $\alpha \in Ra$:

$$A^\alpha = \sum_{i=0}^{n-1} \binom{\alpha}{i} (A - I)^i,$$

gde je za $i \neq 0$ (ponavljamo za svaki slučaj) $\binom{\alpha}{i} = \frac{\alpha\cdot(\alpha-1)\cdot\ldots\cdot(\alpha-i+1)}{i!}$ i $\binom{\alpha}{0} = 1$. Korišćenjem teoreme Cayley-Hamiltona i činjenice da binomna formula važi i za racionalne eksponente neposredno se proveravaju jednakosti:

$$A^\alpha \cdot A^\beta = A^{\alpha+\beta}, \quad (A^\alpha)^\beta = A^{\alpha\cdot\beta};$$

Prema tome, rešenje jednačine $A = x^m$ je $A^{\frac{1}{m}}$.□

**Teorema 57.16** *(A. I. Maljcev).* (*a*) *Svaka torziono slobodna nilpotentna grupa* $\mathbf{G}$ *ima deljivo zatvorenje iste klase nilpotentnosti i svaka dva deljiva zatvorenja grupe* $\mathbf{G}$ *su izomorfna.*

*Za svaki automorfizam* $\varphi$ *grupe* $\mathbf{G}$ *i svaka dva deljiva zatvorenja* $\mathbf{G}_1$ *i* $\mathbf{G}_2$ *grupe* $\mathbf{G}$ *postoji izomorfizam* $\psi \in Is(\mathbf{G}_1, \mathbf{G}_2)$ *takav da je* $\psi|_G = \varphi$;

(*b*) *Svaka torziono slobodna lokalno nilpotentna grupa* $\mathbf{G}$ *ima deljivo zatvorenje i za svaki automorfizam* $\varphi$ *grupe* $\mathbf{G}$ *i svaka dva deljiva zatvorenja* $\mathbf{G}_1$ *i* $\mathbf{G}_2$ *grupe* $\mathbf{G}$ *postoji izomorfizam* $\psi \in Is(\mathbf{G}_1, \mathbf{G}_2)$ *takav da je* $\psi|_G = \varphi$.

**Dokaz.** (*a*) Dokazujemo prvo jedinstvenost (do na izomorfizam) deljivih zatvorenja torziono slobodne nilpotentne grupe $\mathbf{G}$. Neka su $\mathbf{G}_1$ i $\mathbf{G}_2$ dva takva. Njihov direktni proizvod, koji je, jasno, torziono slobodna deljiva nilpotentna grupa, sadrži izomorfnu kopiju grupe $\mathbf{G} - \overline{\mathbf{G}} = \langle\{(g, g) \mid g \in G\}, \cdot\rangle$, a $\overline{\mathbf{G}}_1 = \langle\{(x, e) \mid x \in G_1\}, \cdot\rangle$ i $\overline{\mathbf{G}}_2 = \langle\{(e, y) \mid y \in G_2\}, \cdot\rangle$ su, respektivno, izomorfne kopije grupa $\mathbf{G}_1$ i $\mathbf{G}_2$. Neka je $\sqrt{\overline{\mathbf{G}}}$ deljivo zatvorenje podgrupe $\overline{\mathbf{G}}$ u $\mathbf{G}_1 \times \mathbf{G}_2$. Uočimo da za $i = 1, 2$ važi:

$$\sqrt{\overline{\mathbf{G}}} \cap \overline{\mathbf{G}}_i = \mathbf{E}, \quad \mathbf{G}_1 \times \mathbf{G}_2 = \sqrt{\overline{\mathbf{G}}} \cdot \overline{\mathbf{G}}_i.$$

Zaista, neka je npr. $(a, b) \in \sqrt{\overline{G}} \cap \overline{G}_1$. Onda je $b = e$ i, za neki pozitivan prirodan broj $m$, $a^m = e$, pa je i $a = e$. Što se tiče druge relacije, neka je $(a, b) \in G_1 \times G_2$ i neka je $m$ najmanji pozitivan prirodan broj takav da je $b^m \in G$. Ako je, za $c \in G_1$, $c^m = b^m$, tada je $(a, b) = (c, b)\cdot(c^{-1}a, e) \in \sqrt{\overline{G}}\cdot\overline{G}_1$. Prema tome, $\mathbf{G}_1 \times \mathbf{G}_2 = \overline{\mathbf{G}}_1 \rtimes \sqrt{\overline{\mathbf{G}}} = \overline{\mathbf{G}}_2 \rtimes \sqrt{\overline{\mathbf{G}}}$.

Neka je $(x, e) \in \overline{G}_1$. Onda je, za neke jednoznačno određene elemente $(e, y) \in \overline{G}_2$ i $(u, v) \in \sqrt{\overline{G}}$, $(x, e) = (e, y) \cdot (u, v) = (u, yv)$. Znači, $x = u$ pa zaključujemo: svaki element iz $\mathbf{G}_1$ javlja se kao prva komponenta tačno jednog elementa iz $\sqrt{\overline{\mathbf{G}}}$. Jasno, analogija važi i za elemente podgrupe $\mathbf{G}_2$. Stoga možemo definisati preslikavanje $\psi : G_1 \longrightarrow G_2$ sa: $(x)\psi = y$ akko je $(x, y) \in \sqrt{\overline{G}}$. $\psi$ je evidentno bijektivno a i homomorfno je preslikavanje: ako je, za $x, y \in G_1$ i $u, v \in G_2$, $(x)\psi = u$, $(y)\psi = v$, tj. $(x, u), (y, v) \in \sqrt{\overline{G}}$, tada je i $(xy, uv) \in \sqrt{\overline{G}}$, te je $(xy)\psi = uv = (x)\psi(y)\psi$. Dokaz poslednjeg dela tvrđenja (tačke (*a*)) u osnovi je isti, samo bismo sada umesto podgrupe $\overline{\mathbf{G}}$ (grupe $\mathbf{G}_1 \times \mathbf{G}_2$) posmatrali podgrupu $\langle\{(g, (g)\varphi) \mid g \in G\}, \cdot\rangle$, gde je, naravno, $\varphi$ dati automorfizam grupe $\mathbf{G}$. Očigledno, mogli smo na isti način i ovo dokazati:

*ako su* $\mathbf{G}$ *i* $\mathbf{H}$ *izomorfne torziono slobodne nilpotentne grupe i ako su* $\mathbf{G}_1$ *i* $\mathbf{H}_1$ *njihova deljiva zatvorenja, onda za (svako)* $\varphi \in Is(\mathbf{G}, \mathbf{H})$ *postoji* $\psi \in Is(\mathbf{G}_1, \mathbf{H}_1)$ *takvo da je* $\psi|_G = \varphi$.

Prelazimo sada na dokaz egzistencije deljivog zatvorenja. Ako je grupa $\mathbf{G}$ konačno generisana, prema 57.12 za neko $n = n(\mathbf{G})$ postoji utapanje $\varphi$ grupe $\mathbf{G}$ u grupu $\mathbf{UT}_n(\mathbf{Z})$, koja je pak podgrupa deljive grupe $\mathbf{UT}_n(\mathbf{Ra})$ (57.15). Radikalno zatvorenje grupe $(\mathbf{G})\varphi$ u $\mathbf{UT}_n(\mathbf{Ra})$ $(\sqrt{(\mathbf{G})\varphi})$ je deljivo zatvorenje grupe $(\mathbf{G})\varphi$. Ako je, za $A \in (G)\varphi$ i pozitivan prirodan broj $m$, $B \in \sqrt{(G)\varphi}$ rešenje jednačine $A = X^m$, pisaćemo $B = \sqrt[m]{A}$. Naravno, $\sqrt[m]{A_1} = \sqrt[n]{A_2}$ akko je $A_1^n = A_2^m$.

Razmotrimo i opšti slučaj: grupa $\mathbf{G}$ nije konačno generisana. Na skupu simbola $\{\sqrt[m]{g} \mid g \in G, m = 1, 2, 3, \ldots\}$ definišimo relaciju $\sim$ sa: $\sqrt[m]{a} \sim \sqrt[n]{b}$ akko je $a^n = b^m$ u grupi $\mathbf{G}$. $\sim$ je relacija ekvivalencije; refleksivnost i simetričnost su očigledni, a ako je $\sqrt[k]{a} \sim \sqrt[m]{b}$ i $\sqrt[m]{b} \sim \sqrt[r]{c}$, onda je $a^{mn} = b^{kn} = c^{mk}$, tj. $(a^n)^m = (c^k)^m$ i $a^n = c^k$, odnosno $\sqrt[k]{a} \sim \sqrt[r]{c}$. Na skupu klasa ekvivalencija $\{[\sqrt[m]{a}] \mid a \in G, m \geq 1\}$ definišimo operaciju $\bullet$ sa: $[\sqrt[m]{a}] \bullet [\sqrt[n]{b}] = [\sqrt[m]{a} \cdot \sqrt[n]{b}]$, gde sada elemente $\sqrt[m]{a}$ i $\sqrt[n]{b}$ i operaciju $\cdot$ posmatramo kao elemente i operaciju (ma kog) deljivog zatvorenja grupe $\langle a, b\rangle$. Operacija $\bullet$ je dobro definisana. Jer, ako je $\sqrt[m]{a} \cdot \sqrt[n]{b} = \sqrt[r]{c} = \sqrt[t]{d}$, $c, d \in \langle a, b\rangle$, tada je $c^t = d^r$ i $[\sqrt[r]{c}] = [\sqrt[t]{d}]$; osim toga, ako su $\mathbf{G}_1$ i $\mathbf{G}_2$ dva deljiva zatvorenja grupe $\langle a, b\rangle$,

postoji, kao što smo videli, $\psi \in Is(\mathbf{G}_1, \mathbf{G}_2)$ koji "$m$-ti koren" elementa $a$ u $\mathbf{G}_1$ preslikava u "$m$-ti koren" elementa $a$ u $\mathbf{G}_2$. Grupoid $\langle \{[\sqrt[n]{g}] \mid g \in G, n \geq 1\}, \bullet \rangle$, obeležimo ga sa $\sqrt{\mathbf{G}}$, torziono je slobodna nilpotentna deljiva grupa koja sadrži izomorfnu kopiju grupe $\mathbf{G}$. Asocijativnost je očigledna, jedinični element je $[e]$ $(= [\sqrt[n]{e}]$ za svako $n \geq 1)$, $[\sqrt[n]{g}]^{-1} = [(\sqrt[n]{g})^{-1}] = [\sqrt[n]{g^{-1}}]$; uopšte je $[\sqrt[n]{g}]^m = [\sqrt[n]{g^m}]$ (jer je torziono slobodna nilpotentna grupa $R$-grupa – ovde imamo na umu deljiva zatvorenja konačno generisanih podgrupa grupe $\mathbf{G}$), pa je i sama grupa $\sqrt{\mathbf{G}}$ torziono slobodna. $\sqrt{\mathbf{G}}$ je i deljiva grupa. Rešenje jednačine $[\sqrt[n]{g}] = x^m$ je $[\sqrt[m]{\sqrt[n]{g}}]$. Očigledno, nijedna prava podgrupa grupe $\sqrt{\mathbf{G}}$ koja sadrži (izomorfnu kopiju grupe) $\mathbf{G}$ nije deljiva.

Neka je $\mathbf{G}$ klase nilpotentnosti $s$. Onda je, prema 57.14, deljivo zatvorenje svake njene konačno generisane podgrupe klase nilpotentnosti manje od ili jednako $s$, pa je, za svako $\sqrt[n_0]{g_0}, \ldots, \sqrt[n_{s-1}]{g_{s-1}} \in \sqrt{G}$:

$$[\sqrt[n_0]{g_0}, \ldots, \sqrt[n_{s-1}]{g_{s-1}}] = [\ldots[[\sqrt[n_0]{g_0}, \sqrt[n_1]{g_1}], \sqrt[n_2]{g_2}], \ldots, \sqrt[n_{s-1}]{g_{s-1}}] = e,$$

te je i $\sqrt{\mathbf{G}}$ klase nilpotentnosti $s$.

($b$) Direktna posledica tačke ($a$).■

**Lema 57.17** *Ako je deljiva lokalno nilpotentna torziono slobodna grupa* $\mathbf{G}$ *deljivo zatvorenje svojih podgrupa* $\mathbf{H}$ *i* $\mathbf{K}$, *onda je deljivo zatvorenje i podgrupe* $\mathbf{H} \cap \mathbf{K}$.

**Dokaz.** Neka je $g \in G$. Tada je, za neke pozitivne prirodne brojeve $m$ i $n$, $g^m \in H$, $g^n \in K$. Odatle, $g^{mn} \in H \cap K$, te je $g$ i u deljivom zatvorenju podgrupe $\mathbf{H} \cap \mathbf{K}$.□

**Lema 57.18** *Neka je* $\sqrt{\mathbf{G}}$ *deljivo zatvorenje lokalno nilpotentne torziono slobodne grupe* $\mathbf{G}$. *Ako je* $\mathbf{H}$ *deljiva podgrupa grupe* $\sqrt{\mathbf{G}}$, *tada je* $\mathbf{H}$ *deljivo zatvorenje podgrupe* $\mathbf{H} \cap \mathbf{G}$ *(možemo pisati:* $\mathbf{H} = \sqrt{\mathbf{H} \cap \mathbf{G}}$*). Takođe,* $\mathbf{G} \cap \mathbf{H}$ *je izolovana podgrupa grupe* $\mathbf{G}$ *i među skupovima svih deljivih podgrupa grupe* $\sqrt{\mathbf{G}}$ *i svih izolovanih podgrupa grupe* $\mathbf{G}$ *postoji uzajamno jednoznačna korespondencija.*

**Dokaz.** Ako je $h \in H$, onda je $h^m \in G$ $(\cap H)$ za neki pozitivan prirodan broj $m$, pa je $h \in \sqrt{H \cap G}$. Pretpostavimo dalje da je, za $g \in G$ i pozitivan prirodan broj $n$, $g^n \in G \cap H$. No, kako je $\mathbf{H}$ deljiva grupa, to je, za neko $a \in H$, $a^n = g^n$, pa je $a = g$ i $g \in G \cap H$; dakle, $\mathbf{G} \cap \mathbf{H}$ je izolovana podgrupa grupe $\mathbf{G}$.

Preslikavanje $\varphi$ skupa $\{\mathbf{H} \mid \mathbf{H}$ je deljiva podgrupa grupe $\sqrt{\mathbf{G}}\}$ u skup $\{\mathbf{K} \mid \mathbf{K}$ je izolovana podgrupa grupe $\mathbf{G}\}$ dato sa $(\mathbf{H})\varphi = \mathbf{H} \cap \mathbf{G}$ je bijekcija. Jer, neka je $\mathbf{K}$ izolovana podgrupa grupe $\mathbf{G}$ i neka je $\sqrt{\mathbf{K}}$ njeno deljivo zatvorenje sadržano u $\sqrt{\mathbf{G}}$. Onda za svako $g \in \sqrt{K} \cap \mathbf{G}$ postoji prirodan broj $m = m(g)$ takav da je $g^m \in K$, te je $g \in K$, pošto je $\mathbf{K}$ izolovana podgrupa. Prema tome, $\sqrt{\mathbf{K}} \cap \mathbf{G} = \mathbf{K}$ i $\varphi$ je surjektivno preslikavanje; ostalo je još jasnije.□



**Teorema 57.19** *(Yu. G. Fedorov). Ako je* $\sqrt{\mathbf{G}}$ *deljivo zatvorenje lokalno nilpotentne torziono slobodne grupe* $\mathbf{G}$, $\zeta_0\mathbf{G} \leq \zeta_1\mathbf{G} \leq \cdots \leq \zeta_\alpha\mathbf{G} \leq \cdots$ *viši centralni lanac grupe* $\mathbf{G}$, *a* $\sqrt{\zeta_\alpha\mathbf{G}}$ *deljivo zatvorenje podgrupe* $\zeta_\alpha\mathbf{G}$ *sadržano u* $\sqrt{\mathbf{G}}$, *onda je* $\sqrt{\zeta_\alpha\mathbf{G}} = \zeta_\alpha\sqrt{\mathbf{G}}$.

**Dokaz.** Radi se o uopštenju dela leme 57.14. Koristimo, jasno, transfinitnu indukciju. Slučaj $\alpha = 0$ je trivijalan. Neka je $a \in \sqrt{\zeta_1 G}$ i $g \in \sqrt{G}$. Onda je, za neke pozitivne prirodne brojeve $m, n$, $a^m \in \zeta_1 G = Z(\mathbf{G})$, $g^n \in G$, pa je $a^m g^n = g^n a^m$. Prema 4.46 i 56.4 je $ag = ga$ i $a \in \zeta_1\sqrt{G}$. Neka je sada $a \in \zeta_1\sqrt{G}$. Onda je, jasno, za neko $m \geq 1$, $a^m \in Z(\mathbf{G})$, pa je $a \in \sqrt{\zeta_1 G}$.

Pretpostavimo da je tvrđenje tačno za sve ordinale $\alpha$ manje od $\beta$.

Neka je prvo $\beta$ nasledni ordinal. Pošto je $\zeta_{\beta-1}\mathbf{G}$ izolovana podgrupa grupe $\mathbf{G}$ (46.32), prema prethodnoj lemi je $\sqrt{\zeta_{\beta-1}\mathbf{G}} \cap \mathbf{G} = \zeta_{\beta-1}\mathbf{G}$. Očigledno, faktor grupa $\sqrt{\mathbf{G}}/\sqrt{\zeta_{\beta-1}\mathbf{G}}$ je deljivo zatvorenje podgrupe $(\mathbf{G}\sqrt{\zeta_{\beta-1}\mathbf{G}})/\sqrt{\zeta_{\beta-1}\mathbf{G}}$, $\sqrt{\zeta_\beta\mathbf{G}}/\sqrt{\zeta_{\beta-1}\mathbf{G}}$ je deljivo zatvorenje podgrupe $(\zeta_\beta\mathbf{G}\sqrt{\zeta_{\beta-1}\mathbf{G}})/\sqrt{\zeta_{\beta-1}\mathbf{G}}$. Takođe važi: $(\zeta_\beta\mathbf{G}\sqrt{\zeta_{\beta-1}\mathbf{G}})/\sqrt{\zeta_{\beta-1}\mathbf{G}} = \mathbf{Z}((\mathbf{G}\sqrt{\zeta_{\beta-1}\mathbf{G}})/\sqrt{\zeta_{\beta-1}\mathbf{G}})$. Jasno, za $a \in \zeta_\beta G$ i $g \in G$, iz $(ag)\zeta_{\beta-1}G = (ga)\zeta_{\beta-1}G$ sledi $(ag)\sqrt{\zeta_{\beta-1}G} = (ga)\sqrt{\zeta_{\beta-1}G}$ i stoga je $(\zeta_\beta\mathbf{G}\sqrt{\zeta_{\beta-1}\mathbf{G}})/\sqrt{\zeta_{\beta-1}\mathbf{G}} \leq \mathbf{Z}((\mathbf{G}\sqrt{\zeta_{\beta-1}\mathbf{G}})/\sqrt{\zeta_{\beta-1}\mathbf{G}})$. S druge strane, ako je, za neko $a \in G$ i svako $g \in G$, $(ag)\sqrt{\zeta_{\beta-1}G} = (ga)\sqrt{\zeta_{\beta-1}G}$, tada je $[a, g] \in \sqrt{\zeta_{\beta-1}G} \cap G = \zeta_{\beta-1}G$ (što će reći: $(ag)\zeta_{\beta-1}G = (ga)\zeta_{\beta-1}G$) i $a \in \zeta_\beta G$. Prema prvom delu dokaza i 46.25(4) imamo:

$$\sqrt{\zeta_\beta\mathbf{G}}/\sqrt{\zeta_{\beta-1}\mathbf{G}} = \zeta_1(\sqrt{(\mathbf{G}\sqrt{\zeta_{\beta-1}\mathbf{G}})/\sqrt{\zeta_{\beta-1}\mathbf{G}}}) =$$

$$\zeta_1(\sqrt{\mathbf{G}}/\sqrt{\zeta_{\beta-1}\mathbf{G}}) = \zeta_1(\sqrt{\mathbf{G}}/\zeta_{\beta-1}\sqrt{\mathbf{G}}) = \zeta_\beta\sqrt{\mathbf{G}}/\zeta_{\beta-1}\sqrt{\mathbf{G}},$$

dakle, $\sqrt{\zeta_\beta\mathbf{G}} = \zeta_\beta\sqrt{\mathbf{G}}$.

