NATAŠA BOŽOVIĆ

ŽARKO MIJAJLOVIĆ

UVOD U TEORIJU GRUPA

TEOREME ● ZADACI ● PRIMERI

TREĆE IZDANJE

100 teorema
700 rešenih zadataka

Naučna Knjiga

BEOGRAD, 1990.

Nataša Božović
Žarko Mijajlović

UVOD U TEORIJU GRUPA

Teoreme, primeri i zadaci

Izdavač
IDP „Naučna knjiga"
Beograd, Uzun-Mirkova 5

Recenzenti
Dr *Slaviša Prešić*, red. prof. Univerziteta
u Beogradu
Dr *Branka Alimpić*, prof. Univerziteta u Beogradu

Za izdavača
Dr Blažo Perović

Urednik
Nikola Dončev

Tehnički urednik
Gradimir Savić

Tiraž 1.000 primeraka

ISBN 86-23-20215-5

Štampa: Štamparsko-izdavačko preduzeće „Bakar" - Bor

S A D R Ž A J

U V O D

"Imam neka nova otkrića u analizi. Prvo se odnosi na teoriju jednačina, drugo na integralne funkcije" pisao je 21 godišnji francuski matematičar Everist Galois, noć pre dvoboja u kojem je smrtno ranjen[1]. Rad E. Galoisa objavio je 14 godina posle ovog dogadjaja J. Liouville, i to je predstavljalo početak teorije grupa, jedne od najzanimljivijih oblasti algebre i matematike.

Ova teorija romantičnog porekla posebno je interesantna i značajna zbog svojih primena u mnogim delovima matematike (npr. u geometriji, topologiji, aritmetici), a isto tako i van matematike, na primer u kristalografiji, fizici elementarnih čestica i-rešavanju Rubikove kocke.

Šta su grupe? U osnovi, ova teorija odnosi se na svojstva simetrije koja poseduju bilo koji sistemi ili objekti. Na primer, snežna pahuljica, kristalić leda, može da se javi kao oblik čiji su vrhovi rasporedjeni pod uglom od 60^{o}. Ukoliko se pahuljica rotira za 60^{o} ili neki celi umnožak od 60^{o} , oko ose normalne na ravan pahuljice i koja prolazi kroz centar, tada osnovni oblik pahuljice ostaje nepromenjen, mada su neki vrhovi možda promenili mesto. Takvu transformaciju koja ostavlja oblik invarijantan u okviru sistema naziva se simetričnom operacijom.

Sličan primer je i Rubikova kocka, kod koje su od interesa rotacije njenih slojeva oko osa kocke za 90^{o}. Rešiti kocku znači odrediti niz ovih rotacija kojim se dobija prvobitan raspored Rubikove kocke.

---

1) Protivnik u ovom duelu bio je Pescheux d'Herbinville, oficir francuske artiljerijske garde, a dvoboj se zbio u jutro 30. maja 1832. g. Sledećeg dana E. Galois je umro od smrtonosnih rana. Razlog dvoboja bila je svadja lične prirode a izgleda i izvesna gospodjica Stephany Dumotel.

U algebri dugo je bilo otvoreno pitanje rešivosti algebarskih jednačina $a_0+a_1x+\ldots+a_nx^n=0$ preko radikala, tj. primenom neke formule u kojoj učestvuju jedino elementarne aritmetičke operacije i korenovanje proizvoljnog stepena. Ova jednačina je invarijantna u odnosu na neke permutacije svojih korena, i skup svih ovih permutacija čini grupu, tzv. Galoisovu grupu ove jednačine. O tome i piše E. Galois u svom poslednjem pismu:

"U teoriji jednačina ispitivao sam uslove pod kojim je neka jednačina rešiva preko radikala, to mi je dalo priliku da produbim ovu teoriju, i opišem sve moguće transformacije na nekoj jednačini, pa i na onim koje nisu rešive radikalima...".

Počeci ove teorije javljaju se i kod drugih matematičara onog doba, pa i ranije, na primer kod J.Langrangea (1771), P. Ruffinia, N. Abela, A. Cauchya i drugih. Zatim se teorija grupa brzo razvijala, izmedju ostalog i zbog primena u drugim oblastima matematike. Tako, F. Klein u svom čuvenom Erlangenskom programu (iz 1872. god.)pominje da u osnovi klasifikacija geometrija leži pojam grupe nekih preslikavanja.

Danas se grupe javljaju u velikom broju matematičkih disciplina. Na primer, u topologiji važnu ulogu imaju grupe homologije i grupe homotopije topoloških prostora. Konstrukcija ovih grupa omogućuje da se odredjeni problemi topološke prirode svedu na algebarske. Slična teoriji Galoisa je teorija Picara-Wessio u kojoj se sredstvima teorije grupa izučavaju raširenja diferencijalnih prstena, i ona delimično rešava pitanje rešivosti diferencijalnih jednačina kvadraturom. Ono što su u teoriji Galoisa permutacije, u ovoj teoriji su to grupe nekih matrica.

Spomenimo da postoje mnogobrojne generalizacije pojma grupe čije teorije danas egzistiraju kao potpuno nezavisne matematičke discipline. Najznačajniji primeri ovih algebarskih struktura su semigrupe i kvazigrupe, i njima je posvećeno prvo poglavlje ove knjige. Na ovim strukturama, kao u ostalom i na grupama, izučavaju se i neki specifični problemi, na primer funkcionalne jednačine, i tome su značajne priloge dali i jugoslovenski matematičari (S.Prešić, M.Petrić, B.Alimpić, S.Milić, A.Krapež i drugi).

Pored osnovnih pojmova teorije grupa, u ovoj knjizi mogu se naći mnogobrojni primeri grupa, kao i detaljan pregled različitih konstrukcija nad grupama. Isto tako, detaljno su obradjene neke teme. Recimo, u poglavlju o Abelovim grupama razmatraju se stavovi

reprezentacije za komutativne grupe (za konačno generalisane Abelove grupe kao i za grupe sa deljenjem). Rešive i nilpotentne grupe mogu se uzeti kao uopštenje Abelovih grupa, i one se izučavaju u 9. poglavlju. Ove grupe su od interesa, pa i neophodne za teoriju Galoisa. U osmom poglavlju razmatraju se neke metode za izučavanje konačnih grupa, od kojih je najznačajnije dejstvo odnosno permutacijska reprezentacija grupa koje se delimično izučava i u 4. poglavlju. Primenom ovih metoda detaljno su opisane sve grupe čiji je red manji od 32 (ukupno ih ima 93).

Poglavlja 10, 11 i 12 predstavljaju zasebnu celinu i odnose se na slobodne grupe i neke bliske konstrukcije (slobodan proizvod, amalgamiran proizvod). Poglavlje 10 predstavlja uvod u teoriju univerzalnih algebri s obzirom da se mnogobrojne konstrukcije, definicije, teoreme koje se odnose na grupe bez velikih izmena prenose i na druge algebarske strukture. U poglavlju 11 detaljno se izučavaju slobodne grupe, kao i struktura slobodnih i amalogamiranih proizvoda grupa. Tu se dokazuje i značajna Nielsen-Schreirova teorema o strukturi podgrupa slobodne grupe. U 12. poglavlju razmatra se jedan efektivan način zadavanja široke klase prebrojivih grupa, preko strukturnih jednakosti. Tietze-ove transformacije su operacije nad strukturnim jednakostima, ali koje ne menjaju polaznu grupu, i predstavljaju zgodno sredstvo za izučavanje grupa zadate prezentacijama. Najzad, u istom poglavlju izučavaju se razni problemi neodlučivosti (problem reči, problem konjugacije i sl.) za grupe zadate strukturnim jednakostima.

Poslednje, 13. poglavlje odnosi se na primene teorije grupa na neke elementarne probleme teorije brojeva i teoriju polja. U drugom odeljku ovog poglavlja izlažu se osnove Teorije Galois-a.

Ova knjiga predvidjena je kao uvod u teoriju grupa, i može da služi kao udžbenik za jednogodišnji kurs teorije grupa za studente redovnih studija, ili jedno-semestralni kurs za studente poslediplomskih studija. Naravno, delovi ove knjige mogu se koristiti i za opšte kurseve algebre. Za prvi kurs algebre (Algebra 1) u tu svrhu može da posluži jedan izbor poglavlja i odeljaka iz prvih 9 poglavlja i 13. poglavlja. U slučaju drugog po redu kursa (Algebra 2) od koristi može biti materijal u poglavljima 10, 11, 12. Napomenimo da su se delovi ove knjige već pojavili kao predavanja iz pomenutih predmeta na Prirodno-matematičkom fakultetu u Beogradu i Kragujevcu koje su držali autori, ili

kao vežbe koje su oni takodje držali na istim kursevima kod prof. S. Prešića. Najzad, ova knjiga može biti od interesa i za druge oblasti matematike, svuda gde se javljaju grupe (topologija, geometrija), kao i za studente fizike i mehanike.

Naglasak u ovoj knjizi je na zadacima, s obzirom da je veliki broj zadataka, preko 700, navedeno i rešeno. To omogućava najpre veću samostalnost u radu studenta, a zatim da student vidi svoje mogućnosti u rešavanju zadataka, s obzirom da ima zadataka različitih težina. Napomenimo da se veliki broj zadataka iz ove knjige u drugim knjigama javljaju kao teoreme.

Pored citirane literature, korišćeni su i razni časopisi, u prvom redu American Mathematical Monthly i Matematički vesnik. Veći broj zadataka potiče i sa pismenih ispita iz predmeta Algebra I i Algebra II, kao i sa studentskih takmičenja držanih na Prirodno-matematičkom fakultetu u Beogradu.

Prilikom pisanja ove knjige imali smo veliku pomoć od strane naših kolega kojima dugujemo mnogobrojne korisne sugestije, ispravke, kao i predloge za neke zadatke. To se u prvom redu odnosi na prof. S. Prešića koji je velikim delom i dao inicijativu za pisanje ove knjige, to je bilo još davne 1977. godine. Naročitu zahvalnost dugujemo kolegama S. Krstiću i M. Božiću, B. Veličkoviću i M. Kapetanoviću, koji su velike delove rukopisa pročitali, a isto tako i A. Krapežu za predloge zadataka. Zahvaljujemo se i M. Raškoviću kao i studentima A. Vučiću i N. Blažiću koji su takodje pročitali delove rukopisa i uputili korisne sugestije.

Žarko Mijajlović je napisao sledeća poglavlja: Grupoidi, prva dva odeljka 2. poglavlja, Ciklične grupe, Abelove grupe, Dejstvo i konačne grupe, Slobodne algebre i Addendum, dok je Nataša Božović napisala ova poglavlja: druga dva odeljka 2. poglavlja, Normalne podgrupe, Grupe permutacije, Direktan proizvod, Rešive i nilpotentne grupe, Slobodne grupe i slobodan proizvod i Predstavljanje grupa.

Naravno, oba autora podjednako odgovaraju za tekst u celini.

Beograd, Septembra 1982.

A u t o r i

S I M B O L I

U ovom tekstu koristimo uobičajenu notaciju iz matematičke logike i teorije skupova. Radi odredjenosti navodimo neke od tih oznaka, kao i definicije pojmova koje koristimo na dalje.

Oznake za logičke veznike su $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\Leftrightarrow$ i označavaju redom konjunkciju, disjunkciju, negaciju, implikaciju i ekvivalenciju. Logičke vrednosti složenih formula, izgradjenih pomoću ovih veznika odredjuju se na uobičajen način, v. npr. [23]. Skraćenica akko je zamena za "ako i samo ako".

Implikacijski lanac je zapis oblika $p_0 \Rightarrow p_1 \Rightarrow \ldots \Rightarrow p_n$ i zamenjuje formulu $(p_0 \Rightarrow p_1) \wedge (p_1 \Rightarrow p_2) \wedge \ldots \wedge (p_{n-1} \Rightarrow p_n)$.

Ekvivalencijski lanac je $p_0 \Leftrightarrow p_1 \Leftrightarrow p_2 \Leftrightarrow \ldots \Leftrightarrow p_n$ i zamena je za formulu $(p_0 \Leftrightarrow p_1) \wedge (p_1 \Leftrightarrow p_2) \wedge \ldots \wedge (p_{n-1} \Leftrightarrow p_n)$.

Oznaka za *univerzalni kvantor* je $\forall$, dok se *egzistencijalni kvantor* obeležava sa $\exists$. Tako, formule $(\forall x)\varphi(x)$, $(\exists x)\varphi(x)$, $(\exists_1 x)\varphi(x)$ redom se čitaju:

za svaki x $\varphi(x)$

postoji x takav da je $\varphi(x)$

postoji tačno jedno x tako da je $\varphi(x)$.

Za logičke vrednosti formula sa kvantifikatorima nužno je poznavanje *domena* promenljivih, tj. skupa u kojem promenljive uzimaju vrednost kao i interpretacije operacijskih simbola i znakova konstanata. Naime, u izgradnji formula predikatskog računa učestvuje znak jednakosti kao i simboli konstanata funkcija i relacija. Formule u kojima su sve promenljive pod dejstvom kvantifikatora nazivaju se rečenicama. O interpretaciji ili modelu jezika, odnosno ovakvih skupova simbola, čitalac se može upoznati naprimer u [5] . U ovoj knjizi uglavnom će biti reći o tzv. algebarskim jezicima, tj. jezicima koji se sastoje od simbola konstanata i operacija. U nekoliko prilika koristićemo sledeću teoremu predikatskog

računa 1. reda:

Stav kompaktnosti. Neka je T skup nekih rečenica sa osobinom da svaki konačan podskup od T ima model. Tada postoji model za T.

Skupovnu relaciju pripadanja označavamo sa $\in$. Dakle, ako je $x \in y$, onda kažemo da je x element skupa y. *Inkluzija* je još jedna skupovna relacija: $A \subseteq B \Leftrightarrow \forall x(x \in A \Rightarrow x \in B)$. Važi ovaj uslov *ekstenzionalne jednakosti* skupova: $A = B \Leftrightarrow \forall x(x \in A \Leftrightarrow x \in B)$ tj.

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A.$$

Uobičajene skupovne operacije su presek, unija i razlika skupova i njihove definicije redom su za skupove A, B, odnosno familiju A_i, $i \in I$:

$A \cap B = \{x | x \in A \wedge x \in B\}$ tj. $\bigcap_i A_i = \{x | (\forall i \in I)(x \in A_i)\}$

$A \cup B = \{x | x \in A \vee x \in B\}$ tj. $\bigcup_i A_i = \{x | (\exists i \in I)(x \in A_i)\}$

$A \setminus B = \{x | x \in A \wedge \neg x \in B\}$

Ako je $A \subseteq X$, tada se $X \setminus A$ naziva komplementom skupa A u odnosu na X i često se kraće označava sa A^c.

Partitivan skup skupa A je $\mathcal{P}A = \{X | X \subseteq A\}$.

Proizvod skupova A, B je

$A \times B = \{(x,y) | x \in A \wedge y \in B\}$.

Umesto $A \times A$ pišemo i A^2.

Ako je X_i, $i \in I$, familija nekih skupova, proizvod skupova X_i $(i \in I)$ je

$$\prod_{i \in I} X_i = \{f | (\forall i \in I) f(i) \in A_i \wedge f : I \to \bigcup_{i \in I} A_i\}$$

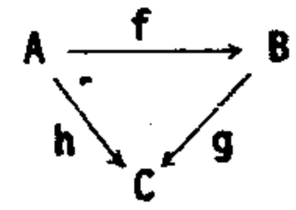
U ovoj formuli koristili smo strelicu - znak za funkciju. Dakle, ako je f preslikavanje skupa A u skup B, onda koristimo oznaku $f : A \to B$. Neki drugi zapisi za funkciju su:

$f : x \mapsto w(x)$, gde je $w(x)$ neki izraz (term)

$f = \langle f(x) | x \in A \rangle$, $f = (f(x)^x) \; x \in A$.

Sve ove složene simbole mi ćemo koristiti u ovoj knjizi. Ako je $f : A \to B$, skup A se naziva *domenom* funkcije f, u oznaci Dom (f) a skup B *kodomenom*. *Skup vrednosti* funkcije f je $f(A) = \{f(x) | x \in A\}$. Ako je $Y \subseteq B$, onda *inverzna slika* skupa Y je $f^{-1}(Y) = \{x \in A | f(x) \in Y\}$. Ako je $X \subseteq A$, *restrikcija* funkcije f na skup X je funkcija $g : X \to B$, gde $(\forall x \in X) g(x) = f(x)$. Koristi se oznaka $g = f \restriction X$. Ako je $f : A \to B$ i $g : B \to C$, *kompozicija (slog, proizvod)* funkcija f i g je funkcija $h : A \to C$ definisana

sa $(\forall x \in A)\ h(x) = g(f(x))$. Koristimo oznaku h=gof ili h=fg (algebarska konvencija) i kažemo da dijagram



komutira.

Funkcija f je 1-1 akko $(\forall x, y \in A)\ (x \neq y \Rightarrow f(x) \neq f(y))$ i koristimo oznaku $f : A \xrightarrow[1\text{-}1]{} B$.

Funkcija f je <u>na</u> akko $(\forall y \in B)(\exists x \in A)\ (y = f(x))$, i koristimo oznaku $f : A \xrightarrow{\text{na}} B$.

Identička funkcija skupa A, $I_A : A \to A$, definisana je sa $(\forall x \in A) I_A(x) = x$.

Prilikom razmatranja beskonačnih skupova važnu ulogu ima

<u>*Aksioma izbora:*</u> *Ako je* X_i, $i \in I$, *neprazna familija nepraznih skupova, od kojih su svaka dva uzajamno disjunktna onda postoji skup Y takav da za svaki* $i \in I$ *sadrži tačno jedan element iz* X_i .

Skup Y iz prethodne rečenice naziva se *izbornim skupom* ili *transverzalom* za funkciju X_1, $i \in I$. Očigledno je da skup Y odredjuje jedinstvenu funkciju $f : I \to \bigcup_i X_1$ tako da $f(I) = Y$ i $(\forall i \in I) f(i) \in X_1$. Ova funkcija naziva se *funkcijom izbora* za familiju X_1, $i \in I$.

Neki skupovi u ovoj knjizi nosiće posebne oznake. To se u prvom redu odnosi na prazan skup, $\emptyset = \{x \mid x \neq x\}$, zatim skup prirodnih brojeva $\{0,1,2,\ldots\}$. Ovaj skup označavamo sa ω. Dakle, $\omega = \{0,1,2,\ldots\}$. Dalje, $N = \omega \setminus \{0\} = \{1,2,3,\ldots\}$. Skup celih brojeva je $Z = \{\ldots, -2,-1,0,1,2,\ldots\}$. Ukoliko drugačije nije rečeno skupove racionalnih, realnih i kompleksnih brojeva označavamo sa Q, R, C, a odgovarajuće strukture polja sa $\underline{Q}$, $\underline{R}$, $\underline{C}$. Dakle, $\underline{Q} = (Q,+,\cdot,0,1)$.

U Von Neumanovoj reprezentaciji prirodni brojevi izgledaju:

$0 = \emptyset$, $1 = \{0\}$, $2 = \{0,1\}$, $3 = \{0,1,2\}$, ... Dakle, $2 \subseteq 5$.

Binarna relacija skupova A, B je svaki podskup $\rho \subseteq A \times B$. Jedan primer binarne relacije je svako preslikavanje $f : A \to B$. Binarna relacija skupa A je svaki podskup $\rho \subseteq A^2$. Važni primeri binarnih relacija su:

Relacija poretka skupa A je svaka binarna relacija $<$ skupa A tako da važe ovi uslovi:

$x \not< x$, tj. relacija $<$ je *refleksivna*

$x \leqslant y \wedge y \leqslant x \Rightarrow x = y$, tj. $\leqslant$ je *antisimetrična*

$x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z$, dakle $\leqslant$ je *tranzitivna*

Par $(A,\leqslant)$ naziva se *uredjenjem*.
Ako je uz to ispunjeno $(\forall x,y \in A)(x<y \vee y<x)$ onda je $\leqslant$ *linearno* uredjenje skupa A. Striktno uredjenje skupa A uvodi se sa
$x<y \Leftrightarrow (x \leqslant y \wedge x \neq y)$.

Element $a \in A$ je
minimalan akko $(\forall x \in A)(\neg x<a)$
maksimalan akko $(\forall x \in A)(\neg a<x)$
najmanji akko $(\forall x \in A)(a \leqslant x)$
najveći akko $(\forall x \in A)(x \leqslant a)$

Gornja (donja) granica skupa $X \subseteq A$ je svaki element $a \in A$ sa osobinom $(\forall x \in X)(x \leqslant a)$ (tj. $(\forall x \in X)(a \leqslant x)$).
Supremum skupa $X \subseteq A$ je najmanja gornja granica skupa X i označava se sa sup X. *Infimum* skupa X je najveća donja granica skupa X i označava se sa inf X. Nemaju svi uredjeni skupovi osobinu da svaki podskup $X \subseteq A$ ima sup X ili inf X. Ako to ipak važi, tada je $(A,\leqslant)$ *kompletno* uredjen. Ako svaki konačan $X \subseteq A$ ima supremum i infinum, tada je $(A,\leqslant)$ *mreža*. Ako svaki neprazan $X \subseteq A$ ima najmanji element, onda je $(A,\leqslant)$ *dobro* uredjenje.

Skup $L \subseteq A$ je lanac akko $(\forall x,y \in L)(x<y \vee y<x)$. Dakle, ako je $(A,\leqslant)$ linearno uredjenje onda je svaki podskup od A lanac.

Sledeći iskazi ekvivalentni su Aksiomi izbora (uz ostale Aksiome teorije skupova, recimo ZF - Zermelo Freankelove teorije skupova):

Princip dobrog uredjenja: *Svaki skup se može dobro urediti.*

Zornova lema: *Neka je $(A,<)$ uredjenje sa osobinom da svaki lanac $L \subseteq A$ ima gornje ograničenje. Tada $(A,<)$ ima maksimalan element.*

Dva skupa X, Y su iste kardinalnosti akko postoji $f : X \xrightarrow[1-1]{na} Y$.
U okviru teorije skupova pokazuje se da se mogu uvesti skupovni objekti, tzv. kardinalni brojevi, koji se mogu pridružiti svakom skupu. Kardinalni broj skupa X označava se sa $|X|$ i važi
$|X| = |Y| \Leftrightarrow (\exists f)(f : X \xrightarrow[1-1]{na} Y)$.

Kardinalni broj konačnog skupa $\{a_1,\ldots,a_n\}$ je n ukoliko za $i \neq j \Rightarrow a_i \neq a_j$. Dalje, $|\omega| = \aleph_0$, $|R| = 2^{\aleph_0}$. *Kontinuum hipoteza* kaže da izmedju $\aleph_0$ i $2^{\aleph_0}$ nema kardinalnih brojeva.

Relacija ekvivalencije skupa A je svaka binarna relacija $\sim$

skupa A sa osobinom

$x \sim x$ $(x,y,z \in A)$

$x \sim y \Rightarrow y \sim x$ tj. $\sim$ je simetrična

$x \sim y \wedge y \sim z \Rightarrow x \sim z$.

Klasa ekvivalencije elementa $a \in A$ je $a/\sim = \{x \in A / x \sim a\}$. Ponegde ćemo ovaj skup označiti i sa C_a. Količnički skup je $A/\sim = \{a/\sim \mid a \in A\}$.

Partioija skupa A je svaka familija $\mathcal{P} = \{X_i \mid i \in I\}$ sa osobinama:

$(\forall i \in I)\ X_i \neq \emptyset$

$(\forall i, j \in I)\ (X_i \cap X_j \neq \emptyset \Rightarrow X_i = X_j)$

$\bigcup_i X_i = A$.

Važi ova teorema o vezi izmedju particija i relacija ekvivalencije:

Neka je $\sim$ relacija ekvivalencije skupa A. Tada je $A/\sim$ partioija skupa A.

Neka je $\mathcal{P}$ partioija skupa A. Tada binarna relacija $\sim$ skupa A definisana sa $x \sim y \Leftrightarrow (\exists X \in \mathcal{P})(x,y \in X)$ jeste relacija ekvivalenoije skupa A.

Ako su $\rho \subseteq A \times B$, $\delta \subseteq B \times C$ binarne relacije, proizvod relacija ρ, δ je relacija $\tau \subseteq A \times C$ definisana sa $(x,y) \in \tau \Leftrightarrow (\exists u \in B)((x,u) \in \rho \wedge (u,y) \in \delta)$; koristi se oznaka $\tau = \delta \circ \rho$.

Inverzna relacija za $\rho \subseteq A \times B$ je $\rho^{-1} \subseteq B \times A$, gde je $\rho^{-1} = \{(x,y) \mid (y,x) \in \rho\}$. *Dijagonalna relacija* skupa A je $\Delta_A = \{(x,y) \mid x \in A\}$. Dakle, $\Delta_A = I_A$.

Ovde je naveden jedino spisak logičkih i skupovnih simbola i definicija, ali ubuduće pretpostavljamo da se poznaju elementarne osobine ovih pojmova. Pod tim podrazumevamo, recimo, De Morganove znakove za logičke (skupovne operacije, ili, na primer zakon asocijacije za slaganje funkcije i relacije. Detaljne dokaze ovakvih i sličnih činjenica, kao i generalizacije čitalac može naći na primer u [23] , ili na kojem savremenom udžbeniku iz matematičke logike.

1. G R U P O I D I

Osnovni pojam koji se razmatra u svim oblastima algebre je pojam algebarske operacije. Od svih algebarskih operacija pokazuje se da *binarne operacije* imaju naročito važnu ulogu, jer upravo one predstavljaju delove definicija fundamentalnih algebarskih struktura kao što su grupe, prsteni i polja.

U ovom poglavlju proučavaćemo osnovne osobine algebarskih struktura sa jednom binarnom operacijom, a isto tako i neke važnije klase ovih struktura (semigrupe i kvazigrupe).

1.1. OSNOVNI POJMOVI

Binarna operacija f nepraznog skupa G je svako preslikavanje $f : G \times G \to G$. Uredjeni par (G,f) naziva se *grupoidom*, u kraćoj oznaci $\underline{G}$. Skup G je *domen* grupoida $\underline{G}$. Za $x,y \in G$ element f(x,y) označava se takodje sa xfy. Umesto slova f često se koriste oznake $\star, \circ, \cdot$ itd. Ako je $\underline{G} = (G,\cdot)$ grupoid i $a,b \in G$, tada je ab kraći zapis za $a \cdot b$.

Element e grupoida $(G,\cdot)$ je desni (levi) jedinični element ukoliko $(\forall a \in G)ae=a$ (odnosno $(\forall a \in G)ea=a$). Ako je e leva i desna jedinica, kažemo da je e *jedinični* ili *neutralni* element grupoida $\underline{G}$.

Grupoid $\underline{H} = (H,\star)$ je *podgrupoid* grupoida $\underline{G} = (G,\circ)$ ukoliko je $H \subseteq G$ i $\star$ je restrikcija operacije $\circ$ na H, tj. $(\forall a,b \in H)a\star b = a\circ b$. Najčešće se za operaciju $\star$ koristi ista oznaka $\circ$.

Termi nad jezikom $(\star)$ su sintaksni izrazi koji se definišu na sledeći način:

(i) promenljive $x_0, x_1, \ldots$ su termi,

(ii) ako su u,v termi tada je $(u\star v)$ term,

(iii) svaki term se dobija konačnom primenom pravila (i) i (ii).

U termima se krajnje zagrade (prva i poslednja) najčešće izostavljaju. Ako je u term, zapis $u(x_1,\ldots,x_n)$ označava da su sve promenljive terma u neke od promenljivih $x_1,\ldots,x_n$.

Neka je $\underline{G}$ grupoid i $X \subseteq G$. Kažemo da je $\underline{G}$ *generisan* skupom X, odnosno da je X skup generatora grupoida $\underline{G}$, ukoliko za svaki $a \in G$ postoji term $u(x_1,\ldots,x_n)$ i elementi $a_1,\ldots,a_n \in X$ tako da je $a = u(a_1,\ldots,a_n)$.

Primeri i zadaci

1.1. Dokazati ili opovrgnuti da je dvojka $(S,\star)$ grupoid, ako:

a) S je skup svih preslikavanja nepraznog skupa X u samog sebe a $\star$ je slaganje funkcija,

b) S je skup svih neprekidnih, realnih funkcija na R, $\star$ je slaganje funkcija,

c) $S=\{(a,b,c) \mid a,b,c\in Q;\ a,b,c\neq 0\}$,
$(a,b,c)\star(x,y,z)=(ax+bz+cy, az+by+cx, ay+bx+cz)$,

d) S je skup svih terma jezika $\{\circ\}$, $u\star v=(u\circ v)$.

Rešenje: a) Jeste grupoid. b) Prema poznatom stavu iz analize, $(S,\star)$ je grupoid. c) $(S,\star)$ nije grupoid budući da $(1,1,1), (1,-2,1)\in S$ ali $(1,1,1)\star(1,-2,1)=(0,0,0)$. d) $(S,\star)$ je grupoid, jer prema pravilima o formiranju terma važi: ako su u,v termi tada je $(u\circ v)$ term.

1.2. Niz skupova R_n definisan je sa $R_0=\emptyset$, $R_{n+1}=\{x \mid x\subseteq R_n\}$ $(n\in\omega)$.
Neka je $R_\omega=\bigcup_{n\in\omega} R_n$. Dokazati da je u svakom od sledećih slučajeva $(R_\omega,\star)$ grupoid, ako je operacija $\star$ definisana sa

a) $x\star y=\{x,y\}$, b) $x\star y=(x,y)$, gde je $(x,y)=\{\{x\},\{x,y\}\}$,

c) $x\star y=\{(x,y),(y,x)\}$.

Rešenje: Prethodno dokazujemo sledeća pomoćna tvrdjenja:

$$(\forall n\in\omega)(x\in R_n \Rightarrow x\subseteq R_n) \qquad (1)$$

$$(\forall n,m\in\omega)(n\geq m \Rightarrow R_m\subseteq R_n) \qquad (2)$$

Dokaz za (1) izvodimo indukcijom po n.

Slučaj n=0 je jednostavan. Neka je $n=k+1$, $k>0$. Dalje, neka je $x\in R_n$; tada $x\subseteq R_k$. Pretpostavimo da je $y\in x$. Kako je $x\subseteq R_k$ to $y\in R_k$, pa prema induktivnoj hipotezi $y\subseteq R_k$. Otuda $y\in R_n$. Stoga $(\forall y\in x)y\in R_n$, te $x\subseteq R_n$.

Dokaz za (2) takodje izvodimo indukcijom po n.

Slučaj n=m je trivijalan. Neka je $n=k+1$, $k\geq m$. Po induktivnoj hipotezi $R_m\subseteq R_k$, te $R_m\in R_n$. Prema (1) $R_m\subseteq R_n$.
Ovim su tvrdjenja (1) i (2) dokazana.
a) Neka su $a,b\in R_\omega$. Tada za neke $m,n\in\omega$ $a\in R_m$ i $b\in R_n$. Pretpostavimo $n\geq m$. Prema (2) $R_m\subseteq R_n$ te $a,b\in R_n$. Otuda $\{a,b\}\in R_{n+1}$, tj. $\{a,b\}\in R_\omega$.
b) $x,y\in R_n \Rightarrow (x,y)\in R_{n+2}$.
c) $x,y\in R_n \Rightarrow x\star y\in R_{n+3}$.

1.3. Dokazati da postoji neprazan skup X takav da $X\times X\subseteq X$.

Rešenje: Prema 1.2.b) važi $R_\omega\times R_\omega\subseteq R_\omega$. Opštije, $(\forall n\in\omega)R_\omega^n\subseteq R_\omega$.

1.4.Odrediti broj različitih grupoida sa domenom A, ako je $|A|=k$.

Rešenje: Svi grupoidi sa domenom A,oblika su (A,f) gde je $f : A \times A \to A$. *Otuda, različitih grupoida ima* k^{k^2} *budući da je* $|A \times A|=k^2$. *Ako je A beskonačan skup, tada* $k^2=k$ *i* $k^k=2^k$, *pa je prema tome ovaj broj jednak* 2^k.

1.5.Neka je A skup i $S=\{A^n \mid n\in\omega\}$, gde $A^n=A\times\ldots\times A$ (n puta). Da li je $(S,\times)$ grupoid?

1.2. KONGRUENCIJE I HOMOMORFIZMI

Relacija ekvivalencije $\sim$ skupa G je *kongruencija* grupoida $(G,\circ)$ ukoliko je $\sim$ saglasna sa operacijom $\circ$, tj. akko $\sim$ ispunjava sledeći uslov:

$$(\forall a,b,c,d\in G)(a\sim c\wedge b\sim d\Rightarrow a\circ b\sim c\circ d).$$

Neka su $\underline{G}=(G,\star)$ i $\underline{H}=(H,\circ)$ grupoidi. Preslikavanje $h : G \to H$ je *homomorfizam* grupoida $\underline{G}$ u grupoid $\underline{H}$ ukoliko važi $(\forall a,b\in G)h(a*b)=h(a)\circ h(b)$. U takvom slučaju koristi se i oznaka $h : \underline{G} \to \underline{H}$.

Razlikujemo sledeće vrste homomorfizama. Neka je $h : \underline{G} \to \underline{H}$. Tada:

h je *utapanje* akko h je 1-1,

h je *epimorfizam* akko h je na,

h je *izomorfizam* akko h je 1-1 i na,

h je *automorfizam* grupoida $\underline{G}$ ukoliko je $h : \underline{G} \to \underline{G}$ izomorfizam. Skup svih automorfizama grupoida $\underline{G}$ označava se sa $\mathrm{Aut}\,\underline{G}$.