Ako je $\beta$ granični ordinal, onda je $\zeta_\beta\mathbf{G} = \bigcup_{\alpha<\beta} \zeta_\alpha\mathbf{G}$. Ako je $g \in \sqrt{\zeta_\beta G}$, tada je, za neko $\alpha < \beta$ i neko $m \geq 1$, $g^m \in \zeta_\alpha G$, pa je $g \in \sqrt{\zeta_\alpha G}$. Znači, $\sqrt{\zeta_\beta\mathbf{G}} \leq \bigcup_{\alpha<\beta} \sqrt{\zeta_\alpha\mathbf{G}}$, a obrat je trivijalan.■

**Korolar 57.20** *Deljivo zatvorenje torziono slobodne ZA-grupe je ZA-grupa.*

## 58 Generalno rešive grupe

U ovom paragrafu definisaćemo nekoliko ekstenzija klase rešivih grupa i reći nešto o njihovim osnovnim osobinama kao i uzajamnim odnosima.

**Definicija 58.1** *SD-grupa je grupa čiji izvodni lanac, eventualno transfinitno produžen, "stiže" do jedinične podgrupe (za granični ordinal* $\beta$ *se definiše:* $\mathbf{G}^{(\beta)} = \bigcap_{\alpha<\beta} \mathbf{G}^{(\alpha)}$, *za nasledni ordinal* $\gamma$ *je standardno* $\mathbf{G}^{(\gamma)} = (\mathbf{G}^{(\gamma-1)})'$*).*

*Rešiv normalni sistem je normalni sistem (47.4) čiji su svi faktori Abelove grupe.*

*Rešiv invarijantni sistem je invarijantni sistem čiji su svi faktori Abelove grupe.*

*$SN$-grupa je grupa koja ima rešiv normalni sistem.*

*$SI$-grupa je grupa koja ima rešiv invarijantni sistem.*

*$\overline{SN}$-grupa je grupa čiji je svaki kompozicioni sistem rešiv.*

*$\overline{SI}$-grupa je grupa čiji je svaki glavni sistem rešiv.*

*$SN^*$-grupa je grupa koja ima rastući rešiv normalni niz.*

*$SI^*$-grupa je grupa koja ima rastući rešiv invarijantni niz.*

**Lema 58.2** *Konačna grupa je $SN$-, $\overline{SN}$-, $SI$- , $\overline{SI}$-, $SN^*$-, $SI^*$-grupa akko je rešiva.*

Jasno, svaka $SD$-grupa je $SI$-grupa i svaka $SI$-grupa je $SN$-grupa. Recimo i to da se klasa $SI$-grupa strogo sadrži u klasi $SN$-grupa.

Svaka slobodna grupa je, pokazali smo (23.31, videti i 48.52), $SD$-grupa, ali ne i rešiva ako nije ciklična (23.28($c$)). Kako je svaka grupa homomorfna slika neke slobodne grupe sledi da homomorfna slika $SD$- ($SI$-, $SN$-) grupe nije nužno $SD$- ($SI$-, $SN$-) grupa. S druge strane imamo

**Lema 58.3** *Homomorfna slika $\overline{SN}$-, $\overline{SI}$-, $SN^*$-, $SI^*$-grupe je, respektivno $\overline{SN}$-, $\overline{SI}$-, $SN^*$-, $SI^*$-grupa. Drugim rečima, date klase grupa su zatvorene za homomorfizme.*

**Dokaz.** Neka je $\mathbf{G}$ $\overline{SN}$-grupa, $\mathbf{H}$ njena netrivijalna normalna podgrupa i $\overline{\mathcal{S}} = \{\overline{\mathbf{K}}_\alpha = \mathbf{K}_\alpha/\mathbf{H} \mid \alpha \in \Omega\}$ kompozicioni sistem faktor grupe $\mathbf{G}/\mathbf{H}$. Onda je $\{\mathbf{E}\} \cup \{\mathbf{K}_\alpha \mid \alpha \in \Omega\}$ normalni sistem grupe $\mathbf{G}$ koji se (kao i svaki drugi), prema 47.5, može proširiti do kompozicionog. No evidentno, prema 8.7 svi novi članovi tog sistema, ukoliko ih ima, netrivijalne su podgrupe grupe $\mathbf{H}$ i stoga je, opet prema 8.7, sistem $\overline{\mathcal{S}}$ rešiv.

Analogan je dokaz za $\overline{SI}$-grupe.

Neka je sada $\mathbf{G}$ $SN^*$-grupa, $\mathcal{S} = \{\mathbf{K}_\alpha \mid 0 \leq \alpha \leq \mu\}$ njen rastući rešiv normalni niz ($\mu$ je ordinal) i neka je $\mathbf{H}$ netrivijalna normalna podgrupa grupe $\mathbf{G}$. Prema teoremi 47.7 i njenom dokazu, rastući nizovi $\mathcal{S}$ i $\{\mathbf{E}, \mathbf{H}, \mathbf{G}\}$ imaju izomorfna proširenja koja su i rastući nizovi. U proširenju sistema $\mathcal{S}$ novi skokovi, ukoliko ih ima, javljaju se u okviru postojećih (novi elementi proširenja javljaju se između "starih" koji čine skok), što će reći da je dobijeno proširenje rešiv sistem. Prema tome, postoji rastući rešiv normalni niz grupe $\mathbf{G}$ koji prolazi kroz $\mathbf{H}$, a odatle, jasno, sledi da i faktor grupa $\mathbf{G}/\mathbf{H}$ ima rastući rešiv normalni niz.

Dokaz za $SI^*$-grupe je sličan.□

**Lema 58.4** *Podgrupa $SD$-, $SN$-, $SI$-, $SN^*$-, $SI^*$-grupe je, respektivno, $SD$-, $SN$-, $SI$-, $SN^*$-, $SI^*$-grupa; kratko (i jasno): date klase grupa su zatvorene za podgrupe.*



**Dokaz.** Tvrđenje je očigledno za $SD$-grupe. U ostalim slučajevima se pozivamo na lemu 47.6, s tim što kada su $SN^*$- i $SI^*$-grupe u pitanju imamo u vidu i primedbu na kraju dokaza te leme.□

**Lema 58.5** ($a$) *Svaka $Z$-grupa je $SI$-grupa;*

($b$) *Svaka $ZA$-grupa je $SI^*$-grupa;*

($c$) *Svaka $ZA$-grupa je $SD$-grupa;*

($d$) *Svaka $\tilde{N}$-grupa je $\overline{SN}$-grupa;*

($e$) *Svaka $N$-grupa je $SN^*$-grupa;*

($f$) *Svaka $SN^*$-grupa je $\overline{SN}$-grupa;*

($g$) *Svaka $SI^*$-grupa je $\overline{SI}$-grupa.*

**Dokaz.** ($a$) i ($b$) je trivijalno.

($c$) Neka je $\mathbf{G}$ $ZA$-grupa. Ako je Abelova, onda je $\mathbf{G}' = \mathbf{E}$. Pretpostavimo stoga da nije Abelova. Prema 55.4 njen transfinitno produženi centralni lanac stiže do cele grupe. Prema tome, $\zeta_1\mathbf{G} = \mathbf{Z}(\mathbf{G})$ je nejedinična podgrupa, prava podgrupa grupe $\zeta_2\mathbf{G}$ (gde je, podsećamo: $\zeta_2\mathbf{G}/\zeta_1\mathbf{G} = \mathbf{Z}(\mathbf{G}/\zeta_1\mathbf{G})$). Stoga, prema 8.18, postoji netrivijalni endomorfizam $\varphi$ grupe $\mathbf{G}$ koji je preslikava u njen centar. Sledi: $\mathbf{G}' \leq \mathbf{Ker}(\varphi) < \mathbf{G}$. Kako je i $\mathbf{G}'$ $ZA$-grupa, to je i $(\mathbf{G}')' = \mathbf{G}''$ prava podgrupa grupe $\mathbf{G}'$, i uopšte, za svaki ordinal $\alpha$, ukoliko već nije $\mathbf{G}^{(\alpha)} = \mathbf{E}$, biće $\mathbf{G}^{(\alpha+1)} < \mathbf{G}^{(\alpha)}$, što će reći da će, eventualno transfinitno produžen, izvodni lanac dostići jediničnu podgrupu.

($d$) Neka je $\mathbf{G}$ $\tilde{N}$-grupa, $\mathcal{S} = \{\mathbf{H}_\alpha \mid \alpha \in \Omega\}$ njen (bilo koji) kompozicioni sistem i neka $\mathbf{H}_\alpha$ i $\mathbf{H}_{\alpha+1}$ čine skok. Tada je $\mathbf{H}_{\alpha+1}/\mathbf{H}_\alpha$ grupa prostog reda, dakle ciklična. U suprotnom bi imala netrivijalnu podgrupu $\mathbf{K}/\mathbf{H}_\alpha$ i odatle $\mathbf{H}_\alpha < \mathbf{K} < \mathbf{H}_{\alpha+1}$. No, grupa $\mathbf{K}$ bi, kao $\tilde{N}$-grupa (54.8), imala normalni sistema $\mathcal{S}_1$ čiji bi jedan term bila podgrupa $\mathbf{H}_\alpha$. Analogno, grupa $\mathbf{H}_{\alpha+1}$ bi imala normalni sistem $\mathcal{S}_2$ čiji bi jedan term bila podgrupa $\mathbf{K}$. No onda bi, za $\mathcal{S}_1' = \{\mathbf{M} \in \mathcal{S}_1 \mid \mathbf{H}_\alpha \leq \mathbf{M} \leq \mathbf{K}\}$ i $\mathcal{S}_2' = \{\mathbf{N} \in \mathcal{S}_2 \mid \mathbf{K} \leq \mathbf{N} \leq \mathbf{H}_{\alpha+1}\}$, normalni sistem $\mathcal{S} \cup \mathcal{S}_1' \cup \mathcal{S}_2'$ bio pravo proširenje kompozicionog sistema $\mathcal{S}$, kontradikcija.

($e$) Dokaz ovog tvrđenja je sadržan u dokazu korolara 56.13 – pokazali smo: u (ma kojoj) $N$-grupi možemo da formiramo rastući normalni niz čiji su faktori ciklične grupe.

($f$) Neka je $\mathbf{G}$ $SN^*$-grupa sa rastućim rešivim normalnim nizom $\mathcal{S} = \{\mathbf{H}_\alpha \mid 0 \leq \alpha \leq \mu\}$, $\mu$ – ordinal, i neka je $\mathcal{T} = \{\mathbf{K}_\beta \mid \beta \in \Omega\}$ njen (ma koji) kompozicioni sistem. Neka $\mathbf{K}_\beta$ i $\mathbf{K}_{\beta+1}$ čine skok. Tada je, za neke susedne ordinale $\alpha, \alpha+1$ ($\leq \mu$), $\mathbf{K}_\beta = \mathbf{K}_\beta(\mathbf{K}_{\beta+1} \cap \mathbf{H}_\alpha) \overset{\text{def}}{=} \mathbf{K}_{\beta,\alpha} < \mathbf{K}_\beta(\mathbf{K}_{\beta+1} \cap \mathbf{H}_{\alpha+1}) \overset{\text{def}}{=} \mathbf{K}_{\beta,\alpha+1} = \mathbf{K}_{\beta+1}$. Jer, pretpostavimo da je za granični ordinal oblika $\gamma+\omega \leq \mu$, gde je, podrazumevamo $\gamma$ ili nula ili granični ordinal, za svako $n \geq k \in \omega$:

$\mathbf{K}_{\beta,\gamma+k} = \mathbf{K}_{\beta,\gamma+n}$. Onda je i $\mathbf{K}_{\beta,\gamma+\omega} = \mathbf{K}_{\beta,\gamma+k}$, jer je (videti komentar koji prethodi teoremi 47.7, a koji ovom prilikom ponavljamo):

$$\mathbf{K}_{\beta,\gamma+\omega} = \mathbf{K}_\beta(\mathbf{K}_{\beta+1} \cap \mathbf{H}_{\gamma+\omega}) = \mathbf{K}_\beta(\mathbf{K}_{\beta+1} \cap \bigcup_{r\in\omega} \mathbf{H}_{\gamma+(k+r)}) =$$

$$\bigcup_{r\in\omega} \mathbf{K}_\beta(\mathbf{K}_{\beta+1} \cap \mathbf{H}_{\gamma+(k+r)}) = \mathbf{K}_{\beta,\gamma+k}.$$

Dalje, kako kompozicioni niz nema pravih proširenja, ako uzmemo da je $\Gamma_1 = \{\alpha' < \mu \mid \mathbf{K}_{\beta,\alpha'} = \mathbf{K}_\beta\}$ i $\Gamma_2 = \{\alpha'' \leq \mu \mid \mathbf{K}_{\beta,\alpha''} = \mathbf{K}_{\beta+1}\}$, minimalni element skupa $\Gamma_2$ biće nasledni ordinal, recimo $\alpha + 1$. No tada je

$$\mathbf{K}_{\beta+1}/\mathbf{K}_\beta = \mathbf{K}_{\beta,\alpha+1}/\mathbf{K}_{\beta,\alpha} \cong \mathbf{H}_{\alpha,\beta+1}/\mathbf{H}_{\alpha,\beta} \cong$$

$$(\mathbf{H}_{\alpha,\beta+1}/\mathbf{H}_\alpha)/(\mathbf{H}_{\alpha,\beta}/\mathbf{H}_\alpha) \leq (\mathbf{H}_{\alpha+1}/\mathbf{H}_\alpha)/(\mathbf{H}_{\alpha,\beta}/\mathbf{H}_\alpha),$$

te je $\mathbf{K}_{\beta+1}/\mathbf{K}_\beta$ Abelova grupa.

($g$) Direktno prema 47.8.□

Naredna teorema je ponovo, kao i u slučaju teoreme 33.43, mali izlet u teoriju uređenih grupa.

**Lema 58.6** *Neka je* $\mathbf{H}$ *normalna konveksna podgrupa parcijalno (linearno) uređene grupe* $\mathbf{G} = \langle G, \cdot, \leq\rangle$ *(videti definiciju* 33.36*). Tada je relacija* $\leq'$ *skupa* $G/H$ *definisana sa:* $aH \leq' bH$ *akko je, za neke elemente* $a_1 \in aH$, $b_1 \in bH$, $a_1 \leq b_1$, *parcijalno (linearno), tzv. indukovano uređenje faktor grupe* $\mathbf{G}/\mathbf{H}$, *za koje konveksnim podgrupama grupe* $\mathbf{G}$ *koje sadrže* $\mathbf{H}$ *odgovaraju konveksne podgrupe grupe* $\mathbf{G}/\mathbf{H}$.

**Dokaz.** Refleksivnost i dobra definisanost (tj. nezavisnost od izbora reprezenata koseta) relacije $\leq'$ su očigledni. Neka je $aH \leq' bH$ i $bH \leq' aH$; recimo da je $ah_1 \leq bk_1$ i $bk_2 \leq ah_2$, gde $h_1, h_2, k_1, k_2 \in H$. Onda dobijamo (antisimetričnost): $h_1k_1^{-1} \leq a^{-1}b \leq h_2k_2^{-1}$ (33.37($a$)), pa kako je $\mathbf{H}$ konveksna podgrupa, $a^{-1}b \in H$ i $aH = bH$. Pretpostavimo dalje da je $aH \leq' bH$ i $bH \leq' cH$; znači, za neke elemente $h_1, h_2, h_3, h_4 \in H$ važi: $ah_1 \leq bh_2$ i $bh_3 \leq ch_4$, odnosno $h_4^{-1}c^{-1} \leq h_3^{-1}b^{-1}$. "Množenje" nejednačina (treće s prvom) daje: $h_4^{-1}c^{-1} \cdot ah_1 \leq h_3^{-1}b^{-1} \cdot bh_2 = h_3^{-1}h_2$, tj. $c^{-1}a \leq h_4h_3^{-1}h_2h_1^{-1}$ ($\in H$). Odatle, $aH \leq' cH$, te je tu i tranzitivnost. Evidentno, iz $aH \leq' bH$ sledi $cH \cdot aH = (ca)H \leq (cb)H = cH \cdot bH$. Opet, ako je, za elemente $h_1, h_2 \in H$, $ah_1 \leq bh_2$ (ostajemo pri $aH \leq' bH$), tada je $ac \cdot c^{-1}h_1c \leq bc \cdot c^{-1}h_2c$, te je i $aH \cdot cH = (ac)H \leq' (bc)H = bH \cdot cH$. Očuvanje linearnosti uređenja (ako ga imamo) je očigledno.

Neka je $\mathbf{K}$ konveksna podgrupa grupe $\mathbf{G}$ koja sadrži $\mathbf{H}$ i neka je, za elemente $a, b \in K$ i $g \in G$, $aH \leq' gH \leq' bH$. Onda je, za neke elemente $h_1, h_2, h_3, h_4 \in H$, $ah_1 \leq gh_2$ i $gh_3 \leq bh_4$, što implicira: $ah_1h_2^{-1} \leq g \leq bh_4h_3^{-1}$ i, stoga, $g \in K$, $gH \in K/H$. Trivijalno pak sledi: ako je $\mathbf{K}/\mathbf{H}$ konveksna podgrupa grupe $\mathbf{G}/\mathbf{H}$, onda je $\mathbf{K}$ konveksna podgrupa grupe $\mathbf{G}$.□



**Teorema 58.7** *Svaka linearno uređena grupa je SN-grupa.*

**Dokaz.** Neka je $\mathbf{G}$ grupa sa linearnim uređenjem $\leq$ i neka je $\mathcal{S}$ skup svih konveksnih podgrupa grupe $\mathbf{G}$; jasno, barem $\mathbf{E}, \mathbf{G} \in \mathcal{S}$. Skup $\mathcal{S}$ je linearno uređen relacijom inkluzije. Jer, neka $\mathbf{A}, \mathbf{B} \in \mathcal{S}$ i $b \in B \setminus A$. Možemo pretpostaviti da je $b > e$ (u suprotnom bismo posmatrali element $b^{-1}$). Za svako $a \in A$ važi $a < b$, inače bismo, za neko $a \in A$ imali $e < b \leq a$ i $b \in A$, protivno pretpostavci. Stoga je, za svako $a \in A$ ili $e \leq a < b$ ili $e \leq a^{-1} < b$, u svakom slučaju je $a \in B$ i $\mathbf{A} < \mathbf{B}$. Neka podgrupe $\mathbf{A}$ i $\mathbf{B}$ iz $\mathcal{S}$ čine skok, znači među njima nema konveksnih podgrupa. Onda je, za svako $b \in B$, $b^{-1}Ab < b^{-1}Bb = B$, a $b^{-1}Ab$ je takođe konveksna podgrupa: ako je, za $a_1, a_2 \in A$, $b^{-1}a_1b \leq c \leq b^{-1}a_2b$, tada je $a_1 \leq bcb^{-1} \leq a_2$, te je $bcb^{-1} \in A$ i $c \in b^{-1}Ab$. Prema tome, $b^{-1}Ab \leq A$ i $\mathbf{A} \lhd \mathbf{B}$. Faktor grupa $\mathbf{B}/\mathbf{A}$ je, prema prethodnoj lemi, linearno uređena relacijom $\leq'$ i kako je bez konveksnih podgrupa, to je prema 33.40 Arhimedova, a onda i Abelova (izomorfna podgrupi aditivne grupe realnih brojeva uređenoj prirodnom relacijom – 33.43).■

**Lema 58.8** *Minimalna normalna podgrupa (ukoliko postoji) SI-grupe je Abelova.*

**Dokaz.** Neka je $\mathbf{A}$ minimalna normalna podgrupa $SI$-grupe $\mathbf{G}$ i $\{\mathbf{H}_\alpha \mid \alpha < \Omega\}$ rešiv invarijantni sistem grupe $\mathbf{G}$. Onda je, za svako $\alpha \in \Omega$, $\mathbf{H}_\alpha \cap \mathbf{A}$ ili jedinična podgrupa ili $\mathbf{A}$. Skupovi $\Omega_1 = \{\alpha \in \Omega \mid \mathbf{H}_\alpha \cap \mathbf{A} = \mathbf{E}\}$ i $\Omega_2 = \{\alpha \in \Omega \mid \mathbf{H}_\alpha \cap \mathbf{A} = \mathbf{A}\}$ čine presek linearno uređenog skupa $\Omega$. $\Omega_1$ je, jasno, zatvoren naniže, pri čemu $\Omega_1$ ima maksimalni i $\Omega_2$ minimalni element. Jer, $(\bigcup_{\alpha\in\Omega_1} \mathbf{H}_\alpha) \cap \mathbf{A} = \bigcup_{\alpha\in\Omega_1}(\mathbf{H}_\alpha \cap \mathbf{A}) = \mathbf{E}$ i, još očiglednije, $(\bigcap_{\alpha\in\Omega_2} \mathbf{H}_\alpha) \cap \mathbf{A} = \mathbf{A}$. Stoga, ako je $\beta$ maksimalni element skupa $\Omega_1$ i $\beta+1$ minimalni element skupa $\Omega_2$, grupe $\mathbf{H}_\beta$ i $\mathbf{H}_{\beta+1}$ formiraju skok, $\mathbf{H}_{\beta+1}/\mathbf{H}_\beta$ je Abelova grupa, pa je i $\mathbf{A} \cong (\mathbf{A} \times \mathbf{H}_\beta)/\mathbf{H}_\beta \leq \mathbf{H}_{\beta+1}/\mathbf{H}_\beta$ Abelova grupa.□.