Ako je $h : \underline{G} \to \underline{H}$ izomorfizam koristi se oznaka $h : \underline{G} \tilde{\to} \underline{H}$. Ako postoji $h : \underline{G} \tilde{\to} \underline{H}$ kažemo da su grupoidi $\underline{G}$ i $\underline{H}$ izomorfni i pišemo $\underline{G} \simeq \underline{H}$.

Osnovnu vezu izmedju homomorfizama i kongruencija iskazuje sledeća

2.1. *Teorema: Neka je* $h : \underline{G} \to \underline{H}$ *homomorfizam i* $\sim$ *relacija skupa G definisana sa* $(\forall x,y\in G)(x\sim y\Leftrightarrow h(x)=h(y))$. *Tada je* $\sim$ *kongruencija grupoida* $\underline{G}$.

Ovako uvedena relacija $\sim$ označava se sa $\ker h$ i naziva se *jezgro* homomorfizma h.

2.2. *Teorema: Neka je* $\sim$ *kongruencija grupoida* $\underline{G}=(G,*)$ *i* $H=G/\sim$ *količnički skup. Tada je operacija* $\circ$ *skupa H uvedena sa* $a/\sim \circ b/\sim = (a*b)/\sim$, $x/\sim$ *je klasa kongruencije elementa* $x\in G$, *dobro definisana i kanonsko preslikavanje* $k : x\mapsto x/\sim$ *je epimorfizam grupoida* $\underline{G}$ *na* $\underline{H}$.

U ovakvom slučaju grupoid $\underline{H}$ označava se sa $\underline{G}/\sim$ i naziva se *količnikom* grupoida $\underline{G}$.

Dokaz ovih teorema dat je u zadacima 2.3. i 2.7.

Primeri i zadaci

2.1. Neka je $(G,\cdot)$ grupoid i ρ relacija ekvivalencije skupa G. Dokazati sledeću ekvivalenciju:

$$(\forall x,y,z\in G)(x\,\rho\,y\Rightarrow(x\cdot z)\,\rho\,(y\cdot z)\wedge(z\cdot x)\,\rho\,(z\cdot y))\iff$$
$$(\forall x,y,u,v\in G)(x\,\rho\,y\wedge u\,\rho\,v\Rightarrow(x\cdot u)\,\rho\,(y\cdot v))$$

Rešenje: ($\Rightarrow$) Neka u $\underline{G}$ važi $x\,\rho\,y\Rightarrow(x\cdot z)\,\rho\,(y\cdot z)\wedge(z\cdot x)\,\rho\,(z\cdot y)$. Dalje, neka su $x,y,u,v\in G$ i pretpostavimo $x\,\rho\,y$, $u\,\rho\,v$. Tada $(x\cdot u)\,\rho\,(y\cdot u)$ i $(y\cdot u)\,\rho\,(y\cdot v)$. Relacija ρ je tranzitivna, stoga $(x\cdot u)\,\rho\,(y\cdot v)$.

($\Leftarrow$) Pretpostavimo da u $\underline{G}$ važi $x\,\rho\,y\wedge u\,\rho\,v\Rightarrow(x\cdot u)\,\rho\,(y\cdot v)$. Neka su $x,y,z\in G$ i $x\,\rho\,y$. Kako je $z\,\rho\,z$ to, prema pretpostavci, $(x\cdot z)\,\rho\,(y\cdot z)$ i $(z\cdot x)\,\rho\,(z\cdot y)$.

2.2. Navesti primer grupoida $(G,\cdot)$ i relacije ekvivalencije ρ skupa G za koju važi $(\forall x,y,z\in G)(x\,\rho\,y\Rightarrow(x\cdot z)\,\rho\,(y\cdot z))$ a ρ ipak nije kongruencija grupoida $\underline{G}$.

Rešenje: Neka je grupoid $\underline{G}$ dat tablicom:

·	a	b	c
a	a	b	c
b	a	b	c
c	a	c	c

i neka je relacija ekvivalencije ρ data particijom $\{\{a,b\},\{c\}\}$. Lako je proveriti da važi $(\forall x,y,z\in G)(x\,\rho\,y\Rightarrow(x\cdot z)\rho(y\cdot z))$. Medjutim, relacija ρ nije kongruencija grupoida $\underline{G}$ budući da jeste $a\,\rho\,b$, $c\,\rho\,c$ ali nije $(c\cdot a)\,\rho\,(c\cdot b)$.

Primer desne kongruencije (koja ne mora biti i leva) grupoida $\underline{G}$ sa jedinicom je relacija $\rho\subseteq G^2$ definisana sa

$$x\,\rho\,y\iff Gx=Gy\,,\qquad Gx=\{g\cdot x\mid g\in G\}.$$

2.3. Neka je $\underline{G}=(G,\cdot)$ grupoid, ρ relacija ekvivalencije skupa G i $\underline{G}/\rho=(G/\rho,\bullet)$ gde je $C_x\bullet C_y=C_{x\cdot y}$. Dokazati: $\underline{G}/\rho$ je grupoid akko je ρ kongruencija grupoida $\underline{G}$.

Rešenje: ($\Rightarrow$) Pretpostavimo da je $\underline{G}/\rho$ grupoid. Budući da je ρ relacija ekvivalencije dokazujemo samo da je ρ saglasna sa operacijom $\cdot$. Pretpostavimo $x\,\rho\,y$, $u\,\rho\,v$; tada $C_x=C_y$, $C_u=C_v$. Stoga $C_x\bullet C_u=C_y\bullet C_v$, pa $C_{x\cdot u}=C_{y\cdot v}$. Prema tome $(x\cdot u)\,\rho\,(y\cdot v)$.

($\Leftarrow$) Pretpostavimo da je ρ kongruencija grupoida $\underline{G}$. Dokazujemo da je operacija $\bullet$ dobro definisana u G/ρ, tj. da za sve $a,b,c,d\in G/\rho$ važi implikacija $a=b\wedge c=d\Rightarrow a\bullet c=b\bullet d$. Neka su $x,y,u,v\in G$ takvi da $C_x=C_y$ i $C_u=C_v$. Tada $x\,\rho\,y$, $u\,\rho\,v$, stoga $(x\cdot u)\,\rho\,(y\cdot v)$, te $C_{x\cdot u}=C_{y\cdot v}$. Otuda $C_x\circ C_u=C_y\circ C_v$

2.4. Neka je $\underline{P}=(P,\cdot)$ grupoid svih kompleksnih polinoma sa jednom promenljivom u odnosu na množenje polinoma. Dokazati da je u sledećim slučajevima preslikavanje $f:\underline{P}\to\underline{C}$ homomorfizam grupoida $\underline{P}$ u multiplikativni grupoid kompleksnih brojeva $(C,\cdot)$. U svakom od tih slučajeva odrediti kongruenciju induciranu homomorfizmom f i odgovarajuće klase ekvivalencije:
a) $f(p)=a_0$ b) $f(p)=a_n$ c) $f(p)=a_0+a_1+\ldots+a_n$, $p(x)=a_0+a_1x+\ldots+a_nx^n$.

Rešenje: Neka su $p(x)=a_0+a_1x+\ldots+a_nx^n$, $q(x)=b_0+b_1x+\ldots+b_mx^m$.

a) $f(p)=a_0=p(0)$, $f(q)=b_0=q(0)$, $(p\cdot q)(x)=a_0b_0+(a_0b_1+a_1b_0)x+\ldots+a_nb_mx^{n+m}$
pa $f(p\cdot q)=a_0b_0$, *tj.* $f(p\cdot q)=f(p)f(q)$. *Kongruencija* ρ *odredjena je sa*
$p\,\rho\,q\Leftrightarrow a_0=b_0\Leftrightarrow p(0)=q(0)$. $C_p=\{r\in P \mid r(0)=p(0)\}$.
c) $f(p)=p(1)$, $f(q)=q(1)$, $f(p\cdot q)=p(1)q(1)$, *pa* $f(p\cdot q)=f(p)f(q)$.
$p\,\rho\,q\Leftrightarrow p(1)=q(1)$, $C_p=\{r\in P \mid r(1)=p(1)\}$.

2.5. Neka u skupu Q racionalnih brojeva relaciji ekvivalencije ρ odgovara particija skupa Q na klase $Q^+=\{x\in Q \mid x>0\}$, $Q^-=\{x\in Q \mid x<0\}$, $\{0\}$. Dokazati da je ρ kongruencija grupoida $\underline{Q}=(Q,\cdot)$ i odrediti tablicu za $\underline{Q}/\rho$.

Rešenje: Tablica za Q/ρ *je*

	Q^+	Q^-	Q_o
Q^+	Q^+	Q^-	Q_o
Q^-	Q^-	Q^+	Q_o
Q_o	Q_o	Q_o	Q_o

$Q_o=\{0\}$

Primetimo da je $x\,\rho\,y$ *akko* $sgn(x)=sgn(y)$, *i da je* $sgn(xy)=sgn(x)sgn(y)$, *tj.* $sgn:(Q,\cdot)\to(\{1,-1,0\},\cdot)$ *je homomorfizam. Otuda* $\underline{Q}/\rho\simeq(\{1,-1,0\},\cdot)$.

2.6. Neka je $f:\underline{G}\to\underline{H}$ homomorfizam grupoida $\underline{G}$ i $\underline{H}$ i neka je $Imf=f(G)$. Dokazati da je Imf podgrupoid grupoida $\underline{H}$.

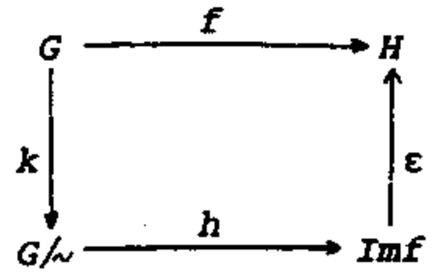
Rešenje: Neka su $\underline{G}=(G,\cdot)$, $\underline{H}=(H,*)$ *i* $x,y\in Imf$. *Tada postoje* $a,b\in G$ *takvi da* $x=f(a)$, $y=f(b)$. *Dalje,* $x*y=f(a)*f(b)=f(a\cdot b)$, *pa je* $x*y\in Imf$. *Prema tome važi* $(\forall x,y\in Imf)x*y\in Imf$, *tj. ispunjen je uslov grupoidnosti u odnosu na operaciju* $*$, *pa je Imf podgrupoid od* $\underline{H}$.

2.7. Neka je $f:\underline{G}\to\underline{H}$ homomorfizam grupoida $\underline{G}$ i $\underline{H}$ i neka je $\sim$ relacija skupa G definisana sa $x\sim y\Leftrightarrow f(x)=f(y)$. Dokazati da je $\sim$ kongruencija grupoida $\underline{G}$. Dokazati $\underline{G}/\sim\simeq Imf$.

Rešenje: Neka je $\underline{G}=(G,\cdot)$, $\underline{H}=(H,*)$. *Lako se proverava da je* $\sim$ *relacija ekvivalencije skupa G; dokazujemo stoga saglasnost* $\sim$ *sa* $\cdot$.
Neka su $x,y,u,v\in G$ *takvi da* $x\sim y$, $u\sim v$. *Otuda* $f(x)=f(y)$ *i* $f(u)=f(v)$, *pa je* $f(x)*f(u)=f(y)*f(v)$. *Kako je f homomorfizam to* $f(xu)=f(yv)$, *tj.* $xu\sim yv$.

Dokazujemo da je $G/\sim \simeq Imf$.

Neka je preslikavanje $h : G/\sim \to Imf$ definisano sa $h(C_x)=f(x)$, gde je C_x klasa ekvivalencije elementa x.



Ako je $C_x=C_y$ tada $x \sim y$, te prema definiciji relacije $\sim$, $f(x)=f(y)$. Stoga važi implikacija $C_x=C_y \Rightarrow h(C_x)=h(C_y)$, $x,y \in G$, što znači da je preslikavanje h dobro definisano. Dalje, neka je $a \in Imf$; tada postoji $b \in G$ takav da $f(b)=a$, tj. $h(C_b)=a$. Prema tome $(\forall y \in Imf)(\exists x \in G/\sim) y=h(x)$, što znači da je h <u>na</u> preslikavanje. Pretpostavimo $h(C_x)=h(C_y)$. Tada $f(x)=f(y)$, pa prema definiciji relacije $\sim$, $x \sim y$, tj. $C_x=C_y$. Prema tome $(\forall u,v \in G/\sim)(h(u)=h(v) \Rightarrow u=v)$, što znači da je h 1-1 preslikavanje. Najzad dokazujemo da je h homomorfizam: $h(C_x * C_y)=h(C_{x \cdot y})=f(x \cdot y)=f(x)*f(y)=h(C_x)*h(C_y)$.

Ako je $k : G \to G/\sim$ kanonsko preslikavanje, tj. $k(x)=C_x$ $(x \in G)$ i $\varepsilon : Imf \to H$ inkluzivno preslikavanje, tj. $\varepsilon(x)=x$ $(x \in Imf)$, primetimo da važi sledeće razlaganje homomorfizma f: $f=\varepsilon h k$.

Takodje primetimo da je k <u>na</u>, h bijekcija a ε 1-1 i da su sva tri preslikavanja homomorfizmi.

2.8.Odrediti sve kongruencije grupoida:

a)

	a	b	c	d
a	b	a	b	b
b	b	b	b	b
c	b	b	b	b
d	b	b	b	b

b)

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	e	f	c	d
c	c	f	d	a	b	e
d	d	e	a	c	f	b
e	e	d	f	b	a	c
f	f	c	b	e	d	a

Rešenje: a) Ima ih ukupno 7. To su sve relacije ekvivalencije σ skupa $\{a,b,c,d\}$ za koje je $a \sigma b$, zatim one za koje je $C_a=\{a\}$, $C_b=\{b\}$. Odgovarajuće particije skupa $\{a,b,c,d\}$ su $\sigma_1=\{\{a,b,c,d\}\}$, $\sigma_2=\{\{a,b,c\},\{d\}\}$, $\sigma_3=\{\{a,b,d\},\{c\}\}$, $\sigma_4=\{\{a,b\},\{c,d\}\}$, $\sigma_5=\{\{a,b\},\{c\},\{d\}\}$, $\sigma_6=\{\{a\},\{b\},\{c\},\{d\}\}$, $\sigma_7=\{\{a\},\{b\},\{c,d\}\}$.

Ove kongruencije moguće je odrediti na više načina.

<u>I način</u>: Odredi se skup svih relacija ekvivalencije skupa $\{a,b,c,d\}$ (ima ih 15), pa se za svaku relaciju ekvivalencije ponaosob utvrdi da li je kongruencija.

<u>II način</u>: Zasniva se na činjenici da se ma koja relacija ρ skupa $\{a,b,c,d\}$ može dopuniti do (neke) kongruencije σ. Prelaz od ρ na σ moguće je ostvariti, recimo, pomoću jednakosne logike. Neka je ρ relacija čiji su parovi, tj. članovi: (x,y), (u,v),... . U vezi sa ρ uoči se skup S_ρ jednakos-

ti $x=y$, $u=v$,... ; ovaj skup ima osnovnu ulogu. Drugim rečima, utvrdi se skup $S=S_\rho$ nekih formula oblika $x=y$, gde $x,y\in\{a,b,c,d\}$ i primenom pravila

$$x=x,\quad \frac{x=y}{y=x},\quad \frac{x=y,\ y=z}{x=z},\quad \frac{x=y}{x\cdot z=y\cdot z},\quad \frac{x=y}{z\cdot x=z\cdot y}$$

traže se sve posledice oblika $u=v$ (gde $u,v\in\{a,b,c,d\}$) skupa S. Ako se sa $S\vdash_J u=v$ označi da je $u=v$ posledica skupa S u jednakosnoj logici, tada je relacija σ skupa $\{a,b,c,d\}$ definisana sa

$$x\,\sigma\,y \Leftrightarrow S\vdash_J x=y$$

najmanja kongruencija grupoida $(\{a,b,c,d\},\cdot)$ takva da $\rho\subseteq\sigma$. Uzimajući različite podskupove S moguće je na opisani način odrediti sve kongruencije grupoida. Na primer, za $S=\{a=c,b=d\}$ imamo:

$a\,\sigma\,a$ *jer* $S\vdash_J a=a$ — $d\,\sigma\,d$ *jer* $S\vdash_J d=d$

$b\,\sigma\,b$ *jer* $S\vdash_J b=b$ — $a\,\sigma\,c$ *jer* $S\vdash_J a=c$

$c\,\sigma\,c$ *jer* $S\vdash_J c=c$ — $b\,\sigma\,d$ *jer* $S\vdash_J b=d$

Iz $a=c$ izvodi se $ab=cb$, odakle $a=b$, pa $a\,\sigma\,b$. Slično, iz $a=b$, $b=d$ izvodi se $a=d$, pa $a\,\sigma\,d$. Nastavljajući ovaj postupak utvrdjuje se da je $\sigma=\{(x,y)\mid x,y\in\{a,b,c,d\}\}$, tj. u ovom slučaju skupu S odgovara kongruencija σ_1. Napomenimo da je $S=S_\rho$ za $\rho=\{(a,c),(b,d)\}$.

Kongruencije σ_i odredjene su sledećim skupovima jednakosti:

σ_1: $\{a=c,a=d\}$, σ_2: $\{a=c\}$, σ_3: $\{a=d\}$, σ_4: $\{a=b,c=d\}$,
σ_5: $\{a=b\}$ σ_6: $\emptyset$ σ_7: $\{c=d\}$

Napomenimo da je moguće da različiti skupovi S, S' odredjuju istu kongruenciju. Tako na primer $S=\{b=c,b=d\}$, $S'=\{a=c,a=d\}$ odredjuju istu kongruenciju σ_1.

b) Ima ih tri i odredjene su particijama $\{\{a\},\{b\},\{c\},\{d\},\{e\},\{f\}\}$, $\{\{a,b,c,d,e,f\}\}$, $\{\{a,c,d\},\{b,e,f\}\}$.

2.9. Neka je S skup, opštije klasa, nekih grupoida koja je zatvorena u odnosu na formiranje proizvoda, tj. važi $A,B\in S\Rightarrow A\times B\in S$. Dokazati da je relacija izomorfizma, $\simeq$, kongruencija za $(S,\times)$.

2.10. Ako je $*$ jedna binarna operacija definisana na skupu S od n elemenata ($n\in\omega$), dokazati da je broj medjusobno različitih grupoida $(S,\cdot)$ izomorfnih sa $\underline{S}=(S,*)$ jednak $n!/|\mathrm{Aut}\,\underline{S}|$, gde je $\mathrm{Aut}\,\underline{S}$ skup automorfizama grupoida $\underline{S}$.

Rešenje: U rešenju koje navodimo koriste se sledeće činjenice iz teorije grupa: (1) $\mathrm{Aut}\,\underline{S}$ je podgrupa grupe $\underline{S}_n$, (2) $|S_n|=n!$, (3) $|\underline{S}_n/\mathrm{Aut}\,\underline{S}|=n!/|\mathrm{Aut}\,\underline{S}|$.

Neka je p jedna permutacija skupa S. Tada p definiše operaciju $*_p$ na S sa $x*_p y = p^{-1}(p(x)*p(y))$. Jasno je da za svaki grupoid $(S,\cdot) \simeq \underline{S}$ postoji permutacija p tako da $(S,\cdot)=(S,*_p)$. Grupoidi $(S,*_p)$ i $(S,*_q)$ biće jednaki akko $p^{-1}(p(x)*p(y))=q^{-1}(q(x)*q(y))$, tj.

$$pq^{-1}(q(x)*q(y))=p(x)*q(y) \qquad (4)$$

Za $q(x)=u$, $q(y)=v$ imamo $pq^{-1}(u*v)=pq^{-1}(u)*pq^{-1}(v)$. Prema tome

$$(S,*_p)=(S,*_q) \quad \text{akko} \quad pq^{-1} \in \mathrm{Aut}\,\underline{S} \qquad (5)$$

Relacija $\sim$ u skupu permutacija skupa S odredjena sa $pq^{-1} \in \mathrm{Aut}\,\underline{S}$ je jedna relacija ekvivalencije skupa S_n (v. zad. 2.3.6.) i C_p je jedan razred grupe $\mathrm{Aut}\,\underline{S}$ u $\underline{S}_n$, pa $|C_p|=|\mathrm{Aut}\,\underline{S}|$. Na osnovu (5) je

$$(S,*_p) \neq (S,*_q) \quad \text{akko nije } p \sim q$$

tj. različitih grupoida $(S,*_p)$ izomorfnih $(S,*)$ ima koliko i razreda grupe $\mathrm{Aut}\,\underline{S}$ u $\underline{S}_n$, pa je prema (3) ovaj broj jednak $n!/|\mathrm{Aut}\,\underline{S}|$.

2.11. Dokazati da grupoid $\underline{G}$ ima idempotentni element akko za svaki grupoid H postoji homomorfizam $f : \underline{H} \to \underline{G}$.

Rešenje: ($\Rightarrow$) Neka je $a \in G$ idempotentni element grupoida $\underline{G}$. Tada je $h : \underline{H} \to \underline{G}$ homomorfizam, gde $(\forall x \in H)h(x)=a$.
($\Leftarrow$) Ako za svaki grupoid $\underline{H}$ postoji homomorfizam $h : \underline{H} \to \underline{G}$, tada i za trivijalni grupoid $(\{e\},\cdot)$ postoji homomorfizam $h : (\{e\},\cdot) \to \underline{G}$. Tada je $a=h(e)$ idempotentni element grupoida $\underline{G}$.

2.12. Neka je $\underline{G}=(G,\bullet)$ grupoid i $f : X \xrightarrow[1-1]{\text{na}} G$. Operacija $*$ na X definisana je sa $a*b=f^{-1}(f(a)\bullet f(b))$. Dokazati da je $(X,*) \simeq \underline{G}$. Ukoliko je $\underline{G}=(R,+)$, $X=R$ (R je skup realnih brojeva) i f jedno od preslikavanja
a) $f(x)=1+x$, b) $f(x)=a+x$, c) $f(x)=a-x$, d) $f(x)=x^3$, e) $f(x)=x^{1/3}$,
odrediti odgovarajuće grupoide $(X,*)$.

Rešenje: a) $x*y=1+x+y$, b) $x*y=a+x+y$, c) $x*y=x+y-a$
d) $x*y=(x^3+y^3)^{1/3}$, e) $x*y=(x^{1/3}+y^{1/3})^3$

2.13. Neka su skupovi R_n ($n \in \omega$) i R_ω definisani kao u zadatku 1.2.
a) Odrediti $|R_n|$, b) Dokazati da je R_ω prebrojiv skup,
c) Dokazati da grupoidi odredjeni u zadatku 1.2.a)b) nisu medjusobno izomorfni, niti je bilo koji od njih konačno generisan.

Rešenje: a) Kako je $R_o=\emptyset$ i $R_{n+1}=P(R_n)$, to $|R_{n+1}|=2^{|R_n|}$. Otuda $|R_o|=0$

$$|R_1|=1, \quad |R_n|=2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}\Big\}n-1, \quad n>2.$$

b) Skupovi R_n su konačni, pa je R_ω prebrojiva unija konačnih skupova. Otuda je R_ω prebrojiv skup.
c) Neka je $x\cdot y \overset{def}{=} \{x,y\}$, $x*y \overset{def}{=} (x,y)$. Grupoid $(R_\omega,\cdot)$ je komutativan, dok $(R_\omega,*)$ to nije. Prema tome, $(R_\omega,\cdot) \neq (R_\omega,*)$.

Dokazujemo da $(R_\omega,\cdot)$ *nije konačno generisan. Pretpostavimo suprotno, tj. da za neki* $n\in\omega$ *izvesni elementi* $a_1,\dots,a_n\in R_\omega$ *generišu* $(R_\omega,\cdot)$. *Tada svaki* a_i *pripada nekom* R_n *pa je* $a_i\in R_n$ *(v.zad. 1.2.); stoga su* a_i *konačni skupovi. Neka je* $k=\max(|a_1|,\dots,|a_n|)$, *tj. neka svaki skup* a_i *ima najviše k elemenata. Sa druge strane, skup* $x\cdot y=\{x,y\}$ *je najviše dvočlan, pa ako bi* $(R_\omega,\cdot)$ *bio generisan elementima* $a_1,\dots,a_n$, *onda bi svaki* $x\in R_\omega$ *imao najviše* $m=\max(2,k)$ *elemenata. Medjutim, za svaki* $n\in\omega$ $R_n\in R_\omega$ *(jer* $R_n\in R_{n+1}\subseteq R_\omega$*), pa je prema a) za neki* $n\in\omega$ $|R_n|>m$; *kontradikcija.*

1.3. S E M I G R U P E

Grupoid $\underline{G}=(G,\cdot)$ zadovoljava *asocijativni zakon* ukoliko važi:

$$(\forall x,y,z\in G)\ (x\cdot y)\cdot z = x\cdot(y\cdot z)\ .$$

3.1. *Definicija: Grupoid* $\underline{G}$ *koji zadovoljava asocijativni zakon naziva se semigrupom ili polugrupom.*

Algebarska struktura $\underline{G}=(G,\cdot,1)$ je *monoid* akko je $(G,\cdot)$ semigrupa i 1 je jedinica algebre $\underline{G}$.

Grupoid (semigrupa) $\underline{G}$ je komutativan ukoliko u $\underline{G}$ važi *komutativni zakon*: $(\forall x,y\in G)\ x\cdot y=y\cdot x$.

Od važnijih teorema za semigrupe izdvajamo uopšteni asocijativni zakon (v.zad. 3.10.-12.) kao i teoremu o funkcijskoj reprezentaciji semigrupa:

3.2. *Teorema: Svaka semigrupa izomorfna je nekoj semigrupi funkcija* $(F,\bullet)$.

Dakle, F je neki skup funkcija $f:A\to A$ skupa A i $\bullet$ je slaganje funkcija. Dokaz ove teoreme dat je u zad. 3.7.

Element a semigrupe $\underline{S}$ je *idempotentan* ukoliko važi: $a^2=a$.

Primeri i zadaci

3.1. Ispitati da li su semigrupe sledeći parovi:

a) $(R,*)$, gde je $x*y=f^{-1}(f(x)+f(y))$, f je jedna utvrdjena permutacija skupa realnih brojeva,

b) $(S,*)$, gde je $S=\{0,1,\dots,n-1\}$, $i*j=i+_n j+_n i\cdot_n j$,

c) $(P(S),*)$, gde je $*$ jedna od skupovnih operacija $\cup$, $\cap$, Δ ,

d) $(M,\cdot)$, M je skup svih kvadratnih matrica reda n nad kompleksnim brojevima za koje je $\sum_{j=1}^{n} a_{ij}=1$, $i=1,2,\dots,n$, a $\cdot$ množenje matrica,

e)

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

G=({a,b,c},*)

f) Svi primeri iz zadataka 1.1. i 1.2.

Rešenje: a) (R,) je semigrupa budući da je f : (R,*) → (R,+) izomorfizam i + je asocijativna operacija.*

b) $(\{0,1,\ldots,n-1\},+_n,\cdot_n)$ *je prsten, pa je*

$$(i*j)*k = i+_n j +_n k +_n i \cdot_n j +_n i \cdot_n k +_n j \cdot_n k +_n i \cdot_n j \cdot_n k = i*(j*k).$$

c) Sve tri skupovne operacije su asocijativne; na primer, asocijativnost simetrične razlike moguće je dokazati na osnovu tautologije $(p \veebar q) \veebar r \Leftrightarrow p \veebar (q \veebar r)$, *gde je* $\veebar$ *ekskluzivna disjunkcija, budući da važi* $x \in A \Delta B \Leftrightarrow x \in A \veebar x \in B$.

d) Množenje matrica je asocijativna operacija, stoga jedino dokazujemo da je (M,·) grupoid. Neka je c=ab gde a,b ∈ M. Tada

$c_{ij} = \sum_k a_{ik} b_{kj}$, , *pa je* $\sum_j c_{ij} = \sum_j \sum_k a_{ik} b_{kj} = \sum_k \sum_j a_{ik} b_{kj} = \sum_k (a_{ik} \sum_j b_{kj})$

$\sum_k a_{ik} = 1$, *tj.* $c \in M$.

e) G je semigrupa (štaviše, grupa).

3.2. Neka je A skup i ∘ slaganje funkcija. Dokazati:

a) $\underline{N}_A = (\{f \mid f : A \xrightarrow{na} A\}, \circ)$ je monoid,

b) $\underline{J}_A = (\{f \mid f : A \xrightarrow[1-1]{} A\}, \circ)$ je monoid,

c) A je konačan skup akko $N_A = J_A$,

d) Dokazati da u $\underline{N}_A$ važi $g \circ f = h \circ f \Rightarrow g = h$, dok u $\underline{J}_A$ važi $f \circ g = f \circ h \Rightarrow g = h$.

Uputstvo: c) Dokazati: (1) Ako je A konačan skup tada

$$(\forall f)(f : A \xrightarrow{na} A \Leftrightarrow f : A \xrightarrow[1-1]{} A)$$

(2) Ako je A beskonačan skup tada postoji $B \subseteq A$, $B \neq A$ *i postoji preslikavanje f,* $f : A \xrightarrow[1-1]{} B$.

3.3. Neka je A skup i ∘ slaganje binarnih relacija. Dokazati:

a) Skup svih binarnih relacija R_A skupa A je monoid u odnosu na ∘

b) Monoidi $\underline{N}_A$, $\underline{J}_A$ iz prethodnog zadatka su podmonoidi monoida $\underline{R}_A$.
Da li su skupovi refleksivnih, tranzitivnih relacija i relacija ekvivalencije skupa A podgrupoidi grupoida $\underline{R}_A$?

Rešenje: Skup refleksivnih relacija skupa A je grupoid, dok skupovi tranzitivnih i relacija ekvivalencije to nisu.

3.4. Dokazati: Grupoid G je **asocijativan akko u G važi**

$$x_1 = y_1 \wedge y_3 = x_1 y_2 \wedge x_3 = x_2 y_1 \Rightarrow x_2 y_3 = x_3 y_2 .$$

Rešenje: ($\Rightarrow$) Pretpostavimo da je G semigrupa. Neka su $x_i, y_i \in G$ i $x_1=y_1$, $y_3=x_1y_2$, $x_3=x_2y_1$. Tada $x_2y_3=x_2(x_1y_2)=(x_2x_1)y_2=(x_2y_1)y_2=x_3y_2$.

($\Leftarrow$) Pretpostavimo da je u G tačna navedena formula. Neka su $x_2, x_1, y_2 \in G$ proizvoljni elementi i neka je $y_3=x_1y_2$, $x_3=x_2y_1$, $y_1=x_1$; prema pretpostavci važi $x_2y_3=x_3y_2$. Otuda, $x_2(x_1y_2)=x_2y_3=x_3y_2=(x_2y_1)y_2=(x_2x_1)y_2$.

3.5. Neka je (S,$*$) semigrupa sa jediničnim elementom e. Odrediti sve operacije $\circ$ skupa S takve da je $a\circ(b*c)=(a\circ b)*c$.

Rešenje: Dokazujemo sledeću ekvivalenciju

$$(\forall a,b,c\in S)\,a\circ(b*c)=(a\circ b)*c \iff (\exists f)(f:S\to S \wedge (\forall a,b\in S)\,a\circ b=f(a)*b)\ .$$

Drugim rečima $x\circ y$ je vida $f(x)*y$ za neku funkciju $f:S\to S$.

($\Rightarrow$) Pretpostavimo da je za sve $a,b,c\in S$ $a\circ(b*c)=(a\circ b)*c$ i neka je $f:S\to S$ definisana sa $f(a)=a\circ e$, $a\in S$. Tada $a\circ(e*b)=(a\circ e)*b$, tj. $a\circ b=f(a)*b$.

($\Leftarrow$) Pretpostavimo da za neko preslikavanje $f:S\to S$ važi $(\forall a,b\in S)\,a\circ b=f(a)*b$. Tada $a\circ(b*c)=f(a)*(b*c)$, $(a\circ b)*c=(f(a)*b)*c$, pa prema asocijativnosti operacije $*$ važi $a\circ(b*c)=(a\circ b)*c$.

3.6. Komutativni grupoid (S,$*$) u kome važi zakon $(x*y)*z=(z*x)*y$ je semigrupa. Dokazati.

Rešenje: Prema navedenom zakonu i komutativnosti operacije $*$, važi $(x*y)*z=(z*x)*y=(y*z)*x=x*(y*z)$.

3.7. Dokazati da je svaka semigrupa izomorfna nekoj semigrupi funkcija.

Rešenje: Neka je $\underline{S}=(S,\cdot)$ semigrupa. Pretpostavimo prvi slučaj, kada $\underline{S}$ ima jedinični element, označen sa e. Dalje, neka je P skup svih preslikavanja iz S u S i $F:S\to P$ definisano sa $F(a)(x)=ax$, $a,x\in S$. Tada $F(ab)(x)=(ab)x=a(bx)=F(a)(F(b)(x))=(F(a)\circ F(b))(x)$; stoga $F(ab)=F(a)\circ F(b)$, tj. $F:(S,\cdot)\to(P,\ )$ je homomorfizam. Dokazujemo da je f 1-1 preslikavanje. Neka je $F(a)=F(b)$. Tada, za svaki x iz S, $F(a)(x)=F(b)(x)$, pa $F(a)(e)=F(b)(e)$, tj. $ae=be$ odakle $a=b$. Prema prethodnom $(S,\cdot)\cong(F(S),\circ)$.