**Korolar 58.9** *Grupa je* $\overline{SI}$*-grupa akko je svaka njena homomorfna slika SI-grupa.*

**Dokaz.** Pravac ($\Longrightarrow$) je jasan; svaka $\overline{SI}$-grupa je trivijalno $SI$-grupa i homomorfna slika $\overline{SI}$-grupe je opet $\overline{SI}$-grupa.

Pretpostavimo sada da je $\mathbf{G}$ grupa čija je svaka homomorfna slika $SI$-grupa (posebno, $\mathbf{G}$ je $SI$-grupa) i neka je $\{\mathbf{H}_\alpha \mid \alpha \in \Omega\}$ njen glavni sistem u kome $\mathbf{H}_\alpha$ i $\mathbf{H}_{\alpha+1}$ čine skok. No tada je $\mathbf{H}_{\alpha+1}/\mathbf{H}_\alpha$ minimalna normalna podgrupa $SI$-grupe $\mathbf{G}/\mathbf{H}_\alpha$, te je prema prethodnoj lemi Abelova.□

**Lema 58.10** *Svaka* $SI^*$*-grupa ispunjava uslov* $\mathcal{D}$ *(videti teoremu* 49.26*).*

**Dokaz.** U osnovi ponavljamo dokaz pomenute teoreme. Krenimo samo. Neka su $\mathbf{A}$ i $\mathbf{B}$ podgrupe $SI^*$-grupe $\mathbf{G}$, $\mathbf{A}$ maksimalna podgrupa grupe $\mathbf{B}$ i neka

je $\mathbf{N}_1$ maksimalna normalna podgrupa grupe $\mathbf{B}$ sadržana u $\mathbf{A}$. Faktor grupa $\mathbf{B}/\mathbf{N}_1$ ima rešiv rastući invarijantni niz: $\overline{\mathbf{E}} < \mathbf{N}/\mathbf{N}_1 = \mathbf{B}_1/\mathbf{N}_1 < \cdots < \mathbf{B}_\mu/\mathbf{N}_1 = \mathbf{B}/\mathbf{N}_1$. Kako je $\mathbf{N}$ normalna podgrupa grupe $\mathbf{B}$ koja strogo sadrži $\mathbf{N}$, to $\mathbf{N} \not\leq \mathbf{A}$ i $\mathbf{AN} = \mathbf{B}$ (primetimo: ako je $\mathbf{N}$ baš $\mathbf{B}$, onda je $\mathbf{B}' \leq \mathbf{N}_1 \leq \mathbf{A}$ i $\mathbf{A}$ je normalna podgrupa grupe $\mathbf{B}$). Sledi (kao i u 49.26): $\mathbf{A} \cap \mathbf{N} = \mathbf{N}_1$.□

**Lema 58.11** (*a*) *Periodična $SN^*$-grupa je lokalno konačna;*

(*b*) *Periodična lokalno rešiva grupa je lokalno konačna.*

(*c*) *$SI$-grupa sa konačno mnogo klasa konjugovanih elemenata je konačna.*

**Dokaz.** (*a*) Neka je $\mathbf{G}$ periodična $SN^*$-grupa i neka je $\{\mathbf{H}_\alpha \mid \alpha \leq \mu\}$, $\mu$ - ordinal, njen rastući rešiv niz. (Transfinitnom) indukcijom pokazujemo da je svaka od podgrupa $\mathbf{H}_\alpha$, $\alpha \leq \mu$, lokalno konačna. Za $\mathbf{H}_0 = \mathbf{E}$ je to (više nego) trivijalno. Pretpostavimo da je tvrđenje tačno za sve ordinale $\beta$ manje od $\alpha$. Ako je $\alpha$ nasledni ordinal, onda su i $\mathbf{H}_\alpha/\mathbf{H}_{\alpha-1}$, kao periodična Abelova grupa, i $\mathbf{H}_{\alpha-1}$, po induktivnoj pretpostavci, lokalno konačne grupe, te je i $\mathbf{H}_\alpha$ lokalno konačna grupa (13.3(*b*)). Ako je $\alpha$ granični ordinal, $\mathbf{H}_\alpha$ je, jasno, kao unija lokalno konačnih grupa, lokalno konačna.

(*b*) Primetimo samo: prema prethodnoj tački je svaka periodična rešiva grupa lokalno konačna.

(*c*) Kako grupa sa konačno mnogo klasa konjugovanih elemenata ne može imati beskonačan invarijantni sistem, svaka takva $SI$-grupa je rešiva. Neka je $\mathbf{G}$ jedna od njih i neka je $\mathbf{E} = \mathbf{H}_0 < \mathbf{H}_1 < \cdots < \mathbf{H}_{n-1} < \mathbf{H}_n = \mathbf{G}$ njen rešiv niz. Abelova grupa $\mathbf{G}/\mathbf{H}_{n-1}$ i sama (kao homomorfna slika grupe sa konačno mnogo klasa konjugovanih elemenata) ima konačno mnogo klasa konjugovanih elemenata, tj. konačna je. Dovoljno je zato da pokažemo da je i $\mathbf{H}_{n-1}$ sa konačno mnogo klasa konjugovanih elemenata. Pretpostavimo suprotno. Onda u $\mathbf{H}_{n-1}$ postoji beskonačno mnogo elemenata $a_1, \ldots, a_n, \ldots$, koji su uzajamno konjugovani u $\mathbf{G}$, ali među kojima nikoja dva nisu konjugovana u $\mathbf{H}_{n-1}$. Neka je, za $i \geq 2$, $a_1 = b_i^{-1} a_i b_i$, $b_i \in G\ (\backslash H)$. Svakako je, za neko $i, j \geq 2$, $i \neq j$, $b_i H_{n-1} = b_j H_{n-1}$, pa ako je $b_j = b_i h$ za $h \in H_{n-1}$, sledi:

$$a_i = b_i a_1 b_i^{-1} = b_i b_j^{-1} a_j b_j b_i^{-1} = (b_i h b_i^{-1})^{-1} a_j (b_i h b_i^{-1}).$$

Ispada da su $a_i$ i $a_j$ konjugovani u $H_{n-1}$, kontradikcija.□

## 59 Lokalne teoreme

Ovog puta trebaće nam nešto od teorije predikatskog računa drugog reda. Pored toga, umesto algebri sada ćemo generalno razmatrati *modele* (u ruskoj literaturi je češći naziv *algebarski sistemi*). Prema tome, u jeziku u kojem definišemo strukture pored funkcijskih na raspolaganju su nam i predikatski (relacijski) simboli. Ako je $f$ funkcijsko slovo arnosti $m$, njegova interpretacija



u datom modelu $\mathbf{A}$, u oznaci $f^{\mathbf{A}}$, je neka $m$-arna operacija nad domenom modela - $A$ ($f^{\mathbf{A}} : A^m \longrightarrow A$); ako je $R$ relacijski simbol arnosti $n$, njegova interpretacija u modelu $\mathbf{A}$, u oznaci $R^{\mathbf{A}}$, je neka $n$-arna relacija nad $A$ ($R^{\mathbf{A}} \subseteq A^n$).

Neprazan podskup $B$ domena modela $\mathbf{A}$ ($\emptyset \neq B \subseteq A$) je domen *podmodela* (**B**) modela $\mathbf{A} = \langle A, (f_i^{\mathbf{A}})_{i\in I}, (R_j^{\mathbf{A}})_{j\in J}\rangle$ akko je zatvoren za sve operacije. To će reći: ako je, za $i \in I$, $f_i$ funkcijsko slovo arnosti $m_i$, onda je $f_i^{\mathbf{A}}|_{B^{m_i}}$ operacija (dužine $m_i$) nad $B$ (uporediti sa 3.1); kraće ćemo tu operaciju obeležiti sa $f_i^{\mathbf{B}}$. Relacijsko slovo $R_j$ arnosti $n_j$ u modelu $\mathbf{B}$ interpretiramo sa $R_j^{\mathbf{A}} \cap B^{n_j}$; naravno, pisaćemo $R_j^{\mathbf{B}}$.

Familija podmodela modela $\mathbf{A}$, $\mathcal{B} = \{\mathbf{B}_k \mid k \in K\}$, je *lokalni sistem* modela $\mathbf{A}$ (videti 17.1), kaže se i *lokalni pokrivač*, akko je $A = \bigcup_{k\in K} B_k$ i svaka dva podmodela iz $\mathcal{B}$ su sadržana u nekom podmodelu iz $\mathcal{B}$.

Pretpostavljamo u nastavku elementarno znanje o predikatskom računu prvog reda i teoriji modela (kakvo se stiče na svakom polaznom kursu iz elemenata matematičke logike). Formule predikatskog računa drugog reda se formiraju kao i formule računa prvog reda, s tim što sada dozvoljavamo i kvantifikovanja predikatskih simbola; u tom smislu ćemo razlikovati dve vrste promenljivih – *predmetne* ("obične") (obeležavaćemo ih sa $x_1, x_2, x_3, \ldots$ ili $x, y, z, \ldots$) i *predikatske promenljive* (obeležavaćemo ih sa $P_1, P_2, P_3, \ldots$ ili $P, Q, R, \ldots$). Predikatski račun drugog reda je mnogo "izražajniji" od predikatskog računa prvog reda. Ilustrovaćemo to, za početak, sa sledećim primerima iz teorije grupa za čiji jezik ćemo uzeti $\mathcal{L} = \{\cdot, ^{-1}, e\}$.

**Primer 59.1** (*a*) *Grupa je prosta akko zadovoljava formulu*

$$\forall P\{[\forall x \forall y(P(x) \wedge P(y) \Longrightarrow P(x \cdot y^{-1})) \wedge \exists x \neg P(x) \wedge \exists x(P(x) \wedge x \neq e)] \Longrightarrow$$
$$\exists x \exists y(P(x) \wedge \neg P(y) \wedge \neg P(y^{-1} \cdot x \cdot y)\}.$$

**Dokaz.** $P$ je unarno relacijsko slovo; antecedent formule u okviru vitičastih zagrada nam kaže da je (svaka) realizacija slova $P$ netrivijalna podgrupa, konsekvent pak da nijedna takva podgrupa nije normalna. U vezi sa ovim primerom videti i 59.11.

(*b*) *Grupa* $\mathbf{G}$ *se može parcijalno urediti akko u njoj važi formula*

$$\exists P\{\forall x \forall y \forall z[P(x,x) \wedge (P(x,y) \wedge P(y,x) \Longrightarrow x = y) \wedge (P(x,y) \wedge P(y,z) \Longrightarrow$$
$$P(x,z)) \wedge (P(x,y) \Longrightarrow P(x \cdot z, y \cdot z) \wedge P(z \cdot x, z \cdot y))]\}.$$

**Dokaz.** $P$ je binarno relacijsko slovo, a njegova realizacija je parcijalno uređenje, saglasno sa operacijom $\cdot$ u grupi (a onda i sa operacijom $^{-1}$).

(*c*) *Grupa* $\mathbf{G}$ *se može linearno urediti akko u njoj važi formula*

$$\exists P\{\forall x \forall y \forall z[P(x,x) \wedge (P(x,y) \wedge P(y,x) \Longrightarrow x = y) \wedge (P(x,y) \wedge P(y,z) \Longrightarrow$$
$$P(x,z)) \wedge (P(x,y) \vee P(y,x)) \wedge (P(x,y) \Longrightarrow (P(x \cdot z, y \cdot z) \wedge P(z \cdot x, z \cdot y))]\}.$$□

Svaka formula predikatskog računa drugog reda je ekvivalentna nekoj formuli u tzv. *preneks normalnoj formi*, dakle formuli kod koje su svi kvantifikatori grupisani na početku formule. Dokaz ovog tvrđenja je u osnovi analogan standardnom dokazu za formule predikatskog računa prvog reda (videti npr. [110], glava II, paragraf 10). Formula je *predmetno-univerzalna* akko je ekvivalentna formuli u preneks normalnoj formuli koja nema egzistencijalnih kvanitifikatora koji bi se odnosili na predmetne promenljive. Formula je *kvazi-univerzalna* akko je dobijena univerzalnim kvantifikovanjem svih slobodnih predikatskih promenljivih u formuli koja je opet dobijena vezivanjem logičkim veznicima predmetno-univerzalnih formula bez slobodnih predmetnih promenljivih. U gornjem primeru u oba slučaja radi se o kvazi-univerzalnim formulama (druga je evidentno predmetno-univerzalna, prva je ekvivalentna jednoj kvazi-univerzalnoj formuli), bolje reći kvazi-univerzalnim rečenicama; kvazi-univerzalne formule su bez slobodnih promenljivih bilo koje vrste.

Kada pišemo za formulu $\Psi$: $\Psi \equiv \Psi(x_1, \ldots, x_m, P_1, \ldots, P_n)$, $m, n \geq 0$, time naglašavamo da je skup slobodnih predmetnih promenljivih formule $\Psi$ podskup skupa $\{x_1, \ldots, x_m\}$, skup slobodnih predikatskih promenljivih podskup skupa $\{P_1, \ldots, P_n\}$. Posebno, ako je npr. $m = 0$, formula $\Psi$ je bez slobodnih predmetnih promenljivih. Ako formula $\Psi$ važi u modelu $\mathbf{A}$ kada slobodne predmetne promenljive "uzmu vrednosti" $a_1, \ldots, a_m$, a realizacija slobodnih predikatskih promenljivih je, respektivno, $P_1^{\mathbf{A}}, \ldots, P_n^{\mathbf{A}}$, to zapisujemo, standardno, sa

$$\mathbf{A} \models \Psi[a_1, \ldots, a_m, P_1^{\mathbf{A}}, \ldots, P_n^{\mathbf{A}}].$$

Prema samoj definiciji važenja formule u modelu je:

$$\mathbf{A} \models \Psi(x_1, \ldots, x_m, P_1, \ldots, P_n)$$

akko

$$\mathbf{A} \models \forall P_1 \ldots \forall P_n \forall x_1 \ldots \forall x_m \Psi(x_1, \ldots, x_m, P_1, \ldots, P_n);$$

naravno, univerzalni kvantifikatori obe vrste su uzajamno "permutabilni".

Nešto moramo reći i o *filtru*. Neprazan podskup $\mathcal{F}$ partitivnog skupa $P(I)$ nepraznog skupa $I$ je filter nad $I$ akko za svako $X, Y \in \mathcal{F}$ i svako $Z \in P(I)$ važi: $X \cap Y \in \mathcal{F}$ i ako je $X \subseteq Z$, tada je $Z \in \mathcal{F}$. Filter je pravi akko je pravi podskup skupa $P(I)$. Jasno, filter $\mathcal{F}$ je pravi akko $\emptyset \notin \mathcal{F}$. Pravi filter koji nije strogo sadržan ni u jednom drugom pravom filtru zove se *ultrafilter*.

Egzistencija ultrafiltra je zagarantovana lemom Zorna; prema njoj je svaki pravi filter sadržan u nekom ultrafiltru. Filter $\mathcal{F}$ (nad $I$) je *glavni* akko je oblika $\{Y \mid Y \supseteq X\}$ (za neki podskup $X$ skupa $I$). Glavni ultrafilter je oblika $\{Y \mid i \in Y\}$ za neko $i \in I$.

**Lema 59.2** *Podskup $\mathcal{X}$ partivnog skupa $P(I)$ sadržan je u nekom pravom filtru (nad $I$) akko ima svojstvo konačnog preseka, tj. akko je presek bilo kojeg konačnog podskupa skupa $\mathcal{X}$ neprazan skup.*



**Dokaz.** Pravac ($\Longrightarrow$) je jasan, a ako $\mathcal{X}$ ima svojstvo konačnog preseka, onda je

$$\mathcal{F} = \{Y \in P(I) \mid Y \supseteq X_1 \cap \ldots \cap X_m,\ X_i \in \mathcal{X},\ i = 1, \ldots, m,\ m = 1, 2, \ldots\}$$

pravi filter (koji sadrži $\mathcal{X}$).□

**Lema 59.3** *Za pravi filter $\mathcal{F}$ nad $I$ sledeći uslovi su ekvivalentni:*

(1) *$\mathcal{F}$ je ultrafilter;*

(2) *Za svako $X \in P(I)$ važi: $X \in \mathcal{F}$ akko $X^c \stackrel{\text{def}}{=} I \setminus X \notin \mathcal{F}$;*

(3) *$\mathcal{F}$ je prost filter, tj. ako je, za $X, Y \in P(I)$, $X \cup Y \in \mathcal{F}$ onda je $X \in \mathcal{F}$ ili $Y \in \mathcal{F}$.*

**Dokaz.** (1) $\Longrightarrow$ (2) Pretpostavimo da je $\mathcal{F}$ ultrafilter. Ako bismo za neko $X \in P(I)$ imali $X, X^c \in \mathcal{F}$, tada $\emptyset \in \mathcal{F}$ i $\mathcal{F} = P(I)$, kontradikcija. Ako bi za $Y \in P(I)$ bilo $Y, Y^c \notin \mathcal{F}$, onda jedna od familija $\mathcal{F} \cup \{Y\}$, $\mathcal{F} \cup \{Y^c\}$ ima svojstvo konačnog preseka. Pretpostavimo suprotno. Tada je, za neke elemente $X_1, X_2$ filtra $\mathcal{F}$, $X_1 \cap Y = X_2 \cap Y^c = \emptyset$, te je $X_1 \cap X_2 = X_1 \cap X_2 \cap I = X_1 \cap X_2 \cap (Y \cup Y^c) = (X_1 \cap X_2 \cap Y) \cup (X_1 \cap X_2 \cap Y^c) = \emptyset \in \mathcal{F}$, kontradikcija. Ali, ako npr. familija $\mathcal{F} \cup \{Y\}$ ima svojstvo konačnog preseka, prema prethodnoj lemi je sadržana u nekom pravom filtru, kontradikcija ponovo.

(2) $\Longrightarrow$ (3) Neka važi (2) ali ne i (3); dakle, za neko $X, Y$ ($\in P(I)$) je $X \cup Y \in \mathcal{F}$, dok $X, Y \notin \mathcal{F}$. Tada $X^c, Y^c \in \mathcal{F}$, pa je i $X^c \cap Y^c = (X \cup Y)^c \in \mathcal{F}$. Sledi: $\emptyset \in \mathcal{F}$, kontradikcija.