Razmotrimo drugi slučaj, kada $\underline{S}$ nema jedinični element. Neka je e novi element tj. $e\notin S$ i $\underline{H}=(S\cup\{e\},*)$, gde je operacija $*$ definisana sa $x*y=x\cdot y$ ako $x,y\in S$, a $e*x=x$, $x*e=x$ inače. Neposredno se proverava da je $\underline{H}$ semigrupa sa neutralnim elementom e i da je $\underline{S}$ podgrupoid od $\underline{H}$. Prema prvom slučaju postoji semigrupa funkcija $\underline{R}=(R,\circ)$ i izomorfizam $F:\underline{H}\xrightarrow{\sim}\underline{R}$. tada je restrikcija $G=F\restriction S$ izomorfizam, $G:\underline{S}\xrightarrow{\sim}(F(S),*)$.

Napomenimo da ukoliko u S važi $x\neq y\Rightarrow(\exists z)(xz\neq yz)$, onda u prethodnoj konstrukciji nije nužno da se $\underline{S}$ proširuje jediničnim elementom.

3.8.U sledećim slučajevima odrediti semigrupe funkcija izomorfne navedenim semigrupama:

a)
·	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

,

b)
·	a	b	c	d
a	b	c	d	b
b	c	d	b	c
c	d	b	c	d
d	b	c	d	b

,

c)
·	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

,

d) $\underline{G}=(G,\cdot)$, $xy=x$, e) $\underline{G}=(G,\cdot)$, $xy=y$.

Rešenje: a) Grupoid $\underline{G}$ ima jedinicu a. Prema prethodnom zadatku odredjujemo utapanje $F:G \to (P,\circ)$, $P=\{f \mid f:G \to G\}$;

$F(a)=\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$, $F(b)=\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$, $F(c)=\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$.

Tada $\underline{G} \simeq (\{F(a),F(b),F(c)\},\circ)$.

Primetimo da je za $F(u)=\begin{pmatrix} a & b & c \\ x & y & z \end{pmatrix}$ niz x,y,z upravo vrsta koja odgovara elementu u.

	a	b	c
⋮	⋮	⋮	⋮
u	x	y	z
⋮	⋮	⋮	⋮

1

b) Ovaj grupoid nema jedinični element, ali s obzirom da u $\underline{G}$ važi $x \neq y \Rightarrow (\exists z)(xz \neq yz)$ (to upravo znači da se x-vrsta i y-vrsta medjusobno razlikuju) to nije nužno da se ovaj grupoid proširuje jediničnim elementom. Otuda

$$G \simeq (\{\begin{pmatrix} a & b & c & d \\ b & c & d & b \end{pmatrix},\begin{pmatrix} a & b & c & d \\ c & d & b & c \end{pmatrix},\begin{pmatrix} a & b & c & d \\ d & b & c & d \end{pmatrix},\begin{pmatrix} a & b & c & d \\ b & c & d & b \end{pmatrix}\},\circ).$$

c) Ukoliko se $\underline{G}$ proširi jedinicom 1, dobija se grupoid G'

	1	a	b	c
1	1	a	b	c
a	a	a	a	a
b	b	a	a	a
c	c	a	a	a

Tada

$$\underline{G'} \simeq (\{\begin{pmatrix} 1 & a & b & c \\ 1 & a & b & c \end{pmatrix},\begin{pmatrix} 1 & a & b & c \\ a & a & a & a \end{pmatrix},\begin{pmatrix} 1 & a & b & c \\ b & a & a & a \end{pmatrix},\begin{pmatrix} 1 & a & b & c \\ c & a & a & a \end{pmatrix}\},\circ),$$

dok

$$\underline{G} \simeq (\{\begin{pmatrix} 1 & a & b & c \\ a & a & a & a \end{pmatrix},\begin{pmatrix} 1 & a & b & c \\ b & a & a & a \end{pmatrix},\begin{pmatrix} 1 & a & b & c \\ c & a & a & a \end{pmatrix}\},\circ) .$$

d) Ako je $G=\{a_i \mid i \in I\}$ tada $F:\underline{G} \to (\{f_i \mid i \in I\},\circ)$ gde $f_i(a_j)=a_i$, $F(a_i)=f_i$.

3.9.Ispitati da li su sledeći grupoidi semigrupe

a)
	a	b	c	d
a	b	c	d	b
b	c	d	b	c
c	d	b	c	d
d	b	c	d	b

b)
	a	b	c	d
a	a	d	b	c
b	c	b	d	a
c	d	a	c	b
d	b	c	a	d

c)
	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

Rešenje. Jedan od načina da se utvrdi zakon asocijativnosti, ukoliko je grupoid konačan, je da se za sve trojke (x,y,z) elemenata grupoida ispita da li važi (xy)z=x(yz). Medjutim, već u slučaju grupoida od 4 elemenata ovakvih provera ima $4^3=64$. Ovaj broj inače vrlo brzo raste; ako je

$|G|=n$, jednak je n^3. S druge strane, prema zad.3.7. ako je $\underline{G}$ semigrupa, tada je $\underline{G}$ izomorfna nekoj semigrupi funkcija, pa motivisani ovom činjenicom, odredjujemo semigrupu funkcija koja je izomorfna grupoidu $\underline{G}$.

a) Proširenje grupoida $\underline{G}$ jedinicom 'daje

	1	a	b	c	d
1	1	a	b	c	d
a	a	b	c	d	b
b	b	c	d	b	c
c	c	d	b	c	d
d	d	b	c	d	b

Ako je preslikavanje F odredjeno kao u zad.3.7. i $f_x=F(x)$, onda

$f_a=\begin{pmatrix}1&a&b&c&d\\a&b&c&d&b\end{pmatrix}$, $f_b=\begin{pmatrix}1&a&b&c&d\\b&c&d&b&c\end{pmatrix}$, $f_c=\begin{pmatrix}1&a&b&c&d\\c&d&b&c&d\end{pmatrix}$, $f_d=\begin{pmatrix}1&a&b&c&d\\d&b&c&d&b\end{pmatrix}$.

Odredjujemo $f_x\circ f_y$ za $x,y\in\{a,b,c,d\}$;

napr. $f_a\circ f_b=\begin{pmatrix}1&a&b&c&d\\c&d&b&c&d\end{pmatrix}=f_c$.

Prema navedenim tablicama lako se proverava da je preslikavanje $F: x\to f_x$ izomorfizam izmedju grupoida $\underline{G}$ i $\underline{P}$, što znači da je $\underline{G}$ semigrupa.

$\underline{P}$:

	f_a	f_b	f_c	f_d
f_a	f_b	f_c	f_d	f_b
f_b	f_c	f_d	f_b	f_c
f_c	f_d	f_b	f_c	f_d
f_d	f_b	f_c	f_d	f_b

b) $\underline{G}$ nije semigrupa.

c) $\underline{G}$ jeste semigrupa.

Napomena: Osim navedenog postupka za proveru asocijativnosti, moguća su i sledeća dva:

(1) Za zadatu operaciju $\cdot$ na konačnom skupu S formiraju se sledeće operacije: $T(x,y,z)=x\cdot yz$ i $T'(x,y,z)=xy\cdot z$,

a od ovih operacije: $T_a(x,y)=T(x,a,y)$, $T'_a(x,y)=T'(x,a,y)$ (za sve $a\in S$).

Potreban i dovoljan uslov asocijativnosti operacije $\cdot$ je da za sve $a\in S$ bude $T_a=T'_a$, tj. sve tablice operacija T_a i T'_a moraju biti jednake. Postupak se može skratiti, jer je dovoljno ispitati samo operacije T_a, T'_a kad a pripada nekom skupu generatora grupoida $(S,\cdot)$.

Ovaj test asocijativnosti naziva se **Light-ov test.**

(2) (A.Krapež) Neka je $\cdot$ binarna operacija na konačnom skupu S. Neka je $T(x,y,z)=x\cdot yz$, $\lambda_{xy}z=T(x,y,z)$ i $T_1=\{\lambda_{xy}\mid x,y\in S\}$.

Operacija $\cdot$ je asocijativna akko:

(i) $g=\{(xy,\lambda_{xy})\mid x,y\in S\}$ je funkcija iz $S\cdot S$ u T_1,

(ii) $(gx)(y)=xy$ za sve $x\in S\cdot S$ i sve $y\in S$.

3.10. Neka je $\underline{G}=(G,\cdot)$ asocijativni grupoid i $(z_1,z_2,\ldots,z_{n+m})=(x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_m)$. Dokazati da u $\underline{G}$ važi $\prod_{i=1}^{n}x_i\cdot\prod_{i=1}^{m}y_i=\prod_{i=1}^{n+m}z_i$.

Rešenje: Dokaz izvodimo indukcijom po m, broju promenljivih y_i.

Slučaj m=1 : $\prod_{i=1}^{n} x_i \cdot \prod_{i=1}^{m} y_i = (\prod_{i=1}^{n} x_i)\cdot y_1 = (\prod_{i=1}^{n} z_i)\cdot z_{n+1} = \prod_{i=1}^{n+1} z_i$.

Pretpostavimo da tvrdjenje važi za m. Tada:

$\prod_{i=1}^{n} x_i \cdot \prod_{i=1}^{m+1} y_i =$	*prema definiciji proizvoda*
$\prod_{i=1}^{n} x_i \cdot ((\prod_{i=1}^{m} y_i)\cdot y_{m+1}) =$	*prema asocijativnom zakonu*
$(\prod_{i=1}^{n} x_i \cdot \prod_{i=1}^{m} y_i)\cdot y_{m+1} =$	*prema induktivnoj hipotezi*
$(\prod_{i=1}^{n+m} z_i)\cdot z_{m+1} =$	*prema definiciji proizvoda*
$\prod_{i=1}^{n+m+1} z_i$	

3.11. Neka je $\underline{G}=(G,\cdot)$ grupoid i $t(x_1,\ldots,x_n)$ term jezika $\{\cdot\}$. Preslikavanje $t^{\underline{G}}$ inducirano termom t je preslikavanje definisano sa

$$t^{\underline{G}}(a_1,\ldots,a_n)=t(a_1,\ldots,a_n),\quad a_1,\ldots,a_n\in G\ .$$

Glavni deo terma t, u oznaci t*, je izraz dobijen brisanjem svih zagrada u t. Ako je $\underline{G}$ asocijativni grupoid, dokazati:

a) $u^* = v^* \Rightarrow u^{\underline{G}} = v^{\underline{G}}$

b) Ukoliko je $u^* = v^*$, tada je u=v posledica asocijativnog zakona.

Rešenje: a) Neka je u term jezika $\{\cdot\}$. Tada je za neke promenljive $x_1,x_2,\ldots,x_n$ $u^* = x_1\cdot x_2\cdot\ldots\cdot x_n$. Indukcijom po složenosti terma, recimo po broju promenljivih x_i, dokazujemo da ako je $u^* = x_1x_2\ldots x_n$, tada $u = \prod_{i=1}^{n} x_i$ važi u grupoidu $\underline{G}$.

To je očigledno ako je $u^* = x_1$.

Neka je u složen term; tada za neke terme u_1,u_2 $u=(u_1\cdot u_2)$ i za neki k, $1\le k<n$, $u_1^*=x_1x_2\ldots x_k$, $u_2^*=x_{k+1}\ldots x_n$. Prema induktivnoj hipotezi, $u_1=\prod_{i=1}^{k} x_i$, $u_2=\prod_{i=k+1}^{n} x_i$ važe u $\underline{G}$, pa $u=\prod_{i=1}^{k} x_i \cdot \prod_{i=k+1}^{n} x_i$ važi u $\underline{G}$. Prema zad. 3.10. $u=\prod_{i=1}^{n} x_i$ važi u $\underline{G}$. Prema prethodnom, ukoliko je $u^*=v^*=x_1\cdots x_n$ onda $u=v=\prod_{i=1}^{n} x_i$ važi u $\underline{G}$, tj. $u^{\underline{G}} = v^{\underline{G}}$.

b) Ako $u^* = v^*$, tada u svim asocijativnim grupoidima važi u=v, stoga je u=v posledica asocijativnog zakona.

3.12. Neka je $\cdot$ asocijativna i komutativna operacija i p permutacija skupa $\{1,2,\ldots,n\}$. Dokazati jednakost $\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} a_{p(i)}$.

Rešenje: Dokaz izvodimo indukcijom po n. U slučaju n=2 tvrdjenje se lako proverava. Pretpostavimo da tvrdjenje važi za n (n > 2) i neka je $p = \prod_{i=1}^{n} a_{p(i)}$, gde je p neka permutacija skupa $\{1,2,\ldots,n+1\}$.

<u>Slučaj p(n+1)=n+1</u>: Restrikcija preslikavanja p na $\{1,2,\ldots,n\}$ je permutacija skupa $\{1,2,\ldots,n\}$, pa je

$P = (\prod_{i=1}^{n} a_{p(i)}) \cdot a_{n+1} =$ *prema induktivnoj hipotezi*

$(\prod_{i=1}^{n} a_i) \cdot a_{n+1} = \prod_{i=1}^{n+1} a_i$

Slučaj $p(n+1)=k_o$ *za neki* $k_o \leq n$: *Neka je niz* $b_1,\ldots,b_n$ *definisan sa* $b_i=a_i$ *ako je* $i<k_o-1$, $b_i=a_{i+1}$ *inače. Dalje, neka je preslikavanje q odredjeno sa* $q(i)=p(i)$ *ako je* $p(i)<k_o$, $q(i)=p(i)-1$ *ukoliko je* $p(i)>k_o$ $(i<n)$. *Lako se proverava da je q permutacija skupa* $\{1,2,\ldots,n\}$ *i da pri tome važi* $P = (\prod_{i=1}^{n} b_{q(i)}) \cdot a_{k_o}$. *Prema induktivnoj hipotezi,* $\prod_{i=1}^{n} b_{q(i)} = \prod_{i=1}^{n} b_i$, *stoga*

$P=((\prod_{i=1}^{n-1} b_i)b_n)\cdot a_{k_o} =$ *prema komutativnom i asocijativnom zakonu i zbog* $b_n=a_{n+1}$

$((\prod_{i=1}^{n-1} b_i)a_{k_o})a_{n+1} =$ *r je permutacija*

$(\prod_{i=1}^{n} a_{r(i)})a_{n+1} =$ $r = \begin{pmatrix} 1 & 2 & \ldots & k_o-1 & k_o & k_o+1 & \ldots & n-1 & n \\ 1 & 2 & \ldots & k_o-1 & k_o+1 & k_o+2 & \ldots & n & k_o \end{pmatrix}$

$(\prod_{i=1}^{n} a_i)a_{n+1} = \prod_{i=1}^{n+1} a_i$ *prema induktivnoj hipotezi .*

3.13. Dokaza i da u svakoj konačnoj semigrupi postoji idempotentan element, tj. ta av a da je $a^2=a$. Navesti primer beskonačne semigrupe u kojoj ne postoji idempotentan element.

Rešenje: *I način:* *Neka je* $a \in S$. *Budući da je* $a^{2^n} \in S$, *u nizu* $a,a^2,\ldots,a^{2^n},\ldots$ *postoji samo konačno mnogo različitih članova, pa za neke prirodne brojeve* n,m, *gde je* $n<m$, *važi* $a^{2^n}=a^{2^m}$. *Odredimo x iz uslova* $2^m+x=2(2^n+x)$. *Tada* $x=2^m-2^{n+1}$, *pa* $b^2=b$, *gde je* $b=a^{2^m-2^{n+1}+2^n}$.

II način: *Dokaz se izvodi indukcijom po broju elemenata u semigrupi. Neka je* $(S,\cdot)$ *konačna semigrupa i pretpostavimo da svaka semigrupa koja ima ma je od* $|S|$ *elemenata ima idempotentan element. Dalje, neka je* $a \in S$ *i neka je H podgrupoid semigrupe* $(S,\cdot)$ *generisan elementom a. Tada za neko* $n \in$, $H=\{a,a^2,\ldots,a^n\}$ *i za* $i,j<n$, $i \neq j$, $a^i \neq a^j$. *Za neki* $k \in \{1,\ldots,n\}$ *je* $a\cdot a^n=a^k$. *Otuda* $a^k \cdot a^{n-k+1}=a^k$, *pa za* $m=n-k+1$ *važi*

$$a^k a^m = a^k, \quad k+m=n+1 \qquad (1)$$

Slučaj $k<m$: *Množeći jednakost (1) sa* a^{m-k} *dobija se* $a^{m-k}a^k a^m = a^{m-k}a^k$, *odakle* $a^m a^m = a^m$, *pa je* a^m *idempotentan element.*

Slučaj $k=m$: *Tada je* a^k *idempotentan element.*

Slučaj $k>m$: *U takvom slučaju* $\{a^k,a^{k+1},\ldots,a^n\}$ *je podgrupoid semigrupe H. Zaista, neka je* $k<p$, $q<n$. *Tada za neki s,* $q=k+s$ *pa* $a^p a^q = a^{p+q} = a^{p+s+k} = a^{p+s}a^k$. *Za neki i,* $0<i<m$, $p+s=i+jm$, *odakle* $a^p a^q = a^{i+jm}a^k = a^i(a^{jm}a^k) = a^i a^k$ *budući da je* $a^k = a^m a^k = a^{2m}a^k = \ldots$.

Otuda, $\{a^k,a^{k+1},\ldots,a^n\}$ *je semigrupa koja ima manje od* $|S|$ *elemenata bu-*

dući da $a^m \in \{a^k, a^{k+1}, \ldots, a^n\}$, *pa po induktivnoj hipotezi postoji idempotentan element* $c \in \{a^k, a^{k+1}, \ldots, a^n\}$.

Jedan primer beskonačne semigrupe bež idempotentnog elementa: neka je $f=\begin{pmatrix}1&2&3&4&\ldots\\2&3&4&5&\ldots\end{pmatrix}$; *tada* $f^{n-1}=\begin{pmatrix}1&2&3&\ldots\\n&n+1&n+2&\ldots\end{pmatrix}$, $n>2$, *pa za* $n \neq m$, $f^n \neq f^m$ *i* $(\{f^n \mid n \in N\}, \cdot)$ *je beskonačna semigrupa bez idempotentnog elementa.*

Drugi primer je multiplikativni grupoid pozitivnih prirodnih brojeva bez jedinice.

3.14. Neka je $(S,\cdot)$ semigrupa generisana elementom a i neka postoje prirodni brojevi p,q $(p \neq q)$ takvi da $a^p=a^q$. Dokazati:
a) Za neke prirodne brojeve m i n je $a^{m+n}=a^m$ i $S=\{a,a^2,\ldots,a^{m+n-1}\}$,
b) $(\{a^m,a^{m+1},\ldots,a^{m+n-1}\},\cdot)$ je ciklična grupa reda n.

Rešenje: a) Pretpostavimo da postoje različiti prirodni brojevi p,q takvi da $a^p=a^q$. *Tada postoji najmanji prirodan broj q takav da za neki* $p<q$ *važi* $a^p=a^q$. *Neka je k najmanji prirodni broj takav da je za neki* $p \in N$, $p<k$ *i* $a^p=a^k$. *Dalje, neka je* $m \in N$ *najmanji broj za koji je* $a^m=a^k$ *i neka je* $m+n=k$.

Dokazujemo da je za $1<i<j<m+n-1$, $a^i \neq a^j$.
Ako je $a^i=a^j$, *tada je* $j<k$, *što je u kontradikciji sa izborom broja k. Otuda, domen grupoida* $\underline{S}$ *je* $S=\{a,a^2,\ldots,a^{m+n-1}\}$ *i S ima m+n elemenata. Prema definiciji brojeva m,n važi* $a^m a^n=a^m$, *tj.* $a^{m+n}=a^m$.

b) Dokazujemo da je $\underline{H}=(H,\cdot)$ *grupa, gde je* $H=\{a^m,a^{m+1},\ldots,a^{m+n-1}\}$.

1° U $\underline{H}$ *važi zakon asocijativnosti budući da je* $\underline{S}$ *semigrupa.*

2° Dokazujemo da je $\underline{H}$ *grupoid. Prethodno primetimo da na osnovu* $a^m a^n=a^m$ *sledi* $(\forall i \in N) a^m a^{in}=a^m$. *Otuda za* $a^{m+i}, a^j \in H$ *i* $i+j=sn+t$, *gde je* $0<t<n-1$, $s,t \in N$, *važi*

$$a^{m+i}a^j=a^m a^{i+j}=a^m a^{sn+t}=a^m a^{sn}a^t=a^m a^t=a^{m+t},$$

i $a^{m+t} \in H$.

3° Dokazujemo da $\underline{H}$ *ima jedinicu. Prema 2°* $a^{mn} \in H$ *i*

$$a^m a^{mn}=a^m a^n a^{(m-1)n}=a^m a^{(m-1)n}=\ldots=a^m,$$

pa za $a^{m+i} \in H$, $a^{m+i}a^{mn}=a^i a^m a^{mn}=a^i a^m=a^{m+i}$.
Dakle, a^{mn} *je jedinica grupoida* $\underline{H}$.

4° Dokazujemo da svaki element $a^i \in H$ *ima inverzni element u* $\underline{H}$ *u odnosu na jedinicu* a^{mn}. *Zaista, lako je videti da je* $a^{i(n-1)} \in H$ *i* $a^i a^{i(n-1)}=a^{mn}$.

Prema prethodnom, $\underline{H}$ *je grupa. Dokazujemo da je* $\underline{H}$ *ciklična grupa.*

Ako je n=1, tvrdjenje je trivijalno; pretpostavimo zato $n>2$. *Neka je* $a^{mn}=a^r$, *gde* $a^r \in H$. *Tada su brojevi r,r+1 uzajamno prosti, pa za svaki j,*

$m<j<m+n-1$, Diofantovska jednačina (videti 13. poglavlje) $(r+1)x-ry=j$ ima rešenje po x,y. Otuda $a^j=a^{(r+j)x-ry}=a^{(r+1)x}{}_{(a^r)}{}^{-y}=a^{(r+1)x}$, pa je a^{r+1} generator grupe $\underline{H}$.

$\underline{H}$ ima n elemenata na osnovu a).

Napomena: Ako je a element polugrupe $\underline{S}$, tada je $S_a=\{a,a^2,a^3,\ldots\}$ podpolugrupa polugrupe $\underline{S}$ generisana elementom a. *Red* elementa a je $r=|S_a|$, a najmanji prirodni broj k (ukoliko postoji) takav da je a^k idempotentan je njegova *karakteristika*. Prema zad.3.13. takav k postoji ako je S_a konačan skup.

Isto tako, prema 3.14., ako je S_a konačan, postoje prirodni brojevi i i p (tzv. *indeks* i *period* elementa a) sa osobinama:

1° $a^{i+p}=a^i$

2° $S_a=\{a,a^2,\ldots,a^{i+p-1}\}$

3° $G_a=\{a^i,a^{i+1},\ldots,a^{i+p-1}\}$ je ciklična grupa.

U sledećim tvrdjenjima iskazuju se neka svojstva ovih brojeva.

Zadatke 3.15,16 predložio je A.Krapež.

3.15. Ako je S_a konačna polugrupa dokazati da je:

a) $r=i+p-1$ b) $k=p\left[\frac{r}{p}\right]$, gde je $[x]$ celobrojni deo broja x.

Rešenje: a) neposredno iz 3.14.

b) Kako je G_a grupa, njen jedinični element je idempotentan, pa element a sa konačnom polugrupom S_a zaista ima (konačnu) karakteristiku.
Ako je $a^{2k}=a^k$ tada je $a^k\in G_a$ i jedinica je grupe G_a, odakle sledi i jedinstvenost ovog idempotentnog elementa. Takodje je $i<k<i+p$.
Ako je $m=k-i$ tada je $a^{i+m}=a^k=a^{2k}=a^{2(i+m)}=a^{i+i+2m}$. Iz 3.14. se vidi da a^{i+m} i A^{i+i+2m} mogu biti jednaki samo ako imaju jednake ostatke po modulu p, tj. $k=i+m=i+2m-m=lp$.
Ako p deli i tada je $\frac{i}{p}=\left[\frac{i-1}{p}\right]+1$. U drugom slučaju je $\left[\frac{i}{p}\right]=\left[\frac{i-1}{p}\right]$ pa je $\left[\frac{i}{p}\right]<\left[\frac{i-1}{p}\right]+1$. U oba slučaja je $\frac{i}{p}<\left[\frac{i-1}{p}\right]+1$; takodje je $\left[\frac{i-1}{p}\right]+1<\frac{i}{p}+1$. Sledi stoga da je $\frac{i}{p}<\left[\frac{i+p-1}{p}\right]<\frac{i}{p}+1$ odakle je $i<p\left[\frac{r}{p}\right]<i+p$.

Oba broja k i $p\left[\frac{r}{p}\right]$ su deljivi sa p i nalaze se izmedju brojeva i-1 i i+p. Sledi da moraju biti jednaki što je i trebalo dokazati.

3.16. Neka je S polugrupa kod koje je za sve $a\in S$ polugrupa S_a konačna, i kod koje su sa i_a,p_a,r_a i k_a označeni redom indeks, period, red i karakteristika elementa a iz S. Neka su i i p najmanji prirodni brojevi (ako takvi

postoje) za koje je $a^{i+p}=a^i$ za sve $a\in S$; neka je r najmanji prirodan broj (ako takav postoji) za koji postoji $m\in N$ $(m<r)$ takav da je $a^{r+1}=a^m$ za sve $a\in S$; neka je, najzad, k najmanji prirodan broj takav da je za sve $a\in S$ a^k idempotentan. Dokazati:

a) $i=\max_{a\in S} i_a$ b) $p=\underset{a\in S}{NZS}\, p_a$ c) $r=i+p-1$ d) $k=p[\frac{r}{p}]$.

Rešenje: a) Za sve $a\in S$ je $a^{p+i}=a^i$ i $a^{i_a+p_a}=a^{i_a}$, pa je $i_a<i$, odakle $\max_{a\in S} i_a \le i$. Kako za sve $a\in S$ važi $a^{\max i_a+p}=a^{\max i_a}$ sledi da je $i<\max_{a\in S} i_a$ pa je $i=\max_{a\in S} i_a$.

b) Za sve $a\in S$ je $a^{i+p}=a^i$ i $a^{i_a+p_a}=a^{i_a}$. Prema definiciji p_a je $p_a<p$. Sledi da je $p=l\,p_a+q$ za $l\ge 0$, $0\le q<p_a$. Odavde je

$$a^i=a^{i+p}=a^{i+lp_a+q}=a^{i-i_a}\,a^{i_a+lp+q}=a^{i-i_a}\,a^{i_a+q}=a^{i+q}$$

pa mora biti $q=0$, tj. $p_a \mid p$. Sledi da je $\underset{a\in S}{NZS}\, p_a \le p$.

Iz $p_a \mid \underset{a\in S}{NZS}\, p_a$ sledi da je $\underset{a\in S}{NZS}\, p_a = m\,p_a$ za $m>0$, $a^{\underset{a\in S}{NZS}\, p_a+i}=a^{i+m\,p_a}=a^i$, pa je $p\le \underset{a\in S}{NZS}\, p_a$.

c) Direktno iz definicije r,p i i.

d) Iz $a^{2k}=a^k$ sledi $i<k<i+p$. Kako je $a^{k+p}=a^k$ biće $p<k$. Ako je $k=lp+q$, tada $p\ge 0$, $0\le q<p$. Odavde, za sve $a\in S$ je $a^k=a^{2k}=a^{k+lp+q}=a^{k+q}$ pa mora biti $q=0$. Znači da $p|k$ što sa $i\le k<i+p$ daje $k=p[\frac{r}{p}]$.

1.4. ALGEBARSKI ZAKONI. PROIZVOD GRUPOIDA

Algebarski zakoni, kraće *zakoni*, jezika $\{*\}$ su formule oblika u=v, gde su u,v termi ovog jezika. Kažemo da grupoid $\underline{G}$ zadovoljava zakon $u(x_1,\dots,x_n)=v(x_1,\dots,x_n)$ ukoliko za sve $a_1,\dots,a_n\in G$ $u(a_1,\dots,a_n)=v(a_1,\dots,a_n)$. Neke važnije algebarske zakone, kao što su *asocijativni* i *komutativni*, već smo upoznali. Zakon $x^2=x$ naziva se zakonom *idempotencije*, a x=x *trivijalnim* zakonom.

4.1. *Definicija: Grupoid $\underline{G}=(G,\cdot)$ je direktni proizvod grupoida $\underline{A}=(A,*)$ i $\underline{B}=(B,\circ)$ ukoliko je $G=A\times B$ i $(\forall a,b\in A)(\forall c,d\in B)$ $(a,c)\cdot(b,d)=(a*b,c\circ d)$.*

Proizvod tri grupoida $\underline{A}$, $\underline{B}$, $\underline{C}$ je grupoid $(\underline{A}\times\underline{B})\times\underline{C}$. Slično se definiše proizvod ma kojih n grupoida $(n\in N)$.

Neka je $\underline{G}_i$ $i\in I$ neprazan skup grupoida, $\underline{G}_i=(g_i,\cdot_i)$ $(i\in I)$. Direktan proizvod grupoida $\underline{G}_i$ $(i\in I)$ je grupoid $\underline{G}=(G,\cdot)$, gde je $G=\prod_{i\in I} G_i$, dok je operacija $\cdot$ definisana sa $(f\cdot g)(i)=f(i)\cdot_i g(i)$ $(i\in I)$, $f,g\in\prod_i G_i$ Direktan proizvod grupoida $\underline{G}_i$, $i\in I$ kraće se naziva *proizvodom* grupoida; oznaka je $\underline{G}=\prod_{i\in I}\underline{G}_i$.

4.2. *Definicija: Neka su* $\underline{G}_i$ $(i\in I)$ *grupoidi sa jedinicama* 1_i . *Direktna suma grupoida* $\underline{G}_i$ $(i\in I)$, *u oznaci* $\underline{G}=\sum_{i\in I}\underline{G}_i$, *je grupoid* $\underline{G}=(G,\cdot)$, *gde je* $G\subseteq\prod_i G_i$ *skup svih funkcija* f *takvih da je za sve* $i\in I$ *sem za konačno mnogo* $f(i)=1_i$. *Operaciją* $\cdot$ *definisana je kao u slučaju proizvoda grupoida.*

Sledećom teoremom se pokazuje da se algebarski zakoni održavaju u odnosu na neke konstrukcije nad grupoidima. U poglavlju 10. o univerzalnim algebrama uverićemo se da ova teorema važi u daleko širem kontekstu.

4.3. *Teorema: (i) Ako zakon* $u=v$ *važi na grupoidu* $\underline{G}$ *tada* $u=v$ *važi na svakom podgrupoidu grupoida* $\underline{G}$.

(ii) Ako je $\underline{H}$ *homomorfna slika grupoida* $\underline{G}$ *i zakon* $u=v$ *važi u* $\underline{G}$, *tada isti zakon važi na grupoidu* $\underline{H}$.

(iii) Neka zakon $u=v$ *važi na svim grupoidima* $\underline{G}_i$ $(i\in I)$. *Tada zakon* $u=v$ *važi na proizvodu* $\prod_{i\in I}\underline{G}_i$.

Za dokaz videti zad.4.5., a za primene zadatke 4.6,7,9,11.

U ovom odeljku razmatra se takodje i problem *nezavisnosti* jednih algebarskih zakona od drugih; videti zad. 4.14 - 17.

Primeri i zadaci

4.1. Dokazati da postoji grupoid koji ne zadovoljava nijedan netrivijalan zakon.

Rešenje: Neka je $\cdot$ *binarni operacijski simbol i* T *skup svih izraza nad promenljivima* $x_1,x_2,\ldots$. *Dalje, neka je* $*$ *operacija definisana sa* $u*v=(u\cdot v)$. *Tada je* $(T,*)$ *grupoid. Dokazujemo da ovaj grupoid zadovoljava jedino zakone vida* $u=u$. *Pretpostavimo suprotno, tj. neka za neke različite terme* $u(x_1,\ldots,x_n)$, $v(x_1,\ldots,x_n)$ *zakon* $u=v$ *važi u* $(T,*)$, *odnosno* $(\forall t_1,\ldots,t_n\in T)\ u(t_1,\ldots,t_n)=v(t_1,\ldots,t_n)$. *Kako su promenljive* $x_1,\ldots,x_n$ *takodje termi, to* $x_1,\ldots,x_n\in T$; *stoga* $u(x_1,\ldots,x_n,*)=v(x_1,\ldots,x_n,*)$. *Medjutim, prema definiciji operacije* $*$ $u(x_1,\ldots,x_n,*)=u(x_1,\ldots,x_n,\cdot)$, $v(x_1,\ldots,x_n,*)=v(x_1,\ldots,x_n,\cdot)$, *pa su termi* $u(x_1,\ldots,x_n,\cdot)$ *i* $v(x_1,\ldots,x_n,\cdot)$ *jednaki, suprotno pretpostavci.*

Napomenimo da pored prethodnog grupoida ima i drugih koji zadovoljavaju jedino trivijalne zakone. Na primer, grupoid $(R_\omega,\cdot)$, *gde* $x\cdot y=(x,y)$ *(videti zad.1.2.), jeste jedan takav grupoid. Dokaz da ovaj grupoid zadovoljava jedino trivijalne zakone može se izvesti indukcijom po složenosti*

terma (napr. po broju operacijskih simbola u termu), koristeći da u $(R_\omega,\cdot)$ *važi implikacija* $x\cdot y=u\cdot v \Rightarrow x=u \wedge y=v$.

4.2.Dokazati da grupoid $(R_\omega,*)$, gde $x*y=\{(x,y),(y,x)\}$ (videti zadatak 1.2.) ne zadovoljava druge zakone sem posledica komutativnog zakona.

Rešenje: Prethodno dokazati da u $(R_\omega,*)$ *važi*

$$x*y=u*v \Rightarrow (x=u \wedge y=v) \vee (x=v \wedge y=u).$$

4.3.Neka je S skup svih reči nad azbukom A (koja ima bar dva elementa) i $\cdot$ operacija dopisivanja (konkatenacije). Dokazati da je $(S,\cdot)$ semigrupa koja pored posledica asocijativnog zakona ne zadovoljava nikakve druge zakone.

Rešenje: Kako je asocijativni zakon ravnotežan[1)]*, to su svi izvedeni zakoni iz asocijativnog takodje ravnotežni (dokaz ovog tvrdjenja može se izvesti indukcijom po dužini dokaza zakona). Pretpostavimo da* $(S,\cdot)$ *zadovoljava zakon* $u=v$ *koji nije posledica asocijativnog zakona. Neka su* $z_1,\ldots,z_m$ *promenljive koje učestvuju u termima u,v. Kako je* $(S,\cdot)$ *semigrupa, prema konvenciji o brisanju zagrada zakon* $u=v$ *može se zapisati u obliku*

$$x_1x_2\ldots x_n=y_1y_2\ldots y_k \qquad (1)$$

s tim da je moguće da ista promenljiva z_i *bude označena različitim slovima* x_i,y_j[2)]*. Dokažimo prvo da je zakon* $u=v$ *ravnotežan. Pretpostavimo da nije, i neka su* $a,b\in A$ *dva različita slova. Kako* $u=v$ *nije ravnotežan zakon, postoji promenljiva* z_i *takva da* z_i *ima p pojavljivanja u termu u i q pojavljivanja u termu v i pritom* $p\neq q$, *recimo* $p>q$. *Promenljivoj* z_i *dodelimo vrednost a, a ostalim promenljivima iz skupa* $\{z_1,\ldots,z_m\}$ *vrednost b. Pri takvoj interpretaciji promenljivih* $z_1,\ldots,z_m$ *vrednosti izraza u i v su redom neke različite reči* $\underline{u}$ *i* $\underline{v}$. *S druge strane* $u=v$ *važi u* $(S,\cdot)$

[1)] *Zakon* $u=v$ *je ravnotežan ukoliko su termi u i v iste dužine i za svaku promenljivu x važi: broj pojavljivanja promenljive x u termu u jednak je broju pojavljivanja promenljive x u termu v.*

[2)] *U zapisu (1) simboli* $x_1,\ldots,x_n,y_1,\ldots,y_k$ *su meta-promenljive. Simbol x je meta-promenljiva ako su njene vrednosti neke druge promenljive, koje su unapred odredjene.*

pa $\underline{u}=\underline{v}$; kontradikcija.

Prema prethodnom $n=k$ i $\{x_1,\ldots,x_n\}=\{y_1,\ldots,y_n\}=\{z_1,\ldots,z_m\}$. S obzirom da (1) nije posledica asocijativnog zakona, preslikavanje $\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ y_1 & y_2 & \ldots & y_n \end{pmatrix}$ nije identička permutacija skupa $\{x_1,\ldots,x_n\}$, tj. postoje $i,j,k<n$ takvi da je niz $y_1y_2\ldots y_n$ jednak nizu $y_1y_2\ldots y_{i-1}x_k y_{i+1}\ldots y_{j-1}x_i y_{j+1}\ldots y_n$ $(i<j)$, gde x_i,x_k označavaju različite promenljive iz skupa $\{z_1,\ldots,z_m\}$, recimo z_1,z_2. Neka se promenljivima z_1,z_2 dodele vrednosti (slova) a,b, a ostalim promenljivima $z_3,\ldots,z_n$ vrednost a. U takvoj interpretaciji, termi u i v kao vrednosti imaju različite reči $\underline{u}$ i $\underline{v}$. S druge strane u=v važi u $(S,\cdot)$, pa $\underline{u}=\underline{v}$; kontradikcija.

4.4. Dokazati da svaki konačni grupoid zadovoljava neki netrivijalni zakon.

Rešenje: Neka je $\underline{G}=(G,\cdot)$ konačan grupoid i $f(x)=x\cdot x$. Tada je $f,f^2,f^3,\ldots$ beskonačan niz preslikavanja skupa G u G. Kako je $\{h \mid h : G \to G\}$ konačan skup, to postoje različiti prirodni brojevi m i n takvi da $f^m=f^n$. Tada u $\underline{G}$ važi zakon $f^n(x)=f^m(x)$.

4.5. Neka su $\underline{G}_1$ i $\underline{G}_2$ grupoidi i Z zakon $t_1=t_2$. Dokazati:

a) Ukoliko je $\underline{G}_1\subseteq\underline{G}_2$ tada: ako u $\underline{G}_2$ važi zakon Z, tada taj zakon važi i u $\underline{G}_1$.

b) Ako je $\underline{G}_2$ homomorfna slika grupoida $\underline{G}_1$ i $\underline{G}_1$ zadovoljava zakon Z, tada i grupoid $\underline{G}_2$ zadovoljava zakon Z.

c) Neka su $\underline{G}_i$, $i\in I$, grupoidi koji zadovoljavaju zakon Z i neka je $\underline{G}=\prod_{i\in I}\underline{G}_i$. Tada grupoid $\underline{G}$ takodje zadovoljava zakon Z.

Rešenje: a) Neka je $\underline{G}_1\subseteq\underline{G}_2$ i pretpostavimo da $t_1(x_1,\ldots,x_n,\cdot)=t_2(x_1,\ldots,x_n,\cdot)$ važi u $\underline{G}_2=(G_2,\circ)$, tj. za sve $a_1,\ldots,a_n\in G_2$ je $t_1(a_1,\ldots,a_n,\circ)=t_2(a_1,\ldots,a_n,\circ)$. Kako je $\underline{G}_1=(G_1,*)$ podgrupoid grupoida $\underline{G}_2$, to za sve $a,b\in G_1$ $a*b=a\circ b$. Otuda za sve $a_1,\ldots,a_n\in G_1$ $t_1(a_1,\ldots,a_n,*)=t_1(a_1,\ldots,a_n,\circ)$, $t_2(a_1,\ldots,a_n,*)=t_2(a_1,\ldots,a_n,\circ)$ pa $t_1(a_1,\ldots,a_n,*)=t_2(a_1,\ldots,a_n,*)$; drugim rečima, zakon $t_1=t_2$ važi u $\underline{G}_1$.

Prethodni argument može se učiniti rigoroznijim ukoliko se koristi sledeće <u>tvrdjenje</u>: neka je t term jezika $\{\cdot\}$ i $\underline{G}\subseteq\underline{H}$. Tada za inducirana preslikavanja (v.zad.3.11.) važi $t^{\underline{G}} = t^{\underline{H}} \restriction G$. Dokaz ovog tvrdjenja može se izvesti indukcijom po složenosti terma t.

b) Indukcijom po složenosti terma t dokazuje se da za homomorfizam $h : \underline{G}_1 \to \underline{G}_2$ važi $(\forall a_1,\ldots,a_n\in G_1)\ h(t(a_1,\ldots,a_n))=t(h(a_1),\ldots,h(a_n))$. Pretpostavimo da u $\underline{G}_1$ važi $u(x_1,\ldots,x_n)=v(x_1,\ldots,x_n)$. Neka su $b_1,\ldots,$

$b_n \in G_2$. *Ako je h* <u>na</u>, *onda za neke* $a_1,\ldots,a_n \in G_1$ $h(a_i)=b_i$, *pa* $u(b_1,\ldots,b_n)=u(h(a_1),\ldots,h(a_n))=h(u(a_1,\ldots,a_n))=h(v(a_1,\ldots,a_n))=v(h(a_1),\ldots,h(a_n))=v(b_1,\ldots,b_n)$.

c) Neka je $\underline{G}=\prod_{i\in I}\underline{G}_i$ *i* $\pi_i : G \to G_i$ *projekcija, tj.* $(\forall f\in G)\pi_i(f)=f(i)$. *Neposredno se proverava da važi sledeće:*

1° π_i *je homomorfizam,* *2°* $f=g$ *akko* $(\forall i\in I)\pi_i(f)=\pi_i(g)$.

Otuda, ukoliko zakon $u(x_1,\ldots,x_n)=v(x_1,\ldots,x_n)$ *važi u svim grupoidima* $\underline{G}_i$, *za* $f_1,\ldots,f_n\in G$ *i za sve* $i\in I$ *je*

$\pi_i(u(f_1,\ldots,f_n))=u(\pi_i(f_1),\ldots,\pi_i(f_n))=v(\pi_i(f_1),\ldots,\pi_i(f_n))=\pi_i(v(f_1,\ldots,f_n))$.

Stoga, $u(f_1,\ldots,f_n)=v(f_1,\ldots,f_n)$.

4.6. Dokazati sledeća tvrdjenja:

a) Proizvod komutativnih grupoida je komutativan grupoid.

b) Proizvod semigrupa je semigrupa.

c) Proizvod monoida je monoid.

Uputstvo: Koristiti prethodni zadatak.

4.7. Neka su $\underline{G}_1$, $\underline{G}_2$ grupoidi i $h : \underline{G}_1 \to \underline{G}_2$ homomorfizam. Ukoliko je s izvedena operacija, tj. postoji term t takav da $s(x_1,\ldots,x_n)=t(x_1,\ldots,x_n)$, $x_1,\ldots,x_n\in G$, tada je h homomorfizam i u odnosu na operaciju s.

Uputstvo: Videti zad.4.5.b)

4.8. Dokazati da je skup prirodnih brojeva kofinalan[1)] u skupu realnih brojeva.

<u>Napomena</u>: Sledeći zadatak daje još jednu konstrukciju nad grupoidima - to je *unija* grupoida.

4.9. Neka je $(I, <)$ linearno uredjenje i G_i $(i\in I)$ grupoidi takvi da $i\le j \Rightarrow G_i\subseteq G_j$, $(i,j\in I)$.

a) Na skupu $G=\bigcup_{i\in I}G_i$ definisati grupoid $\underline{G}$ tako da $\underline{G}_i\subseteq\underline{G}$ za svaki $i\in I$.

b) Neka je $J\subseteq I$ kofinalan u $(I, <)$ i neka za svaki $j\in J$ $\underline{G}_j$ zadovoljava zakon u=v. Dokazati da prethodno definisani grupoid $\underline{G}$ zadovoljava isti zakon.

---

1) Skup $J\subseteq I$ je *kofinalan* u uredjenju $(I, <)$ ukoliko važi $(\forall i\in I)(\exists j\in J)\ i<j$

Rešenje: a) Neka su $\underline{G}_i=(G_i,*_i)$. Operaciju $*$ na $\underline{G}$ odredjujemo na sledeći način. Neka su $x,y\in G$; tada postoje $i,j\in I$ takvi da $x\in G_i$, $y\in G_j$. Dalje, $i\leq j$ ili $j\leq i$; pretpostavimo $i\leq j$. Neka je $x*y=x*_j y$. Operacija $*$ je dobro definisana budući da za $x\in G_i$, $y\in G_j$, uz pretpostavku $i\leq j$, važi $G_i\subseteq G_j$, odakle $x,y\in G_j$ i $x*_i y=x*_j y$.

b) Prethodno dokazati da na svakom grupoidu $\underline{G}_i$, $i\in I$, važi zakon $u=v$. Dalje, iskoristiti sledeću činjenicu: ako su $a_1\in G_{i_1},\ldots,a_n\in G_{i_n}$, tada postoji j, $j>i_1,\ldots,i_n$ takav da $a_1,\ldots,a_n\in G_j$.

4.10. Neka grupoid $\underline{G}$ ima jedinicu. Dokazati:

a) U grupoidu $\underline{G}$ postoji maksimalni podgrupoid koji zadovoljava komutativni zakon.

b) U grupoidu $\underline{G}$ postoji maksimalni podgrupoid koji je grupa.

c) Za ma koji skup zakona Z postoji maksimalni podgrupoid koji zadovoljava sve zakone iz skupa Z.

Rešenje: a) Neka je F skup svih komutativnih podgrupoida grupoida $\underline{G}$. F je neprazan skup budući da $(\{1\},\cdot)\in F$, gde je 1 jedinica grupoida $\underline{G}$. Dalje, neka je $L=\{G_i \mid i\in I\}$ lanac (u odnosu na inkluziju) grupoida iz F, i neka je $\underline{S}=\bigcup_{i\in I} G_i$ (videti prethodni zadatak). $\underline{S}$ je komutativan podgrupoid grupoida $\underline{G}$, tj. $\underline{S}\in F$. Prema tome ispunjeni su uslovi Zorn-ove leme, odakle sledi da postoji maksimalni element u F.

4.11. Dokazati sledeća tvrdjenja:

a) Grupoid izomorfan grupi je grupa.

b) Ako je grupoid $\underline{G}$ homomorfna slika grupe $\underline{H}$, tada je $\underline{G}$ grupa.

Uputstvo: Videti zad.4.5.

4.12. Svaka komutativna semigrupa $(S,\cdot)$ u kojoj važe zakoni skraćivanja (kancelacije) utapa se u neku Abel-ovu grupu. Dokazati.

Rešenje: Prema rešenju zadatka 3.7. možemo pretpostaviti da S ima jedinicu, u oznaci 1. Dalje, primetimo da je $\underline{S}^2=S\times S$ takodje komutativna semigrupa sa jedinicom. Neka je relacija $\sim$ na S^2 odredjena sa $(a,b)\sim(c,d)\Leftrightarrow ad=bc$. Dokazujemo da je $\sim$ kongruencija grupoida $\underline{S}^2$. Dokažimo, recimo, tranzitivnost ove relacije. Neka je $(a,b)\sim(c,d)$ i $(c,d)\sim(u,v)$. Otuda $ad=bc$ i $cv=du$, odakle $adv=bcv$ i $bcv=bdu$. Dakle, $adv=bdu$, pa prema komutativnom zakonu i zakonu kancelacije važi $av=bu$, tj. $(a,b)\sim(u,v)$.

Relacija $\sim$ je saglasna sa operacijom grupoida $\underline{S}^2$. Zaista, neka je $(a,b)\sim(c,d)$ i $(p,q)\sim(r,s)$. Otuda $ad=bc$ i $ps=qr$, pa $adps=bcqr$, tj.

$(ap,bq)\sim(cr,ds)$. Postoji stoga količnički grupoid $\underline{S}^2/\sim$ i on je homomorfna slika komutativnog monoida $\underline{S}^2$, što znači da je $\underline{S}^2/\sim$ takodje komutativan monoid. Kako je $C_{(a,b)}\circ C_{(b,a)}=C_{(ab,ba)}=C_{(1,1)}$ i $C_{(1,1)}$ je jedinica grupoida $\underline{S}^2/\sim$, to je $\underline{S}^2/\sim$ Abel-ova grupa.
Preslikavanje $f: x \to C_{(x,1)}$ je utapanje semigrupe $\underline{S}$ u Abel-ovu grupu $\underline{S}^2/\sim$.

4.13. Dokazati da grupoid $(N,\cdot)$ ne zadovoljava druge zakone osim posledica asocijativnog i komutativnog zakona, ako je $\cdot$ obično množenje prirodnih brojeva.

Rešenje: Koristiti sledeći stav aritmetike: ako su $p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, $q_1^{\beta_1}q_2^{\beta_2}\ldots q_m^{\beta_m}$ dva razlaganja prirodnog broja n na proste faktore p_i, q_j tako da za $i\neq j$, $p_i\neq p_j$, $q_i\neq q_j$, tada $k=m$ i postoji permutacija f skupa $\{1,2,\ldots,k\}$ tako da $q_i=p_{f(i)}$, $\alpha_i=\beta_{f(i)}$. Takodje iskoristiti činjenicu da su komutativni i asocijativni zakon ravnotežni, i da su svi zakoni izvedeni iz ovih takodje ravnotežni.

4.14. Odrediti bar jedan grupoid $(G,*)$ koji ne zadovoljava asocijativni zakon ali u kojem važi

$$x*(y*(z*u))=(x*y)*(z*u)=x*((y*z)*u)=((x*y)*z)*u\ .$$

Rešenje: Grupoid $\underline{G}$ odredjen tablicom

	0	1	2	3	4
0	0	0	0	0	0
1	0	2	4	0	0
2	0	3	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0

zadovoljava navedene zakone i nije asocijativan. Primetimo da je $(1\cdot 1)\cdot 1=2\cdot 1=3$, $1\cdot(1\cdot 1)=1\cdot 2=4$.
Inače, $\underline{G}$ je odredjen sledećom konstrukcijom. Neka je jezik $L=\{*,a,0\}$ i $G=\{0\}\cup\{t \mid t$ je term jezika $\{*,a\}$, slovo a ima najviše 3 pojavljivanja u termu $t\}$. U skup G uvodi se sledeća operacija $\cdot$: $u\cdot v=(u*v)$ ukoliko je broj slova u $(u*v)$ manji ili jednak 3, $u\cdot v=0$ inače (termi u,v ne sadrže simbol 0). Dalje, $0\cdot t=0$, $t\cdot 0=0$, $0\cdot 0=0$.
Lako je videti da je $G=\{0,a,(a*a),a*(a*a),(a*a)*a\}$. Kodiranjem $\begin{pmatrix} 0 & a & (a*a) & (a*a)*a & a*(a*a) \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix}$ *ovaj grupoid ima reprezentaciju datu tablicom.*

4.15. Odrediti bar jedan konačan grupoid koji ne zadovoljava zakon $(xy)z=x(zy)$.

Uputstvo: Videti prethodni zadatak.

4.16. Dokazati da asocijativni zakon nije posledica zakona $xy=yx$, $(xy)(zu)=x(y(zu))$.

Uputstvo: Videti zadatak 4.14.

4.17. Konstruisati nekomutativnu semigrupu u kojoj važe zakoni $xyz=xzy=yxz=yzx=zxy=zyx$.

4.18. Neka je $\cdot$ binarni operacijski simbol i $u=v$ netrivijalni zakon jezika $\{\cdot\}$. Dokazati da postoji konačan grupoid u kojem ovaj zakon ne važi.

Rešenje: Dokaz koji navodimo sličan je rešenju zadatka 4.14. Neka je $u=v$ netrivijalni zakon jezika $\{\cdot\}$, gde je $\cdot$ binarni operacijski simbol. Dalje, neka je $n=max(složenost(u),složenost(v))$, gde je složenost(t) recimo broj operacijskih simbola u t, i $x_1,\ldots,x_k$ promenljive koje imaju pojavljivanja u izrazima u,v. Tada ima konačno mnogo izraza čija je složenost manja ili jednaka n, u kojima su jedine promenljive neke od $x_1,\ldots,x_k$. Neka je F skup svih ovakvih izraza, 0 novi znak (tj. $0\notin F$) i $G=\{0\}\cup F$. Operacija $\circ$ u G definisana je na sledeći način: neka su $u',v'\in F$; ako je složenost$(u'\cdot v')<n$ tada $u'\circ v'=(u'\cdot v')$, inače $u'\circ v'=0$. Dalje, $u'\circ 0=0\circ u'=0\circ 0=0$.

(G,$\circ$) je konačan grupoid. Ako je zakon $u=v$ netrivijalan, tada su izrazi u,v medjusobno različiti. Otuda, ukoliko se promenljive u izrazima u,v interpretiraju samim sobom, vrednosti izraza u,v postaju upravo redom u,v, odakle $u(x_1,\ldots,x_k,\ )\neq v(x_1,\ldots,x_k,\ )$, tj. zakon $u=v$ ne važi u $\underline{G}$.

4.19. Neka je W skup reči nad bar dvočlanom azbukom A i $a\in A$. Dokazati da operacija $x*y=a\cdot x\cdot y$ u W, gde je $\cdot$ operacija dopisivanja reči, ne zadovoljava netrivijalne zakone.

Rešenje: Neka je $A'=A-\{a\}$ i S najmanji podskup od W koji ima svojstva
1° $A'\subseteq S$, 2° $x,y\in S \Rightarrow axy\in S$ (simbol $\cdot$ izostavljamo).
Tada je S skup izraza nad skupom promenljivih A' sa operacijskim simbolom a, predstavljenih u poljskoj notaciji. Neka je operacija $\circ$ u S odredjena sa $x\circ y$=term od x,y (u poljskoj notaciji). Prema rešenju zadatka 4.1. (S,$\circ$) ne zadovoljava nijedan netrivijalan zakon. Ako (W,$*$) zadovoljava neki netrivijalni zakon Z, tada i (S,$\circ$) zadovoljava Z, budući da je $(S,\circ)\subseteq(W,*)$, što je kontradikcija.

4.20. Dokazati da postoje prebrojivo generisani ali ne i konačno generisani neizomorfni grupoidi $\underline{G}$ i $\underline{H}$ koji sem trivijalnih ne zadovoljavaju druge zakone.

Rešenje: Neka je $\underline{G}=(R_\omega,\circ)$, *gde* $x\circ y=(x,y)$, *i neka je* $\underline{H}=(W,*)$ *grupoid iz zadatka 4.19. nad prebrojivom azbukom. Ako je* ϕ *formula*

$$(\forall x,y,z,u)(x*y=z*u \Rightarrow x=z \wedge y=u)$$

tada $\underline{G} \models \phi$ *dok* $\underline{H} \models \neg\phi$ *budući da je za* $x=a$, $y=aa$, $z=aa$, $u=a$ $x*y=z*u$ *i* $x\neq z$, $y\neq u$. *Otuda* $\underline{G} \neq \underline{H}$.

4.21. Neka zakon u=v važi u svakom konačno generisanom podgrupoidu grupoida $\underline{G}$. Dokazati da u=v važi u $\underline{G}$.

4.22. (S.Prešić) Neka je $\underline{G}$ konačan grupoid i $n\in N$. Dokazati da postoji $m\in N$ takav da za neke elemente $a_1,\ldots,a_n\in G^m$ važi: za svaki zakon $u(x_1,\ldots,x_n)=v(x_1,\ldots,x_n)$, u=v važi u $\underline{G}$ akko $u(a_1,\ldots,a_n)=v(a_1,\ldots,a_n)$ važi u $\underline{G}^m$.

Rešenje: Neka je $|G|=k$. *Tablica provere zakona u=v u* $\underline{G}$ *je oblika:*

k^n

x_1	x_2	...	x_n	u	v	
a_1^1	a_2^1		a_n^1			
⋮	⋮		⋮			
a_1^m	a_2^m		a_n^m			*i-ta vrsta*

$a_1 \quad a_2 \qquad a_n$

Neka je $m=k^n$ *i* $a_j\in G^m$, *gde je* a_j *m-torka* $(a_j^1,\ldots,a_j^m)$. *Pretpostavimo da u* $\underline{G}^m$ *važi* $u(a_1,\ldots,a_n)=v(a_1,\ldots,a_n)$ *i neka su* π_i *projekcije. Budući da se proizvoljna n-torka* $(c_1,\ldots,c_n)$ *elemenata grupoida* $\underline{G}$ *pojavljuje u nekoj, recimo i-toj, vrsti, to je* $c_1=\pi_i(a_1),\ldots, c_n=\pi_i(a_n)$, *pa kako su* π_i *homomorfizmi, sledi*

$$u(c_1,\ldots,c_n)=u(\pi_i(a_1),\ldots,\pi_i(a_n))=\pi_i u(a_1,\ldots,a_n)=$$

$$\pi_i v(a_1,\ldots,a_n)=v(\pi_i(a_1),\ldots,\pi_i(a_n))=v(c_1,\ldots,c_n)\ ;$$

prema tome zakon u=v važi u $\underline{G}$.

S druge strane, ako u=v važi u $\underline{G}$, *prema zad. 4.5.c) ovaj zakon važi i u* $\underline{G}^m$, *pa* $u(a_1,\ldots,a_n)=v(a_1,\ldots,a_n)$.

4.23. Generalisati prethodni zadatak. Tačnije, ako je $\underline{G}$ bilo koji grupoid, dokazati da postoji stepen $\underline{G}^k$ grupoida $\underline{G}$ (k može biti i beskonačan kardinalni broj) i $f_1,f_2,\ldots\in G^k$ takvi da važi: za svaki zakon $u(x_1,\ldots,x_n)=v(x_1,\ldots,x_n)$ u=v važi u $\underline{G}$ akko je u $\underline{G}^k$ ispunjeno $u(f_1,\ldots,f_n)=v(f_1,\ldots,f_n)$.

4.24. Dokazati da se u prethodnom zadatku "stepen $\underline{G}^k$" može zameniti izrazom "prebrojiv grupoid $\underline{H}$".

Rešenje: Za $\underline{H}$ se može izabrati podgrupoid grupoida $\underline{G}^k$ koji je generisan elementima $f_1, f_2, \ldots$. Broj k i $f_1, f_2, \ldots$ su kao u zadatku 4.23.

4.25. Neka je $\underline{A}$ izvestan model, tj. operacijsko-relacijska struktura i $\phi(x,y,z)$ formula jezika strukture $\underline{A}$. Operacija $\star$ skupa A je *definabilna* u $\underline{A}$ formulom ϕ, odnosno $\phi(x,y,z)$ odredjuje operaciju $\star$ u $\underline{A}$, ukoliko za sve $x,y,z \in A$ važi $z=x\star y \Leftrightarrow \phi(x,y,z)$. Ispitati da li su sledećim formulama odredjene operacije u $\underline{A}$:

a) $(x|z \wedge y|z) \wedge ((\forall u)(x|u \wedge y|u) \Rightarrow z|u)$, $\underline{A}$ je struktura prirodnih brojeva,

b) $(x+y)^2 = x^2 + y^2 + 2z$, $\underline{A}=(Z,+,q)$, Z je skup celih brojeva, $q(x)=x^2$,

c) $(x \geq z \wedge y \geq z) \wedge ((\forall u)(x \geq u \wedge y \geq u) \Rightarrow u < z)$, $\underline{A}=(A,\leq)$ je parcijalno uredjenje,

d) $z^2 + zx + y = 0$, $\underline{A}$ je polje realnih (kompleksnih) brojeva.

Rešenje: U svim slučajevima potrebno je proveriti da li važi

$$(\forall x)(\forall y)(\exists_1 z)\ \phi(x,y,z)\ .$$

a) $x\star y = NZS(x,y)$ (najmanji zajednički sadržalac brojeva x,y)

b) Operacija $\star$ je množenje celih brojeva.

c) U opštem slučaju $\phi(x,y,z)$ ne odredjuje operaciju u $\underline{A}$. Tačnije, formula ϕ odredjuje operaciju u $\underline{A}$ akko $\underline{A}$ je donja polumreža, tj. za svaka dva elementa $x,y \in A$ postoji $inf(x,y)$.

d) Formula ϕ ne odredjuje operaciju u $\underline{A}$.

4.26. Neka su $\underline{G}_i$, $i \in I$, grupoidi sa jedinicom 1. Dokazati:

a) Ako je I konačan skup, tada je $\prod_{i\in I}\underline{G}_i = \sum_{i\in I}\underline{G}_i$,

b) $\sum_{i\in I}\underline{G}_i = \{f \in \prod_i |G_i| \mid (\exists n \in \omega)(\forall i \geq n) f(i)=1\}$, gde je $I \subseteq \omega$.

4.27. Neka su $\underline{G}_i$, $i \in I$, grupoidi sa jedinicom, gde $(\forall i \in I)|G_i| > 2$. Odrediti kardinalne brojeve grupoida $\sum_{i\in I}\underline{G}_i$, $\prod_{i\in I}\underline{G}_i$.

Rešenje: Ako je I konačan skup tada $|\sum_{i\in I} G_i| = |\prod_{i\in I} G_i| = \prod_{i\in I}|G_i|$.

Ako je I beskonačan skup tada

$$|\prod_{i\in I} G_i| = \prod_{i\in I}|G_i| \ , \quad |\sum_{i\in I} G_i| = \sup_J\{|\prod_{i\in J} G_i| \mid J \subseteq I,\ J \text{ konačan skup}\}.$$

1.5. KVAZIGRUPE

5.1. Definicija: Grupoid $\underline{G}=(G,\cdot)$ je kvazigrupa ukoliko za sve $a,b\in G$ jednačine $ax=b$, $ya=b$ imaju jedinstvena rešenja po x,y u $\underline{G}$.

Lupa (ili *petlja*) je kvazigrupa sa jedinicom.

U slučaju kvazigrupa pojam izomorfizma ima generalizaciju. Naime, neka su $\underline{G}$, $\underline{H}$ kvazigrupe i f,g,h 1-1 preslikavanja skupa G na H koja zadovoljavaju uslov $(\forall x,y\in G)\ f(x*y)=g(x)\cdot h(y)$. Tada trojku (f,g,h) nazivamo *izotopijom* kvazigrupa $\underline{G}$ i $\underline{H}$ i koristimo oznaku $(f,g,h):\underline{G}\simeq\underline{H}$.

Pojam izotopije neposredno se prenosi na grupoide i tada važi sledeća

5.2. Teorema: Ako je grupoid $\underline{G}$ izotopan nekoj kvazigrupi, tada je $\underline{G}$ takodje kvazigrupa.

Dokaz je dat u zadatku 5.4.

Primeri i zadaci

5.1. Utvrditi koji od sledećih grupoida su kvazigrupe:

a) $(R,*)$, $x*y=x^3+x+3y$,

b) $(Z\times Z,*)$, $(a,b)*(x,y)\doteq\left(\left[\frac{a+x}{2}\right],\ a+x+2b+2y\right)$.

Rešenje: a) $(R,*)$ je kvazigrupa. Očigledno, jednačina $x*y=z$ ima jedinstveno rešenje po y za sve $x,z\in R$. Takodje, ova jednačina ima jedinstveno rešenje po x za sve $y,z\in R$. Zaista, primetimo da ona glasi $x^3+x+3y=z$. Pošto je ovo kubna jednačina, egzistencija elementa $a\in R$ takvog da je $a^3+a+3y=z$ je obezbedjena. Kako je

$$\frac{\partial}{\partial x}(x^3+x+3y)=3x^2+1>0,$$

to je a jedinstveno odredjeno.

b) $(Z\times Z,*)$ je kvazigrupa.

5.2. Dokazati da je proizvod kvazigrupa takodje kvazigrupa.

Rešenje: Neka su $\underline{K}_i=(K_i,*_i)$ kvazigrupe, $\underline{K}=(K,*)=\prod_{i\in I}\underline{K}_i$ i $a,b\in\prod_{i\in I}K_i$. Za svako $i\in I$ jednačine $a(i)*_i x=b(i)$, $y*_i a(i)=b(i)$ imaju jedinstvena rešenja u $\underline{K}_i$. Neka su to x_i,y_i; tada i jednačine $a*x=b$, $y*a=b$ imaju jedinstvena rešenja u $\underline{K}$ i ona su $(x(i):i\in I)$, $(y(i):i\in I)$.

5.3.Dokazati da je lupa $\underline{G}$ grupa akko $\underline{G}$ zadovoljava uslov

$$(\phi)\quad x_1y_2=x_2y_1 \wedge x_1y_4=x_2y_3 \wedge x_3y_2=x_4y_1 \Rightarrow x_3y_4=x_4y_3 .$$

Rešenje: ($\Rightarrow$) Neka je $\underline{G}$ grupa. Dokazujemo da $\underline{G}$ zadovoljava uslov (ϕ). Neka je $x_1y_2=x_2y_1$, $x_1y_4=x_2y_3$, $x_3y_2=x_4y_1$ gde $x_i,y_i \in G$. Dalje, za ma koje $x,y \in G$ važi $(xy)^{-1}=y^{-1}x^{-1}$. Otuda $x_3y_4=x_3y_2(x_1y_2)^{-1}x_1y_4=x_4y_1(x_2y_1)^{-1}x_2y_3 = x_4y_3$.

($\Leftarrow$) Neka je $\underline{G}$ lupa koja zadovoljava (ϕ) i zamenimo $x_1=y_1=1_G$ u (ϕ). Tada u $\underline{G}$ važi $x_2=y_2 \wedge y_4=x_2y_3 \wedge x_3y_2=x_4 \wedge x_3y_4=x_4y_3$, pa dokaz dalje teče kao u zad. 3.4.

Napomena: Prethodno tvrdjenje ima sledeći tablični preizraz. Kvazigrupa $\underline{G}$ je grupa akko za ma koju četvornu podtablicu Cayley-eve tablice za $\underline{G}$ važi

	y_1	y_2	y_3	y_4
x_1		q		r
x_2	q		r	
x_3		p		
x_4	p			

$\Rightarrow$

	y_1	y_2	y_3	y_4
x_1		q		r
x_2	q		r	
x_3		p		s
x_4	p		s	

5.4.Dokazati da je grupoid koji je izotopan kvazigrupi, takodje kvazigrupa.

Rešenje: Neka je $\underline{G}$ kvazigrupa, $\underline{H}$ grupoid i $(f,g,h) : \underline{H} \to \underline{G}$ izotopija. Za $a,b \in H$ jednačina $ax=b$ u $\underline{H}$ ima jedinstveno rešenje, budući da njen prenos (transfer) $a'x=b'$ u $\underline{G}$ ima jedinstveno rešenje ($g(a)=a'$, $f(b)=b'$). Isti slučaj je sa jednačinom $ya=b$.

5.5.Neka je S klasa svih kvazigrupa. Dokazati da je izotopija, u oznaci $\simeq$ kongruencija za $(S,\times)$, gde je $\underline{G}\times\underline{H}$ proizvod kvazigrupa.

5.6.Dokazati da je svaka kvazigrupa izotopna nekoj lupi.

Rešenje: Neka je $\underline{G}=(G,\cdot)$ kvazigrupa i $a \in G$ jedan odredjen element. Za svaki $b \in G$ postoji tačno jedan $x \in G$ takav da $xa=b$. Prema tome postoji jedinstvena funkcija $\lambda : G \xrightarrow[1-1]{na} G$ tako da $(\forall b \in G)\lambda(b)a=b$, tj. $\lambda(x)a=x$. Tada je $G'=(G,*)$ kvazigrupa, gde $x*y \overset{def}{=} \lambda(x)y$. Primetimo da je $x*a=\lambda(x)a=x$, tj. a je desna jedinica grupoida $\underline{G}'$. Takodje, (i_G,λ,i_G) je jedna izotopija iz $\underline{G}$ na $\underline{G}'$.