(3) $\Longrightarrow$ (1) Neka važi (3) ali ne i (1). Onda je filter $\mathcal{F}$ strogo sadržan u nekom pravom filtru $\mathcal{F}_1$. Neka je $Z \in \mathcal{F}_1 \setminus \mathcal{F}$. No, $Z \cup Z^c = I \in \mathcal{F}$ i kako nije $Z \in \mathcal{F}$, mora biti $Z^c \in \mathcal{F}$. Stoga $\emptyset \in \mathcal{F}_1$, kontradikcija.□

Ako je $\mathcal{A} = \{\mathbf{A}_i \mid i \in I\}$ lokalni sistem (pokrivač) modela $\mathbf{A}$ i, za $i \in I$, $I_i \stackrel{\text{def}}{=} \{j \in I \mid A_i \subseteq A_j\}$, onda familija $\mathcal{D} = \{I_i \mid i \in I\}$ ima svojstvo konačnog preseka: ako su, za $i, j \in I$, podmodeli $\mathbf{A}_i$ i $\mathbf{A}_j$ sadržani u (podmodelu) $\mathbf{A}_k$, tada je $I_i \cap I_j \supseteq I_k$. Prema tome, $\mathcal{D}$ je sadržan u nekom ultrafiltru $\mathcal{F}$. Ako u svakom podmodelu $\mathbf{A}_i$ ($i \in I$) imamo realizaciju nekog predikata $P$ arnosti $n$ – $P^{\mathbf{A}_i}$, onda je jedna realizacija predikata $P$ u $\mathbf{A}$, obeležimo je, prema knjizi [78] po kojoj i teče ova priča, sa $lim\, P^{\mathbf{A}_i}$, data sa:

$$(a_1, \ldots, a_n) \in lim\, P^{\mathbf{A}_i} \text{ akko } \{i \in I \mid a_1, \ldots, a_n \in A_i,\ (a_1, \ldots, a_n) \in P^{\mathbf{A}_i}\} \in \mathcal{F}.$$

U opštem, $lim\, P^{\mathbf{A}_i} \cap A_j^n$ nije jednako sa $P^{\mathbf{A}_j}$. Ali, ako je $P^{\mathbf{A}}$ ($\subseteq A^n$) jedna realizacija predikata $P$ u $\mathbf{A}$ i $P^{\mathbf{A}_i} = P^{\mathbf{A}} \cap A_i^n$, tada je $lim\, P^{\mathbf{A}_i} = P^{\mathbf{A}}$. Jer, ako je (za $a_1, \ldots, a_n \in A$) $a_1, \ldots, a_n \in A_k$ (relacija inkluzije je usmerena), biće, zbog $I_k \in \mathcal{F}$: $(a_1, \ldots, a_n) \in P^{\mathbf{A}}$ akko $\{i \in I \mid a_1, \ldots, a_n \in A_i,\ (a_1, \ldots, a_n) \in P^{\mathbf{A}_i}\} \in \mathcal{F}$. Stoga je, proizilazi, svaka realizacija predikata $P$ u $\mathbf{A}$ neki "limes".

**Teorema 59.4** *Za predmetno-univerzalnu formulu $\Phi$ imamo:*

*(a) ako $\Phi$ važi u modelu $\mathbf{A}$, onda važi i u svakom njegovom podmodelu;*

*(b) ako $\Phi$ važi u svakom podmodelu nekog lokalnog sistema modela $\mathbf{A}$, onda važi i u $\mathbf{A}$.*

**Dokaz.** $(a)$ Pretpostavićemo da je formula $\Phi \equiv \Phi(x_1, \ldots, x_m, P_1, \ldots, P_n)$, $m, n \geq 0$, u preneks normalnoj formi, a arnost predikatskih promenljivih, redom, $k_1, \ldots, k_n$. Neka je dalje $\mathbf{B}$ podmodel modela $\mathbf{A}$. Indukcijom po broju kvantifikatora (obe vrste) dokazujemo: za sve elemente $b_1, \ldots, b_m$ iz $B$ i sve realizacije $P_1^{\mathbf{A}}, \ldots, P_n^{\mathbf{A}}$ predikatskih promenljivih u $\mathbf{A}$ važi:
ako

$$\mathbf{A} \models \Phi[b_1, \ldots, b_m, P_1^{\mathbf{A}}, \ldots, P_n^{\mathbf{A}}],$$

onda

$$\mathbf{B} \models \Phi[b_1, \ldots, b_m, P_1^{\mathbf{A}} \cap B^{k_1}, \ldots, P_n^{\mathbf{A}} \cap B^{k_n}].$$

Ako je $\Phi$ bez kvantifikatora, to je (gotovo) očigledno. Tvrđenje je, naime, (sigurno) očigledno za tzv. *bazične formule* – atomarne i negacije atomarnih (prema samoj definiciji podmodela), a svaka kvantifikatorski slobodna formula ekvivalentna je nekoj formuli u *disjunktivnoj normalnoj formi*, tj. nekoj disjunkciji čiji su disjunkti konjunkcije bazičnih formula. Pretpostavimo sada da je tvrđenje tačno za sve formule sa manje od $n$ $(> 0)$ kvantifikatora i neka je $\Phi$ formula sa $n$ kvantifikatora. Tada je $\Phi$ formula jednog od oblika: (1) $\forall x \Psi(x_1, \ldots, x_m, x, P_1, \ldots, P_n)$; (2) $\forall P \Psi(x_1, \ldots, x_m, P_1, \ldots, P_n, P)$; (3) $\exists P \Psi(x_1, \ldots, x_m, P_1, \ldots, P_n, P)$, gde je $\Psi$ predmetno-univerzalna formula (u preneks normalnoj formi) sa $n - 1$ kvantifikatora. Slučajevi (1) i (2) su trivijalni; napomenimo samo da je svaka relacija nad skupom $B$ restrikcija nekih relacija nad skupom $A$. Razmotrimo treći, uzimajući da je predikatska promenljiva $P$ arnosti $k$.

(3) Prema uslovu je, za neku interpretaciju predikatske promenljive $P$ – $P^{\mathbf{A}}$: $\mathbf{A} \models \Psi[b_1, \ldots, b_m, P_1^{\mathbf{A}}, \ldots, P_n^{\mathbf{A}}, P^{\mathbf{A}}]$. Odatle je, prema induktivnoj hipotezi:

$$\mathbf{B} \models \Psi[b_1, \ldots, b_m, P_1^{\mathbf{A}} \cap B^{k_1}, \ldots, P_n^{\mathbf{A}} \cap B^{k_n}, P^{\mathbf{A}} \cap B^k],$$

dakle i

$$\mathbf{B} \models \exists P \Psi[b_1, \ldots, b_m, P_1^{\mathbf{A}} \cap B^{k_1}, \ldots, P_n^{\mathbf{A}} \cap B^{k_n}],$$

tj.

$$\mathbf{B} \models \Phi[b_1, \ldots, b_m, P_1^{\mathbf{A}} \cap B^{k_1}, \ldots, P_n^{\mathbf{A}} \cap B^{k_n}].$$

$(b)$ Neka predmetno-univerzalna formula $\Phi \equiv \Phi(x_1, \ldots, x_m, P_1, \ldots, P_n)$, data u preneks normalnoj formi, važi u svakom podmodelu nekog lokalnog sistema $\mathcal{A} = \{\mathbf{A}_i \mid i \in I\}$ modela $\mathbf{A}$ i neka je $\mathcal{F}$ ultrafilter nad $I$ koji sadrži



familiju $\{I_i \mid i \in I\}$, gde je, podsećamo, $I_i = \{j \in I \mid A_i \subseteq A_j\}$. Pokazujemo, što je i dovoljno, da za svako $a_1, \ldots, a_m$ iz $A$ važi: iz

$$\{i \in I \mid a_1, \ldots, a_m \in A_i,\ \mathbf{A}_i \models \Phi[a_1, \ldots, a_m, P_1^{\mathbf{A}_i}, \ldots, P_n^{\mathbf{A}_i}]\} \in \mathcal{F}$$

sledi

$$\mathbf{A} \models \Phi[a_1, \ldots, a_m, lim\, P_1^{\mathbf{A}_i}, \ldots, lim\, P_n^{\mathbf{A}_i}].$$

Zaista, $\{i \in I \mid a_1, \ldots, a_m \in A_i\} \in \mathcal{F}$ (pošto $\mathcal{F}$ sadrži familiju $\{I_i \mid i \in I\}$), a ako $a_1, \ldots, a_m \in A_k$, po uslovu teoreme $\mathbf{A}_k \models \Phi[a_1, \ldots, a_m, P_1^{\mathbf{A}_k}, \ldots, P_n^{\mathbf{A}_k}]$. Ne zaboravljamo, naravno, i to ćemo stalno imati na umu u diskusijama koje slede, da je svaka realizacija u $\mathbf{A}$ (bilo kog) predikata "limes" (videti napomene koje prethode teoremi). Dokaz date implikacije je opet indukcijom po broju kvantifikatora.

Ako je $\Phi$ bez kvantifikatora važiće zapravo ekvivalencija:

$$\{i \in I \mid a_1, \ldots, a_m \in A_i,\ \mathbf{A}_i \models \Phi[a_1, \ldots, a_m, P_1^{\mathbf{A}_i}, \ldots, P_n^{\mathbf{A}_i}]\} \in \mathcal{F}$$

akko

$$\mathbf{A} \models \Phi[a_1, \ldots, a_m, lim\, P_1^{\mathbf{A}_i}, \ldots, lim\, P_n^{\mathbf{A}_i}].$$

Njen dokaz je indukcijom po broju logičkih veznika. Pretpostavićemo da imamo samo konjunkciju $(\wedge)$ i negaciju $(\neg)$ (to nam je dozvoljeno jer ovi veznici čine tzv. *bazu* propozicionalnog računa – svaki drugi logički veznik se može preko njih izraziti). Neka je $\Phi$ bez kvantifikatora. Ako je atomarna formula, slučajevi $\Phi \equiv t_1 = t_2$ (gde su $t_1, t_2$ termi datog jezika) i $\Phi \equiv R(t_1, \ldots, t_r)$, gde je $R$ relacijsko slovo datog jezika, su trivijalni, a treći slučaj, $\Phi \equiv P(t_1, \ldots, t_s)$, rešava definicija "limesa". U induktivnom koraku imamo dva slučaja: $\Phi \equiv \Psi(x_1, \ldots, x_m, P_1, \ldots, P_n) \wedge \Theta(x_1, \ldots, x_m, P_1, \ldots, P_n)$ i $\Phi \equiv \neg\Psi(x_1, \ldots, x_m, P_1, \ldots, P_n)$. Za prvi nam je dovoljan samo filter, za drugi nam baš treba ultrafilter:

$\mathbf{A} \models \Phi[a_1, \ldots, a_m, lim\, P_1^{\mathbf{A}_i}, \ldots, lim\, P_n^{\mathbf{A}_i}]$
akko
$\mathbf{A} \not\models \Psi[a_1, \ldots, a_m, lim\, P_1^{\mathbf{A}_i}, \ldots, lim\, P_n^{\mathbf{A}_i}]$
akko (prema induktivnoj hipotezi)
$\{i \in I \mid a_1, \ldots, a_m \in A_i,\ \mathbf{A}_i \models \Psi[a_1, \ldots, a_m, P_1^{\mathbf{A}_i}, \ldots, P_n^{\mathbf{A}_i}]\} \notin \mathcal{F}$
akko
$\{i \in I \mid a_1, \ldots, a_m \notin A_i$ ili $\mathbf{A}_i \not\models \Psi[a_1, \ldots, a_m, P_1^{\mathbf{A}_i}, \ldots, P_n^{\mathbf{A}_i}]\} \in \mathcal{F}$
akko
$\{i \in I \mid a_1, \ldots, a_m \in A_i,\ \mathbf{A}_i \models \Phi[a_1, \ldots, a_m, P_1^{\mathbf{A}_i}, \ldots, P_n^{\mathbf{A}_i}]\} \in \mathcal{F}$;
u slučaju poslednje ekvivalencije ponovo se pozivamo na: $\{I_i \mid i \in I\} \subseteq \mathcal{F}$.

U nastavku pretpostavljamo da je tvrđenje tačno za sve predmetno-univerzalne formule (u preneks normalnoj formi) sa manje od $l$ $(> 0)$ kvantifikatora i neka je $\Phi$ sa $l$ kvantifikatora. Kao i u tački $(a)$ razlikujemo slučajeve:

$(i)$ $\Phi \equiv \forall x\, \Psi(x_1, \ldots, x_m, x, P_1, \ldots, P_n)$;

$(ii)$ $\Phi \equiv \forall P\, \Psi(x_1, \ldots, x_m, P_1, \ldots, P_n, P)$

i

$(iii)$ $\exists P\, \Psi(x_1, \ldots, x_m, P_1, \ldots, P_n, P)$.

$(i)$ Ako $a, a_1, \ldots, a_m \in A_i$, onda je, po uslovu teoreme, za svako $j \in I_i$ i svaku realizaciju $P_1^{\mathbf{A}_j}, \ldots, P_n^{\mathbf{A}_j}$ predikata $P_1, \ldots, P_n$ u $\mathbf{A}_j$:

$\mathbf{A}_j \models \Psi[a_1, \ldots, a_m, a, P_1^{\mathbf{A}_j}, \ldots, P_n^{\mathbf{A}_j}]$.

Dakle,

$(I_i \subseteq) \{j \in I \mid a_1, \ldots, a_m, a \in A_j,\ \mathbf{A}_j \models \Psi[a_1, \ldots, a_m, a, P_1^{\mathbf{A}_j}, \ldots, P_n^{\mathbf{A}_j}]\} \in \mathcal{F}$,

te po induktivnoj pretpostavci:

$\mathbf{A} \models \Psi[a_1, \ldots, a_m, a, lim\, P_1^{\mathbf{A}_i}, \ldots, lim\, P_n^{\mathbf{A}_i}]$.

Znači, $\mathbf{A} \models \Phi[a_1, \ldots, a_m, lim\, P_1^{\mathbf{A}_i}, \ldots, lim\, P_n^{\mathbf{A}_i}]$.

$(ii)$ Neka je $P$ arnosti $k$ i $R$ ma koja $k$-arna relacija nad $A$ $(R \subseteq A^k)$. Opet će, po uslovu teoreme, važiti: ako $a_1, \ldots, a_m \in A_i$, onda:

$\mathbf{A}_i \models \Psi[a_1, \ldots, a_m, P_1^{\mathbf{A}_i}, \ldots, P_n^{\mathbf{A}_i}, R \cap A_i^k]$,

(gde su, kao i ranije, $P_1^{\mathbf{A}_i}, \ldots, P_n^{\mathbf{A}_i}$ proizvoljne realizacije predikata $P_1, \ldots, P_n$), pa prema induktivnoj pretpostavci:

$\mathbf{A} \models \Psi[a_1, \ldots, a_m, limP_1^{\mathbf{A}_i}, \ldots, limP_n^{\mathbf{A}_i}, R]$.

Stoga $\mathbf{A} \models \forall P\, \Phi[a_1, \ldots, a_m, lim\, P_1^{\mathbf{A}_i}, \ldots, lim\, P_n^{\mathbf{A}_i}]$.

$(iii)$ Prema uslovu teoreme, u svakom podmodelu koji sadrži elemente $a_1$, $\ldots$, $a_m$ postoji interpretacija predikatske promenljive $P$, neka je to $P^{\mathbf{A}_i}$, za koju je:

$\mathbf{A}_i \models \Psi[a_1, \ldots, a_m, P_1^{\mathbf{A}_i}, \ldots, P_n^{\mathbf{A}_i}, P^{\mathbf{A}_i}]$.

Prema induktivnoj hipotezi

$\mathbf{A} \models \Psi[a_1, \ldots, a_m, lim\, P_1^{\mathbf{A}_i}, \ldots, lim\, P_n^{\mathbf{A}_i}, lim\, P^{\mathbf{A}_i}]$;

znači,

$\mathbf{A} \models \exists P\, \Psi[a_1, \ldots, a_m, lim\, P_1^{\mathbf{A}_i}, \ldots, lim\, P_n^{\mathbf{A}_i}]$.■

**Teorema 59.5** *(A. I. Maljcev). Ako kvazi-univerzalna formula $\Phi$ važi u svakom podmodelu lokalnog sistema $\mathcal{A} = \{\mathbf{A}_i \mid i \in I\}$ modela $\mathbf{A}$, tada važi i u modelu $\mathbf{A}$.*

**Dokaz**. $\Phi$ je oblika $\forall P_1 \ldots \forall P_n\, \Psi$, gde je $\Psi$ formula dobijena vezivanjem logičkim veznicima predmetno-univerzalnih formula bez slobodnih predmetnih promenljivih i sa slobodnim predikatskim promenljivima iz skupa $\{P_1, \ldots, P_n\}$. $\Psi$ je pak ekvivalentna formuli u *konjunktivnoj normalnoj formi*, dakle formuli oblika $\bigwedge \Psi_r$, gde je svaka formula $\Psi_r$ jednog od oblika: (1) $\Theta_1 \vee \ldots \vee \Theta_t$; (2) $\neg\Theta_1 \vee \ldots \vee \neg\Theta_u$; (3) $\Theta_1 \vee \ldots \vee \Theta_t \vee \neg\Omega_1 \vee \ldots \vee \neg\Omega_u$, gde su opet $\Theta_l$, $\Omega_k$ predmetno-univerzalne formule bez predmetnih slobodnih promenljivih. Jasno, dovoljno je, jer se radi o konjunkciji, da razmotrimo samo ove slučajeve. Treći je tu "najopštiji", te upravo na njemu demonstriramo dokaz. Fiksiraćemo u diskusiji realizacije predikatskih promenljivih u $\mathbf{A}$, $P_1^{\mathbf{A}}, \ldots, P_n^{\mathbf{A}}$, slobodnih predikatskih promenljivih $P_1, \ldots, P_n$. Pretpostavimo da data formula ne važi u $\mathbf{A}$, tj.



da nijedna od formula $\Theta_1, \ldots, \Theta_t$ ne važi u $\mathbf{A}$, dok s druge strane, sve formule $\Omega_1, \ldots, \Omega_u$ važe u $\mathbf{A}$. Prema tački $(b)$ prethodne teoreme za svako $\Theta_j$ postoji neki podmodel $\mathbf{A}_{i_j}$ u kome $\Theta_j$ ne važi: $\mathbf{A}_{i_j} \not\models \Theta[P_1^{\mathbf{A}} \cap A_{i_j}^{k_1}, \ldots, P_n^{\mathbf{A}} \cap A_{i_j}^{k_n}]$; naravno, ne mora svaka od predikatskih promenljivih $P_1, \ldots, P_n$ biti slobodna u $\Theta_j$, ali je ovakav način pisanja (znači, bez obzira da li neka od njih, ili čak nijedna, nije slobodna u $\Theta_j$) standardan u teoriji modela. Ako su $\mathbf{A}_{i_1}, \ldots, \mathbf{A}_{i_t}$ podmodeli modela $\mathbf{A}_i$, tada u $\mathbf{A}_i$ ne važi nijedna od formula $\Theta_1, \ldots, \Theta_t$, dok važe sve formule $\Omega_1, \ldots, \Omega_u$; i jedno i drugo je posledica tačke $(a)$ prethodne teoreme. Priozilazi da $\Psi_r$ ne važi u $\mathbf{A}_i$, kontradikcija.■

**Korolar 59.6** $(a)$ *Ako je svaka konačno generisana podgrupa grupe $\mathbf{G}$ prosta i $\mathbf{G}$ je prosta grupa;*

$(b)$ *Ako se svaka konačno generisana podgrupa grupe $\mathbf{G}$ može parcijalno (linearno) urediti, onda se i grupa $\mathbf{G}$ može parcijalno (linearno) urediti.*

Učinimo ovde jednu malu digresiju u izlaganju, ponukanu već učinjenim izletom u teoriju modela. Bez ulaženja u detalje i bez dokaza navešćemo kriterijum za *aksiomatizibilnost* klase modela jezika prvog reda (zainteresovani se upućuju na [26], [66], [112]). Prvo neophodne definicije i tvrđenja.