Slično, za svaki $b \in G$ postoji tačno jedan $x \in G$ takav da je $a*x=b$, pa postoji jedinstvena funkcija $\mu : G \xrightarrow[1-1]{na} G$ takva da je za sve $x \in G$ $a*\mu(x)=x$. Neka je $\underline{G}''=(G,\circ)$, gde $x\circ y \overset{def}{=} x*\mu(y)$. Tada je $(i_G,\lambda,\mu) : \underline{G} \to \underline{G}''$ izotopija i a je jedinica kvazigrupe $\underline{G}''$, tj. $\underline{G}''$ je lupa. Detaljnije: $a\circ x=a*\mu(x)=x$ pa je a leva jedinica kvazigrupe $\underline{G}''$. Kako je $a*\mu(a)=a$, tj. $\lambda(a)\mu(a)=a$,

to zbog $\lambda(a)a=a$ i jedinstvenosti rešenja po x jednačine $\lambda(a)x=a$, sledi $\mu(a)=a$. Stoga $x\circ a=x*\mu(a)=x*a=\lambda(x)a=x$, dakle a je desna jedinica kvazigrupe $\underline{G}$".

5.7. Neka su grupe $\underline{G}_1$ i $\underline{G}_2$ izotopne. Dokazati da su one izomorfne.

Rešenje: Neka su $\underline{G}_1=(G_1,*)$, $\underline{G}_2=(G_2,\cdot)$ grupe i $(f,g,h):\underline{G}_1\to\underline{G}_2$ izotopija. Tada za sve $x,y\in G_1$ $f(x*y)=g(x)h(y)$. Zamenjujući u ovoj formuli redom x,y sa jedinicom grupe G_2 dobija se $f(x)=g(x)a'$, $f(y)=b'h(y)$, gde $a'=h(1)$, $b'=g(1)$. Otuda $g(x)=f(x)a$, $h(x)=bf(x)$, gde su a,b inverzni elementi za a',b' u G_2. Dalje, $f(x*y)=f(x)abf(y)$ pa $f(x*y)c=(f(x)c)(f(y)c)$, gde $c=ab$, pa je $F:G_1\to G_2$, $F(x)=f(x)c$, izomorfizam grupa $\underline{G}_1$ i $\underline{G}_2$.

5.8. Neka je $\underline{G}$ kvazigrupa i $I(\underline{G})$ skup svih izotopija $(f,g,h):\underline{G}\to\underline{G}$. Dokazati da je $(I(\underline{G}),\cdot)$ grupa, gde je $(f,g,h)\cdot(f',g',h')=(ff',gg',hh')$.

5.9. Neka kvazigrupa $\underline{G}$ ima n elemenata, $n\in\mathbb{N}$. Dokazati da je broj različitih kvazigrupa na skupu G izotopnih kvazigrupi $\underline{G}$ jednak $(n!)^3/|I(\underline{G})|$.

Uputstvo: Slično rešenju zadatka 2.10.

2. GRUPE: AKSIOME, PRIMERI, PODGRUPE

Grupe su posebna vrsta semigrupa u kojima je moguće izvoditi u odredjenom smislu deljenje. Ovaj pojam je nastao u vezi sa rešavanjem algebarskih jednačina P(x)=0 preko radikala, i potiče od Everista Galois-a (1811-1832), od koga dolazi i sam naziv - "grupa".

Zanimljivo je da grupe permutacija koje je E.Galois proučavao, predstavljaju prvu pojavu apstraktnih algebarskih struktura, tj. struktura koje nisu brojevnog karaktera. Grupe su privukle pažnju velikog broja matematičara u čijim se radovima pokazalo da se one javljaju u svim oblastima matematike, od grupovnih klasifikacija u geometriji do primena u kvantnoj mehanici.

2.1. AKSIOME

Aksiome grupe potiču od A.Cayley-a koji ih je uveo 1854-te godine.

1.1. *Definicija:* *Grupa* *je svaka algebarska struktura* $\underline{G}=(G,*,e)$, *gde je* $(G,*)$ *semigrupa,* e *jedinični element ove semigrupe i u njoj za svaki* $a\in G$ *jednačine* $a*x=e$, $y*a=e$ *imaju rešenje po* x,y *u* $\underline{G}$.

Dokazuje se da su rešenja jednačina u prethodnoj definiciji jedinstvena i jednaka, pa se u $\underline{G}$ uvodi unarna operacija $^{-1}$ tako da za svaki $a\in G$ važi $a*a^{-1}=e$, $a^{-1}*a=e$. Element a^{-1} naziva se *inverznim* elementom za a.

Stepen elementa a je $a^n=a*a*\ldots*a$ (n puta), $n\in N$; pri tom je, po definiciji, $a^0=e$, i $a^{-n}=(a^{-1})^n$.

1.2. *Teorema:* *U svakoj grupi* $\underline{G}$ *za cele brojeve* n,m *važi:*
(i) $(x^{-1})^n=(x^n)^{-1}$ *(ii)* $x^{n+m}=x^n\cdot x^m$ *(iii)* $(x^n)^m=x^{nm}$

Dokaz: (i) Neka je $z=(xy)^{-1}$. Tada $(xy)^{-1}xy=e$, odakle množenjem sa desna, prvo sa y^{-1}, potom sa x^{-1} nalazimo

$$(xy)^{-1}=y^{-1}x^{-1} \qquad (1)$$

Višestrukom primenom jednakosti (1) dobijamo

$$(x_1\cdot x_2\cdots x_n)^{-1}=x_n^{-1}\cdots x_2^{-1}\cdot x_1^{-1} \qquad (2)$$

Uzimajući $x_1=\ldots=x_n=x$ dobija se tvrdjenje (i).

(ii) Ako su m,n prirodni brojevi tvrdjenje sledi prema zad.1.3.10.

Neka je $m>0$, $n=-k$, $k>0$. Ako je $m>k$ neka je $m=l+k$. Tada, koristeći (i)

imamo $x^m \cdot x^n = x^l \cdot x^k \cdot x^{-k} = x^l = x^{m+n}$. Ako je $m < k$, tada $n = -m-l$ za neki $l > 0$, pa $x^m \cdot x^n = x^m \cdot x^{-m} \cdot x^{-l} = x^{-l} = x^{m+n}$.

Najzad, ako su $m,n < 0$, neka je $m=-k$, $n=-l$, $k,l > 0$. Tada $x^{m+n} = x^{-(k+l)} = (x^{-1})^{k+l} = (x^{-1})^k \cdot (x^{-1})^l = x^{-k} \cdot x^{-l} = x^m \cdot x^n$.

(iii) Ako je $n > 0$, onda prema (ii) $(x^m)^n = x^m \cdot x^m \cdots x^m$ (n puta) $= x^{m+\ldots+m} = x^{mn}$. Ako je $n=-k$, $k > 0$, onda prema (i) i već dokazanom

$$x^{mn} = x^{-mk} = (x^{-1})^{mk} = ((x^{-1})^m)^k = ((x^m)^{-1})^k = (x^m)^{-k} = (x^m)^n. \quad \blacktriangledown$$

Abel-ova ili komutativna grupa je svaka grupa $\underline{G}$ koja zadovoljava komutativni zakon $x \cdot y = y \cdot x$. Naziv je po norveškom matematičaru N.Abel-u (1802-1829).

Primeri i zadaci

1.1. Neka semigrupa $\underline{G}$ zadovoljava jedan od sledećih skupova aksioma:

a) $(\exists u)(\forall x)(xu=x \wedge ux=x \wedge (\exists y)(xy=u \wedge yx=u))$,

b) $1 \cdot x = x$, $x \cdot 1 = x$, $(\forall x)(\exists y)(xy=1 \wedge yx=1)$

c) $x \cdot 1 = x$, $x \cdot x' = 1$ d) $1 \cdot x = x$, $(\forall x)(\exists y)(yx=1)$

e) $(\forall x,y)(\exists z)xz=y$, $(\forall x,y)(\exists z)zx=y$.

Dokazati da je $\underline{G}$ u svakom od ovih slučajeva grupa. Odrediti odgovarajući jezik u kojem su ove aksiome formulisane.

Rešenje: c) $x' \cdot x = x' \cdot x \cdot 1 = x' \cdot x \cdot x' \cdot (x')' = x' \cdot 1 \cdot x'' = x' \cdot x'' = 1$. *Dalje,* $1 \cdot x = x \cdot x' \cdot x = x \cdot 1 = x$.

Odgovarajući jezici su:

a) $L=\{\cdot\}$, $\cdot$ *je binarni operacijski simbol*

b) $L=\{\cdot,1\}$, $\cdot$ *je binarni operacijski simbol, 1 je znak konstante*

c) $L=\{\cdot,',1\}$, $\cdot$ *je binarni operacijski simbol,* $'$ *je unarni operacijski simbol, 1 je znak konstante.*

1.2. Neka je $\underline{G}$ grupa i $*$ operacija u G definisana sa $a*b=ab^{-1}$, gde $a,b \in G$.

Dokazati:

a) $1=a*a$, $a^{-1}=(a*a)*a$, $ab=a*((b*b)*b)$ $(a,b \in G)$,

b) Neka je $(G,*)$ grupoid koji zadovoljava zakon $(x*z)*(y*z)=x*y$ i pretpostavimo da svaka jednačina $a*x=b$ ima rešenje po x u G. Ukoliko se $1, ^{-1}, \cdot$ definišu jednakostima datim pod a), tada je $(G,\cdot,^{-1},1)$ grupa.

Rešenje: a) Na primer, $a*((b*b)*b)=a*((bb^{-1})*b)=a*(1*b)=a*b^{-1}=a(b^{-1})^{-1}=ab$.

b) Neka je $xy=x*((y*y)*y$, $x'=(x*x)*x$, $d \in G$ *i* $e=d*d$.

1° Dokazujemo da je e jedinica grupoida $(G,\cdot)$. Ispunjeno je

$$e*e=(d*d)*(d*d)=d*d=e \text{ , tj. } e*e=e \qquad (1)$$

Dalje, $(e*x)*(e*x)=e*e=e$, odakle

$$(e*x)*(e*x)=e \qquad (2)$$

Za svaki $a \in G$ jednačina $a*x=b$ ima rešenje po x, pa neka je c takav da $e*c=a$. Tada na osnovu (2) $a*a=(e*c)*(e*c)=e$, tj.

$$x*x=e \ . \qquad (3)$$

Neka je n takav da $a*n=a$. Tada $a*e=(a*n)*(n*n)=a*n=a$, tj.

$$x*e=x \ . \qquad (4)$$

Dalje, $ea=e*((a*a)*a)=(a*a)*((a*a)*a)=a*(a*a)=a*e=a$, pa prema tome važi

$$ex=x \ . \qquad (5)$$

Sa druge strane, $xe=x*((e*e)*e)=x*(e*e)=x*e=x$, tj.

$$xe=x \ . \qquad (6)$$

Prema tome e je jedinica grupoida $(G,\cdot)$.

2° Dokazujemo $xx'=x'x=e$. Kako je $x'=(x*x)*x=e*x$, to

$x'x=x'*((x*x)*x)=x'*(e*x)=x'*x'=e$. Otuda

$$x'x=e \ . \qquad (7)$$

S druge strane, $xx'=x*((x'*x')*x')=x*(e*x')=x*(e*(e*x))=x*((x*x)*(e*x))$ $x*(x*e)=x*x=e$, odakle

$$xx'=e \ . \qquad (8)$$

3° Dokazujemo $(xy)z=x(yz)$. Prethodno odredjujemo još neke veze izmedju operacija $\cdot$ i $*$. Tako je $x*y'=x*(e*y)=x*((y*y)*y)=xy$, odakle

$$xy=x*y' \ . \qquad (9)$$

Dalje, $x'' = (e*x)'=e*(e*x)=(x*x)*(e*x)=x*e=x$, tj.

$$x''=x \ . \qquad (10)$$

Prema tome preslikavanje $f : G \to G$, $f(x)=x'$, je 1-1 i na. Prema (9) važi $(xy)z=(xy)*z'=(x*y')*z'$, odakle

$$(xy)z=(x*y')*z'. \qquad (11)$$

Dalje, koristeći izvedene zakone u 1° i 2° dobija se

$x(yz)=x*(((yz)*(yz))*(yz))=x*(e*(yz))=x*(e*(y*z'))=x*((z'*z')*(y*z'))$ $=x*(z'*y)$, tj.

$$x(yz)=x*(z'*y) \ . \qquad (12)$$

Otuda $(xy)z=x(yz)$ akko

$$(x*y')*z'=x*(z'*y) \ . \qquad (13)$$

S obzirom da je preslikavanje f involutivno, tj. f zadovoljava $f(f(x))=x$, operacija $\cdot$ je asocijativna akko

$$(x*y')*z=x*(z*y) \ . \qquad (14)$$

Ova jednakost dobijena je iz (13) zamenom z sa z'.

Dalje, $(x*y')*z=(x*y')*(z*e)=(x*(e*y))*(z*e)=(x*(e*y))*((z*y)*(e*y))=$

x(z*y), tj. jednakost (14) važi, što znači da je operacija · asocijativna.*

1.3.Neka je (G,*) grupoid koji zadovoljava

a*((((a*a)*b)*c)*(((a*a)*a)*c))=b .

Dokazati da je (G,·) grupa ukoliko je · odredjena jednakošću u zad.1.2.a).

*Rešenje: Primetiti da za sve a,b∈G jednačina a*x=b po x ima rešenje,*

$x=(((a*a)*b)*c)*((a*a)*a)*c)$.

1.4.Neka je G grupa. Polazeći od definicije grupe dokazati:

a) U G postoji tačno jedan jedinični element, koji je idempotentan,

b) Za svaki a∈G postoji tačno jedan b∈G koji je inverzan za a,

c) U G važe zakoni skraćivanja (kancelacije):

ax=bx ⇒a_b, xa=xb ⇒a=b .

Rešenje: a) Neka su e,n dve jedinice. Tada en=n jer je e leva jedinica; takodje en=e jer je n desna jedinica. Otuda e=n.

c) Jedan dokaz je: ax=bx ⇒ $axx^{-1}=bxx^{-1}$ *⇒ ae=be ⇒ a=b. Dakle, ax=bx ⇒ a=b.*

1.5.Dokazati da je grupoid G grupa ukoliko jednačine ax=b, ya=b imaju bar po jedno rešenje po x,y za sve a,b∈G, i ako asocijativni zakon važi za bilo koju trojku (a,b,c) različitih lemenata.

1.6.Neka je G konačna semigrupa u kojoj važe zakoni skraćivanja. Dokazati da je G grupa.

Rešenje: Neka je a∈G i f : G⟶G definisano sa f(x)=ax. Kako važi zakon skraćivanja f je 1-1. Kako je G konačan skup to je onda f na. Otuda za bilo koji b∈G jednačina ax=b ima rešenje po x. Slično se dokazuje da i jednačina ya=b ima rešenje po y, pa je G grupa.

1.7.Dokazati da je konačna semigrupa S sa jedinicom u kojoj važi ovakav zakon skraćivanja: ax=xb ⇒a=b, Abel-ova grupa.

Rešenje: Kako je (ab)a=a(ba), to na osnovu navedenog zakona skraćivanja sledi ab=ba. Prema tome G je komutativna semigrupa, pa važe zakoni kancelacije ac=bc ⇒a=b, ca=cb ⇒a=b; tvrdjenje sledi prema zad.1.6.

1.8.Neka je S semigrupa sa desnom jedinicom e i pretpostavimo da u S važi (∀x)(∃y) yx=e .

a) Dokazati da S ne mora biti grupa,

b) Da li je S grupa ukoliko: 1° S ima tačno jednu desnu jedinicu?

2° Svaki x∈S ima tačno jedan levi inverzni element?

Rešenje: a) Neka je na skupu S sa bar dva elementa definisana operacija $\cdot$ *$xy=x$. Tada u $(S,\cdot)$ za bilo koji $e\in S$ važi $(\forall x)xe=x$ i $(\forall x)(\exists y)yx=e$. U ovakvom slučaju $(S,\cdot)$ nije grupa.*

b) 1° Neka je e jedinstvena desna jedinica u $\underline{S}$ i za svaki $x\in S$ neka je x' takav da $x'x=e$. Dokazujemo $xx'=e$. Neka je $a=xx'$. Tada $a^2=xx'xx'=xex'=xx'=a$, tj. $a^2=a$. Otuda $a'aa=a'a$, pa $ea=e$. Prema prethodnom sledi da za sve $x\in S$, $xa=(xe)a=x(ea)=xe=x$. Stoga je a desna jedinica, pa kako $\underline{S}$ ima tačno jednu desnu jedinicu, $a=e$. Otuda $xx'=e$, $xe=x$, pa prema zad. 1.1.c), $\underline{S}$ je grupa.

2° Semigrupa $\underline{S}$ navedena pod a) ima desnu jedinicu e i svaki $x\in S$ ima tačno jedan levo inverzni element (upravo e), ali $\underline{S}$ nije grupa.

1.9. Neka semigrupa $\underline{S}$ zadovoljava zakone skraćivanja i $(\forall x)(\exists y)\ xyx=x$. Dokazati da je $\underline{S}$ grupa.

Rešenje: Neka je $a\in S$ i $b\in S$ takav da $aba=a$. Dalje, za $e=ab$ važi $e^2=(ab)(ab)=(aba)b=ab=e$, tj. $e^2=e$. Neka je $x\in S$. Tada $(xe)e=xe^2=xe$, tj. $(xe)e=xe$. Na o$novu zakona skraćivanja onda je $xe=x$, što znači da *je e desna jedinica semigrupe $\underline{S}$. Slično, $e(ex)=ex$, pa $ex=x$; dakle, e je jedinica semigrupe $\underline{S}$. Kako grupoid ima najviše jednu jedinicu, to za sve $x,y\in S$ za koje je $xyx=x$, važi $xy=e$. S druge strane, $(\forall x\in S)(\exists y\in S)\ xy$*$x=x$, pa svaki $x\in S$ ima desni inverzni element; prema zad.1.1.c) $\underline{S}$ je grupa.

2.2. PRIMERI GRUPA

U ovom odeljku navodimo više primera grupa. Karakteristični primeri dati su u zadacima 2.2., 2.6., 2.7. i 2.13.
Ovde se takodje upoznajemo sa tabličnim predstavljanjem grupa, koje je naročito pogodno za prikazivanje grupa sa malim brojem elemenata. Tako, u zadatku 2.3., primer c) predstavlja Klein-ovu četvornu grupu, a primer f) grupu kvaterniona.

U vezi sa pravilnim n-touglima, uvodi se pojam *dijedarske* grupe. Naime, ako je P_n pravilan n-tougao, sa D_n označavamo skup svih izometrija ravni tog n-tougla koje prevode n-tougao P_n u samog sebe.

2.1. *Definicija: Dijedarska grupa pravilnog n-tougla P_n je grupa $\underline{D}_n=(D_n,\circ)$ gde je $\circ$ slaganje preslikavanja.*

Grupa $\underline{D}_n$ je *grupa simetrije* n-tougla P_n.

Pokazuje se da je D_n generisana sa dva elementa, ρ i σ, gde je ρ rotacija oko centra n-tougla P_n za ugao $2\pi/n$, a σ je refleksija P_n oko neke ose simetrije ovog n-tougla; takodje, važe relacije (videti zad. 12.1.40.)

$$\rho^n=1, \quad \sigma^2=1, \quad \sigma\rho=\rho^{n-1}\sigma \qquad (1)$$

Pri tom je $r(\rho)=n$, $r(\sigma)=2$ ($r(a)$ je red elementa a; videti odeljak 2.4.)

Jednakosti (1) nazivamo *strukturnim jednakostima* grupe D_n.

Kako je svaka druga grupa, koja je generisana nekim elementima ρ i σ sa struturnim jednakostima (1), izomorfna sa D_n, to ubuduće naziv "dijedarske grupe" koristimo i za takve grupe.

Primeri i zadaci

2.1. Ispitati koji su od sledećih parova $(S,\cdot)$ grupe:

a) $S=\{(a,b) \mid a,b\in Q,\ a\neq 0\}$, $(a,b)\cdot(c,d)=(ac,bc+c+d)$,

b) $S=\{\frac{1+2m}{1+2n} \mid m,n\in Z\}$, operacija $\cdot$ je množenje racionalnih brojeva,

c) $S=R$, operacija $\cdot$ definisana je sa $x\cdot y=f^{-1}(f(x)+f(y))$, gde je f permutacija skupa R,

d) $S=\{a+bi \mid a,b\in R;\ a^2+b^2=1\}$, operacija $\cdot$ je množenje kompleksnih brojeva

e) $S=\{\frac{ax+b}{cx+d} \mid a,b,c,d\in R,\ ad-bc=1\}$, operacija $\cdot$ je slaganje funkcija.

Rešenje: a) Jeste grupa; jedinica je $(1,-1)$, a inverzni za (x,y) je $(1/x,-(x+y+1)/x)$.

b) Jeste grupa.

c) $(S,\cdot)$ je grupa i $f:(R,+)\to(S,\cdot)$ je izomorfizam.

d) $(S,\cdot)$ je grupa.

e) Jeste grupa.

2.2. Dokazati da je $\underline{Z}_n=(\{0,1,\ldots,n-1\},+_n)$ komutativna grupa, gde je $+_n$ sabiranje po modulu n.

Rešenje: Primetimo da je $a+_n b=a+b$ ako je $a+b\leq n-1$, a inače $a+_n b=r$ ukoliko je $a+b=n+r$. Prema tome, $\underline{Z}_n$ je grupoid sa neutralnim elementom 0. Dokazujemo da je operacija $+_n$ asocijativna. Lako je videti da je $a+_n(b+_n c)=a+b+c-\alpha n$, $(a+_n b)+_n c=a+b+c-\beta n$, gde $\alpha,\beta\in\{0,1,2\}$.

Takodje, $0<a+_n(b+_n c)\leq n-1$, $0<(a+_n b)+_n c\leq n-1$. Pretpostavimo $\alpha\neq\beta$, recimo $\alpha>\beta$. Tada

$$a+_n(b+_n c)=a+b+c-\alpha n\leq a+b+c-(\beta+1)n=a+b+c-\beta n-n, \qquad (1)$$

budući da je $\alpha \geq \beta+1$. S druge strane, $a+b+c-\beta n < n$ (jer $0 < (a+_n b)+_n c < n$) pa zbog (1) $a+_n b+_n c < 0$, što je kontradikcija. Slično se razmatra slučaj $\alpha < \beta$. Inverzni za $a \neq 0$ je $n-a$.

2.3. Ispitati da li su navedenim tablicama odredjene grupe i odrediti koje su od njih Abel-ove:

a)

	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

b)

	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

c)

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

d)

	i	f_1	f_2	f_3	g_1	g_2
i	i	f_1	f_2	f_3	g_1	g_2
f_1	f_1	i	g_1	g_2	f_2	f_3
f_2	f_2	g_2	i	g_1	f_3	f_1
f_3	f_3	g_1	g_2	i	f_1	f_2
g_1	g_1	f_3	f_1	f_2	g_2	i
g_2	g_2	f_2	f_3	f_1	i	g_1

e)

	1	f	g_1	g_2	h_1	h_2
1	1	f	g_1	g_2	h_1	h_2
f	f	1	h_1	h_2	g_1	g_2
g_1	g_1	h_1	g_2	1	h_2	f
g_2	g_2	h_2	1	g_1	f	h_1
h_1	h_1	g_1	h_2	f	g_2	1
h_2	h_2	g_2	f	h_1	1	g_1

f)

	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

Rešenje: Svi grupoidi dati tablicama osim pod a) su grupe. Grupe b), c) i e) su Abel-ove, dok d) i f) to nisu.

Dokažimo da je grupoid G dat pod d) grupa.

<u>I način</u> (pomoću Cayley-eve teoreme o funkcijskoj reprezentaciji semigrupa). Iz tablice se vidi da je i jedinica grupoida G. Neposrednim posmatranjem tablice vidi se da se svaki $g \in G$ pojavljuje tačno jedanput u svakoj vrsti i koloni tablice, što znači da za proizvoljne $a,b \in G$ jednačine $ax=b$, $ya=b$ imaju jedinstvena rešenja po x,y u G. Otuda, G je bar lupa. Asocijativnost je moguće proveriti direktno, ispitujući za sve $a,b,c \in G$ da li je $(ab)c=a(bc)$, što dovodi do opsežnog računa. Medjutim, asocijativnost je moguće proveriti koristeći Cayley-evu teoremu o reprezentaciji semigrupa (videti teoremu 1.3.2.). Radi toga svakom elementu g iz G dodeljujemo jednu funkciju $\underline{g}$, $\underline{g}(x)=g \cdot x$. Tablica za $(\underline{G},\circ)$, gde je $\underline{G}$ skup tih funkcija, a $\circ$ slaganje preslikavanja je oblika:

	$\underline{i}$	$\underline{f}_1$	$\underline{f}_2$	$\underline{f}_3$	$\underline{g}_1$	$\underline{g}_2$
$\underline{i}$	$\underline{i}$	$\underline{f}_1$	$\underline{f}_2$	$\underline{f}_3$	$\underline{g}_1$	$\underline{g}_2$
$\underline{f}_1$	$\underline{f}_1$	$\underline{i}$	$\underline{g}_1$	$\underline{g}_2$	$\underline{f}_2$	$\underline{f}_3$
$\underline{f}_2$	$\underline{f}_2$	$\underline{g}_2$	$\underline{i}$	$\underline{g}_2$	$\underline{f}_3$	$\underline{f}_1$
$\underline{f}_3$	$\underline{f}_3$	$\underline{g}_1$	$\underline{g}_2$	$\underline{i}$	$\underline{f}_1$	$\underline{f}_2$
$\underline{g}_1$	$\underline{g}_1$	$\underline{f}_3$	$\underline{f}_1$	$\underline{f}_2$	$\underline{g}_2$	$\underline{i}$
$\underline{g}_2$	$\underline{g}_2$	$\underline{f}_2$	$\underline{f}_3$	$\underline{f}_1$	$\underline{i}$	$\underline{g}_1$

Budući da je, očigledno, preslikavanje $F: g \longmapsto \underline{g}$ izomorfizam, zaključujemo (prema pomenutoj Cayley-evoj teoremi) da je G semigrupa, pa prema tome i grupa.

II način (ideja izomorfizma). Skup permutacija skupa {1,2,3} čini grupu u odnosu na slaganje funkcija. Ako su ove permutacije date sa

$n = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $p_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, $p_2 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, $p_3 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$, $q_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$,

$q_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, *tada je* $F = \begin{pmatrix}i & f_1 & f_2 & f_3 & g_1 & g_2\\ n & p_1 & p_2 & p_3 & q_1 & q_2\end{pmatrix}$ *izomorfizam, pa je G grupa.*

Grupoid G dat narednom tablicom je komutativan akko je simetričan u odnosu na glavnu dijagonalu. Kako ovaj nije simetričan, to G nije Abel-ova grupa.

	... x ... y ...
x	xy
⋮	
y	yx
⋮	

Napomena: Grupe b) i e) su ciklične, redom C_4, C_6. Grupa c) je Klein-ova četvorna grupa, u oznaci V, grupa d) je grupa permutacija S_3, dok je grupa f) grupa kvaterniona.

2.4. Dokazati da je $(S,\cdot)$ grupa ako je $\cdot$ množenje realnih brojeva:

a) $S = \{a + b\sqrt{2} \mid a,b \in Q,\ a^2 + b^2 \neq 0\}$,

b) $S = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a,b,c \in Q,\ a^2 + b^2 + c^2 \neq 0\}$.

Rešenje: b) Grupoidnost: Neka su $x,y \in S$, $x = a_1 + b_1\sqrt[3]{2} + c_1\sqrt[3]{4}$, $y = a_2 + b_2\sqrt[3]{2} + c_2\sqrt[3]{4}$, gde $a_i,b_i,c_i \in Q$, $a_i^2 + b_i^2 + c_i^2 \neq 0$. Tada

$xy = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, *gde*

$$a = a_1a_2 + 2b_1c_2 + 2b_2c_1,\quad b = a_1b_2 + a_2b_1 + 2c_1c_2,\quad c = a_1c_2 + b_1b_2 + a_2c_1 \ . \qquad (1)$$

Jasno je da $a,b,c \in Q$. Dokazujemo da je $a^2 + b^2 + c^2 \neq 0$, tj. bar jedan od a,b,c je različit od 0. Prethodno dokazujemo sledeće tvrdjenje:

Ako su $a,b,c \in Q$ i $s = \sqrt[3]{2}$ tada: $(a + bs + cs^2 = 0) \Leftrightarrow (a = 0 \wedge b = 0 \wedge c = 0)$ (2)

Dokaz dela ($\Leftarrow$) ovog tvrdjenja je trivijalan pa dokazujemo ($\Rightarrow$). Iz $a+bs+cs^2=0$ sledi $a^3+2b^3+4c^3+3a^2bs+3ab^2s^2=0$, odakle koristeći $a+bs=-cs^2$

$$a^3+2b^3+4c^3-6abc=0 \qquad (3)$$

Kako su $a,b,c\in Q$ za neke $p_a,p_b,p_c\in Z$, $q_a,q_b,q_c\in N$ važi $a=p_a/q_a$, $b=p_b/q_b$, $c=p_c/q_c$. Prema (3) sledi

$$x^3+2y^3+4z^3=6xyz\ , \qquad (4)$$

gde $x=p_aq_bq_c$, $y=p_bq_aq_c$, $z=p_cq_aq_b$.

Dokazujemo da su sva rešenja Diofantovske jednačine

$$x^3+2y^3+4z^3=6xyzu \qquad (5)$$

upravo $(0,0,0,r)$, $r\in\omega$. Pretpostavimo suprotno, da postoje $x,y,z\in\omega$ koji nisu svi 0 i zadovoljavaju (5). Neka je $n\in\omega$ najveći takav da $2^n \mid x,y,z$ i neka su $x=2^nx_1$, $y=2^ny_1$, $z=2^nz_1$. Prema (5) sledi $x_1^3+2y_1^3+4z_1^3=6x_1y_1z_1u$ i bar jedan od x_1,y_1,z_1 je neparan. Dalje, na osnovu poslednje jednakosti neposredno sledi $2 \mid x_1^3$, pa $2 \mid x_1$. Uzimajući $x_1=2x_2$ dobija se $y_1^3+2z_1^3+4x_2^3=6x_2y_1z_1u$, odakle $2 \mid y_1^3$, tj. $2 \mid y_1$. Slično se izvodi da $2 \mid z_1$, što je u kontradikciji sa činjenicom da nisu svi x_1,y_1,z_1 deljivi sa 2. Prema tome, tvrdjenje (2) je dokazano.

Na osnovu prethodnog iz $a_1^2+b_1^2+c_1^2\neq0$ sledi $x,y\neq0$, pa $xy\neq0$, odakle $a+bs+cs^2\neq0$, tj. $a^2+b^2+c^2\neq0$.

<u>Asocijativnost</u> važi za množenje realnih brojeva, stoga važi i na skupu S.

<u>$1\in S$</u> jer $1=1+0\cdot\sqrt[3]{2}+0\cdot\sqrt[3]{4}$.

<u>Postojanje inverznog elementa</u>: Razmotrimo jednačinu

$$(a_1+b_1s+c_1s^2)(a_2+b_2s+c_2s^2)=1 \qquad (6)$$

po nepoznatim a_2,b_2,c_2. Kako je $x_1+y_1s+z_1s^2=x_2+y_2s+z_2s^2$ akko $(x_1-x_2)+(y_1-y_2)s+(z_1-z_2)s^2=0$ akko $x_1-x_2=0$, $y_1-y_2=0$, $z_1-z_2=0$, to na osnovu (1) jednačina (6) ekvivalentna je sa sledećim sistemom jednačina

$$a_1a_2+2c_1b_2+2b_1c_2=1,\quad b_1a_2+a_1b_2+2c_1c_2=0,\quad c_1a_2+b_1b_2+a_1c_2=0\ . \qquad (7)$$

Ovo je sistem linearnih jednačina po a_2,b_2,c_2 sa determinantom $D=a_1^3+2b_1^3+4c_1^3-6a_1b_1c_1$. Kako je $a_1^2+b_1^2+c_1^2\neq0$, to na osnovu ranijeg razmatranja $D\neq0$, pa sistem (7) ima jedinstvena rešenja; ona su $a_2=(a_1^2-2b_1c_1)/D$, $b_2=(a_1b_1-2c_1^2)/D$, $c_2=(b_1^2-a_1c_1)/D$. Primetimo da su ova rešenja racionalni brojevi i bar jedan od a_2,b_2,c_2 je različit od 0. Otuda svaki $x\in S'$ ima inverzni element.

<u>Napomena</u>: Tvrdjenjem (2) se ustvari iskazuje da $\sqrt[3]{2}$ nije koren kvadratnog polinoma u polju racionalnih brojeva. Inače, ovo tvrdjenje neposredno sledi na osnovu nesvodljivosti polinoma x^3-2 u polju racionalnih brojeva.

2.5.Neka je n prirodan broj i $S=\{m\in N \mid (m,n)=1,\ m<n\}$ ((m,n)=1 označava da su m i n uzajamno prosti). Dokazati da je $(S,\cdot_n)$ grupa, gde je $\cdot_n$ množenje po modulu n.

Rešenje: Množtvo S je skup svih invertibilnih elemenata prstena $\underline{Z}_n=(Z_n,+_n,\cdot_n)$ *(videti poglavlje o brojevima), pa je* $(S,\cdot_n)$ *grupa.*

2.6.Neka je S_X skup svih permutacija skupa X i $\circ$ slaganje funkcija. Dokazati da je $(S_X,\circ)$ grupa.

Rešenje: Ako su $f,g : X \xrightarrow[1-1]{na} X$ *tada takodje* $f\circ g : X \xrightarrow[1-1]{na} X$, *pa je* $(S_X,\circ)$ *grupoid. Slaganje preslikavanja je asocijativno. Identička funkcija* I_X *skupa X je jedna permutacija skupa X. Za* $f\in S_X$, $f^{-1}=\{(x,y) \mid (y,x)\in f\}$ *i važi* $f\circ f^{-1}=f^{-1}\circ f=I_X$.

2.7.Neka je G grupoid i Aut G skup svih automorfizama grupoida G. Dokazati da je (Aut G ,$\circ$) grupa, gde je $\circ$ slaganje funkcija.

Rešenje: Dokazati - ako su $f,g : G \tilde{\to} G$ *tada* $f\circ g : G \tilde{\to} G$ *tj. f∘g je homomorfizam i* $f\circ g : G \xrightarrow[1-1]{na} G$.
Takodje, ako je $f\in$ Aut G *tada* $f^{-1}\in$ Aut G . *Zaista, neka je* $f\in$ Aut G , $x,y\in G$ *i* $z=f^{-1}(xy)$. *Kako je f na , za neke* $a,b\in G$ *je* $x=f(a)$, $y=f(b)$ *pa* $z=f^{-1}(f(a)f(b))=f^{-1}(f(ab))=ab=f^{-1}(x)f^{-1}(y)$.

2.8.Dokazati da je $(Z\times Q,*)$ grupa, gde je $(x,y)*(u,v)=(x+u,2^u y+v)$.

2.9.Neka je S_a kvadratna matrica reda n oblika

$$\begin{bmatrix} a & a & \dots & a \\ a & a & \dots & a \\ \dots & \dots & \dots & \dots \\ a & a & \dots & a \end{bmatrix}$$

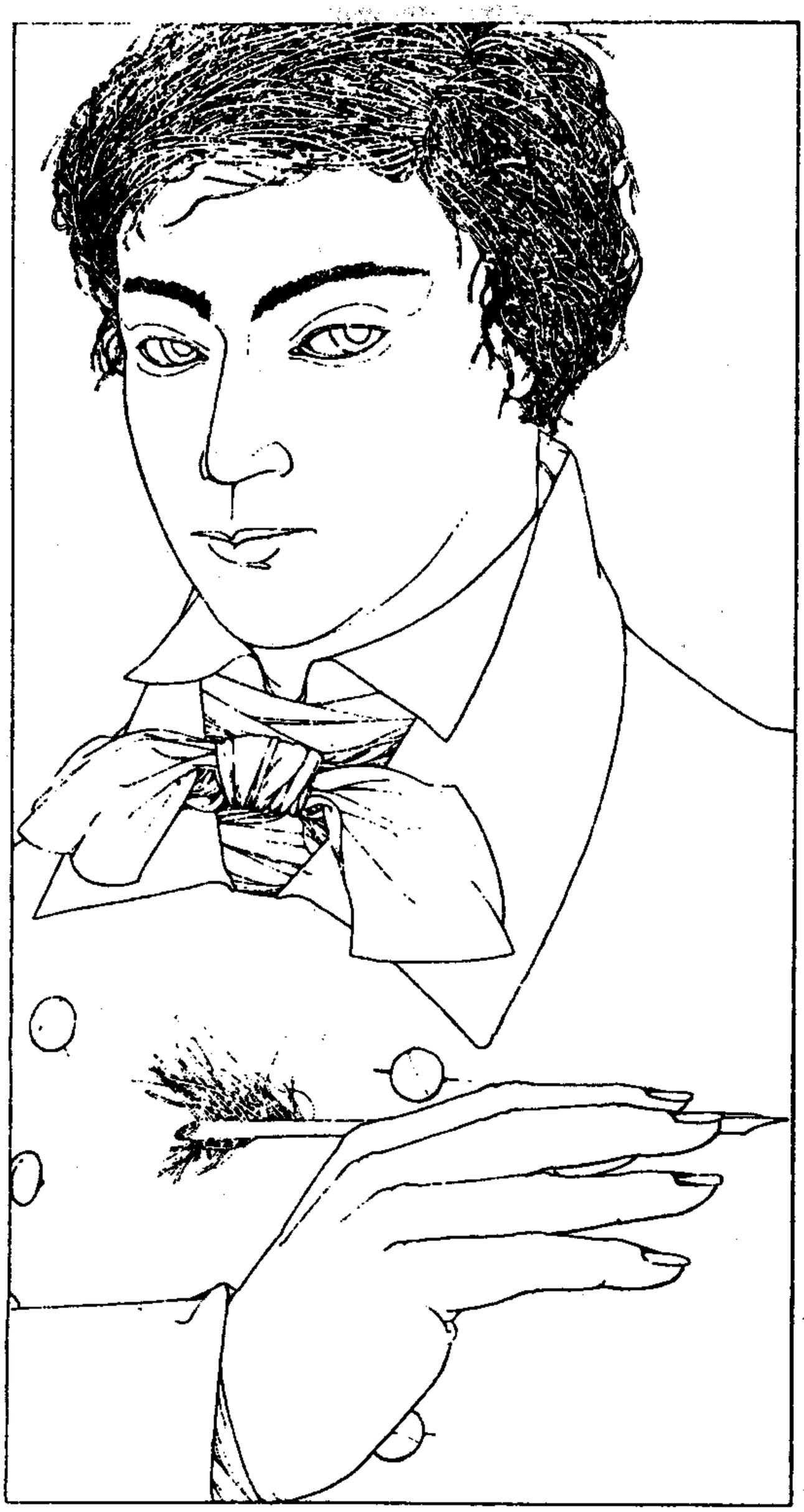
gde $a\in R$. Ako je $X=\{S_a \mid a\in R,\ a\neq 0\}$ dokazati da je $(X,\cdot)$ grupa, gde je $\cdot$ množenje matrica.

Rešenje: Lako se proverava da je $S_a S_b=S_{nab}$. *Dakle* $(X,\cdot)$ *je asocijativni grupoid, budući da je množenje matrica asocijativno. Jedinični element ove grupe je matrica* $S_{1/n}$ *dok je inverzni za* S_a *matrica* S_{1/n^2a}.

Napomena: Preslikavanje $F : R\setminus\{0\} \to X$ *definisano sa* $F(a)=S_{a/n}$ *je jedan izomorfizam grupa* $(R\setminus\{0\},\cdot)$ *i* $(X,\cdot)$.

2.10.Neka je $S=\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \mid a,b\in Q;\ a+b\sqrt{2}>0\}$. Dokazati da je $(S,\cdot)$ grupa, gde je $\cdot$ množenje matrica.

Rešenje: Grupoid $(S,\cdot)$ *izomorfan je grupi* Aut A , *gde je* $A=(Q(\sqrt{2}),+,<)$, $Q(\sqrt{2})=\{x+y\sqrt{2} \mid x,y\in Q\}$.



Crtež David A. Johnsona prikazuje
E. Galoisa u dobi od 17 godina
(Scientific American, April 1982)

2.11. Neka je X polje skupova[1]. Dokazati da je (X,Δ) Abel-ova grupa, Δ je simetrična razlika skupova.

Rešenje: Kako je $x \Delta y = (x \setminus y) \cup (y \setminus x)$, *to je* (X,Δ) *grupoid. Operacija* Δ *je asocijativna, što se može ustanoviti, na primer, na osnovu* $a \in (x \Delta y) \Leftrightarrow (a \in x \veebar a \in y)$ *i tautologije* $(p \veebar q) \veebar r \Leftrightarrow p \veebar (q \veebar r)$[2] *Svaki element je inverzan samom sebi, budući da važi* $x \Delta x = \emptyset$. *Jedinica je* $\emptyset$ *jer* $x \Delta \emptyset = \emptyset \Delta x = x$.

2.12. Dokazati da je $(S,\cdot)$ grupa, gde je $S=\{x \in C \mid (\exists n \in \omega) x^{p^n}=1\}$, C je skup kompleksnih brojeva, p prost broj, a $\cdot$ množenje kompleksnih brojeva

Rešenje: Grupoidnost: neka su $x,y \in S$. *Tada za neke* $n,m \in \omega$, $x^{p^m}=1$, $y^{p^n}=1$, *odakle* $(xy)^{p^{m+n}}=(x^{p^m})^{p^n} \cdot (y^{p^n})^{p^m}=1 \cdot 1=1$.

Asocijativnost sledi na osnovu asocijativnosti množenja kompleksnih brojeva.

Očito $1 \in S$. *Ako je* $x \in S$, *tj.* $x^{p^n}=1$ *za neki n, tada takodje* $(1/x)^{p^n}=1$, *dakle inverzni za x je* $1/x$.

2.13. Neka je p prost broj i $Z(p^\infty)=\{\frac{m}{p^n}+Z \mid m,n \in \omega,\ n>1,\ 0<m<p^n\}$ [3]

Dokazati da je $\underline{Z}(p^\infty)=(Z(p^\infty),\dot{+})$ Abel-ova grupa, ako je

$$(\frac{m}{p^n}+Z) \dot{+} (\frac{s}{p^r}+Z) \overset{def}{=\!=} (\frac{m}{p^n}+\frac{s}{p^r})+Z.$$ [4]

Rešenje: Dokazujemo da je $(Z(p^\infty),+)$ *grupoid. Neka su* $x,y \in Z(p^\infty)$, *gde* $x=r/p^m+Z$, $y=s/p^n+Z$. *Pretpostavimo* $p^m<p^n$. *Tada* $x+y=(r/p^m+s/p^n)+Z$. *Dalje,* $r/p^m+s/p^n=(rp^{n-m}+s)/p^n$. *Neka su* $k,t \in \omega$ *takvi da* $rp^{n-m}+s=kp^n+t$, $0<t<p^n$. *Tada* $x+y=(kp^n+t)/p^n+Z=(t/p^n+k)+Z=t/p^n+(k+Z)=t/p^n+Z$, *jer* $k+Z=Z$. *Dalje, operacija* $\dot{+}$ *je dobro definisana. Zaista neka je* $r/p^m+Z=s/q^n+Z$, $a/u^i+Z=b/v^j+Z$. *Za neke* $x,y \in Z$ *je* $r/p^m-s/q^n=x$, $a/u^i-b/v^j=y$, *odakle* $(b/v^j+Z)+(s/q^n+Z)=(b/v^j+s/q^n)+Z=$ $(r/p^m+a/u^i+x+y)+Z=(r/p^m+a/u^i)+Z$. *Neutralni element ove grupe je Z.*

---

[1] Neprazno mnoštvo skupova X je *polje skupova* ukoliko je zatvoreno u odnosu na skupovne operacije $\cup, \cap, \setminus$.

[2] $\veebar$ je ekskluzivna disjunkcija.

[3] $x+Z=\{x+y \mid y \in Z\}$.

[4] Ova grupa je tzv. *Prüfer-ova* p- grupa.

2.14.Dokazati da u D_n važi $\rho^i\sigma=\sigma\rho^{-i}$, $i\in N$.

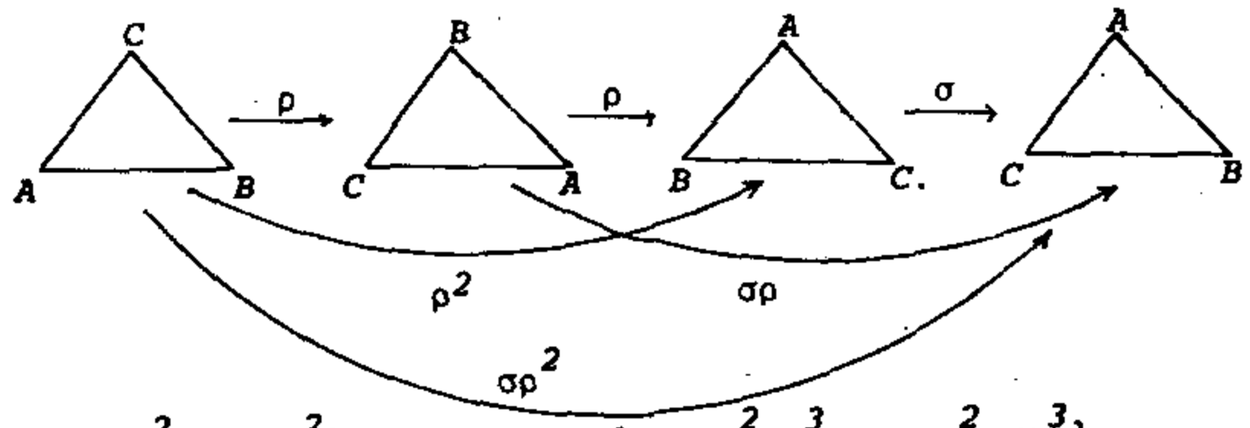
Rešenje: $\rho^i\sigma=\rho^{i-1}\rho\sigma=\rho^{i-1}\sigma\rho^{n-1}=\rho^{i-1}\sigma\rho^{-1}=\ldots=\sigma(\rho^{-1})^i=\sigma\rho^{-i}$

2.15.Dokazati da je $|D_n|=2n$.

Rešenje: $D_n=\{1,\rho,\rho^2,\ldots,\rho^{n-1},\sigma,\sigma\rho,\ldots\ \ \ \ ^{n-1}\}$. *Kako je* $r(\rho)=n$, $r(\sigma)=2$, *lako se pokazuje da su nabrojani elem* *i različiti.*

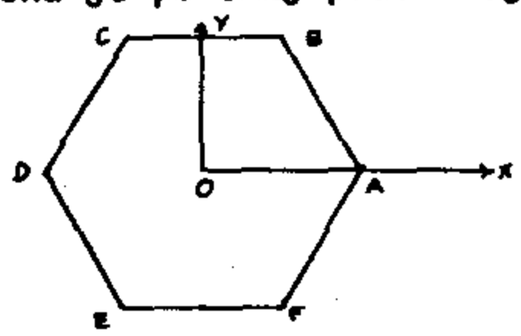
2.16.Odrediti grupe D_3 i D_4.

Rešenje:



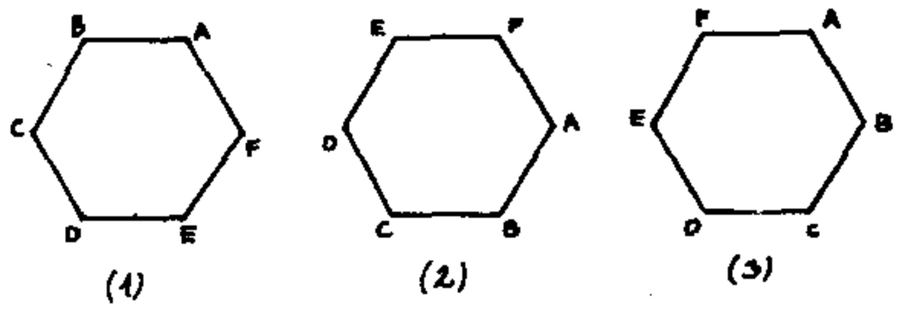
Dakle, $D_3=\{1,\rho,\rho^2,\sigma\rho,\sigma\rho^2\}$, $D_4=\{1,\rho,\rho^2,\rho^3,\sigma\rho,\sigma\rho^2,\sigma\rho^3\}$.

2.17.Neka je položaj pravilnog šestougla ABCDEF u ravni xOy kao na slici:



Dokazati da skup svih rotacija u (tro-dimenzionalnom) prostoru oko osa Ox, Oy i Oz, koje preslikavaju šestougao na sebe, čini grupu.

Rešenje: Sve tražene rotacije su: I, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b, gde je a rotacija oko ose Oz za ugao $\pi/3$ a koja dovodi dati šestougao u položaj (1);



b je rotacija koja dovodi šestougao iz početnog položaja u položaj (2), tj. to je rotacija oko ose Ox za ugao π.

Ako su p,q dve rotacije tada je pq kompozicija preslikavanja p i q. Tako, na primer, rotacija ab dovodi šestougao iz početnog položaja u položaj (3). Neka je S skup navedenih permutacija a $\cdot$ slaganje preslikavanja. Tada je $(S,\cdot)$ grupa, budući da je I jedinični element, važi zakon asocijacije za slaganje funkcija i svaki element ima inverzni; na primer, $a^{-1}=a^5$, $b^{-1}=b$, $(ab)^{-1}=ba^5=ab$. Primetimo da za elemente a,b važi $a^6=I$, $b^2=I$, $ba=a^5b$. Ova grupa je grupa simetrije pravilnog šestougla, tj. dijedarska grupa D_6.

2.18.Dokazati ekvivalenciju: $n \mid m \Leftrightarrow D_n \subseteq D_m$.

Rešenje: ($\Rightarrow$) Pretpostavimo $n \mid m$ *i neka je* $D_m = \langle \sigma, \rho \rangle$, $\sigma^2=1$, $\rho^m=1$. *Za neki k je* $m=nk$ *pa je* $\langle \sigma, \tau \rangle_{D_m}$ *grupa* D_n, *gde je* $\tau=\rho^k$. *Primetimo da je* $r(\tau)=n$ *i (prema zad. 2.14.),* $\tau\sigma=\rho^k\sigma=\sigma\rho^{-k}=\sigma\tau^{-1}=\sigma\tau^{n-1}$.
($\Leftarrow$) Neka je $D_n \subseteq D_m$. *Tada prema Lagrange-ovoj teoremi* $|D_n|$ *deli* $|D_m|$ *tj.* $2n \mid 2m$, *odakle* $n \mid m$.

2.19.Odrediti broj s elemenata reda 2 u D_n.

Rešenje: Ako je $n \in 2N+1$ *onda* $s=n$ *(pravilan n-tougao ima n osa simetrije).*
Ako je $n \in 2N$ *onda* $s=n+1$ *(pravilan n-tougao ima n osa simetrije i jedan centar simetrije).*

2.20.Dokazati: a) $x \in D_n \Rightarrow r(x)=2 \vee r(x) \mid n$,
b) $k \in \{1,2\} \vee k \mid n \Rightarrow (\exists x \in D_n) r(x)=k$.

Rešenje: Svaki $x \in D_n$ *je refleksija (dakle reda 2) ili pripada cikličnoj podgrupi rotacija* $\langle \rho \rangle_{D_n}$.

2.21.Neka su $m,n \in Z \setminus \{0\}$, A(m) i B(m) podgrupe grupe $\underline{Q}=(Q,+)$ definisane sa $A(m)=\langle \frac{1}{m} \rangle$, $B(m)=\langle \frac{1}{m}, \frac{1}{m^2}, \frac{1}{m^3}, \ldots \rangle$ i neka je $m=p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ razlaganje broja m na proste faktore. Dokazati:

a) $A(-m) = A(m)$, $B(-m) = B(m)$,
b) $A(m) = A(p_1^{n_1}) + \ldots + A(p_k^{n_k})$, $B(m) = B(p_1) + \ldots + B(p_k)$,
gde je $X + Y = \{x+y \mid x \in X, y \in Y\}$
c) $B(m) = A(m) + \frac{1}{m} A(m) + \frac{1}{m^2} A(m) + \ldots$
d) $B(mn) = B(m)B(n)$, $A(mn) = A(m)A(n)$
e) Ako je H konačno generisana podgrupa grupe Q, tada $(\exists m \in N)\ H = A(m)$
f) $(m,n)=1 \Leftrightarrow A(m) \cap A(n) = Z$, $(m,n)=1 \Rightarrow B(m) \cap B(n) = Z$
g) $A(m) \subseteq B(m)$
h) $m \mid n \Leftrightarrow A(m) \subseteq A(n)$, $m \mid n \Rightarrow B(m) \subseteq B(n)$
i) $A(m) \cap A(n) = A(k)$, $k = NZD(m,n)$

2.3. PODGRUPE

3.1. Definicija: Podgrupa grupe $G=(G,\cdot,e)$ je svaki podskup $H\subseteq G$ takav da $e\in H$ i u odnosu na restrikciju $*$ operacije $\cdot$ na H, struktura $(H,*,e)$ jeste grupa.

Ukoliko je H podgrupa grupe G tada koristimo oznaku $H<G$.
Nadalje, u skladu sa dogovorom u uvodu, umesto G pišemo samo G, i shodno tome $H<G$.

Red grupe G je $|G|$.
Levi *razred* ili *koset* podgrupe H grupe G je svaki skup oblika
$aH=\{ah \mid h\in H\}$, $a\in G$. Slično se definiše desni razred Ha. Napominjemo da je moguće govoriti o razredima bilo kojeg skupa X, recimo $aX=\{ax \mid x\in X\}$.

3.2. Teorema (Lagrange): Neka je $H<G$. Tada važi
(i) $\mathcal{H}=\{aH \mid a\in G\}$ je jedno razbijanje skupa G,
(ii) Za svaki $a\in G$ $|aH|=|H|$,
(iii) Ako je G konačna grupa tada $|H| \mid |G|$, tj. red podgrupe H deli red grupe G.

Dokaz: (i) Neka je $\sim$ relacija skupa G definisana sa $x\sim y \Leftrightarrow x^{-1}y\in H$. Prema zadatku 3.6. $\sim$ je relacija ekvivalencije skupa G i klasa ekvivalencije elementa $a\in G$ je aH. Dakle, $G/\sim=\mathcal{H}$ i $\mathcal{H}$ je particija (ili razbijanje) skupa G.
(ii) Neka je $f: H\to aH$ preslikavanje definisano sa $f(x)=ax$. Očigledno, f je na. Dalje, ako je $f(x)=f(y)$ onda $ax=ay$, odakle sledi $x=y$, tj. f je 1-1.
(iii) Kako je $\mathcal{H}$ particija skupa G, to postoji neki skup indeksa I i $a_i\in G$ $(i\in I)$ tako da za $i\neq j$ $a_iH\cap a_jH=\emptyset$ i $\mathcal{H}=\{a_iH \mid i\in I\}$. Dakle, G je disjunktna unija skupova a_iH, $i\in I$, odakle sledi $|G|=\sum_{i\in I}|a_iH|$. Prema (ii) je $|a_iH|=|H|$, pa $|G|=|I|\cdot|H|$. ▼

Neka je $\mathcal{H}$ particija iz prethodne teoreme. *Indeks* podgrupe H u grupi G je $|\mathcal{H}|$. Za indeks se koristi oznaka $|G:H|$. Dakle $|G:H|$ je broj levih (desnih) razreda podgrupe H u G. Prema Lagrange-ovoj teoremi važi jednakost

$$|H|\cdot|G:H|=|G|$$

pa prema tome i indeks podgrupe H takodje deli red grupe G.

Ako je $S \subseteq G$ tada S određuje najmanju podgrupu H koja sadrži S; to je $H = \bigcap \{K \mid S \subseteq K < G\}$. U takvom slučaju S se naziva skupom *generatora* grupe H, i koristi se oznaka $H = \langle S \rangle_G$ [1)]

3.3. *Teorema:* *Neka je H podgrupa grupe G generisana skupom S. Tada je*

$$H = \{s_1^{\alpha_1} s_2^{\alpha_2} \ldots s_n^{\alpha_n} \mid n \in \omega;\ s_1, \ldots, s_n \in S;\ \alpha_1, \ldots, \alpha_n \in Z\}. \quad (1)$$

Dokaz: Neka je A skup na desnoj strani jednakosti (1). Neposredno se proverava da je $A < G$ i $S \subseteq A$, dakle $H \subseteq A$. S druge strane, svaka podgrupa K grupe G koja sadrži S očito sadrži A, pa je

$A \subseteq \bigcap \{K \mid S \subseteq K < G\}$, tj. $H \subseteq A$. ▼

U svakoj grupi G mogu se uočiti izvesni važni primeri podgrupa, koje se definišu na sledeći način:

3.4. *Definicija:* *(i) Centar grupe G je* $Z(G) = \{x \in G \mid (\forall y \in G)\ xy = yx\}$.

(ii) Ako su $x, y \in G$, *element* $x^{-1}y^{-1}xy$ *naziva se komutatorom elemenata x, y i označava se sa* $[x, y]$. *Komutant grupe G je grupa G′ generisana skupom* $\{[x, y] \mid x, y \in G\}$.

(iii) Neka je $A \subseteq G$. *Centralizator skupa A (u G) je*

$$C(A)_G = \{x \in G \mid (\forall a \in A)\ ax = xa\}$$ [1)].

(iv) Normalizator skupa A u G je $N(A)_G = \{x \in G \mid xA = Ax\}$ [1)].

Neposredno se proverava da su Z(G), G′, C(A) i N(A) podgrupe grupe G. Za centralizator C({a}) i normalizator N({a}) elementa $a \in G$, koristimo redom oznake C(a), N(a).

Primeri i zadaci

3.1. Neka je $G = (G, \cdot)$ grupa. a) Dokazati ekvivalenciju

$$\text{H je podgrupa grupe } G \iff \begin{array}{l}\text{(i) } H \subseteq G,\ H \neq \emptyset \\ \text{(ii) } (\forall x, y)(x, y \in H \to xy^{-1} \in H)\end{array}$$

b) Da li se uslov (ii) može zameniti nekim od sledećih uslova:

1° $(\forall x, y)(x, y \in H \Rightarrow xy \in H)$, 2° $(\forall x, y)(x, y \in H \Rightarrow x^{-1}y \in H)$.

3° $(\forall x, y)(x, y \in H \Rightarrow xyx^{-1}y^{-1} \in H)$?

Rešenje: a) *($\Rightarrow$) Ako je $H < G$, tada je (i) ispunjeno po definiciji podgrupe. Jedan dokaz za (ii) je sledeći implikacijski lanac*

$$a, b \in H \Rightarrow a \in H,\ b^{-1} \in H \Rightarrow ab^{-1} \in H$$

($\Leftarrow$) Dokazujemo da je $(H, \cdot)$ grupa, tj. da važi: $e \in H$, za svaki $a \in H$ posto-

---

1) Indeks G se izostavlja ukoliko je jasno o kojoj je grupi reč.

ji $a^{-1}\in H$ *i operacija* $\cdot$ *je zatvorena i asocijativna u H. Zaista:*
zbog (i), u H postoji bar jedan element a, pa je

$$a\in H \Rightarrow aa^{-1}\in H \Rightarrow e\in H\ ;$$

$$a\in H \Rightarrow a\in H,\ e\in H \Rightarrow ea^{-1}\in H \Rightarrow a^{-1}\in H\ ;$$

$$a\in H,\ b\in H \underset{②}{\Rightarrow} a\in H,\ b^{-1}\in H \overset{①}{\Rightarrow} a(b^{-1})^{-1}\in H \Rightarrow ab\in H\ ;$$

operacija $\cdot$ *je asocijativna u H jer je asocijativna u G.*

① *koristeći da je* $e\in H$

② *koristeći prethodno dokazano:* $a\in H \Rightarrow a^{-1}\in H$

b) Uslov (ii) iz a) se ne može zameniti uslovom 1° (kojim je obezbedjena samo zatvorenost operacije $\cdot$*) kao ni uslovom 3°, dok se može zameniti uslovom 2°.*

3.2.Neka je u grupi $\underline{G}=(G,\cdot)$ H konačan neprazan podskup. Dokazati:
a) $H<G$ akko $H\cdot H=H$, b) ako je $(H,\cdot)$ grupoid, tada je $H<G$,
c) $H<G$ akko $H\cdot H\subseteq H$.

Rešenje: a) $HH=\{h \mid (\exists h_1,h_2\in H)\ h=h_1h_2\}$
($\Rightarrow$*) Neka je* $H<G$*; tada*

$$h\in HH \Rightarrow (\exists h_1,h_2\in H)\ h=h_1h_2 \underset{①}{\Rightarrow} h\in H\ ,\quad \text{odakle}\quad HH\subseteq H;$$

$$h\in H \underset{2}{\Rightarrow} h\in H,\ e\in H \Rightarrow he\in HH \Rightarrow h\in HH\ ,\quad \text{odakle}\quad H\subseteq HH;$$

dakle, $HH=H$.

① *jer* $H<G$

② $e\in H$ *jer* $H<G$

($\Leftarrow$*)* $HH=H$
Neka je $H=\{h_1,h_2,\ldots,h_n\}$*, gde su* $h_1,\ldots,h_n$ *medjusobno različiti elementi. Ako je* $g\in H$*, tada* $h_1g,h_2g,\ldots,h_ng\in HH$*, tj. zbog* $HH=H$ $h_1g,\ldots,h_ng\in H$*. Elementi* $h_1g,\ldots,h_ng$ *su medjusobno različiti (jer važe zakoni skraćivanja, tj. iz* $h_ig=h_jg$ *sledi* $h_i=h_j$*) pa su skupovi* $\{h_1,\ldots,h_n\}$ *i* $\{h_1g,\ldots,h_ng\}$ *jednaki. Otuda, element g koji je u H, pripada i drugom skupu, tj.*
$(\exists h_i\in H)\ h_ig=g$ *; ili, za neki* h_i, $h_i=e$, *odnosno* $e\in H$.
Dalje, neka je $h\in H$*; kako* $e\in H$ *biće:* $(\exists h_j\in H)\ h_jh=e$, *tj.* $h^{-1}\in H$.
Dakle, $H<G$.
b) $(H,\cdot)$ *je grupoid i* $H\subseteq G$*; dakle,* $\cdot$ *je zatvorena i asocijativna operacija u H. Dalje se, isto kao u a), dokazuje da* $e\in H$ *i da za svaki* $a\in H$ *i* $a^{-1}\in H$.

3.3.Neka je u grupi $\underline{G}=(G,\cdot)$, $H<G$ i $H\neq G$. Dokazati da je $\langle G\setminus H\rangle = G$.

Rešenje: Neka $a\in G\setminus H$ *i* $h\in H$. *Tada* $ha\in H$ *ili* $ha\in G\setminus H$. *Ako je* $ha\in H$ *tada* $h^{-1}(ha)\in H$, *tj.* $a\in H$ *što je kontradikcija jer* $a\notin H$. *Stoga* $ha\in G\setminus H$, *tj. postoji* b, $b\in G\setminus H$ *tako da je* $ha=b$, *tj.* $h=ba^{-1}$. *Kako je* $G=H\cup(G\setminus H)$, *ovim je tvrdjenje dokazano.*

3.4.Neka je H podgrupa grupe G. Dokazati:

a) $x^{-1}Hx$ je takodje podgrupa u G, ako je x proizvoljni element iz G,

b) $H^{-1}=H$, c) $H\cdot H=H$.

Rešenje: a) Neka je $H<G$ *i neka su* $a,b\in H$. *Tada*

$$x^{-1}ax\in x^{-1}Hx,\ x^{-1}bx\in x^{-1}Hx \underset{①}{\Rightarrow} (x^{-1}ax)(x^{-1}bx)\in x^{-1}Hx$$

$$e\in H \Rightarrow x^{-1}ex\in x^{-1}Hx \Rightarrow e\in x^{-1}Hx$$

$$x^{-1}ax\in x^{-1}Hx \underset{②}{\Rightarrow} (x^{-1}ax)^{-1}\in x^{-1}Hx$$

① *jer* $ab\in H$

② *jer* $a^{-1}\in H$, *tj.* $x^{-1}a^{-1}x\in x^{-1}Hx$

b) $H^{-1}=\{h^{-1}\mid h\in H\}$

$$a\in H^{-1} \Rightarrow (\exists h\in H)\ a=h^{-1} \underset{③}{\Rightarrow} a\in H$$

$$a\in H \Rightarrow a^{-1}\in H \Rightarrow (a^{-1})^{-1}\in H^{-1} \Rightarrow a\in H^{-1},$$

odakle $H=H^{-1}$. ③ $h^{-1}\in H$ *zbog* $H<G$

3.5.Odrediti sve podgrupe sledećih grupa:

a) Klein-ove grupe, b) S_3, c) C_{12}, d) $(Z,+)$, e) $(Q,+)$

Rešenje: b) Elementi grupe S_3 *su*

$$I=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad f=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad g=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

$$h=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\quad j=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad k=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

Uzimajući $1=I$, $a=f$, $b=g$ *imamo* $h=a^2$, $j=ba$, $k=ba^2$ *i važe sledeće jednakosti:* $a^3=1$, $b^2=1$, $(ab)^2=1$.

Po Lagrange-ovoj teoremi, prave podgrupe grupe S_3 *mogu biti reda 2 i 3; dakle, te podgrupe su ciklične. Stoga, za svaki od elemenata grupe* S_3 *ispitujemo da li je on generator grupe* C_2 *ili* C_3.

1 generiše trivijalnu podgrupu $E=\{1\}$;

$a^3=1$; *a generiše cikličnu podgrupu reda 3,* $H_1=\{1,a,a^2\}$;

$(a^2)^3=1$; a^2 *takodje generiše podgrupu* H_1;

$b^2=1$; *b generiše cikličnu podgrupu reda 2,* $H_2=\{1,b\}$;

$(ba)^2=1$ jer je $(ab)^2=1$, tj. $abab=1$ odakle $baba=1$; dakle ba generiše cikličnu podgrupu reda 2, $H_3=\{1,ba\}$;

$(ba^2)^2=1$ jer $baabaa=baba^2aa=baba=1$; znači ba^2 generiše $H_4=\{1,ba^2\}$.

Prema tome, S_3 ima šest podgrupa: trivijalne E i S_3, i prave H_1, H_2, H_3 i H_4.

c) Podgrupe C_{12} su: E, C_{12}, $H_1=\{1,a^6\}$, $H_2=\{1,a^4,a^8\}$, $H_3=\{1,a^3,a^6,a^9\}$, $H_4=\{1,a^2,a^4,a^6,a^8,a^{10}\}$.

d) Podskupovi $Zn=\{zn \mid z\in Z\}$ su podgrupe grupe $(Z,+)$ za sve $n\in N$. To su ciklične podgrupe generisane sa n.

Treba ispitati ima li $(Z,+)$ drugih podgrupa, različitih od navedenih.