**Definicija 59.7** $(a)$ *Modeli $\mathbf{A}$ i $\mathbf{B}$ jezika prvog reda $\mathcal{L}$ su elementarno ekvivalentni, u oznaci $\mathbf{A} \equiv \mathbf{B}$, akko za svaku rečenicu $\Phi$ jezika $\mathcal{L}$ važi: $\mathbf{A} \models \Phi$ akko $\mathbf{B} \models \Phi$.*

$(b)$ *Podmodel $\mathbf{A}$ modela $\mathbf{B}$ je elementaran podmodel akko za svaku formulu $\Phi(x_1, \ldots, x_n)$ i svaku $n$-torku $a_1, \ldots, a_n$ modela $\mathbf{A}$ važi: $\mathbf{A} \models \Phi[a_1, \ldots, a_n]$ akko $\mathbf{B} \models \Phi[a_1, \ldots, a_n]$.*

$(c)$ *Klasa $\mathcal{K}$ modela jezika prvog reda $\mathcal{L}$ je aksiomatizabilna akko postoji skup rečenica $T$ jezika $\mathcal{L}$ takav da je $\mathcal{K}$ upravo klasa svih modela (teorije) $T$.*

Neka je dat neprazan skup modela istog jezika $\mathcal{L}$, $\{\mathbf{M}_i \mid i \in I\}$, i neka je $\mathcal{F}$ ultrafilter nad $I$. Relacija $\sim$ skupa $\prod_{i \in I} M_i$ definisana sa: $f \sim g$ akko $\{i \in I \mid (i)f = (i)g\} \in \mathcal{F}$ je relacija ekvivalencije. Na skupu svih klasa ekvivalencije $\{[f] \mid f \in \prod_{i \in I} M_i\}$, kraće označenog sa $\prod_{\mathcal{F}} M_i$, definišemo interpretaciju funkcijskih i relacijskih simbola jezika $\mathcal{L}$ na sledeći način (funkcijske znake dosledno pišemo sa desne strane):

$([f_1], \ldots, [f_m])F^{\prod_{\mathcal{F}} M_i} = [\langle((i)f_1, \ldots, (i)f_m)F^{M_i} \mid i \in I\rangle]$

posebno je, za konstante $c$: $c^{\prod_{\mathcal{F}} M_i} = [\langle c^{M_i} \mid i \in I\rangle]$;

$([f_1], \ldots, [f_n]) \in R^{\prod_{\mathcal{F}} M_i}$ akko $\{i \in I \mid ((i)f_1, \ldots, (i)f_n) \in R^{M_i}\} \in \mathcal{F}$.

Lako se proverava da su definicije korektne (tj. da ne zavise od iz izbora reprezenata klasa ekvivalencije), a dobijeni model – $\prod_{\mathcal{F}} \mathbf{M}_i$ – zove se *ultraproizvod* familije modela $\{\mathbf{M}_i \mid i \in I\}$ *modulo (ultrafilter)* $\mathcal{F}$. Ako su svi modeli $\mathbf{M}_i$, $i \in I$, jednaki – $\mathbf{M}_i = \mathbf{M}$ – onda govorimo o *ultrastepenu* modela $\mathbf{M}$ *modulo* $\mathcal{F}$; ostaje oznaka – $\prod_{\mathcal{F}} \mathbf{M}$.

U sledećim teoremama zadržavamo uvedene "objekte" i notaciju.

**Teorema 59.8** *(Teorema Losa). Za svaku rečenicu $\Phi$ jezika $\mathcal{L}$ važi:*

$$\prod_{\mathcal{F}} M_i \models \Phi \text{ akko } \{i \in I \mid \mathrm{M}_i \models \Phi\} \in \mathcal{F};$$

**Teorema 59.9** *Preslikavanje $\varphi : M \longrightarrow \prod_{\mathcal{F}} \mathrm{M}$ definisano sa: $(a)\varphi = [\langle a \mid i \in I\rangle]$ je elementarno utapanje modela $\mathrm{M}$ u ultrastepen $\prod_{\mathcal{F}} \mathrm{M}$, tj. $(\mathrm{M})\varphi$ je elementaran podmodel ultrastepena $\prod_{\mathcal{F}} \mathrm{M}$; posebno, $\mathrm{M} \equiv \prod_{\mathcal{F}} \mathrm{M}$.*

I konačno

**Teorema 59.10** *(d) Klasa modela $\mathcal{K}$ je aksiomatizabilna akko je zatvorena za ultraproizvode i elementarnu ekvivalentnost.*

Kada se ovo zna, (relativno) lako se pokazuje aksiomatizabilnost odnosno neaksiomatizabilnost mnogih "sorti" grupa. Dajemo samo tri primera.

**Primer 59.11** *Klasa prostih grupa nije aksiomatizabilna.*

**Dokaz.** Neka je $\mathcal{F}$ neglavni ultrafilter nad skupom $\{n \in \omega \mid n \geq 5\}$ i neka je, za $\alpha = \langle \alpha_n \rangle_{n\geq 5} \in \prod_{n\geq 5} A_n$, $k_n^\alpha$ broj elemenata koji "pomera" permutacija $\alpha_n$ $(\in A_n)$. Tada grupa $\prod_{\mathcal{F}} \mathbf{A}_n$ nije prosta (što će reći da familija prostih grupa nije zatvorena za ultraproizvode), jer je, prema 9.8,

$\{[\alpha] \mid$ skup $\{k_n^\alpha \mid n \geq 5\}$ ima supremum $\}$

domen njene netrivijalne normalne podgrupe.□

U nekim slučajevima od neposredne je koristi dokaz da posmatrana familija grupa nije varijetet.

**Primer 59.12** *Klase nilpotentnih i rešivih grupa nisu aksiomatizabilne.*

**Dokaz.** Već smo pokazali da klasa nilpotenih grupa nije varijetet – kartezijanski proizvod $\prod_{n\geq 2}^{c} \mathbf{D}_{2^n}$ nije nilpotentna grupa, dok su svi njegovi faktori nilpotentne grupe (videti primer 48.9$(c)_1$ i napomenu uz njega). Ali ni ultraproizvod $\prod_{\mathcal{F}} \mathbf{D}_{2^n}$, gde je $\mathcal{F}$ ma koji neglavni ultrafilter nad skupom $\{n \in \omega \mid n \geq 2\}$, nije nilpotentna grupa. Doista, pretpostavimo da je to nilpotentna grupa klase $k$. No, u svakoj grupi $\mathbf{D}_{2^n}$, gde je $n > k$, možemo izabrati elemente $a_n^1, \ldots, a_n^{k+1}$ takve da je $[a_n^1, \ldots, a_n^{k+1}] \neq e$, pa je onda i za elemente datog ultraproizvoda $\overline{a}_1 = [\langle a_m^1 \rangle_{m\geq 2}], \ldots, \overline{a}_{k+1} = [\langle a_m^{k+1} \rangle_{m\geq 2}]$, gde $a_j^i$ $(\in D_{2^j})$ za $2 \leq j \leq k$ i $1 \leq i \leq k+1$ biramo proizvoljno, $[\overline{a}_1, \ldots, \overline{a}_{k+1}]$ nejedinični element, kontradikcija.

Potpuno analogno se pokazuje i da klasa rešivih grupa nije aksiomatizabilna.□

Deljive grupe su pak primer familije grupa koja nije varijetet, ali koja je aksiomatizabilna (no ne i konačno aksiomatizabilna – s tim u vezi videti korolar 7.6).



**Primer 59.13** *Klase cikličnih i slobodnih grupa nisu aksiomatizabilne.*

**Dokaz.** Pomenute klase grupa imaju jedan jedini (do na izomorfizam) zajednički element – beskonačnu cikličnu grupu. Jednim (kontra)primerom pokazujemo neaksiomatizabilnost obe familije. Neka je $\mathcal{F}$ ma koji neglavni ultrafilter nad skupom prirodnih brojeva. Tada su, prema 59.9, grupe $\mathbf{Z}$ i $\prod_{\mathcal{F}} \mathbf{Z}$ elementarno ekvivalentne. No grupa $\prod_{\mathcal{F}} \mathbf{Z}$ je kardinalnosti kontinuum (to nam je poznato iz teorije skupova), dakle nije ciklična, a pošto je i Abelova, nije ni slobodna grupa.□.

Čitaocu s nešto prakse u teoriji modela prepuštamo da ponudi još neke dokaze za navedene primere kao i da ispita aksiomatizabilnost brojnih drugih klasa grupa pomenutih u ovoj knjizi, a mi se vraćamo našoj temi. Pokazujemo prvo, u nastavku, kako se i svojstva: biti $SN$-, $SI$-, $Z$-, $\overline{SN}$-, $\overline{SI}$-, $\overline{Z}$-, $\tilde{N}$- grupa mogu izraziti kvazi-univerzalnim rečenicama.

Uspostavimo prvo korespondenciju između normalnih sistema podgrupa date grupe $\mathbf{G}$ i binarnih relacija na $G$ koje ispunjavaju određene uslove.

Za normalni sistem podgrupa $\mathcal{S}$ definišemo binarnu relaciju $P_{\mathcal{S}}^G$ skupa $G$ sa: $P_{\mathcal{S}}^G(a,b)$ (tj. $(a,b) \in P_{\mathcal{S}}^G$) akko u $\mathcal{S}$ postoji podgrupa $\mathbf{H}$ takva da $a \in H$ i $b \notin H$. Onda u grupi $\mathbf{G}$ važi (podrazumevajući da je interpretacija relacijskog slova $P$ baš $P_{\mathcal{S}}^G$):

$\Phi_1 \equiv \forall x\, \neg P(x,x)$;
$\Phi_2 \equiv \forall x \forall y \forall z (P(x,y) \wedge P(y,z) \Longrightarrow P(x,z))$;
$\Phi_3 \equiv \forall x \forall y \forall z (P(x,z) \wedge \neg P(y,z) \Longrightarrow P(x,y))$;
$\Phi_4 \equiv \forall x \forall y \forall z (P(x,z) \wedge P(y,z) \Longrightarrow P(xy^{-1},z))$;
$\Phi_5 \equiv \forall x (x \neq e \Longrightarrow P(e,x))$;
$\Phi_6 \equiv \forall x \forall y (P(x,y) \Longrightarrow P(y^{-1}xy,y))$.

Sve je manje-više očigledno. Osvrnimo se samo na šesto svojstvo. Neka $P_{\mathcal{S}}^G(a,b)$ i neka je $\mathbf{H}^* = \bigcup\{\mathbf{H} \in \mathcal{S} \mid b \notin H\}$, $\mathbf{K}^* = \bigcap\{\mathbf{K} \in \mathcal{S} \mid b \in K\}$. Podgrupe $\mathbf{H}^*$ i $\mathbf{K}^*$ obrazuju skok (videt dokaz leme 47.3), pa je $\mathbf{H}^*$ normalna podgrupa grupe $\mathbf{K}^*$ i, jasno, zbog $P_{\mathcal{S}}^G(a,b)$ je $b^{-1}ab \in H^*$; stoga $P_{\mathcal{S}}^G(b^{-1}ab, b)$.

Pretpostavimo sada da je $P^G$ binarna relacija na $G$ koja ispunjava uslove $\Phi_1 - \Phi_6$. Za nejedinični element $b \in G$ neka je $H_b \stackrel{\text{def}}{=} \{a \in G \mid P^G(a,b)\}$. Prema $\Phi_5$, $H_b$ je neprazan skup koji je, prema $\Phi_4$, i domen podgrupe – $\mathbf{H}_b$. Ako familiji $\mathcal{S} = \{\mathbf{H}_b \mid b \in G \setminus \{e\}\}$ pridružimo presek i uniju svih njenih nepraznih podfamilija kao i celu grupu $\mathbf{G}$, dobićemo potpun sistem podgrupa – $\mathcal{S}_{P^G}$. Jer, skup $\mathcal{S}$ je linearno uređen relacijom inkluzije. Zaista, pretpostavimo da za $a \neq b$ nije ni $\mathbf{H}_a \leq \mathbf{H}_b$ ni $\mathbf{H}_b \leq \mathbf{H}_a$ i neka je $c \in H_a \setminus H_b$, $d \in H_b \setminus H_a$. No, tada iz $P^G(c,a)$ i nije $P^G(d,a)$ sledi, prema $\Phi_3$, $P^G(c,d)$. Analogno, $P^G(d,b)$ i nije $P^G(c,b)$ daju $P^G(d,c)$, te je, zbog tranzitivnosti relacije $P^G$, $P^G(c,c)$, kontradiktorno sa njenom irefleksivnošću. Zbog irefleksivnosti relacije je i $\bigcap \mathcal{S} = \mathbf{E}$. Ostale detalje provere preuzimamo iz dokaza leme 47.2. No taj sistem je zbog $\Phi_6$ i normalan. Recimo da podgrupe $\mathbf{H}$, $\mathbf{K}$ čine skok i da je $a \in H$, $b \in K \setminus H$. Tada je, za neko $c$, $a \in H_c$, $b \notin H_c$. Znači, $P^G(a,c)$,

nije $P^G(b,c)$, pa imamo i $P^G(a,b)$. Prema $\Phi_6$ je i $P^G(b^{-1}ab,b)$, što implicira $b^{-1}ab \in H_b \subseteq H$ ($\mathbf{H}_b \geq \mathbf{K}$ bi dalo $b \in H_b$, tj. $P^G(b,b)$, kontradikcija).

Takođe važi: $P^G_{\mathcal{S}_{PG}} = P^G$, $\mathcal{S}_{P\mathcal{S}} = \mathcal{S}$. Ako $P^G(a,b)$, onda $a \in H_b$ i $b \notin H_b$, pa $P^G_{\mathcal{S}_{PG}}(a,b)$. Opet, ako $P^G_{\mathcal{S}_{PG}}(a,b)$ i ako, za $H \in \mathcal{S}_{PG}$, $a \in H$ i $b \notin H$, tada je (bez obzira da li je podgrupa $\mathbf{H}$ dobijena kao unija ili presek nekog nepraznog podskupa skupa $\{\mathbf{H}_c \mid c \in G \setminus \{e\}\} \subseteq \mathcal{S}_{PG}$), za neki element $d$, $a \in H_d$, $b \notin H_d$; dakle, $P^G(a,d)$ i nije $P^G(b,d)$, a odatle $P^G(a,b)$.

Zaključujemo: preslikavanje $\varphi : \{\mathcal{S} \mid \mathcal{S}$ je normalni sistem grupe $\mathbf{G}\} \longrightarrow \{P^G \mid P^G$ je binarna relacija na $G$ koja ispunjava uslove $\Phi_1 - \Phi_6\}$ dato sa $(\mathcal{S})\varphi = P^G_{\mathcal{S}}$ bijektivno je preslikavanje. Prema tome, priča o normalnim sistemima svodi se na priču o binarnim relacijama sa svojstvima $\Phi_1 - \Phi_6$. Posebno važi

**Lema 59.14** *(a) $\mathcal{S}$ je rešiv normalni sistem grupe $\mathbf{G}$ akko $P^G_{\mathcal{S}}$ ispunjava uslove $\Phi_1 - \Phi_5$ i*

$\Phi_7 \equiv \forall x \forall y (x \neq e \wedge \neg P(x,y) \wedge \neg P(y,x) \Longrightarrow P([x,y],x))$;

*(b) $\mathcal{S}$ je invarijantan sistem grupe $\mathbf{G}$ akko $P^G_{\mathcal{S}}$ ispunjava uslove $\Phi_1 - \Phi_5$ i*
$\Phi_8 \equiv \forall x \forall y \forall z (P(x,y) \Longrightarrow P(z^{-1}xz,y))$;

*(c) $\mathcal{S}$ je centralni sistem grupe $\mathbf{G}$ akko $P^G_{\mathcal{S}}$ ispunjava uslove $\Phi_1 - \Phi_5$ i*
$\Phi_9 \equiv \forall x \forall y (x \neq e \Longrightarrow P([x,y],x))$.

**Dokaz.** *(a)* ($\Longrightarrow$) Neka je $\mathcal{S}$ rešiv normalni sistem grupe $\mathbf{G}$. Već smo konstatovali da $P^G_{\mathcal{S}}$ ispunjava uslove $\Phi_1 - \Phi_6$. Pokažimo da ispunjava i uslov $\Phi_7$ (koji sa prvih pet implicira $\Phi_6$). Neka za nejedinični element $a$ i neki element $b$ (grupe $\mathbf{G}$) nije ni $P^G_{\mathcal{S}}(a,b)$ ni $P^G_{\mathcal{S}}(b,a)$. To će reći da $a$ i $b$ pripadaju istim podgrupama sistema $\mathcal{S}$, pa ako je $\mathbf{H}^* = \bigcup\{\mathbf{H} \in \mathcal{S} \mid a,b \notin H\}$ i $\mathbf{K}^* = \bigcap\{\mathbf{K} \in \mathcal{S} \mid a,b \in K\}$, onda podgrupe $\mathbf{H}^*$, $\mathbf{K}^*$ obrazuju skok. Kako je $\mathbf{H}^*$ normalna podgrupa grupe $\mathbf{K}^*$ i $\mathbf{K}^*/\mathbf{H}^*$ Abelova grupa, to je $(\mathbf{K}^*)' \leq \mathbf{H}^*$; posebno, $[a,b] \in H^*$, pa $P^G_{\mathcal{S}}([a,b],a)$.

($\Longleftarrow$) Uslovi $\Phi_1 - \Phi_5$ garantuju da je $\mathcal{S}$ ($= \mathcal{S}_{P^G_{\mathcal{S}}}$) potpun sistem. Neka podgrupe $\mathbf{H}$, $\mathbf{K}$ čine skok (u sistemu $\mathcal{S}$) i neka $a \in H$, $b \in K \setminus H$. Dakle, $P^G_{\mathcal{S}}(a,b)$. Pretpostavimo: $b^{-1}ab \in K \setminus H$. Onda iz: nije $P^G_{\mathcal{S}}(b^{-1}ab, b^{-1})$ i nije $P^G_{\mathcal{S}}(b^{-1}, b^{-1}ab)$ sledi $P^G_{\mathcal{S}}([a,b],b^{-1})$. Zbog toga je $[b^{-1}, b^{-1}ab]$ = [a,b] $= a^{-1} \cdot b^{-1}ab \in H$, pa je i $b^{-1}ab \in H$, kontradikcija. Uslov $\Phi_7$ nam isto tako kaže da ako su $a,b \in K \setminus H$, tada je $[a,b] \in H$. Prema tome, $\mathbf{K}' \leq \mathbf{H}$, te je faktor grupa $\mathbf{K}/\mathbf{H}$ Abelova grupa.

*(b)* ($\Longrightarrow$) Neka je $\mathcal{S}$ invarijantan sistem i $P^G_{\mathcal{S}}(a,b)$. Onda je, za neku podgrupu $\mathbf{H}$ iz $\mathcal{S}$, $a \in H$ i $b \notin H$. No, $\mathbf{H}$ je normalna podgrupa grupe $\mathbf{G}$, pa je $P^G_{\mathcal{S}}(c^{-1}ac,b)$ za svako $c \in G$.

($\Longleftarrow$) Neka $P^G_{\mathcal{S}}$ ispunjava uslove $\Phi_1 - \Phi_5$ i $\Phi_8$. Ponavljamo: $\mathcal{S} = \mathcal{S}_{P^G_{\mathcal{S}}}$ je, zbog uslova $\Phi_1 - \Phi_5$, potpun sistem. Da bismo dokazali da je i invarijantan, dovoljno je da pokažemo da su sve podgrupe $\mathbf{H}_a$, $a \in G \setminus \{e\}$, normalne. Ali



to je neposredna posledica uslova $\Phi_8$: $a \in H_b$ akko $P^G_{\mathcal{S}}(a,b)$, a ako $P^G_{\mathcal{S}}(a,b)$ tada, za svako $c \in G$, $P^G_{\mathcal{S}}(c^{-1}ac,b)$, odnosno $c^{-1}ac \in H_b$.

*(c)* ($\Longrightarrow$) Neka je $\mathcal{S}$ centralni sistem, $a \neq e$, $\mathbf{H}^* = \bigcup\{\mathbf{H} \in \mathcal{S} \mid a \notin H\}$, $\mathbf{K}^* = \bigcap\{\mathbf{K} \in \mathcal{S} \mid a \in K\}$. Podgrupe $\mathbf{H}^*$ i $\mathbf{K}^*$ čine skok, te je $\mathbf{H}^* \lhd \mathbf{K}^*$ i $\mathbf{K}^*/\mathbf{H}^* \leq \mathbf{Z}(\mathbf{G}/\mathbf{H}^*)$, tj. $[\mathbf{K}^*, \mathbf{G}] \leq \mathbf{H}^*$, i stoga je, za svako $b \in G$, $[a,b] \in H^*$, odnosno $P^G_{\mathcal{S}}([a,b],a)$.

($\Longleftarrow$) Neka $P^G_{\mathcal{S}}$ ispunjava uslove $\Phi_1 - \Phi_5$ i $\Phi_9$ i neka podgrupe $\mathbf{H}$, $\mathbf{K}$ čine skok (u sistemu $\mathcal{S}$). Ako je $a \in K \setminus H$, prema $\Phi_9$ je $[a,b] \in H$ za svako $b \in G$. Drugim rečima, $(\mathbf{K}' \leq) [\mathbf{K}, \mathbf{G}] \leq \mathbf{H}$, znači, $\mathbf{H}$ je normalna podgrupa grupe $\mathbf{G}$ i $\mathbf{K}/\mathbf{H} \leq \mathbf{Z}(\mathbf{G}/\mathbf{H})$.□

**Lema 59.15** *Sistem podgrupa $\mathcal{S}$ grupe $\mathbf{G}$, ne nužno rešiv, ima najviše tri terma akko $P^G_{\mathcal{S}}$ ispunjava uslove $\Phi_1 - \Phi_5$ i*

$$\forall x \forall y \forall z (x \neq e \wedge P(x,y) \Longrightarrow \neg P(y,z)).$$

**Teorema 59.16** *(Teorema Maljceva). Lokalna teorema važi za svojstva: biti $SN$-, $SI$- , $Z$-, $\overline{SN}$-, $\overline{SI}$-, $\overline{Z}$-, $\widetilde{N}$-grupa (videti definiciju 17.1); kaže se i jednostavnije: lokalna teorema važi za svojstva $SN$, $SI$ , $Z$, $\overline{SN}$, $\overline{SI}$, $\overline{Z}$, $\widetilde{N}$.*

**Dokaz.** Već smo nagovestili da se svako od navedenih svojstava može opisati nekom kvazi-univerzalnom formulom (što uključuje, naravno, i predmetno-univerzalne formule). I zaista su, prema prethodnim dvema lemama (i u njima korišćenoj notaciji), ta svojstva redom zadata sa:

$SN$: $\exists P (\Phi_1 \wedge \Phi_2 \wedge \Phi_3 \wedge \Phi_4 \wedge \Phi_5 \wedge \Phi_7)$;
$SI$: $\exists P (\Phi_1 \wedge \Phi_2 \wedge \Phi_3 \wedge \Phi_4 \wedge \Phi_5 \wedge \Phi_7 \wedge \Phi_8)$;
$Z$: $\exists P (\Phi_1 \wedge \Phi_2 \wedge \Phi_3 \wedge \Phi_4 \wedge \Phi_5 \wedge \Phi_9)$.

Adekvatne formule za preostala svojsta su nešto komplikovanije i kako bismo pojednostavili notaciju, jednostavno ćemo reći, dosledno sledeći tekst iz [78] (doduše ne i terminologiju), recimo: $P$ je normalna relacija (tj. definiše normalni sistem), ili još jednostavnije: $P$ je normalno, umesto da pišemo $\exists P (\Phi_1 \wedge \Phi_2 \wedge \Phi_3 \wedge \Phi_4 \wedge \Phi_5 \wedge \Phi_6)$.

$\overline{SN}$ : $\forall P (P$ je normalno $\Longrightarrow \exists Q (Q$ je rešivo i normalno $\wedge$

$$\forall x \forall y (P(x,y) \Longrightarrow Q(x,y));$$

$\overline{SI}$ : $\forall P (P$ je invarijantno $\Longrightarrow \exists Q (Q$ je rešivo i invarijantno $\wedge$

$$\forall x \forall y (P(x,y) \Longrightarrow Q(x,y));$$

$\overline{Z}$ : $\forall P (P$ je invarijantno $\Longrightarrow \exists Q (Q$ je centralno $\wedge$

$$\forall x \forall y (P(x,y) \Longrightarrow Q(x,y));$$

$\tilde{N}$ : $\forall P\,(P$ ima najviše tri terma $\Longrightarrow \exists Q\,(Q$ je normalno $\wedge$

$$\forall x \forall y\,(P(x,y) \Longrightarrow Q(x,y)).\blacksquare$$

**Napomena**. Konstatujmo samo: lokalna teorema ne važi za svojstva: biti $SD$-, $SN^*$-, $SI^*$-, $ZA$-, $ZD$-, $N$-grupa.

**Lema 59.17** *Lokalna teorema važi za svojstvo $S$ (tj. svojstvo biti $S$-grupa).*

**Dokaz**. Neka grupa $\mathbf{G}$ ima svojstvo $S$ lokalno i neka je $\mathcal{S} = \{\mathbf{H}_i \mid i \in I\}$ lokalni sistem podgrupa sa svojstvom $S$. Ako je, za $i \in I$, $\mathbf{P}_i$ jedinstvena Sylowa $p$-podgrupa (pod)grupe $\mathbf{H}_i$, onda je, očigledno, $\bigcup_{i\in I} P_i$ domen jedinstvene Sylowe $p$-podgrupe grupe $\mathbf{G}$.□

**Korolar 59.18** (*a*) *Klase lokalno konačnih i generalno nilpotentnih grupa za koje važi lokalna teorema, kao i klase lokalno konačnih $\tilde{N}$- i $S$-grupa, podudaraju se sa klasom lokalno konačnih i lokalno nilpotentnih grupa;*

(*b*) *Klase lokalno konačnih i generalno rešivih grupa za koje važi lokalna teorema podudaraju se sa klasom lokalno konačnih i lokalno rešivih grupa.*

**Dokaz**. Direktno, prema prethodnoj lemi i teoremi i 55.2, 48.28 i 58.2.□

**Korolar 59.19** *Svaka lokalno nilpotentna grupa je $S$-grupa.*

**Dokaz**. Direktno, prema 48.33 i 59.17.□

**Korolar 59.20** *Za grupu $\mathbf{G}$ koja ispunjava uslov minimalnosti podgrupa sledeći uslovi su ekvivalentni:*

(1) $\mathbf{G}$ *je $ZA$-grupa;*

(2) $\mathbf{G}$ *je $N$-grupa;*

(3) $\mathbf{G}$ *je lokalno konačna $S$-grupa.*

**Lema 59.21** *$SN$-grupa koja ispunjava uslov minimalnosti podgrupa je rešiva.*

**Dokaz**. Neka je $\mathbf{G}$ $SN$-grupa koja ispunjava uslov minimalnosti podgrupa i neka je $\{\mathbf{H}_\alpha \mid \alpha \in \Omega\}$ njen (ma koji) rešiv normalni sistem. Zbog uslova minimalnosti podgrupa radi se zapravo o rastućem rešivom normalnom nizu – linearno uređen skup bez beskonačnog opadajućeg lanca je dobro uređen. $\mathbf{G}$ je, dakle, periodična $SN^*$-grupa, stoga i lokalno konačna (58.11(*a*)). Prema korolaru 59.18 $\mathbf{G}$ je $SI$-grupa, odnosno, opet zbog uslova minimalnosti podgrupa, $SI^*$-grupa. Zbog uslova minimalnosti podgrupa $\mathbf{G}$ sadrži i jedinstvenu minimalnu podgrupu konačnog indeksa – neka je to $\mathbf{H}$ (skup podgrupa konačnog indeksa mora imati minimalni element, a prema 3.18 u pitanju je jedinstven, znači i najmanji element tog skupa). Pokazujemo da je $\mathbf{H}$ Abelova grupa.



Kao $SI^*$-grupa $\mathbf{H}$ sadrži normalnu Abelovu nejediničnu podgrupu $\mathbf{A}$. Prema 33.35 je $\mathbf{A}$ direktna suma konačno mnogo Prüferovih i primarnih cikličnih grupa, pa je centralizator u $\mathbf{H}$ ma kog njenog elementa konačnog indeksa u $\mathbf{H}$, dakle i u $\mathbf{G}$, znači baš jednak $\mathbf{H}$; $\mathbf{A}$ sadrži samo konačno mnogo elemenata istog reda i kako je normalna podgrupa grupe $\mathbf{H}$, sa svakim elementom sadrži i sve njegove konjugate iz $\mathbf{H}$. Proizilazi: $\mathbf{A} \leq \mathbf{Z}(\mathbf{H}) = \mathbf{Z}_0$. Pretpostavimo $\mathbf{Z}_0 \neq \mathbf{H}$. Onda je $\mathbf{H}/\mathbf{Z}_0$ $SI^*$-grupa koja ispunjava uslov minimalnosti podgrupa i ima, upravo smo videli, netrivijalni centar – $\mathbf{Z}_1/\mathbf{Z}_0$. Ako je $a \in Z_1$, tada svaki konjugat elementa $a$ u $\mathbf{H}$ pripada kosetu $aZ_0$ (za $b \in H$ je $aZ_0 = (bZ_0)^{-1}\,aZ_0\,bZ_0 = (b^{-1}ab)Z_0$). Neka je $a' = ac$ $(c \in Z_0)$ jedan takav. Elementi $a$ i $a'$ su istog reda i pošto je $ac = ca$, red elementa $c$ deli red elementa $a$. No, na raspolaganju nam je samo konačno mnogo takvih (naravno, opet prema 33.35), što će reći da $a$ ima samo konačno mnogo konjugata u $\mathbf{H}$, tj. da je centralizator elementa $a$ u $\mathbf{H}$ konačnog indeksa i stoga jednak $\mathbf{H}$, tj. da $a \in Z_0$ i uopšte, $\mathbf{Z}_1 = \mathbf{Z}_0$, kontradikcija.

S obzirom da su grupe $\mathbf{H}$ i $\mathbf{G}/\mathbf{H}$ rešive ($\mathbf{G}/\mathbf{H}$ je konačna $SI^*$-grupa), to je i $\mathbf{G}$ rešiva grupa.

U vezi sa ovim tvrđenjem videti i teoremu 49.22.□

Imajući u vidu da je periodična $S$-grupa direktni proizvod svojih Sylowih podgrupa, prethodna dva tvrđenja sublimiramo ograničavajući se na $p$-grupe.

**Teorema 59.22** *Sledeći uslovi su ekvivalentni za $p$-grupu $\mathbf{G}$ koja ispunjava uslov minimalnosti podgrupa:*

(1) $\mathbf{G}$ *je rešiva;*

(2) $\mathbf{G}$ *sadrži deljivu Abelovu podgrupu konačnog indeksa;*

(3) $\mathbf{G}$ *je $ZA$-grupa;*

(4) $\mathbf{G}$ *je $N$-grupa;*

(5) $\mathbf{G}$ *je lokalno konačna.*

**Dokaz**. Ekvavalentnost uslova (1) i (2) je dokazana u 49.22, ekvivalentnost uslova (3), (4) i (5) "garantuje" prethodni korolar.

(3) $\Longrightarrow$ (1) Prema 58.5, ako je $\mathbf{G}$ $ZA$-grupa, onda je i $SI$-, znači i $SN$-grupa, pa je prema prethodnoj lemi i rešiva.

(1) $\Longrightarrow$ (5) I ovo nam je već dato – 58.11.■

**Definicija 59.23** *Rešiva $p$-grupa koja ispunjava uslov minimalnosti podgrupa zove se Černikova $p$-grupa.*

**Lema 59.24** *Klasa Černikovih $p$-grupa je zatvorena za podgrupe, homomorfizme i ekstenzije.*

**Dokaz**. Direktno prema 13.3(*d*) i 49.6.□

## 60 Lokalno rešive grupe

Na kraju i reč-dve o lokalno rešivim grupama.

**Lema 60.1** *Podgrupe, homomorfne slike i direktni proizvodi lokalno rešivih grupa su lokalno rešive grupe.*

**Dokaz.** Neka je $\mathbf{H}$ normalna podgrupa lokalno rešive grupe $\mathbf{G}$. Ako je, za elemente $g_1, \ldots, g_n$ grupe $\mathbf{G}$, $\mathbf{K} = \langle g_1, \ldots, g_n \rangle$, tada je $\langle g_1 H, \ldots, g_n H \rangle = (\mathbf{KH})/\mathbf{H} \cong \mathbf{K}/(\mathbf{H} \cap \mathbf{K})$, dakle, $\langle g_1 H, \ldots, g_n H \rangle$ je rešiva grupa.

Jasno, kada su u pitanju direktni proizvodi, dovoljno je da posmatramo slučaj samo dve grupe. Neka su $\mathbf{G}$ i $\mathbf{H}$ lokalno rešive grupe. Onda je, za ma koji konačan skup elemenata iz $\mathbf{G} \times \mathbf{H}$, $\langle (g_1, h_1), \ldots, (g_n, h_n) \rangle \leq \mathbf{G}_1 \times \mathbf{H}_1$, gde je $\mathbf{G}_1 = \langle g_1, \ldots, g_n \rangle$, $\mathbf{H}_1 = \langle h_1, \ldots, h_n \rangle$ (a direktni proizvod konačno mnogo rešivih grupa je rešiva grupa).□

Već znamo da su, prema teoremi 59.16, lokalno rešive grupe i $SI$-grupe. U narednom korolaru dajemo i jedan "direktni" dokaz tog stava.

**Definicija 60.2** *Neka je* $\mathbf{H}$ *dostižna i* $\mathbf{K}$ *normalna podgrupa grupe* $\mathbf{G}$ *i neka je* $\mathbf{K} \leq \mathbf{H}$.

*Faktor grupa* $\mathbf{H}/\mathbf{K}$ *je kompozicioni faktor akko je prosta grupa.*

*Faktor grupa* $\mathbf{H}/\mathbf{K}$ *je glavni faktor akko je minimalna normalna podgrupa grupe* $\mathbf{G}/\mathbf{K}$.

**Lema 60.3** *Svaki glavni faktor lokalno rešive grupe je Abelova grupa.*

**Dokaz.** Neka je $\mathbf{G}$ lokalno rešiva grupa. Pošto je homomorfna slika lokalno rešive grupe lokalno rešiva, dovoljno je da pokažemo da je minimalna normalna podgrupa grupe $\mathbf{G}$, neka je to $\mathbf{H}$, Abelova. Pretpostavimo da $\mathbf{H}$ nije Abelova grupa. Onda je, za neke elemente $a, b$ iz $H$, $[a, b] = c \neq e$. Kako je $\mathbf{H}$ minimalna normalna podgrupa, važi: $\mathbf{H} = \langle \{g^{-1} c g \mid g \in G\} \rangle$, pa je, za neke elemente $g_1, \ldots, g_k$ iz $G$, $a, b \in \langle g_1^{-1} c g_1, \ldots, g_k^{-1} c g_k \rangle$. Neka je $\mathbf{K}$ rešiva grupa $\langle a, b, g_1, \ldots, g_k \rangle$ i $\mathbf{A} = \langle \{d^{-1} c d \mid d \in K\} \rangle$. Zbog $a, b \in A$ imamo i $c \in A'$, pa je $\mathbf{A} = \mathbf{A}'$. Ali kao podgrupa grupe $\mathbf{K}'$ (jer je $c \in K'$) $\mathbf{A}$ je rešiva grupa, te mora biti $\mathbf{A} = \mathbf{E}$, dakle i $c = e$, kontradikcija.□

**Korolar 60.4** *Lokalno rešiva grupa je $SI$-grupa.*

*Prosta lokalno rešiva grupa je prostog reda.*

**Dokaz.** Prema 47.5($b$) svaki invarijantan sistem se može proširiti do glavnog, a prema prethodnoj lemi faktori tog sistema su Abelove grupe.□

**Korolar 60.5** *Neka je* $\mathbf{G}$ *lokalno rešiva grupa koja ispunjava uslov maksimalnosti normalnih podgrupa. Tada je* $\mathbf{G}^{(\alpha)} = \mathbf{E}$ *za neki ordinal* $\alpha$.



**Dokaz.** Pretpostavimo da je, za neki ordinal $\beta$, $\mathbf{E} \neq \mathbf{G}^{(\beta)} = \mathbf{G}^{(\beta+1)} = \cdots$. Ako je $\mathbf{H}$ maksimalni element familije normalnih podgrupa grupe $\mathbf{G}$ koje su ujedno i prave podgrupe grupe $\mathbf{G}^{(\beta)}$, onda je $\mathbf{G}^{(\beta)}/\mathbf{H}$ glavni faktor i kao takav Abelov. Ali tada je $\mathbf{G}^{(\beta+1)} = (\mathbf{G}^{(\beta)})' \leq \mathbf{H} < \mathbf{G}^{(\beta)}$, kontradikcija.□

**Korolar 60.6** *Lokalno rešiva grupa koja ispunjava uslov minimalnosti normalnih podgrupa je $SI^*$-grupa.*

**Dokaz.** Direktno prema 60.3.□

**Lema 60.7** *(D. H. McLain). Neka je* $\mathbf{G}$ *lokalno rešiva grupa koja ispunjava uslov maksimalnosti normalnih podgrupa. Tada za svaki prirodan broj $k$ postoji prirodan broj $m = m(k, \mathbf{G})$ takav da za svaki niz pozitivnih prirodnih brojeva $r_1, \ldots, r_k$ važi* $\mathbf{G}^{(m)} \leq \gamma_{r_k}(\ldots(\gamma_{r_2}(\gamma_{r_1}\mathbf{G}))\ldots)$.

**Dokaz.** Indukcijom po $k$. Za $k = 0$, $0$ $(= m(0, \mathbf{G}))$ zadovoljava trivijalno. Pretpostavimo da je tvrđenje tačno za $k$ $(\geq 0)$ i neka je $m = m(k, \mathbf{G})$ korespondentni prirodan broj. Faktor grupa $\mathbf{G}/\mathbf{G}^{(m+1)}$ je rešiva grupa koja ispunjava uslov maksimalnosti normalnih podgrupa (8.7), pa je prema 49.21 konačno generisana. Ako je $\{g_1 G^{(m+1)}, \ldots, g_t G^{(m+1)}\}$ njen generatorni skup i $\mathbf{H} = \langle g_1, \ldots, g_t \rangle$, tada je $\mathbf{G} = \mathbf{H}\mathbf{G}^{(m+1)}$. Podgrupa $\mathbf{H}$ je rešiva sa izvodnim nizom dužine, recimo $s$; znači $\mathbf{H}^{(s)} = \mathbf{E}$. Neka su $r_1, \ldots, r_k, r_{k+1}$ pozitivni prirodni brojevi. Prema 46.30 je $\mathbf{G} = \mathbf{H}\gamma_{r_{k+1}}\mathbf{G}^{(m+1)}$, a odatle je, prema induktivnoj hipotezi i 46.26: $\mathbf{G}^{(s)} \leq \mathbf{H}^{(s)}\gamma_{r_{k+1}}\mathbf{G}^{(m+1)} = \gamma_{r_{k+1}}\mathbf{G}^{(m+1)} \leq \gamma_{r_{k+1}}(\gamma_{r_k}(\ldots(\gamma_{r_2}(\gamma_{r_1}\mathbf{G}))\ldots))$. Stoga za $m(k+1, \mathbf{G})$ možemo uzeti $s$.□

Za narednu teoremu potrebna nam je sledeća

**Definicija 60.8** *Nilpotentna dužina rešive grupe je dužina njenog najkraćeg normalnog niza čiji su svi faktori nilpotentne grupe.*

**Teorema 60.9** *(D. H. McLain). Neka je* $\mathbf{G}$ *lokalno rešiva grupa koja ispunjava uslov maksimalnosti normalnih podgrupa. Tada su sledeći uslovi ekvivalentni:*

(1) $\mathbf{G}$ *je rešiva grupa;*

(2) *Nilpotentne dužine svih konačno generisanih podgrupa su ograničene.*

**Dokaz.** (1) $\Longrightarrow$ (2) Trivijalno; nilpotentna dužina podgrupe rešive grupe je očigledno manja od ili jednaka nilpotentnoj dužini grupe.