Neka je $(H,+)$ proizvoljna netrivijalna podgrupa grupe $(Z,+)$: $H=\{z_1,z_2,\dots\}$.

Neka je z_i najmanji pozitivni broj iz H (takav broj postoji jer je H netrivijalna podgrupa, pa za svaki $z\in H$ postoji njemu inverzni $-z\in H$).

Tada, za $z\in H$ postoje prirodni brojevi k,r takvi da je

$$z=kz_i+r, \quad 0<r<z_i .$$

Odavde, $r=z-kz_i$ tj. $r\in H$ (jer $z\in H$ i $\underbrace{z_i+\dots+z_i}_{k}\in H$). Kako je $0<r<z_i$ i z_i je najmanji pozitivni broj iz H, sledi $r=0$, odnosno $z=kz_i$, pa otuda $H=Zz_i$. Dakle, svaka podgrupa je oblika Zn.

3.6. Ako su F i H podgrupe grupe $\underline{G}=(G,\cdot)$, dokazati da su sledeće relacije skupa G relacije ekvivalencije:

a) $x\rho y \Leftrightarrow xy^{-1}\in H$, b) $x\rho y \Leftrightarrow x^{-1}y\in H$,

c) $x\rho y \Leftrightarrow (\exists f\in F)(\exists h\in H)\ x=fyh$, d) $x\rho y \Leftrightarrow (\exists g\in G)\ y=g^{-1}xg$.

Odrediti odgovarajuće klase ekvivalencije.

Rešenje: a) $e\in H \Rightarrow (\forall x\in G)\ xx^{-1}\in H \Rightarrow (\forall x\in G)\ x\rho x$

$$x\rho y \Rightarrow xy^{-1}\in H \Rightarrow (xy^{-1})^{-1}\in H \Rightarrow yx^{-1}\in H \Rightarrow y\rho x$$

$$x\rho y \wedge y\rho z \Rightarrow xy^{-1}\in H \wedge yz^{-1}\in H \Rightarrow xy^{-1}yz^{-1}\in H \Rightarrow x\rho z$$

pa je ρ relacija ekvivalencije. Klase ekvivalencije su

$$C_x=\{y \mid y\rho x\}=\{y \mid yx^{-1}\in H\}=\{y \mid (\exists h\in H)\ y=hx\}=\{hx \mid h\in H\}=Hx$$

tj. za relaciju ρ klase ekvivalencije su desni razredi od H u G.

b) Slično, za ovako definisanu relaciju ρ, klase ekvivalencije su levi razredi od H u G.

d) $C_x=\{g^{-1}xg \mid g\in G\}$.

Napomena: ako je G konačna grupa, tada za svako $a\in G$ $|C_a|$ deli $|G|$.

3.7.Neka je $H<G$. Dokazati: a) $Hx=H$ akko $x\in H$,

b) $Hx=Hy$ akko $xy^{-1}\in H$; $xH=yH$ akko $x^{-1}y\in H$,

c) Svaka dva desna (leva) razreda od H u G se ili poklapaju ili nemaju zajedničkih elemenata,

d) Broj desnih razreda podgrupe H u G jednak je broju levih razreda od H u G.

Rešenje: Koriste se rezultati prethodnog zadatka.

a) $C_x=Hx$, $C_e=He=H$. *Takodje* $x\in C_x$.

Otuda, ako je $Hx=H$ *onda* $x\in H$.

Ako je $x\in H$ *tada* $C_x\cap C_e\neq\emptyset$ *tj.* $Hx=He$ *odnosno* $Hx=H$

b) Kako je $x\rho y \Leftrightarrow xy^{-1}\in H$, *to* $C_x=Hx$, $C_y=Hy$, *pa tvrdjenje sledi na osnovu* $x\rho y \Leftrightarrow C_x=C_y$.

c) Desni (odnosno levi) razredi su klase ekvivalencije relacije ρ *definisane u prethodnom zadatku pod a) (odnosno b)); stoga su oni ili disjunktni ili se poklapaju.*

d) Dosta je odrediti bar jedno 1-1 preslikavanje skupa svih desnih razreda od H u G, u skup odgovarajućih levih razreda. Jedno takvo preslikavanje je $f(Hx)=x^{-1}H$.

Zaista, $Hx=Hy$ *akko* $f(Hx)=f(Hy)$, *tj.* $x^{-1}H=y^{-1}H$ *jer prema b)*

$Hx=Hy$ *akko* $xy^{-1}\in H$, $x^{-1}H=y^{-1}H$ *akko* $xy^{-1}\in H$.

3.8.Presek familije podgrupa grupe G je takodje podgrupa u G. Dokazati.

Rešenje: Neka su $H_i<G$ $(i\in I)$, *i neka je* $H=\bigcap_{i\in I}H_i$. *Tada*

$$x,y\in H \Rightarrow (\forall i\in I)\ x,y\in H_i \Rightarrow (\forall i\in I)\ xy^{-1}\in H_i \Rightarrow xy^{-1}\in H,$$

odnosno, prema zadatku 3.1., $H<G$.

3.9.Dokazati da je (skupovna) unija dve podgrupe, podgrupa akko se jedna sadrži u drugoj.

Rešenje: Neka su $H<G$, $F<G$. *Tada* $H\cup F$, *u opštem slučaju, nije obavezno grupa; jer, ako* $a,b\in H\cup F$ *ne mora da bude* $ab^{-1}\in H\cup F$. *Dokažimo da je navedeni uslov u zadatku potreban i dovoljan da je* $H\cup F<G$.

($\Leftarrow$*) Očigledno*

($\Rightarrow$*) Neka je* $H\cup F<G$ *i neka, suprotno tvrdjenju, postoje elementi* $h\in H$, $f\in F$ *takvi da*

$$h\notin F,\quad f\notin H. \qquad (1)$$

Kako su $h,f\in H\cup F$, *a* $H\cup F<G$, *biće* $hf\in H\cup F$. *Ako* $hf\in H\cup F$ *tada:*

$hf\in H$; $h\in H$ *pa* $h^{-1}\in H$, *tj.* $h^{-1}hf\in H$ *odakle* $f\in H$

ili

$hf\in F$; $f\in F$ *pa* $f^{-1}\in F$, *tj.* $hff^{-1}\in F$ *odakle* $h\in F$

U oba slučaja dolazi se do kontradikcije u odnosu na (1).

3.10. Ako su H i F podgrupe grupe G, tada je $FH < G$ akko $FH = HF$. Dokazati.

Rešenje: ($\Rightarrow$) *Neka je* $FH < G$. *Koristeći zadatak 3.4.b) imamo*

$$HF = H^{-1}F^{-1} = (FH)^{-1} = FH$$

($\Leftarrow$) *Neka je* $HF = FH$. *Tada,*

grupoidnost: $(HF)(HF) = H(FH)F = H(HF)F = HHFF = HF$;

jedinični element: kako $e \in H$, $e \in F$, *to* $e \in HF$;

zatvorenost u odnosu na inverzni element: $(HF)^{-1} = F^{-1}H^{-1} = FH = HF$

3.11. Neka su F i H podgrupe konačne grupe $(G,\cdot)$. Dokazati:

a) $G = FH$ ili $|G| \geq |F| + |H|$,

b) $|F| \cdot |H| \leq |F \cap H| \cdot |F \vee H|$, gde je $F \vee H = \langle F \cup H \rangle$.

Rešenje: a) Pretpostavimo $FH \neq G$. *Tada* $F \neq G$, *pa kako po Lagrange-ovoj teoremi* $|F|$ *deli* $|G|$ *to je* $|G| > 2|F|$. *Slično* $|G| > 2|H|$, *odakle nalazimo* $2|G| > 2|F| + 2|H|$.

b) Neka je $f : F \times H \to G$ *preslikavanje definisano jednakošću* $f(x,y) = x \cdot y$. *Tada, očigledno* $f(F \times H) = FH$. *Relacija* $\sim$ *skupa* $F \times H$ *definisana sa*

$$(x,y) \sim (x',y') \Leftrightarrow f(x,y) = f(x',y')$$

je relacija ekvivalencije. Za $a,x \in F$ *i* $b,y \in H$ *je*

$$(x,y) \sim (a,b) \Leftrightarrow xy = ab \Leftrightarrow a^{-1}x = by^{-1} .$$

Kako $a^{-1}x \in F$, $by^{-1} \in H$, *to*

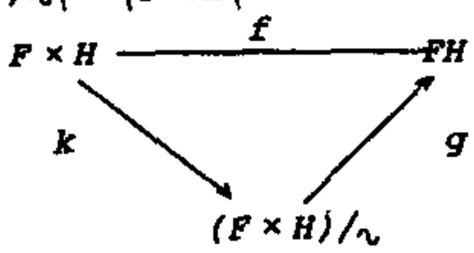
$$(x,y) \sim (a,b) \Rightarrow a^{-1}x,\ by^{-1} \in F \cap H$$

pa je klasa ekvivalencije para (a,b) :

$$(a,b)/_{\sim} = \{(ah, h^{-1}b) \mid h \in F \cap H\};$$

dakle, $|(a,b)/_{\sim}| = |F \cap H|$.

Dijagram



k je kanonsko preslikavanje komutira; f je <u>*na*</u> *i g je bijekcija.*

Otuda sledi $|FH| = |(F \times H)/_{\sim}| = |F \times H| / |F \cap H| = \frac{|F| \cdot |H|}{|F \cap H|}$, *jer svaka klasa ekvivalencije ima* $|F \cap H|$ *elemenata. Dalje,* $FH \subseteq F \vee H$, *pa* $|F| \cdot |H| / |F \cap H| \leq |F \vee H|$.

3.12. Dokazati da je presek podgrupa konačnog indeksa u grupi G, podgrupa takodje konačnog indeksa u G.

3.13. Opisati grupe koje imaju tačno jednu pravu podgrupu.

Rešenje: Neka je $(G,\cdot)$ *grupa koja ima tačno jednu pravu podgrupu H.*

Razrešimo prvo problem da li je G ciklična grupa.
Ako nije ciklična, tada za $x \in G \ (x \neq e)$, *ciklična podgrupa* $\langle x \rangle$ *generisana sa x jednaka je H. Kako to važi za svako* $x \in G$, *odavde* $G \subseteq H$, *tj. G je ciklična, suprotno pretpostavci.*
Dakle, G je ciklična grupa, tj. $G = \langle a \rangle$, *za neko* $a \in G$. *Odredimo red grupe G.*
Ako je $|G| = \infty$, *tada* $(G, \cdot) \simeq (Z, +)$, *tj. G ima beskonačno mnogo podgrupa. Prema tome, red je konačan. Neka je* $|G| = n$. *Ako je prirodni broj n takav da ima dva medjusobno različita delioca* $d_1, d_2 > 2$, *tada elementi* a^{n/d_1} *i* a^{n/d_2} *generišu dve različite podgrupe grupe G, reda* d_1 *i* d_2. *Stoga,* $n = p^2$. *p je prost broj.*

3.14. Okazati da beskonačna grupa ima beskonačno mnogo podgrupa.

Šenje: Neka je G beskonačna grupa. Ako je ona periodična, tj. svi elementi su joj konačnog reda, onda ona ima beskonačno mnogo podgrupa.
Ako nije periodična, znači da ima bar jedan element, a, beskonačnog reda. Za njega važi: $a^n \neq a^k$ *za svaka dva broja* $n, k \in Z$, $n \neq k$.
Stoga u podgrupi $\langle a \rangle$ *grupe G, postoje sledeće podgrupe*

$$H_n = \{ e, a^n, a^{2n}, \ldots, a^{-n}, a^{-2n}, \ldots \}, \quad n \in N$$

za koje važi

$$n_1 \neq n_2 \Rightarrow H_{n_1} \neq H_{n_2}$$

3.15. Neka je G grupa i $G_1, \ldots, G_n$ njene podgrupe. Ako je G konačna unija nekih koseta grupa $G_1, \ldots, G_n$, tada za neki $k \leq n$ važi: $|G : G_k| < \infty$.

Rešenje: Pretpostavimo da je za sve $k \leq n$ $|G : G_k| = \infty$ *i da je* $G = C_1^1 \cup \ldots \cup C_{m_1}^1 \cup C_1^2 \cup \ldots \cup C_{m_2}^2 \cup \ldots \cup C_1^n \cup \ldots \cup C_{m_n}^n$ *gde je* C_j^i *koset grupe* G_i. *Kako* $|G : G_1| = \infty$ *to postoji koset C grupe* G_1 *i* $C \neq C_j^1$, $j \leq m_1$.
Kako je $C \cap C_j^1 = \emptyset$ *za sve j i* $C \subseteq G$ *to je* $C \subseteq C_1^2 \cup \ldots \cup C_{m_n}^n$. *Za neki y je* $C = G_1 y$ *pa* $G_1 \subseteq C_1^2 y^{-1} \cup \ldots \cup C_{m_n}^n y^{-1}$. *Kako je za neke* x_j $C_j^1 = G_1 x_j$ *to onda* $G = \bar{C}_1^2 \cup \ldots \cup \bar{C}_{m_n}^n$, *tj. G je konačna unija koseta grupa* $G_2, \ldots, G_n$. *Ponavljajući ovaj postupak n-1 puta, sledi da je G konačna unija koseta grupe* G_n; *recimo,* $G = K_1^n \cup \ldots \cup K_{r_n}^n$ *pa* $|G : G_n| < \infty$, *suprotno pretpostavci.*
Dakle, za neki $i \leq n$ *je* $|G : G_i| < \infty$.

3.16. Ako je F polje, tada F nije konačna unija svojih pravih podpolja.

Rešenje: Neka je $F = K_1 \cup \ldots \cup K_n$, K_i *su podpolja od F.*
1° F je konačno: tada je multiplikativna grupa ciklična; neka je $F = \langle \alpha \rangle$. *Za neki i,* $\alpha \in K_i$ *pa* $F \subseteq K_i$.

2° F je beskonačno: prema 3.15., za neki $i<n$ $|F^+ : K_i^+|<\infty$, F^+ je aditivna grupa polja F. Tada je K_i takodje beskonačno. Neka je $a\in E\setminus K_i$. Ako je $k_1\neq k_2$ tada $K_1+k_1a\neq K_i+k_2a$, jer ako je $p+k_1a=q+k_2a$ za $p,q\in K_i$, onda $a\in K_i$ zbog $a=\frac{p-q}{k_2-k_1}$. Dakle, ima beskonačno mnogo kosета grupe K_i^+, tj. $|F^+ : K_i^+|=\infty$.
Otuda, ne postoji $a\in F\setminus K_i$, tj. $F=K_i$.

3.17. Neka su A,B,C<G. Dokazati: Ako je $A\subseteq B\cup C$ tada $A\subseteq B$ ili $A\subseteq C$.

Rešenje: Neka je $A\subseteq B\cup C$. Tada $A=(A\cap B)\cup(A\cap C)$, i $A\cap B$, $A\cap C<G$, pa prema zad. 2.3.9. sledi $A\cap B=A$ ili $A\cap C=A$.

2.4. RED ELEMENTA

4.1.Definicija: Red elementa a grupe G, u oznaci r(a), je red podgrupe H generisane elementom a.

Kako je $H=\{a^n \mid n\in Z\}$, to je $r(a)=|\{a^n \mid n\in Z\}|$. Element a je konačnog reda ukoliko je r(a) prirodan broj, inače je a beskonačnog reda.

Neposredna posledica Lagrange-ove teoreme o podgrupama je sledeće tvrdjenje:

4.2.Teorema: Ako je G konačna grupa i $a\in G$, tada red elementa a deli red grupe G.

Grupe kod kojih su svi elementi konačnog reda nazivaju se *periodičnim* ili *grupe sa torzijom*. Jedan primer periodične grupe je Prüfer-ova grupa $Z(p^\infty)$, p je prost broj.

Primeri i zadaci

4.1.Dokazati da su u grupi G sledeći elementi istog reda:
a) a i a^{-1}, b) a i $g^{-1}ag$ $(g\in G)$, c) ab i ba .

Rešenje: a) $(a^{-1})^{r(a)}=(a^{r(a)})^{-1}=e^{-1}=e \Rightarrow r(a^{-1})\leq r(a)$.
Otuda $r((a^{-1})^{-1})\leq r(a^{-1})$, tj. $r(a)\leq r(a^{-1})$, odakle $r(a)=r(a^{-1})$.
b) Slično, koristeći jednakost

$$(\forall a,g\in G)(\forall n\in N)(g^{-1}ag)^n=g^{-1}a^ng$$

treba odrediti $(g^{-1}ag)^{r(a)}$ i $a^{r(g^{-1}ag)}$.
c) Koristeći jednakost $ba=b(ab)b^{-1}$.

4.2.Neka je G konačna grupa reda n. Dokazati da važi:
a) $(\forall a\in G)\ r(a)\mid n$, b) $(\forall a\in G)\ a^n=e$.

Rešenje: a) Ako je red elementa $a\in G$ jednak k, tj.

$$\langle a\rangle = \{e,a,a^2,\ldots,a^{k-1}\}\ ,\ k\leq n$$

po teoremi Lagrange-a, $k\mid n$.

b) Neka je $r(a)=m$; koristeći a), $n=km$ pa je $a^n=a^{mk}=(a^m)^k=e$.

4.3.Neka je G Abel-ova grupa i neka su elementi $a,b\in G$ takvi da je $r(a)=n$, $r(b)=m$. Dokazati da r(ab) deli NZS(n,m).

Rešenje: Ako je $d=NZS(n,m)$ tada $m\mid d$ i $n\mid d$, dakle $(ab)^d=a^db^d=ee=e$. Dalje, neka je $u=r(ab)$. Prema prethodnom $u<d$. Neka je $d=ku+r$, $0\leq r<u$. Tada iz $(ab)^d=e$, $(ab)^u=e$ sledi $(ab)^r=e$, pa prema izboru broja u sledi $r=0$.

4.4.Neka je G grupa i neka su a i b njena proizvoljna dva elementa konačnog reda. Koliki je red elementa ab?

Rešenje: Neka su $a,b\in G$ takvi da je $r(a)=n$, $r(b)=m$. Prema prethodnom zadatku r(ab) deli NZS(n,m) ako su a,b iz Abel-ove grupe G. Dakle, ako su a i b komutativni elementi konačnog reda, i element ab je konačnog reda.

Postavlja se pitanje da li red elementa ab može biti beskonačan u slučaju $ab\neq ba$. Sledeći primer daje pozitivan odgovor.

Neka je M grupa matrica reda 2 nad poljem Q racionalnih brojeva. Elementi

$$a=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix} \quad i \quad b=\begin{bmatrix}0 & 1\\ -1 & -1\end{bmatrix}$$

su konačnog reda i to: $r(a)=4$, $r(b)=3$. Medjutim,

$$ab=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\ ,\ (ab)^2=\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}\ ,\ (ab)^3=\begin{bmatrix}1 & 3\\ 0 & 1\end{bmatrix}\ ,\ldots,\ (ab)^k=\begin{bmatrix}1 & k\\ 0 & 1\end{bmatrix}\ ,\ldots$$

odnosno $(\forall n\in N)(ab)^n\neq E$

4.5.Ako je red grupe G prost broj, tada je G ciklična grupa. Dokazati.

Rešenje: Neka je $|G|=p$, p je prost broj. Po teoremi Lagrange-a, G nema pravih podgrupa. Neka je $a\in G$, $a\neq e$. Ciklična podgrupa $\langle a\rangle$ generisana elementom a nije jedinična podgrupa (jer je $a\neq e$); dakle, $\langle a\rangle=G$.

4.6.Neka je f homomorfizam grupe G_1 u G_2. i neka je $a\in G_1$ konačnog reda. Dokazati da je: a) $r(f(a))\mid r(a)$,
b) ako je f izomorfizam, tada $r(a)=r(f(a))$.

4.7. Neka je $|G|=n$ i $m| n$. Dokazati da je broj $|\{x\in G| x^m=e\}|$ deljiv sa m.

4.8. Neka je $Z(p^\infty)$ Prüfer-ova grupa. Dokazati:

a) svi elementi iz $Z(p^\infty)$ su konačnog reda,

b) za sve $n\in N$ i sve $a\in Z(p^\infty)$, jednačina $nx=a$ ima rešenje u $Z(p^\infty)$,

c) $(\forall x\in Z(p^\infty))\ x=0\vee px=0\vee p^2x=0\vee\ldots$

4.9. Neka je G konačna grupa i n prirodan broj takav da $(n,|G|)=1$. Dokazati da jednačina $x^n=a$ ima rešenje po x za svaki $a\in G$.

Rešenje: Neka je $\varphi: x\to x^n$, $x\in G$. Dokazujemo da je φ 1-1. Neka je $m=|G|$. Kako su m,n uzajamno prosti, to postoje $i,j\in Z$ takvi da $im+jn=1$. Dakle, ako je $\varphi(x)=\varphi(y)$ imamo $x=x^{mi+nj}=x^{nj}=y^{nj}=y^{mi+nj}=y$ jer redovi elemenata x,y dele red grupe G, tj. m. Dakle, φ je 1-1. Kako je G konačan skup i $\varphi: G\xrightarrow[1-1]{} G$ sledi da je φ na, tj. u G važi $(\forall y)(\exists x)x^n=y$.

3. NORMALNE PODGRUPE

Medju podgrupama grupe G, posebnu ulogu imaju *normalne* podgrupe. One su u tesnoj vezi sa homomorfnim likovima grupe G, tj. sa njenim količničkim grupama, kao i sa **kongruencijama grupe G** (o čemu će detaljno biti reči u odeljku 2 ovog poglavlja).

3.1. DEFINICIJE I OSNOVNI PRIMERI

Uvedimo prethodno neke oznake.

Neka $\mathrm{Hom}(G_1,G_2)$ označava skup svih homomorfizama grupe G_1 u grupu G_2 (definicija homomorfizma je data u poglavlju 1.).

Endomorfizam grupe G je svaki homomorfizam $f:G\to G$.

Automorfizam grupe G je svaki homomorfizam $f:G \xrightarrow[1-1]{na} G$. Skup svih automorfizama grupe G označava se sa Aut G.

Automorfizam $\sigma_x : G \to G \quad (x \in G)$, za koji je

$$\sigma_x(a)=x^{-1}ax \text{ , za sve } a \in G$$

je *unutrašnji automorfizam* grupe G. Skup svih ovakvih automorfizama označava se sa Inn G.

Pomoću skupova preslikavanja Inn G, Aut G, End G definišu se normalne, karakteristične i potpuno invarijantne podgrupe grupe G.

1.1.Definicija: Podgrupa H grupe G je normalna, u oznaci $H \lhd G$, ako je

$$(\forall x \in G)\ xH = Hx \ .$$

Odnosno, $H \lhd G$ ako je $(\forall x \in G)\ \sigma_x(H) = H$ (zad. 1.1.b), tj. ako je H invarijantna u odnosu na sve unutrašnje automorfizme grupe G. Otuda i termin *invarijantna podgrupa*.

Lako se dokazuje da je za svaki $g \in G$ i $H < G$ ispunjeno $g^{-1}Hg = H$; medjutim, nije uvek $g^{-1}Hg = H$, tj. nije svaka podgrupa normalna. Skup svih normalnih podgrupa grupe G označava se sa $\mathcal{N}(G)$.

Prema definiciji 1.1., jedinična podgrupa {1} i sama grupa G su normalne podgrupe u G - tzv. *trivijalne* podgrupe grupe G. Normalna podgrupa H u G, različita od trivijalnih, je *prava* normalna podgrupa, u oznaci $H \lhd\!\!\lhd G$.

Grupa G koja nema pravih normalnih podgrupa je *prosta*.

Skupovi preslikavanja $\mathrm{Hom}(G_1,G_2)$ i $\mathrm{End}\,G=\mathrm{Hom}(G,G)$, u opštem slučaju nisu grupe u odnosu na slaganje preslikavanja (ne postoji f^{-1} za svako f iz $\mathrm{Hom}(G_1,G_2)$). Medjutim, $\mathrm{Aut}\,G$ i $\mathrm{Inn}\,G$ jesu grupe. Pri tom je $\mathrm{Inn}\,G$ normalna podgrupa grupe $\mathrm{Aut}\,G$ (zad. 1.7.a).

Normalne podgrupe se dobro opisuju pomoću sledećeg pojma (videti Teoremu o homomorfizmu).

1.2.*Definicija:* *Jezgro homomorfizma* $f: G_1 \to G_2$, *u oznaci* $\ker f$, *je*

$$\ker f = \{x \mid x\in G_1 \wedge f(x) = e_2\}\ ,\quad e_2 \text{ je jedinica grupe } G_2.$$

U poglavlju 12 posebnu ulogu ima tzv. normalno zatvorenje podgrupe, koje se ovako definiše:

1.3.*Definicija:* *Normalno zatvorenje podgrupe H u grupi G, u oznaci* $[H]_G$ *je presek svih normalnih podgrupa u G koje sadrže H.*

Kada je jasno o kojoj grupi G je reč, pišemo samo $[H]$. O $[H]$ će detaljnije biti reči **u zadacima 1.20. i 1.21.**

U grupi G definiše se relacija *konjugacije*, u iznaci $\sim^c$, na sledeći način

$$x \sim^c y \overset{def}{\iff} (\exists g\in G)\ x = g^{-1}yg \qquad (x,y\in G)$$

Ova relacija je (v.zad. 2.3.6.) relacija ekvivalencije u G. Njene klase ekvivalencije nazivaju se *klase konjugacije*.

Napomena: za slaganje funkcija koristimo sledeće označavanje:

$$(f\circ g)(x) = f(g(x)), \qquad fg(x) = g(f(x))\ .$$

Primeri i zadaci

1.1.Neka je $H<G$. Dokazati da su sledeći uslovi ekvivalentni:

a) $H\lhd G$, b) $(\forall x\in G)\ x^{-1}Hx = H$, c) $(\forall x\in G)\ \sigma_x(H)\subseteq H$,

d) H je unija klasa konjugacije nekih elemenata iz G,

e) $(\forall x,y\in G)\ Hx\cdot Hy = Hxy$

Rešenje: *a)* $\Leftrightarrow$ *b)* : $(\forall x\in G)\ xH = Hx \Leftrightarrow (\forall x\in G)\ x^{-1}xH = x^{-1}Hx$

$$\Leftrightarrow (\forall x\in G)\ H = x^{-1}Hx$$

b) $\Leftrightarrow$ *c)* : $(\forall x\in G)\ x^{-1}Hx = H \Rightarrow (\forall x\in G)(\forall h\in H)\ x^{-1}hx\in H$

$$\Rightarrow (\forall x\in G)(\forall h\in H)\ \sigma_x(h)\in H \Rightarrow (\forall x\in G)\sigma_x(H)\in H$$

$$(\forall x\in G)\sigma_x(H)\subseteq H \Rightarrow (\forall x\in G)\ x^{-1}Hx\subseteq H \Rightarrow (\forall x\in G)(x^{-1}Hx\subseteq H \wedge xHx^{-1}\subseteq H)$$

$\Rightarrow (\forall x\in G)(x^{-1}Hx\subseteq H \wedge H\subseteq x^{-1}Hx) \Rightarrow (\forall x\in G)\ H=x^{-1}Hx$

c) $\Leftrightarrow$ d) : $H=\bigcup_{i<I} C_{a_i} \Leftrightarrow (\forall h\in H)\ C_h\subseteq H \Leftrightarrow (\forall x\in G)(\forall h\in H)\ x^{-1}hx\in H$
$\Leftrightarrow (\forall x\in G)\ \sigma_x(H)\subseteq H$

a) $\Leftrightarrow$ e) : *Neka* $a\in Hx$, $b\in Hy$, *tj. za neke* $h_1,h_2\in H$: $a=h_1x$, $b=h_2y$.
Tada $ab=h_1xh_2y=h_1xh_2(x^{-1}x)y=h_1(xh_2x^{-1})xy$.

Zbog a) $xh_2x^{-1}\in H$, *pa i* $h_1(xh_2x^{-1})\in H$; *dakle,* $ab\in Hxy$. *Kako je* $Hxy\subseteq Hx\cdot Hy$ *(jer hxy=hxey), to je* $Hx\cdot Hy=Hxy$.

Obratno: $(\forall h_1,h_2\in H)(\exists h\in H)\ h_1xh_2y=hxy \Rightarrow (\forall h_1,h_2\in H)(\exists h\in H)\ xh_2=h_1^{-1}hx$
$\Rightarrow (\forall h_2\in H)(\exists h'\in H)\ xh_2=h'x \Rightarrow xH\subseteq Hx$.
Slično, $Hx\subseteq xH$.

1.2.Dokazati da je svaka podgrupa H, koja je indeksa 2 u grupi G, normalna u G.

Rešenje: Neka je $|G:H|=2$. *Tada:*
ako je $x\in H$, *onda* $xH=H=Hx$;
ako je $x\in G\setminus H$, *onda* $xH=G\setminus H=Hx$
(jer, ako je za neke $h_1,h_2\in H$, $xh_1=h_2$ *tada* $h_2h_1^{-1}\in H$, *tj.* $x\in H$*).*
Dakle, $(\forall x\in G)\ xH=Hx$, *tj.* $H\lhd G$.

1.3.Ako je $H\lhd G$ i $H<F<G$, dokazati da je $H\lhd F$.

Rešenje: $H\lhd G$, *dakle* $(\forall h\in H)(\forall g\in G)\ g^{-1}hg\in H$.
Specijalno, $(\forall h\in H)(\forall f\in F)\ f^{-1}hf\in H$, $(H<F<G)$, *dakle* $H\lhd F$.

1.4.Navesti primere grupa kod kojih je $H\lhd F$, $F\lhd G$ ali nije $H\lhd G$, **pa otuda zaključiti da relacija $\lhd$ nije tranzitivna.**

Rešenje: Neka je G dijedarska grupa D_4 *(o dijedarskim grupama videti 2. poglavlje). To je grupa reda 8 sa strukturnim jednakostima* $a^4=e$, $b^2=e$, $(ab)^2=e$; *elementi su joj:* $e,a,a^2,a^3,b,ab,a^2b,a^3b$.

Tablica ove grupe je

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Jedna njena normalna podgrupa je $F=\{e,a^2,b,a^2b\}$, *i za* $H=\{e,b\}$, $H\lhd F$. *Prema zad. 1.1., ako je* $H\lhd G$ *onda* $(\forall h\in H)(\forall g\in G)\ g^{-1}hg\in H$, *što nije tačno. Npr.* $b\in H$, *ali* $aba^{-1}\notin H$: $aba^{-1}=aba^3=a^2b$, $a^2b\notin H$. *Dakle, nije* $H\lhd G$.

1.5. Dokazati da su sve podgrupe Abel-ove grupe, normalne. Da li važi i obrat: ako su sve podgrupe grupe normalne, da li je G Abel-ova grupa?

Rešenje: Ako je G Abel-ova grupa i $H<G$, *tada*

$$(\forall g\in G)(\forall h\in H)\ gh=hg \Leftrightarrow (\forall g\in G)(\forall h\in H)\ g^{-1}hg=h$$
$$\Rightarrow (\forall g\in G)\ g^{-1}Hg=H \Rightarrow H\lhd G\ .$$

Obrat ne važi. Sve podgrupe grupe kvaterniona K *su normalne, a* K *nije Abel-ova*[1].

1.6. Dokazati da su sledeće podgrupe normalne u grupi G:

a) Ker f , gde je f homomorfizam grupe G u grupu G_1

b) Komutant G´, c) Centar Z(G), d) Podgrupa H , **ako je** $H<Z(G)$,

e) Z(H), gde je $H\lhd G$, f) Svaka podgrupa H u G koja sadrži komutant G´

Rešenje: a) Neka su e,e_1 *redom jedinični elementi grupa* G,G_1.

Važi Ker $f<G$ ***jer***

ako $x,y\in\ker f$, *onda* $f(xy)=f(x)f(y)=e_1e_1=e_1$ *pa* $xy\in\ker f$;

kako je $f(xe)=f(x)=f(x)f(e)$, *tj.* $f(e)=e_1$, *to* $e\in\ker f$;

ako $x\in\ker f$, *onda* $f(xx^{-1})=e_1=f(x)f(x^{-1})$, *tj.* $e_1=e_1f(x^{-1})$, *pa* $x^{-1}\in\ker f$.

Važi Ker $f\lhd G$ ***jer***

za proizvoljne elemente $x\in\ker f$ *i* $g\in G$ *je*

$f(g^{-1}xg)=f(g^{-1})f(x)f(g)=f(g)^{-1}e_1f(g)=e_1$, *odakle* $g^{-1}xg\in\ker f$

b) Neka su x,y,z *proizvoljni elementi iz G. Tada*

$$z^{-1}[x,y]z=z^{-1}xzz^{-1}yzz^{-1}x^{-1}zz^{-1}y^{-1}z=[z^{-1}xz,z^{-1}yz]\ .$$

Zbog $[z^{-1}xz,z^{-1}yz]\in G'$, *je* $G'\lhd G$.

c) Za sve $x\in G$ *i* $y\in Z(G)$, $x^{-1}yx=y$, *tj.* $x^{-1}yx\in Z(G)$.

d) Ako $h\in H$ *i* $x\in G$, *tada* $x^{-1}hx=x^{-1}xh=h$, *jer* $h\in Z(G)$.

e) Neka su $x\in G$, $h\in H$, $y\in Z(H)$; *tada je, koristeći* $xhx^{-1}\in H$

$$(x^{-1}yx)h=x^{-1}y(xhx^{-1})x=x^{-1}(xhx^{-1})yx=h(x^{-1}yx)\ .$$

Dakle, $x^{-1}yx\in Z(H)$, *tj.* $Z(H)\lhd G$.