(2) $\Longrightarrow$ (1) Pretpostavimo da je prirodan broj $k$ supremum nilpotentnih dužina konačno generisanih podgrupa grupe $\mathbf{G}$ i neka je $m = m(k, \mathbf{G})$ broj iz prethodne leme. Već smo videli da je $\mathbf{G} = \mathbf{H}\mathbf{G}^{(m+1)}$ za neku konačno generisanu podgrupu $\mathbf{H}$. Neka je, dalje, $\mathbf{H} = \mathbf{H}_0 > \mathbf{H}_1 > \cdots > \mathbf{H}_l = \mathbf{E}$ normalni niz grupe $\mathbf{H}$ čiji su faktori nilpotentne grupe $(l \leq k)$ i neka je, za $i = 1, \ldots, l$,

$\mathbf{H}_{i-1}/\mathbf{H}_i$ klase nilpotentnosti $r_i$; dakle, $\gamma_{r_i}(\mathbf{H}_{i-1}/\mathbf{H}_i) = (\gamma_{r_i}\mathbf{H}_{i-1}\,\mathbf{H}_i)/\mathbf{H}_i = \overline{\mathbf{E}}$ (46.25(5)), pa je $\gamma_{r_i}\mathbf{H}_{i-1} \leq \mathbf{H}_i$. Ako je $l < k$, izaberimo proizvoljno $r_{l+1}, \ldots, r_k$. Prema prethodnoj lemi i 46.26 imamo:

$$\mathbf{G}^{(m)} \leq \gamma_{r_k}(\ldots(\gamma_{r_2}(\gamma_{r_1}\mathbf{G}))\ldots) \leq \gamma_{r_k}(\ldots(\gamma_{r_2}(\gamma_{r_1}\mathbf{H}))\ldots)\,\mathbf{G}^{(m+1)} = \mathbf{G}^{(m+1)},$$

pa je prema 60.5 $\mathbf{G}^{(m)}$ jedinična grupa.■

**Korolar 60.10** *Lokalno superrešiva grupa* $\mathbf{G}$ *koja ispunjava uslov maksimalnosti normalnih podgrupa je superrešiva.*

**Dokaz.** Neka je $\mathbf{H}$ konačno generisana podgrupa grupe $\mathbf{G}$. Pošto je $\mathbf{H}$ superrešiva grupa, njena izvodna podgrupa je nilpotentna (50.13). Prema tome, nilpotentna dužina svake konačno generisane podgrupe grupe $\mathbf{G}$ je manja od ili jednaka 2. Prema prethodnoj teoremi i 49.21, $\mathbf{G}$ je konačno generisana rešiva, a onda i superrešiva grupa.□

# Bibliografija


[1] Adams F. J., *Lectures on Lie Groups*, W. A. Benjamin, Inc., New York – Amsterdam, 1969.

[2] Адян С. И., *Неразрешимость некоторых алгоритмических проблем теории групп*, Тр. Моск. матем. о-ва 6 (1957), 231 – 298

[3] Адян С. И., *Проблема Бернсайда и тождества в группах*, "Наука", Москва, 1975.

[4] eds. Adian S. I., Boone W. W., Higman G., *Word Problems* II, North-Holland Publishing Company, 1980.

[5] Alperin J. L., Bell R. B., *Groups and Representations*, Graduate Texts in Mathematics 162, Springer-Verlag, New York, 1995.

[6] Anderson M., Feil T., *Lattice Ordered Groups*, D. Reidel Publishing Company, Dordrecht, Holland, 1988.

[7] Aschbacher M., *Finite Group Theory*, Cambridge University Press, Cambridge, 1986.

[8] Baer R., *Situation der Untergruppen und Struktur der Gruppe*, S-B. Heidelberg. Akad., Vol. 2 (1933), 12 – 17.

[9] Baer R., *Sylow Theorems for Infinite Groups*, Duke Math. J. vol. 6 (1940), 598 – 614.

[10] Bakić R., *On a Theorem of Frobenius*, Publ. Inst. Math. Beograd 61(75) (1997), 41 – 43.

[11] Baumslag B., Chandler B., *Theory and Problems of Group Theory*, McGraw-Hill Book Company, 1968.

[12] Baumslag G., *Lecture Notes on Nilpotent Groups*, American Mathematical Society, Providence, Rhode Island, 1971.

[13] Behrendt G., Neumann P. M., *On the Number of Normal Subgroups of an Infinite Group*, J. London Math. Soc. (2), 23 (1981), 429 – 432.

[14] Bogdanović S. M., Ćirić M. D., *Polugrupe*, Prosveta, Niš, 1993.

[15] Бокуть Л. А., Кукин Г. П., *Неразрешимые алгоритмические проблемы для полугрупп, групп и колец*, Итоги Науки и Техники, серия Алгебра. Топология. Геометрия, Том 25, Москва, 1987, 3 – 66.

[16] Božović N., Mijajlović Ž., *Uvod u teoriju grupa*, Naučna knjiga, Beograd, 1990.

[17] eds. Boone W. W., Cannonito F. B., Lyndon R. C., *Word Problems – Decision Problems and the Burnside Problem in Group Theory*, North-Holland Publishing Company, Amsterdam - London, 1973.

[18] Britton J. L., *Solution of the Word Problem for Certain Types of Groups*, I, Proc. Glasgow Math. Ass. 3 (1956), 45 – 54.

[19] Brookes C. J. B., Smith H., *A Remark on Products of Locally Soluble Groups*, Bull. Austral. Math. Soc. Vol. 30 (1984), 175 – 177.

[20] Бурбаки Н., *Группы и алгебры Ли*, "Мир", Москва, 1972.

[21] Burns J. E., *The Foundation Period in the History of Group Theory*, The American Mathematical Monthly, Volume XX, Number 5, May, 1913.

[22] Burnside W., *Theory of Groups of Finite Order*, 2nd ed., Dover Publications, Inc, 1955.

[23] Burrow M., *Representation Theory of Finite Groups*, Academic Press, New York, 1965.

[24] Chabet P., *Some Sylow 2-Groups Which Cannot Occur in Simple Groups*, Journal of Algebra 18 (1971), 506 – 510.

[25] Чандлер Б., Магнус В., *Развитие комбинаторной теории групп*, "Мир", Москва, 1985.

[26] Chang C. C., Keisler H. J., *Model Theory*, North-Holland Publishing Company, 1973.

[27] Cherlin G., *Model Theoretic Algebra – Selected Topics*, Springer-Verlag, 1976.

[28] Clapham C. R. J., *Finitely Presented Groups with Word Problem of Arbitrary Degrees of Insolubility*, Proc. London Math. Soc. 14 (1964), 633 – 676

[29] Cohen D. E., *Combinatorial Group Theory: a topological qpproach*, Cambridge University Press, 1989.



[30] Cohn P. M., *Universal Algebra*, Mathematics and Its Applications, Volume 6, D. Reidel Publishing Company, 1981.

[31] Crvenković S., *Word Problems for Varieties of Algebras (a survey)*, Filomat (Niš) 9:3 (1995), Algebra, Logic and Discrete Mathematics, Niš, April 14 – 16, 427 – 448.

[32] Cutler D., Flanigan F., Galovich S., Hayes D., Missel C., *On the Category of Normal Embeddings of a Group*, Journal of Algebra 74 (1982), 55 – 75.

[33] Cutler D., Irwin J., Pfaendtner J., Snabb T., *Direct Sums of Cyclic Summands*, Commentarii Mathematici, Universitatis Sancti Pauli, Vol. 32, No. 2 (1983), 171 – 176.

[34] Черников С. Н., *Группы с заданными свойствами системы подгрупп*, "Наука", Москва, 1980.

[35] Чупона Ѓ., Трпеновски Б., *Предавања по алгебра, книга* II, Универзитет "Кирил и Методиј", Скопје, 1973.

[36] Dieudonné J., *La géométrie des groupes classiques*, Springer-Verlag, Berlin – Heidelberg – New York, 1971.

[37] Dixon J. D., *Problems in Group Theory*, Dover Publications, Inc, 1973.

[38] Dixon M. R., Tomkinson M. J., *The Local Conjugacy of Some Sylow Basis in a Class of Locally Finite Groups*, J. London Math. Soc. (2), 21 (1980), 225 – 228.

[39] Durbin J. R., McDonald M., *Groups with a Characteristic Cyclic Series*, Journal of Algebra 18 (1971), 453 – 460.

[40] Eklof P. C., *Some Model Theory of Abelian Groups*, The Journal of Symbolic Logic, Vol. 37, No. 2, June 1972, 335 – 342.

[41] Eklof P. C., Fischer E. R., *The Elementary Theory of Abelian Groups*, Annals of Mathematical Logic, Volume 4, No. 2 (1972), 115 – 171.

[42] Erdös P., Ivić A., *On the Iterates of the Enumerating Function of Finite Abelian Groups*, Bulletin XCIC Acad. Serbe 1989 Sciences Mathématiques No 17, 13 – 22.

[43] Eršov Ju. L. *Theories of Nonabelian Varieties of Groups*, Proceedings of the Tarski Symposium, Proceedings of Symposia in Pure Mathematics – volume XXV (1974), 255 – 264.

[44] Feigelstock S., *Additive Groups of Rings*, Pitman Advanced Publishing Program, Boston – London – Melbourne, 1983.

[45] Feit W., *Characters of Finite Groups*, W. A. Benjamin, Inc., New York, 1967.

[46] Feit W., Thompson G. J., *Solvability of Groups of Odd Order*, Pacif. J. Math. 13(1963), 775 – 1029.

[47] Fitzpatrick P., *Order Conjugacy in Finite Groups*, Proc. R. Ir. Acad. Vol. 85A, No. 1 (1985), 53 – 58.

[48] Фридман А. А., *О взаимоотношении между проблемой тождества и проблемой сопряженности в конечноопределенных группах*, Тр. Моск. матем. о-ва 9 (1960), 329 – 356

[49] Fried E., Kollár J. *Automorphism Groups of Fields*, Colloquia Mathematica Societatis János Bolyai, 29. Universal Algebra, Esztergon (Hungary), 1977, 293 – 303.

[50] Фукс Л., *Бесконечные абелевы группы, т.* 1 (1974), *т.* 2 (1977), "Мир", Москва

[51] Gagen T. M., *Topics in Finite Groups*, London Mathematical Society Lecture Note Series 16, Cambridge University Press, Cambridge, 1976.

[52] Георгиев Г., *Геометрические группы и эволюция идеи пространства*, *Издательство Киевского Универцитета*, 1968.

[53] Glauberman G., *Central Elements in Core-Free Groups*, Journal of Algebra 4 (1966), 403 – 420.

[54] Голод Е. С., *О ниль-алгебрах и финитно-аппроксимируемых р-группах*, Изв. АН СССР сер. матем. 28 (1964), 273 – 276.

[55] Горенстейн Д., *Конечные простые группы*, "Мир", Москва, 1985.

[56] Gould M., *Automorphism Groups of Free Algebras and Direct Powers*, Colloquia Mathematica Societatis János Bolyai, 29. Universal Algebra, Esztergon (Hungary), 1977, 331 – 334.

[57] Grätzer G., *Universal Algebra*, D. Van Nostrand Company, Inc., 1968.

[58] Griffith P. A., *Infinite Abelian Group Theory*, University of Chicago Press, Chicago, 1970.

[59] Grossman I., Magnus W., *Grupe i njihovi grafovi*, Školska knjiga, Zagreb, 1975.



[60] eds. Gruenberg K. W., Roseblade J. E., *Group Theory: essays for Philip Hall*, Academic Press, London, 1984.

[61] Grulović M. Z., *Svojstvo amalgamiranja*, Radovi Instituta za Matematiku, br. 1, 1992, 124 – 143.

[62] Грушко И. А., *О базисах свободного произведения групп*, Матем. сб. 8 (1940), 169 – 182.

[63] Hall M., Jr., *Generators and Relations in Groups – the Burnside Problem*, Lectures on Modern Mathematics, volume II, John Wiley & Sons, Inc., New York, London, Sydney, 1964.

[64] Higgins P. J., *Grushko's Theorem*, Journal of Algebra 4 (1966), 365 – 372.

[65] Higman G., Neumann B. H., Neumann H. N., *Embedding Theorems for Groups*, J. London Math. Soc., vol. 24 (1954), 233 – 236.

[66] Hodges W., *Model Theory*, Encyclopedia of Mathematics and its Applications, Volume 42, Cambridge University Press, 1994.

[67] Холл М., *Теория групп*, Издательство иностранной литературы, Москва, 1962.

[68] Holt D. F., *Transfer Theorems in Locally Finite Groups*, J. London Math. Soc. (2), 21 (1980), 229 – 236.

[69] Humphreys J. E., *Linear Algebraic Groups*, Springer-Verlag, New York – Heidelberg – Berlin, 1975.

[70] Hungerford T. W., *Algebra*, Holt, Rinehart and Winston, Inc., 1974.

[71] Huppert B., *Endliche Gruppen* I, Springer-Verlag, Berlin – Heidelberg – New York, 1967.

[72] Isbell J. R., *Zassenhaus' Theorem Supersedes the Jordan-Hölder Theorem*, Advances in Mathematics 31 (1979), 101 – 103.

[73] Jacobson N., *Lectures in Abstract Algebra, vol.* I, D. Van Nostrand Company, Inc., Toronto - New York - London, 1951.

[74] Jónsson B., *Universal Relational Systems*, Math. Scand. 4 (1956), 193 – 208.

[75] Kaloujnine L., *Sur les groupes abéliens primaires sans élements de hauteur infinite*, C. R. Acad. Sci. Paris, vol. 225 (1947), 713 – 715.

[76] Kaplansky I., *Infinite Abelian Groups*, Ann Arbor, The University of Michigan Press, 1971.

[77] Каргаполов М. И., Сиб. матем. ж., 4, No. 1 (1962), 232 –235.

[78] Каргаполов М. И., Мерзляков Ю. И., *Основы теории групп*, "Наука", Москва, 1982.

[79] Khazal R., Mukherjee N. P., *A Note on Maximal Subgroups in Finite Groups*, Riv. Mat. Univ. Parma (4) 15 (1989), 165 – 173.

[80] Клиффорд А., Престон Г., *Алгебраическая теория полугрупп, том* 1, "Мир", Москва, 1972.

[81] Кокорин А. И., Копытов В. М., *Линейно упорядоченные группы*, "Наука", Москва, 1972.

[82] Копытов В. М., *Решеточно упорядоченные группы*, "Наука", Москва, 1984.

[83] Кондратьв А. С., Махнев А. А., Старостин А. И., *Конечые группы*, Итоги Науки и Техники, серия Алгебра. Топология. Геометрия, Том 27, Москва, 1989, 3 – 120.

[84] Кострикин А. И., *О проблеме Бернсайда*, Изв. АН СССР: Сер. матем., 23, No. 1 (1959), 3 – 34.

[85] Кострикин А. И., Чубаров И. А., *Представления конечных групп*, Итоги Науки и Техники, серия Алгебра. Топология. Геометрия, Том 23, Москва, 1985, 119 – 196.

[86] Kron A., *Elementarna teorija skupova*, Matematički institut, Beograd, 1992.

[87] Krstić S., *Fixed Subgroups of Automorphisms of Free by Finite Groups: an Extension of Cooper's proof*, Arch. Math., Vol. 48 (1987), 25 – 30.

[88] Krstić S., *Actions of Finite Groups on Graphs and Related Automorphisms of Free Groups*, Journal of Algebra, Vol. 124, No. 1, July 1989, 119 – 138.

[89] Krstić S., *A Uniqueness Decomposition Theorem for Actions of Finite Groups on Free Groups*, Journal of Pure and Applied Algebra 61 (1989), 29 – 48.

[90] Kurepa D., *Viša algebra* I, II, Zavod za izdavanje udžbenika, Beograd, 1971.



[91] Kurepa S., *Konačno dimenzionalni vektorski prostori i primjene*, Tehnička knjiga, Zagreb, 1967.

[92] Курош А. Г., *Теория групп*, "Наука", Москва, 1967.

[93] Кэртис Ч., Райнер И., *Теория представлений конечных групп и ассоциативных алгебр*, "Наука", Москва, 1969.

[94] Lambek J., *Lectures on Rings and Modules*, Chelsea Publishing Company, New York, 1976.

[95] Lennox J. C., *A Note on Quasinormal Subgroups of Finitely Generated Groups*, J. London Math. Soc. (2), 24 (1981), 127 – 128

[96] Линдон Р., Шупп П., *Комбинаторная теория групп*, "Мир", Москва, 1980.

[97] Macdonald I. D., *The Theory of Groups*, Oxford University Press, 1968.

[98] Macintyre A., *On $\omega_1$-Categorical Theories of Abelian Groups*, Fundamenta Mathematicae LXX (1971), 253 – 270.

[99] Macintyre A., *On Algebraically Closed Groups*, Annals of Mathematics, vol. 96, No. 1, July, 1972, 53 – 97.

[100] Madarász R. Sz., Crvenković S., *Relacione algebre*, Matematički Institut, Beograd, 1992.

[101] Magnus W., Karrass A., Solitar D., *Combinatorial Group Theory*, 2nd ed., Dover Publications, Inc., New York, 1976.

[102] Maier B. J., *Existentially Closed Torsion-Free Nilpotent Groups of Class Three*, The Journal of Symbolic Logic, Vol. 49, No. 1, March 1984, 220 – 230.

[103] Malone J. J., *p-Groups with Non-Abelian Automorphism Groups and All Automorphism Central*, Bull. Austral. Math, Soc., Vol. 29 (1984), 35 – 37.

[104] Мальцев А. И., *Об одном общем методе получения локальных теорем теории групп*, Учен. зап. Ивановск. пед. ин-та, 1941, No. 1, 3 – 9.

[105] Мальцев А. И., *Нильпотентные группы без кручения*, Изв. АН СССР, сер. мат., 1949, 13, No. 3, 201 – 212.

[106] Мальцев А. И., *Два замечания о нильпотентных группах*, Мат. св., 1955, 37, No. 3, 567 – 572.

[107] Мальцев А. И., *Модельные соответствия*, Изв. АН СССР, сер. мат., 1959, 23, No. 3, 313 – 336.

[108] McCool J., Pietrowski A., *On Free Products with Amalgamation of Two Infinite Cyclic Groups*, Journal of Algebra 18 (1971), 377 – 383.

[109] McKenzie R., *Subdirect Powers of Non-Abelian Groups*, Houston Journal of Mathematics, Volume 8, No. 3, 1982, 389 – 399.

[110] Mendelson E., *Introduction to Mathematical Logic*, 2nd ed., D. Van Nostrand Company, 1979.

[111] Мерзляков Ю. И., *Рациональные группы*, "Наука", Москва, 1980.

[112] Mijajlović Ž., *An Introduction to Model Theory*, University of Novi Sad, Institute of Mathematics, Novi Sad, 1987.

[113] Милич С., *Об одном доказательстве теоремы Шрейера в структурах*, Математички Весник 6(21) 1969 стр. 161 – 162.

[114] Miller A. G., Blichfeldt H. F., Dickson L. E., *Theory and Applications of Finite Groups*, Dover Publications, Inc., New York (reprint izdanja iz 1916), 1961.

[115] Miller D. W., *On a Theorem of Hölder*, The American Mathematical Monthly, Vol. 65, No. 4, 1958, pp. 252-254.

[116] Мишина А. П., *Абелевы группы*, Итоги Науки и Техники, серия Алгебра. Топология. Геометрия, Том 23, Москва, 1985, 51 – 118.

[117] Mišina A. P., Skornjakov L. A., *Abelian Groups and Modules*, American Mathematical Society Translations, Series 2, Volume 107, Rhode Island, 1976.

[118] Morris S. A., *Varieties of Topological Groups; a survey*, Colloquium Mathematicum, vol. XLVI, fasc. 2, 1982, 147 – 165.

[119] Mostowski A. W., *On the Decidability of Some Problems in Special Classes of Groups*, Fundamenta Mathematicae LIX (1966), 123 – 135.

[120] Müller O., *Über p-Automorphismen endlicher p-Gruppen*, Dissertation, der Mathematischen Fakultät der Eberhard – Karls – Universität zu Tübingen, Tübingen, 1979.

[121] Мясников А. Г., Ремесленников В. Н., *Теоретико-модельные вопросы теории групп*, Итоги Науки и Техники, серия Алгебра. Топология. Геометрия, Том 27, Москва, 1989, 16 – 22.



[122] Neumann B. H., *On the Number of Generators of a Free Product*, J. London Math. Soc., 18, 12 – 20

[123] Neumann B. H., *A Note on Algebraically Closed Groups*, J. London Math. Soc. 27 (1952), 247 – 249.

[124] Neumann H., *Varieties of Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Bd. 37, Springer-Verlag, Berlin – Heidelberg – New York, 1967.

[125] Новиков П. С., *Об алгоритмической неразрешимости проблемы тождества*, ДАН СССР 85 (1952), 709 – 712

[126] Новиков П. С., *Неразрешимость проблемы сопряженности в теории групп*, Изв. АН СССР, Сер. матем., 18 (1954), 485 – 524

[127] Новиков П. С., Адян С. И., *О бесконечых периодеческих группах*, Изв. АН СССР, Сер. матем., 32 (1968), 212 – 244.

[128] Ольшанский А. Ю., *Бесконачная группа с подгруппами простых порядков*, Изв. АН СССР, Сер. матем., 44, No. 2 (1980), 309 – 321.

[129] Ольшанский А. Ю., *Геометрия определяющих соотношений в группах*, "Наука", Москва, 1989.

[130] O'Neil J. D., *On Summands of Direct Products of Abelian Groups*, Commentationes Mathematicae, Universitatis Carolinae, 24,3 (1983), 407 – 413.

[131] Pazderski G., *Die Ordnungen, zu denen nur Gruppen mit gegebenen Eigenschaften gehören*, Arch. Math. 10 (1959), 331 – 343.

[132] Perić, V., *Algebra* I, II, Svjetlost, Sarajevo, 1980.

[133] Плоткин Б. И., *Группы автоморфизмов алгебраических систем*, "Наука", Москва, 1966.

[134] Понтрягин Л. С., *Непрерывные группы*, *"Наука", Москва*, 1973.

[135] Постников М. М., *Группы и алгебры Ли*, "Наука", Москва, 1982.

[136] Prest M., *Model Theory and Modules*, London Mathematical Society, Lecture Note Series 130, Cambridge University Press, 1988.

[137] Prešić S., *On Quasi-algebras and the Word Problem*, Publ. Inst. Math. Beograd 26(40) (1979), 255 – 268.

[138] Procesi C., *The Burnside Problem*, Journal of Algebra 4 (1966), 421 – 425.

[139] Ремесленников В. Н., Романьков В. А., *Теоретико-модельные и алгоритмические вопросы теории групп*, Итоги Науки и Техники, серия Алгебра. Топология. Геометрия, Том 21, Москва, 1983, 3 – 79.

[140] Robinson D. J. S., *A Course in the Theory of Groups*, Springer-Verlag, New York, 1982.

[141] Rose J. S., *A Course in Group Theory*, Cambridge University Press, 1978.

[142] Rotman J. J., *The Theory of Groups, an Introduction*, Allyn and Bacon, Inc., Boston, 1973.

[143] Saracino D., *Wreath Products and Existentially Complete Solvable Groups*, Transactions of the American Mathematical Society, Volume 197, 1974, 327 – 339.

[144] Saracino D., *Existentially Complete Nilpotent Groups*, Israel Journal of Mathematics, Vol. 25, 1976, 241 – 248.

[145] Scapellato R., Verardi L., *Sur les ensembles generateurs minimaux d'un groupe fini*, Ann. Sci. Univ. "Blaise Pascal", Clermont II, Ser. Math., Fasc. $26^{\text{eme}}$ Clermont-Ferrand, 1990, 51 – 60.

[146] Schenkman E., *Group Theory*, D. Van Nostrand Company, Inc., 1965.

[147] Schiefelbusch L., *Sylow 2-Subgroups of Simple Groups*, Journal of Algebra 31 (1974), 131 – 153.

[148] Scott W. R., *Algebraically Closed Groups*, Proc. Amer. Math. Soc. 2 (1951), 118 –121.

[149] Scott W. R., *Group Theory*, Dover Publications, Inc. (reprint prvog izdanja iz 1964), New York, 1987

[150] Седова Е. И., *О группах с абелевыми подгруппами конечных рангов*, Алгебра и логика, 21, No. 3 (1982), 321 – 343.

[151] Серр Ж.-П., *Линейные представления конечныкх групп*, "Мир", Москва, 1970.

[152] Shoenfield J. R., *Mathematical Logic*, Addison-Wesley Publishing Company, 1967.

[153] Stojaković M., *Elementi linearne algebre*, Zavod za izdavanje udžbenika, Beograd, 1970.

[154] Stojaković M., *Teorija jednačina*, Naučna knjiga, Beograd, 1973.



[155] Stojaković Z., Paunić D., *Zbirka zadataka iz algebre; grupe, prsteni, polja*, Institut za matematiku, Novi Sad, 1993.

[156] Супруненко Д. А., *Группы матриц*, "Наука", Москва, 1972.

[157] Suzuki M., *Structure of a Group and the Structure of Its Lattice of Subgroups*, Springer-Verlag, Berlin, 1956.

[158] Шеметков Л. А., *Формации конечных групп*, "Наука", Москва, 1978.

[159] Шунков В. П., *Об одном классе p-групп*, Алгебра и Логика, 9, §5 (1970), 579 – 615.

[160] Шунков В. П., *$M_p$-группы*, "Наука", Москва, 1990

[161] Ušan J., *n-Groups, $n \geq 2$, as Varieties of Type $\langle n, n-1, n-2\rangle$* (u štampi)

[162] Vojvodić G., Šešelja B., *A Note on the Modularity of the Lattice of Weak Congruences on a Finite Group*, Contributions to General Algebra 5, Proc. of the Salzburg Conference, Wien 1987, 415 – 419.

[163] Vujošević S., *Matematička logika – o mogućnostima formalnog metoda*, CID, Podgorica, 1996.

[164] Warfield R. B., Jr., *Nilpotent Groups*, Lecture Notes in Mathematics 513, Springer-Verlag, Berlin, 1976.

[165] Weinstein M., *Examples of Groups*, Polygonal Publishing House, 1977.

[166] Weyl H., *The Classical Groups; their invariants and representation*, Princeton University Press, 1946.

[167] Залешкий А. Е., *Линейные группы*, Итоги Науки и Техники, серия Алгебра. Топология. Геометрия, Том 21, Москва, 1983, 135 – 182.

[168] Zassenhaus H. J., *The Theory of Groups*, 2nd ed., Chelsea Publishing Company, New York, 1958.

[169] Zieschang H., Vogt E., Coldewey H.-D., *Flächen und ebene diskontinuierliche Gruppen*, Springer-Verlag, Berlin – Heidelberg – New York, 1970.

[170] Zippin L., *Countable Torsion Groups*, Annals of Mathematics, Vol. 36. No. 1, January 1935, 86 – 99.

[171] Желобенко Д. П., Штерн А. И., *Представления групп Ли*, "Наука", Москва, 1983.

# Notacija

| | | |
|---|---|---|
| $\mathbf{Z}$ | Aditivna grupa celih brojeva | 4 |
| $\mathbf{Ra}$ | Aditivna grupa racionalnih brojeva | 4 |
| $\mathbf{Re}$ | Aditivna grupa realnih brojeva | 4 |
| $+_n$ | Sabiranje po modulu $n$ | 5 |
| $\mathbf{Z}_n$ | (Ciklična) grupa sa domenom $n = \{0, \ldots, n-1\}$ i operacijom sabiranja po modulu $n$ | 5 |
| $\cdot_n$ | Množenje po modulu $n$ | 5 |
| $S_A$ | Skup bijektivnih preslikavanja skupa $A$ na sebe | 6 |
| $\mathbf{S}_A$ | Simetrična grupa skupa $A$ | 6 |
| $\mathbf{G} \cong \mathbf{H}$ | Grupe $\mathbf{G}$ i $\mathbf{H}$ su izomorfne | 8 |
| $Hom(\mathbf{G}, \mathbf{H})$ | Skup svih homomorfnih preslikavanja grupe $\mathbf{G}$ u grupu $\mathbf{H}$ | 8 |
| $Is(\mathbf{G}, \mathbf{H})$ | Skup svih izomorfnih preslikavanja grupe $\mathbf{G}$ na grupu $\mathbf{H}$ | 8 |
| $\mathbf{End(G)}$ | Polugrupa endomorfizama grupe $\mathbf{G}$ | 9 |
| $\mathbf{Aut(G)}$ | Grupa automorfizama grupe $\mathbf{G}$ | 9 |
| $\mathbf{Inn(G)}$ | Grupa unutrašnjih automorfizama grupe $\mathbf{G}$ | 10 |
| $u_g$ | Unutrašnji automorfizam koji odgovara elementu $g$ | 10 |
| $\mathbf{H} \leq \mathbf{G}$ | $\mathbf{H}$ je podgrupa grupe $\mathbf{G}$ | 13 |
| $\mathbf{H} < \mathbf{G}$ | $\mathbf{H}$ je prava podgrupa grupe $\mathbf{G}$ | 13 |
| $\mathbf{E}$ | Jedinična podgrupa (ma koje) grupe | 13 |
| $\mathbf{Z(G)}$ | Centar grupe $\mathbf{G}$ | 14 |
| $\mathbf{C}(a)$ | Centralizator elementa $a$ | 14 |
| $\mathbf{C(H)}$ | Centralizator podgrupe $\mathbf{H}$ | 14 |
| $\mathbf{D}_n$ | Dijedarska grupa stepena $n$ (i reda $2n$) | 16 |
| $\mathbf{p}^\infty$ | Prüferova $p$-grupa | 17 |
| $[\mathbf{G} : \mathbf{H}]$ | Indeks podgrupe $\mathbf{H}$ grupe $\mathbf{G}$ | 18 |
| $\mathbf{H} \lhd \mathbf{G}$ | $\mathbf{H}$ je normalna podgrupa grupe $\mathbf{G}$ | 27 |
| $\mathbf{Core(H)}$ | Srž podgrupe $\mathbf{H}$ | 29 |





| | | |
|---|---|---|
| $\mathbf{N(A)}$ | Normalizator podgrupe $\mathbf{A}$ | 29 |
| $\mathbf{N_H(A)}$ | Normalizator podgrupe $\mathbf{A}$ u podgrupi $\mathbf{H}$ | 29 |
| $\mathbf{G/H}$ | Faktor grupa grupe $\mathbf{G}$ po normalnoj podgrupi $\mathbf{H}$ | 32 |
| $\mathbf{Ker}(\varphi)$ | Jezgro homomorfizma $\varphi$ | 32 |
| $\langle A \rangle$ | Podgrupa generisana skupom $A$ | 39 |
| $\langle a \rangle$ | Ciklična grupa generisana elementom $a$ | 39 |
| $\mathbf{Q}$, $\mathbf{Q}_8$ | Grupa kvaterniona | 40 |
| $\mathbf{Fr(G)}$, $\mathbf{Frat(G)}$, $\mathbf{\Phi(G)}$ | Frattinijeva podgrupa grupe $\mathbf{G}$ | 41 |
| $\mathbf{A}^{\mathbf{G}}$, $[A]_{\mathbf{G}}$ | Normalno zatvorenje podgrupe $\mathbf{A}$ grupe $\mathbf{G}$ | 43 |
| $[a, b]$ | Komutator elemenata $a$ i $b$ | 51 |
| $\mathbf{G}'$ | Komutatorska (izvodna) podgrupa grupe $\mathbf{G}$ | 51 |
| $[A, B]$ | Podgrupa generisana skupom $\{[a,b] \mid a \in A, b \in B\}$ | 51 |
| $\mathbf{G}^{(n)}$ | $(\mathbf{G}^{(n-1)})'$, gde je $\mathbf{G}^{(0)} = \mathbf{G}$ | 51 |
| $\mathbf{S}_n$ | Grupa permutacija skupa $n = \{0, \ldots, n-1\}$ | 78 |
| $\mathbf{A}_n$ | Alternativna grupa (stepena $n$) | 84 |
| $\prod_{i \in I} G_i$ | Direktni proizvod familije skupova $\{G_i \mid i \in I\}$ | 105 |
| $\prod^c_{i \in I} \mathbf{G}_i$ | Kartezijanski (kompletni direktni) proizvod familije grupa $\{\mathbf{G}_i \mid i \in I\}$ | 105 |
| $\prod_{i \in I} \mathbf{G}_i$ | Direktni proizvod familije grupa $\{\mathbf{G}_i \mid i \in I\}$ | 105 |
| $\prod^d_{i \in I} G_i$ | Domen direktnog proizvoda familije grupa $\{\mathbf{G}_i \mid i \in I\}$ | 105 |
| $S(f)$ | Nosač (potpora) elementa $f$ $(\in \prod_{i \in I} G_i)$ | 106 |
| $\mathbf{H}^i$ | $i$-ta komponenta podgrupe $\mathbf{H}$ grupe $\prod_{i \in I} \mathbf{G}_i$ | 108 |
| $\mathbf{G} = \mathbf{H} \rtimes \mathbf{K}$, $\mathbf{G} = \mathbf{K} \ltimes \mathbf{H}$ | $\mathbf{G}$ je poludirektni proizvod podgrupa $\mathbf{H}$ i $\mathbf{K}$, gde je $\mathbf{H}$ normalni faktor | 149 |
| $\mathbf{A} \times_\theta \mathbf{B}$ | Ekstenzija (izomorfne slike) grupe $\mathbf{A}$ grupom $\mathbf{B}$ koja realizuje $\theta$ $(\in Hom(\mathbf{B}, \mathbf{Aut(A)})$ | 166 |
| $\mathbf{A}\ Wr\ \mathbf{B}$ | Neograničeni (kartezijanski) spleteni (venačni) proizvod grupe $\mathbf{A}$ sa grupom permutacija $\mathbf{B}$ | 170 |
| $\mathbf{A}\ wr\ \mathbf{B}$ | Ograničeni (direktan) spleteni (venačni) proizvod grupe $\mathbf{A}$ sa grupom permutacija $\mathbf{B}$ | 171 |
| $s_p$ | Broj Sylowih $p$-podgrupa u datoj grupi | 186 |
| $\mathbf{I} \lhd \mathbf{R}$ | $\mathbf{I}$ je ideal prstena $\mathbf{R}$ | 221 |
| $\mathbf{F}[x]$ | Prsten polinoma s koeficijentima iz polja $\mathbf{F}$ | 223 |
| $\mathbf{K/F}$ | Polje $\mathbf{K}$ je ekstenzija polja $\mathbf{F}$ | 223 |
| $\overline{\mathbf{F}}$ | Algebarsko zatvorenje polja $\mathbf{F}$ | 227 |

| | | |
|---|---|---|
| $\mathbf{GF}(q)$ | Konačno (Galoisovo) polje reda $q$ | 229 |
| $\mathbf{GL}_m(\mathbf{F})$, $\mathbf{GL}(m,\mathbf{F})$ | Generalna linearna grupa – grupa regularnih matrica formata $m \times m$ sa elementima iz polja $\mathbf{F}$ (s obzirom na matrično množenje) | 230 |
| $\mathbf{GL}_m(q)$, $\mathbf{GL}(m,q)$ | Generalna linearna grupa koja odgovara konačnom polju reda $q$ | 230 |
| $\mathbf{SL}_m(\mathbf{F})$, $\mathbf{SL}(m,\mathbf{F})$ | Specijalna linearna grupa | 231 |
| $\mathbf{SL}_m(q)$, $\mathbf{SL}(m,q)$ | Specijalna linearna grupa koja odgovara konačnom polju reda $q$ | 231 |
| $\mathbf{PSL}_m(\mathbf{F})$, $\mathbf{PSL}(m,\mathbf{F})$ | Projektivna unimodularna grupa | 233 |
| $\mathbf{PSL}_m(q)$, $\mathbf{PSL}(m,q)$ | Projektivna unimodularna grupa koja odgovara konačnom polju reda $q$ | 233 |
| $(A;P)$ | Prezentacija (postavka) grupe; $A$ – skup izvodnih simbola, $P$ – skup odrednica | 253 |
| $\mathbf{G}_{(A;P)}$ | (Kanonička) grupa određena prezentacijom $(A;P)$ | 256 |
| $\mathbf{F}_A$ | Slobodna grupa (sa prezentacijom $(A;\emptyset)$) | 277 |
| $\mathbf{G}(R)$ | Verbalna podgrupa grupe $\mathbf{G}$ s obzirom na skup reči $R$ | 293 |
| $\mathcal{V}(R)$ | Varijetet grupa određen skupom (zakona) $R$ | 295 |
| $\mathbf{G} = \prod^*_{i\in I} \mathbf{G}_i$, $\mathbf{G} = Fr_{i\in I}\mathbf{G}_i$ | $\mathbf{G}$ je slobodni proizvod familije (pod)grupa $\{\mathbf{G}_i \mid i \in I\}$ | 306 |
| $\mathbf{G} = \mathbf{G}_1 * \mathbf{G}_2$ | $\mathbf{G}$ je slobodni proizvod (pod)grupa $\mathbf{G}_1$, $\mathbf{G}_2$ | 306 |
| $\sum_{i\in I} \mathbf{A}_i$ | Direktna suma familije Abelovih grupa $\{\mathbf{A}_i \mid i \in I\}$ | 351 |
| $\sum^d_{i\in I} A_i$ | Domen direktne sume familije Abelovih grupa $\{\mathbf{A}_i \mid i \in I\}$ | 351 |
| $\mathbf{A}_1 \oplus \mathbf{A}_2$ | Direktna suma Abelovih grupa $\mathbf{A}_1$, $\mathbf{A}_2$ | 351 |
| $\sum^c_{i\in I} \mathbf{A}_i$ | Kompletna direktna (kartezijanska) suma familije Abelovih grupa $\{\mathbf{A}_i \mid i \in I\}$ | 351 |
| $\sum_{i\in I} A_i$ | Domen kompletne direktne sume familije Abelovih grupa $\{\mathbf{A}_i \mid i \in I\}$ | 351 |
| $t\mathbf{A}$ | Periodična podgrupa (periodični deo) Abelove grupe $\mathbf{A}$ | 352 |
| $S(\mathbf{A})$ | Sokla (cokla) Abelove grupe $\mathbf{A}$ | 352 |
| $\mathbf{A}_p$ | Podgrupa Abelove grupe $\mathbf{A}$ sa domenom $\{a \in A \mid$ red elementa $a$ je stepen prostog broja $p\}$ | 353 |
| $r(\mathbf{A})$ | Rang Abelove grupe $\mathbf{A}$ | 367 |
| $r_0(\mathbf{A})$ | Torziono slobodni rang Abelove grupe $\mathbf{A}$ | 367 |
| $r_p(\mathbf{A})$ | Rang podgrupe $\mathbf{A}_p$ Abelove grupe $\mathbf{A}$ | 368 |



| | | |
|---|---|---|
| $\mathbf{A}[n]$ | Podgrupa Abelove grupe $\mathbf{A}$ sa domenom $\{a \in A \mid na = 0\}$ | 381 |
| $n\mathbf{A}$ | Podgrupa Abelove grupe $\mathbf{A}$ sa domenom $\{a \in A \mid a$ je deljivo sa $n\}$ | 381 |
| $h(a)$ | Visina elementa $a$ Abelove grupe | 382 |
| $h_{\mathbf{B}}(a)$ | Visina elementa $a$ Abelove grupe $(\mathbf{A})$ u podgrupi $\mathbf{B}$ | 382 |
| $\mathbf{I}(\mathbf{A})$, $\mathbf{E}(\mathbf{A})$ | Injektivni (deljivi) omotač Abelove grupe $\mathbf{A}$ | 394 |
| $fin\, r(\mathbf{A})$ | Finalni rang ($p$-Abelove) grupe $\mathbf{A}$ | 452 |
| $\tau(\mathbf{A})$ | Tip Ulma Abelove grupe $\mathbf{A}$ | 462 |
| $\gamma_\alpha\mathbf{G}$ | $\alpha$-ti član (transfinitno produženog) nižeg centralnog lanca grupe $\mathbf{G}$ | 505 |
| $\zeta_\alpha\mathbf{G}$ | $\alpha$-ti član (transfinitno produženog) višeg centralnog lanca grupe $\mathbf{G}$ | 505 |
| $\mathbf{Fit}(\mathbf{G})$, $\mathbf{R}(\mathbf{G})$ | Fittingova nilradikalna podgrupa grupe $\mathbf{G}$ | 538 |
| $\sqrt{\mathbf{H}}$ | Deljivo zatvorenje podgrupe $\mathbf{H}$ deljive torziono slobodne nilpotentne grupe | 613 |

# Indeks

# Sadržaj