---

[1] Nekomutativne grupe čije su sve podgrupe normalne su **tzv.** ***Hamilton-ove*** **grupe**

f) Prema zad. 2.12. G/G' je Abel-ova grupa, tj, sve podgrupe su joj normalne. Koristeći Teoremu o korespodenciji, normalne su i sve podgrupe u G koje sadrže G'.

1.7. U sledećim primerima grupa H i G, dokazati da je $H \lhd G$:

a) $G = \mathrm{Aut}\, F$, $H = \mathrm{Inn}\, F$, gde je F proizvoljna grupa,

b) G je S_4 a H Klein-ova **četvorna grupa,**

c) G je $(Z^3,\star)$, gde je $(a_1,a_2,a_3)\star(b_1,b_2,b_3) = (a_1+(-1)^{a3}b_1, a_2+b_2, a_3+b_3)$ a H je podgrupa generisana elementom (1,0,0).

Rešenje: a) $\sigma_x\sigma_y(a) = y^{-1}(x^{-1}ax)y = (xy)^{-1}axy = \sigma_{xy}(a)$;

$\sigma_e \in Inn\, G$, *jer* $(\forall g \in G)e^{-1}ge = g$, $(\sigma_e = I)$;

inverzni element za σ_x *je* $\sigma_{x^{-1}}$: $\sigma_x\sigma_{x^{-1}}(a) = (x^{-1})^{-1}(x^{-1}ax)x^{-1} = a$.

Dakle, $Inn\, G < Aut\, G$.

Dalje, dokazujemo da je za proizvoljne $f \in Aut\, G$, $\sigma_x \in Inn\, G$, *ispunjeno* $f^{-1}\sigma_x f \in Inn\, G$. *Zaista,*

$$f^{-1}\sigma_x f(a) = (\sigma_x f(f^{-1}(a)) = f(x^{-1}f^{-1}(a)x) = f(x)^{-1}af(x) = \sigma_{f(x)}(a).$$

1.8.Odrediti sve normalne podgrupe grupa:

a) S_3, b) S_4, c) S_n, d) K (grupa kvaterniona)

Rešenje: a) Jedina prava normalna podgrupa grupe S_3 *je* $\{(1),(123),(132)\}$.

b) Opisujemo jedan postupak odredjivanja svih normalnih podgrupa date grupe (zadacima 2.13. i 2.14. opisane su i neke druge mogućnosti rešavanja ovog problema).

Datu konačnu grupu G razdelimo prvo na klase konjugacije K_i. *Prema zad. 1.1.d), normalne podgrupe su unije klasa konjugacije. Formiramo stoga unije ovih klasa, ali takve da je ukupan broj elemenata u uniji delilac broja* $|G|$ *(Lagrange-ova teorema* ***o podgrupama).***

U slučaju grupe S_4, *postoji pet klasa konjugacije (prema zad.* **2.4.1** *svi elementi u ovim klasama su jednakih redova):*

K_1 - *sa jednim elementom prvog reda*

K_2 - ***tri elementa drugog reda***

K_3 - ***šest elemenata drugog reda***

K_4 - ***osam elemenata trećeg reda***

K_5 - ***šest elemenata četvrtog reda***

Delioci broja $|S_4| = 24$ *su 2,3,4,6,8,12; s obzirom na kardinalne brojeve klasa* K_i $(i=1,\ldots,5)$ *jedine dve mogućnosti su*

- *unija klasa K_1 i K_2, tj. Klein-ova četvorna grupa,*
- *unija klasa K_1, K_2 i K_4, tj. grupa A_{12} (parnih permutacija reda 12).*

Pored ovih, normalne su i trivijalne podgrupe: jedinična i cela grupa S_4.

c) Videti zad. 4.1.17.

d) Sve podgrupe su normalne.

1.9. Dokazati da je presek proizvoljne familije normalnih podgrupa u G takodje normalna podgrupa u G.

Rešenje: $N = \bigcap_{i\in I} N_i$, $Nx = (\bigcap_{i\in I} N_i)x = \bigcap_{i\in I} N_i x = x(\bigcap_{i\in I} N_i) = xN$.

1.10. Ako je $N \lhd G$, $H < G$, dokazati: a) $N \cap H \lhd G$, b) $NH < G$.

1.11. Ako su $H \lhd G$, $F \lhd G$, tada je i $HF \lhd G$. Dokazati.

Rešenje: $HF = \bigcup_{x\in F} Hx = \bigcup_{x\in F} xH = FH$, *pa je prema zad. 2.3.10.* $HF < G$.
Kako je $xHFx^{-1} = xHx^{-1}xFx^{-1} = HF$ *za svako* $x \in G$, *to je* $HF \lhd G$.

1.12. Ako su $H \lhd G$, $F \lhd G$, tada je i $\langle H \cup F \rangle \lhd G$. Dokazati.

Rešenje: ***Neka je*** $N = \langle H \cup F \rangle$. *Dokazujemo da je* $N = HF$.
Kako $H, F \subseteq N$, *to je i* $HF \subseteq N$. *Važi i obratno,* $N \subseteq HF$ *jer je prema prethodnom zadatku* $HF < G$ *a* N *je najmanja podgrupa takva da* $H \cup F \subseteq N$. *Stoga je, ponovo koristeći prethodni zadatak,* $N \lhd G$.

1.13. Ako je $H < G$, tada je $H < N(H)$ i $N(H)$ je najveća podgrupa u G u kojoj je H normalna podgrupa. Dokazati.

Rešenje: $N(H) = \{n \mid n \in G \wedge Hn = nH\}$. *Kako je* $Hn = nH = H$ *za* $n \in H$, *to* $H < N(H)$.
Pri tome je $n^{-1}Hn = H$ *za sve* $n \in N(H)$, *tj.* $H \lhd N(H)$, *i ni za jedno* $x \in G \setminus N(H)$ *nije* $x^{-1}Hx = H$ *pa je* $N(H)$ *zaista najveća podgrupa u* G *u kojoj je* H *normalna podgrupa.*

1.14. Dokazati da iz $H \lhd G$ sledi $C(H) \lhd G$.

Rešenje: Neka je $H \lhd G$, *i neka je* $h \in H$, $x \in C(H)$, $y \in G$. *Tada:*

$yhy^{-1} \in H$, *jer je* $H \lhd G$, *i* $x(yhy^{-1}) = (yhy^{-1})x$, *jer je* $x \in C(H)$.

Odavde je

$(y^{-1}xy)h = h(y^{-1}xy)$ *odnosno* $y^{-1}xy \in C(H)$ *za sve* $y \in G$.

1.15. Dokazati da je za podgrupu H grupe G ispunjeno
a) $C(H) = \bigcap_{h\in H} N(h)$, b) $C(H) \lhd N(H)$.

Rešenje: $C(H) = \{x \in G \mid (\forall h \in H) hx = xh\} = \bigcap_{h \in H} \{x \in G \mid hx = xh\} = \bigcap_{h \in H} C(h)$.

Odavde je $C(H) < N(H)$. *Kako je* $H \lhd N(H)$ *(zad. 1.13.), to je i* $C(H) \lhd N(H)$ *(zad. 1.14.).*

1.16. Dokazati da je broj elemenata konjugovanih elementu a u grupi G jednak indeksu $|G : C(a)|$. Specijalno, ako je $|G| < \infty$, $|G : C(a)| \mid |G|$.

Rešenje: Neka je x proizvoljni element iz G i C(x) njegov centralizator. Neka je, dalje, ϕ *preslikavanje skupa konjugovanih elemenata za element x, na skup napr. levih razreda podgrupe C(x):*

$$\phi(axa^{-1}) = a\,C(x) \quad , \quad a \in G.$$

Preslikavanje ϕ *je dobro definisano i 1-1:*

$$axa^{-1} = bxb^{-1} \Leftrightarrow xa^{-1}b = a^{-1}bx \Leftrightarrow a^{-1}b \in C(x) \Leftrightarrow a\,C(x) = b\,C(x) \ .$$

1.17. Dokazati da je $H \lhd G$ akko $N(H) = G$.

Rešenje: Prema zad. 1.13.

1.18. Odrediti centar Z(G) sledećih grupa G:

a) Grupe svih matrica oblika $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$, gde su a,b,c proizvoljni elementi polja $(F,+,\cdot)$, a 0 i 1 su redom neutralni i jedinični element iz F; operacija grupe G je množenje matrica;

b) Grupe svih nesingularnih matrica reda n sa elementima iz polja F (u odnosu na množenje matrica).

Rešenje: a) $Z(G) = \left\{ \begin{bmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \mid x \in F \right\}$, $Z(G) \simeq (F,+)$.

b) $Z(G) = (S,\circ)$ *gde je* $S = \left\{ \begin{bmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a \end{bmatrix} \mid a \in F,\ a \neq 0 \right\}$

1.19. Ako je $H \lhd G$ i $H \cap G' = \{1\}$, dokazati da je $H < Z(G)$.

Rešenje: Neka $h \in H$, $x \in G$. *Tada* $x^{-1}hx \in H$ *(jer je* $H \lhd G$*), pa i* $h^{-1}x^{-1}hx \in H$. *Kako je* $h^{-1}x^{-1}hx \in G'$, *to je* $h^{-1}x^{-1}hx \in H \cap G'$, *tj.* $hx = xh$; *odavde* $H < Z(G)$.

1.20. Dokazati da je za normalno zatvorenje $[H]_G$ podgrupe H u grupi G ispunjeno

$$[H]_G = \langle g^{-1}hg \mid g \in G,\ h \in H \rangle .$$

Rešenje: $[H]_G = \bigcap\{N \mid H < N \lhd G\}$. *Neka je* $S = \langle g^{-1}hg \mid g \in G,\ h \in H \rangle$;

kako je $H < [H]_G$ *i* $[H]_G \lhd G$, *to je* $S < [H]_G$.

Dokazujemo da je $S \lhd G$.

Neka je $s \in S$; *tada je* $s = (g_1^{-1}h_1g_1)^{n_1} \ldots (g_k^{-1}h_kg_k)^{n_k}$ *za neke* $g_i \in G$, $h_i \in H$, $n_i \in Z$, $k \in N$ $(i=1,\ldots,k)$.

Odnosno,

$$s = (g_1^{-1}a_1g_1)\ldots(g_k^{-k}a_kg_k), \text{ gde je } a_i = h_i^{n_i} \quad (i=1,\ldots,k), \text{ tj.}$$

$a_i \in H$. *Neka je* $g \in G$; *tada*

$$g^{-1}sg = g^{-1}(g_1^{-1}a_1g_1)\,gg^{-1}(g_2^{-1}a_2g_2)\,g\,g^{-1}\ldots g\,g^{-1}(g_k^{-1}a_kg_k)g$$

$$= (g_1g)^{-1}a_1(g_1g)(g_2g)^{-1}a_2(g_2g)\ldots(g_kg)^{-1}a_k(g_kg).$$

Dakle, $g^{-1}sg \in S$ *za svako* $g \in G$, *tj.* $S \lhd G$.

Kako je $[H]_G$ *najmanja normalna podgrupa koja sadrži H (a S je normalna i sadrži H) to je* $[H]_G < S$. *Otuda* $S = [H]_G$.

1.21. Ako je $\phi : G \xrightarrow{na} H$ homomorfizam i ako je $S < G$, dokazati da je

$$\phi([S]_G) = [\phi(S)]_H .$$

Rešenje:

$$[\phi(S)]_H = \langle h^{-1}\phi(s)h \mid h \in H,\ s \in S \rangle \underset{①}{=} \langle \phi(g)^{-1}\phi(s)\phi(g) \mid g \in G, s \in S \rangle$$

$$= \langle \phi(g^{-1}sg) \mid g \in G, s \in S \rangle = \phi(\langle g^{-1}sg \mid g \in G, s \in S \rangle) = \phi([S]_G)$$

① *homomorfizam* ϕ *je* <u>na</u>, *pa je* $(\forall h \in H)(\exists g \in G)\ h = \phi(g)$.

3.2. <u>KOLIČNIČKE GRUPE, HOMOMORFIZMI, KONGRUENCIJE</u>

Ako je $N \lhd G$, tada su levi i desni razredi podgrupe N u G jednaki. Skup svih razreda po N u G, u odnosu na množenje

$$K_1K_2 = \{k_1k_2 \mid k_1 \in K_1,\ k_2 \in K_2\} \qquad (*)$$

čini grupu (v.zad. 2.1. i 2.2.).

2.1. <u>*Definicija*</u>: *Grupa svih razreda po normalnoj podgrupi N u G, u odnosu na operaciju (*) je* <u>količnička</u> *ili* <u>faktor-grupa G/N</u> *grupe G.*

Ako je ρ relacija kongruencije u grupi G, tada je skup svih klasa ekvivalencija u odnosu na množenje klasa, grupa. Označavamo je sa G/ρ i nazivamo faktor-grupom G po kongruenciji ρ .
U zadatku 2.12. pokazano je, izmedju ostalog, da postoji 1-1 veza izmedju svih normalnih podgrupa i relacija kongruencije

u grupi G.

Relacija

$$a \equiv b(\mathrm{mod}\, H) \Leftrightarrow ab^{-1} \in H$$

je kongruencija u grupi G, (H<G), i naziva se *kongruencijom po modulu podgrupe H*. Označavamo je i sa $a \equiv_H b$.

Sledeća teorema uspostavlja vezu izmedju normalnih podgrupa, faktor-grupa i homomorfizama.

2.2. *Teorema o homomorfizmu:* *Neka je* $f : G_1 \xrightarrow{na} G_2$ *homomorfizam čije je jezgro H. Tada je* $H \triangleleft G_1$ *i* $G_1/H \simeq G_2$.
Obratno, neka je $H \triangleleft G_1$ *i* $f : G_1 \to G_1/H$ *preslikavanje definisano sa* $f(x) = Hx$, $(x \in G_1)$. *Tada je f homomorfizam čije je jezgro H.*

Dokaz: Neka je $f : G_1 \to G_2$ i $\ker f = H$. Prema zad. 1.6.a) je $H \triangleleft G_1$.
Preslikavanje $\phi : G_1/H \to G_2$ definisano sa $\phi(Ha) = f(a)$ je izomorfizam.
Zaista:

$$\phi(Ha\,Hb) = \phi(Hab) = f(ab) = f(a)f(b) = \phi(Ha)\phi(Hb) .$$

Dalje, $\phi(Ha) = \phi(Hb) \Leftrightarrow f(a) = f(b) \Leftrightarrow f(a)f(b^{-1}) = 1 \Leftrightarrow ab^{-1} \in H$

$$\overset{①}{\Leftrightarrow} Ha = Hb$$

① v.zad. 2.3.7.

tj. ϕ je dobro definisano homomorfno preslikavanje koje je 1-1 i

$$f(G_1) = \phi(G_1/H) = G_2, \quad \text{pa je} \quad G_1/H \simeq G_2 .$$

Obrat: neka je $H \triangleleft G_1$, $f : G_1 \to G_1/H$ gde je $f(x) = Hx$. Tada

$$f(xy) = Hxy = Hx\,Hy = f(x)f(y)$$

$$\ker f = \{x \mid x \in G_1 \wedge f(x) = 1\} \overset{②}{=} \{x \mid x \in G_1 \wedge Hx = H\} \overset{③}{=} \{x \mid x \in H\} = H$$

② prema zad. 2.1. H je jedinični element u G_1/H .

③ v.zad. 2.3.7. ▼

Preslikavanje f iz ove teoreme naziva se *prirodni* ili *kanonski* homomorfizam.
Zaključujemo da su normalne podgrupe grupe G upravo jezgra homomorfizama te grupe, a da su faktor-grupe za G u stvari njeni homomorfni likovi.

2.3. *Teorema o korespodenciji:* *Neka je* $f : G \to G/N$ $(N \triangleleft G)$, *prirodni homomorfizam. Tada*

a) Postoji 1-1 i na preslikavanje ϕ *skupa svih podgrupa H grupe G koje sadrže podgrupu N, u skup svih podgrupa* $\bar{H}$ *grupe G/N, definisano sa*

$$\phi(H) = \bar{H} = \{f(h) \mid h \in H\}$$

b) $K<H$ *akko* $\bar{K}<\bar{H}$; $|H:K| = |\bar{H}:\bar{K}|$ *(gde su K,H podgrupe grupe G koje sadrže N).*

c) $K\triangleleft H$ *akko* $\bar{K}\triangleleft\bar{H}$; $H/K \simeq \bar{H}/\bar{K}$

Dokaz: a) Preslikavanje ϕ, definisano pomoću homomorfizma f ($\phi(H)=\bar{H} = \{f(h) \mid h\in H\} = f(H)$) je, pre svega, dobro definisano.
Jer, $f: G \to G/N$ je prirodni homomorfizam, pa za podgrupe H iz G, koje sadrže N, važi $f(H) = H/N$ i $f(H)<G/N$ (v.zad. 2.3.c)).
Dalje, ϕ je 1-1 preslikavanje: neka su H i K podgrupe u G koje sadrže N, i neka je $H/N = K/N$; tada

$$x\in H \Leftrightarrow (\exists y\in K)Nx = Ny \underset{①}{\Rightarrow} (\exists y\in K)xy^{-1}\in N \underset{②}{\Rightarrow} (\exists y\in K)xy^{-1}\in K$$
$$\Rightarrow (\exists y\in K)xy^{-1}y\in K \Rightarrow x\in K$$

① prema 2.3.7.b) ② jer $N<K$

Slično, iz $x\in K$ sledi $x\in H$. Dakle, $H = K$.
Dokažimo još da za svaku podgrupu $\bar{H}$ grupe G/N postoji podgrupa H, $N<H<G$, tako da je $\bar{H} = \phi(H)$. Označimo $H = f^{-1}(\bar{H})$. Prema zad. 2.3.d) je $H<G$. Kako je f <u>na</u> preslikavanje, to je $\bar{H} = f(H)$, tj. $\bar{H} = \phi(H)$.

b) Ako je $K<H$ tada $f(K)<f(H)$, prema zad. 2.3.
S druge strane, pretpostavimo $\bar{K}<\bar{H}$. Neka je $k\in K$; tada $Nk\in\bar{K}$, dakle $Nk\in\bar{H}$, pa za neki $h\in H$ $Nk = Nh$. Otuda $Nhk^{-1} = N$, tj. $hk^{-1}\in N$. Kako je $N<K$, to $hk^{-1}\in K$, pa $(hk^{-1})k\in K$, dakle $h\in H$. Prema prethodnom, $K<H$.

Dalje, neka je $N<K<H$ i neka je $\psi: K/H \to \bar{K}/\bar{H}$ definisano sa $\psi(Kh) = \bar{K}\bar{h}$, $h\in H$, gde je $\bar{h} = f(h) = Nh$.
Preslikavanje ψ je 1-1: neka je $\bar{K}\bar{h}_1 = \bar{K}\bar{h}_2$, $h_1,h_2\in H$; tada $\bar{K}\bar{h}_1\bar{h}_2^{-1} = \bar{K}$, tj. $\overline{Kh_1h_2^{-1}} = \bar{K}$, odakle sledi $\overline{h_1h_2^{-1}}\in\bar{K}$. Prema tome $Nh_1h_2^{-1} = Nk$ za neki $k\in K$, pa $h_1h_2^{-1}k^{-1}\in N\subseteq K$, odakle sledi $h_1h_2^{-1}\in K$, tj. $Kh_1 = Kh_2$.
S druge strane, očigledno je $\psi(K/H) = \bar{K}/\bar{H}$ odakle

$$|K:H| = |K/H| = |\bar{K}/\bar{H}| = |\bar{K}:\bar{H}|.$$

c) Neka je $K\triangleleft H$. Prema zad. 2.3. je $f(K)\triangleleft f(H)$, (tj. $\bar{K}\triangleleft\bar{H}$). Obratno, ako je $f(K)\triangleleft f(H)$, tada je $f^{-1}(f(K))\triangleleft f^{-1}(f(H))$. Kako je $f^{-1}(f(K)) = NK$ i $NK = K$ jer $N<K$, i slično za $f^{-1}(f(H))$, to je $K\triangleleft H$.
Izomorfizam $H/K \simeq (H/N)/(K/N)$ sledi na osnovu Druge teoreme o izomorfizmu. ▼

2.4. *<u>Prva teorema o izomorfizmu</u>: Ako je* $H\triangleleft G$ *i* $F<G$, *tada je*

$$H\cap F \triangleleft F \quad i \quad HF/H \simeq F/(H\cap F) .$$

Dokaz: Prema zad. 1.10.a) je $H\cap F\triangleleft G$, pa je i $H\cap F\triangleleft F$.

Neka je $\phi : G \to G/H$ prirodni homomorfizam, a $\phi_1 : F \to G/H$ njegova restrikcija na F. Preslikavanje ϕ_1 je homomorfizam i

$$\ker \phi_1 = \{x \mid x \in F \wedge \phi_1(x) = e\} = \{x \mid x \in F \wedge x \in H\} = H \cap F.$$

Stoga je $F/(H \cap F) \simeq \phi_1(F)$ (v. Teoremu o homomorfizmu).

Dalje je, prema zad. 1.10.b) $HF < G$, pa je $H \lhd HF$. Za svaki $f \in F$ je $\phi_1(f) = fH$, a $fH \in FH/H$. S druge strane, svaki element grupe FH/H je oblika fhH, gde je $f \in F$, $h \in H$. Kako je $fhH = fH = \phi_1(f)$, to je

$$\phi_1(F) = FH/H \ . \ \blacktriangledown$$

2.5. *Druga teorema o izomorfizmu:* *Ako su* $H, F \lhd G$ *i* $H < F$, *tada je*

$$F/H \lhd G/H \quad i \quad (G/H)/(F/H) \simeq G/F \ .$$

Dokaz: Neposredno iz Teoreme o **korespondenciji.**
Kako je $H \lhd G$, biramo prirodni homomorfizam $f : G \to G/H$, $G/H = \bar{G}$. Zbog $H < F$ je $\bar{F} = F/H$. Prema c) iz Teoreme o korespodenciji je $G/F \simeq G/F \simeq (G/H)/(F/H)$. $\blacktriangledown$

2.6. *Lema Zassenhaus-a:* *Ako su* $H, H_1, F, F_1 < G$ *i* $H_1 \lhd H$, $F_1 \lhd F$, *tada je*

$$H_1(H \cap F_1) \lhd H_1(H \cap F), \quad F_1(F \cap H_1) \lhd F_1(F \cap H) \quad i$$

$$\frac{H_1(H \cap F)}{H_1(H \cap F_1)} \simeq \frac{F_1(F \cap H)}{F_1(F \cap H_1)}$$

Dokaz slične leme za proizvoljne algebre dat je u poglavlju 10.

Primeri i zadaci

2.1. Ako je $N \lhd G$, tada je skup svih razreda od N u G, u odnosu na operaciju

$$K_1K_2 = \{k_1k_2 \mid k_1 \in K_1, k_2 \in K_2\}$$

grupa reda $|G : N|$. Dokazati.

Rešenje: Definisana operacija nad razredima je asocijativna:

$$(K_1K_2)K_3 = \{(k_1k_2)k_3 \mid k_1 \in K_1, k_2 \in K_2, k_3 \in K_3\}$$

$$= \{k_1(k_2k_3) \mid k_1 \in K_1, k_2 \in K_2, k_3 \in K_3\} = K_1(K_2K_3) \ ;$$

"proizvod" razreda je razred: $Nx\,Ny = Nxy$;

jedinični element je N : $N\,Nx = Nx$, $Nx\,N = N\,Nx = Nx$;

inverzni element za Nx *je* Nx^{-1} : $NxNx^{-1} = NNxx^{-1} = N$

2.2.Neka je $H<G$. Dokazati da je formulom $HxHy=Hxy$ definisana operacija u skupu G/H akko $H \triangleleft G$..

Rešenje: ($\Leftarrow$) Koristiti zad. 1.1.e)

($\Rightarrow$) Pretpostavimo

$$HxHy=Hxy \qquad (1)$$

Tada $HxH=Hx$ *odakle za sve* $h_1,h\in H$ *postoji* $h_2\in H$ *tako da* $h_1xh=h_2x$, *tj.* $xh=h'x$ *; stoga* $xH\subseteq Hx$.

Navodimo i primer za koji je $H<G$ *ali nije* $H\triangleleft G$, *i formulom (1) nije definisana operacija nad (desnim) razredima.*

Neka je $G=S_3$, *tj.* $G=\langle a,b;\ a^2=e,b^3=e,ba=ab^2\rangle$ *i* $H=\{e,a^2\}$ *Prema zad. 1.8.a) H nije normalna u* S_3. *Elementi grupe G su:* e,a,b,b^2,ab,ab^2. *Desni razredi po H su :* $\{e,a\}$, $\{b,ab\}$, $\{b^2,ab^2\}$

$$\{e,a\} = Ha = He = H$$

$$\{b,ab\} = Hb = Hab$$

$$\{b^2,ab^2\} = Hb^2 = Hab^2$$

Prema (1) je : $HbHb^2=Hbb^2=H$, $HbHab^2=Hbab^2=Hab$. *Odavde, kako je* $H\neq Hab$, *sledi* $HbHb^2\neq HbHab^2$, *iako je* $Hb=Hb$, $Hb^2=Hab^2$. *Dakle, operacija nad desnim razredima nije dobro definisana.*

2.3.Neka je f homomorfizam grupe G_1 na grupu G_2. Dokazati:

a) $f(e_1)=e_2$ (e_1 i e_2 su redom jedinični elementi u grupama G_1 i G_2),

b) $f(g^{-1})=f(g)^{-1}$, za svako $g\in G_1$

c) Ako je $H<G_1$ tada $f(H)<G_2$; ako je $H\triangleleft G_1$ tada $f(H)\triangleleft G_2$,

d) Ako je $F<G_2$ tada $f^{-1}(F)<G_1$; ako je $F\triangleleft G_2$ tada $f^{-1}(F)\triangleleft G_1$,

e) Ako neki zakon $t_1=t_2$ važi u G_1, tada on važi i u G_2,

f) $|G_2|\leqslant|G_1|$,

g) Ako je $G_1=\langle S\rangle$ tada $G_2=\langle f(S)\rangle$, gde je $f(S)=\{f(s)\mid s\in S\}$,

h) Ako su $H_1,H_2<G_1$ tada $f(H_1H_2)=f(H_1)f(H_2)$.

Koja od ovih tvrdjenja ostaju tačna ako f nije na preslikavanje?

Rešenje: c) Ako $f(x)\in f(H)$ *i* $f(y)\in f(H)$ *gde su* $x,y\in H$, *tada*

$$f(x)f(y)=f(xy) \text{ tj. } f(x)f(y)\in f(H);$$

neka je $e_1\in G_1$, $e_2\in G_2$ *i* $x\in H$; *tada* $f(x)f(e_1)=f(x)$ *tj.* $f(e_1)=e_2$,

dakle $e_2\in f(H)$;

kako je $f(x)f(x^{-1})=f(xx^{-1})=f(e_1)=e_2$, *to ako* $f(x)\in f(H)$ *i inverzni* $f(x^{-1})\in f(H)$;

Dakle, iz $H<G_1$ *sledi* $f(H)<G_2$.

Neka je $H\triangleleft G_1$. *Kako je f na preslikavanje, za svaki* $g_2\in G_2$ *postoji* $g_1\in G_1$

tako da $f(g_1)=g_2$, *pa je za* $x\in H$:

$$g_2^{-1}f(x)g_2 = f(g_1^{-1})f(x)f(g_1) = f(g_1^{-1}xg_1) = f(x')$$

za neki $x'\in H$, *jer je* $H\lhd G_1$; *stoga je i* $f(H)\lhd G_2$.

d) Slično kao pod c)

e) Kao kod grupoida (v. Teoremu 1.4.3.)

f) $|G_2| \leqslant |G_1|$ *jer je f* <u>*na*</u> *preslikavanje.*

g) Svaki element g_1 *iz* G_1 *može se predstaviti u obliku* $g_1 = s_1^{i_1}s_2^{i_2}\ldots s_k^{i_k}$ $(s_j\in S,\ i_j\in Z)$. *Kako*

$(\forall g_2\in G_2)(\exists g_1\in G_1)\ g_2=f(g_1)$, *to je za* $g_2\in G_2$ *i neki* $g_1\in G_1$

$$g_2 = f(g_1) = f(s_1^{i_1}s_2^{i_2}\ldots s_k^{i_k}) = f(s_1^{i_1})f(s_2^{i_2})\ldots f(s_k^{i_k}) = f(s_1)^{i_1}\ldots f(s_k)^{i_k}$$

h) $f(H_1)f(H_2) = \{f(h_1)f(h_2) \mid h_1\in H_1, h_2\in H_2\} = \{f(h_1h_2) \mid h_1\in H_1, h_2\in H_2\}$

$$= f(H_1H_2)$$

Ako preslikavanje f nije <u>*na*</u>, *tada ne važi drugi deo tvrdjenja c), zatim e), f) i g).*

2.4. Neka je G grupa, $x\in G$ i $x\mapsto x^3$ 1-1 homomorfizam. Dokazati da je G komutativna grupa.

Rešenje: $(xy)^3 = x^3y^3$ *pa* $xyxyxy = x^3y^3$ *tj.*

$$yxyx = x^2y^2 \qquad (1)$$

Otuda

$$xyxyx = x^3y^2 \qquad (2)$$

pa kako je prema (1) $xyxy = y^2x^2$ *to iz (2) :* $y^2x^3 = x^3y^2$. *Zamenjujući y sa* y^3 *imamo* $y^6x^3 = x^3y^6$ *pa je* $(y^2x)^3 = (xy^2)^3$. *Preslikavanje* $x\mapsto x^3$ *je 1-1; stoga* $y^2x = xy^2$. *Dalje,* $x^2y^2 = x(xy^2) = x(y^2x) = y^2x^2$ *tj.* $x^2y^2 = y^2x^2$ *pa prema (1)* $yxy = y^2x^2$ *odakle* $xy = yx$.

2.5. Ako je $N\lhd G$ i $H\leqslant G$, dokazati: a) $NH = HN$ i $NH\leqslant G$,
b) Ako je $f : G \to G/N$ prirodni homomorfizam, tada $NH = f^{-1}(f(H))$.

2.6. Neka je M skup svih transformacija kompleksne ravni, definisanih na sledeći način

$$f(z) = \frac{az+b}{cz+d} \qquad (1)$$

gde su $a,b,c,d\in Z$ i $ad-bc=1$ [1]. Dokazati:
a) $\underline{M} = (M,\circ)$ je grupa, ako je operacija **slaganja funkcija:**

---

[1] Ovako definisana grupa naziva se *modularnom.*

b) grupa $\underline{M}$ je generisana elementima: 1^0 $(-\frac{1}{z})$ i $(z+1)$ kao i 2^0 $(-\frac{1}{z})$ i $\frac{z-1}{z}$

c) grupa $\underline{M}$ je izomorfna faktor-grupi grupe M_2 matrica reda 2 sa elementima iz Z i determinantom jednakom 1.

Rešenje: b) Neka su $f:z\mapsto -1/z$, $g:z\mapsto z+1$ *i* $i:z\mapsto z$. *Tada je* $f^2=i$ *i* $g^n(z)=z+n$ $(n\in N)$. *Otuda, ako je* $M'<M$ *generisana elementima f,g, onda bilo koji element* $h\in M'$ *je oblika*

$$h=g^{q_o} f g^{q_1} f \ldots f g^{q_n}, \quad q_o,\ldots,q_n \in Z.$$

Tada

$$g^{q_o} f g^{q_1}: z\mapsto q_o+\frac{1}{-q_1+z}, \quad g^{q_o} f g^{q_1} f: z\mapsto q_o+\frac{1}{-q_1+\frac{1}{z}}, \ldots,$$

$$(1)\quad g^{q_o} f g^{q_1} f \ldots g^{q_n} f: z\mapsto q_o+\cfrac{1}{-q_1+\ddots\cfrac{1}{-q_{n-1}+\frac{1}{z}}}, \quad q_o,..,q_n\in Z$$

tj. bilo koji element grupe M' je verižni razlomak.

Neka su nizovi P_n, Q_n *definisani na sledeći način:*

$P_o=a_o$, $P_1=-a_o a_1+1$, $Q_o=1$, $Q_1=-1$

$$(2)\quad P_{k+1}=-q_{k+1}P_k+P_{k-1}, \quad Q_{k+1}=-q_{k+1}Q_k+P_{k-1}$$

Tada za verižni razlomak u (1) važi

$$(3)\quad P_{n+1}=z\cdot P_n+P_{n-1}, \quad Q_{n+1}=z\cdot Q_n+Q_{n-1}$$ *i takodje za svaki* $k\leq n$

$$(4)\quad \frac{P_k}{Q_k}=q_o+\cfrac{1}{-q_1+\ddots+\cfrac{1}{-q_k}}, \quad \frac{P_{n+1}}{Q_{n+1}}=q_o+\cfrac{1}{-q_1+\ddots+\cfrac{1}{-q_n+\frac{1}{z}}}$$

Sada dokazujemo da je $M'=M$, *tj. da je svaki racionalan izraz* $\frac{az+b}{cz+d}$, *gde* $ad-bc=1$, *predstavljiv u vidu verižnog razlomka (1) Prethodno primetimo da važi*

(5) P_k *i* Q_n *su uzajamno prosti za* $k\leq n$; *b i d su uzajamno prosti.*

(6) $P_k Q_{k-1} - Q_k P_{k-1}=\varepsilon(k)$, *gde* $\varepsilon(k)=-1$ *za* $k<n$, *i* $\varepsilon(n)=1$

(7) Svaki racionalan broj predstavljiv je u vidu verižnog razlomka (4).

Zato, neka su $q_o,\ldots,q_{n-1} \in Z$ takvi da važi

$$b/d = q_o + \cfrac{1}{-q_1 + \ddots + \cfrac{1}{-q_{n-1}}}$$

Prema (2-4) za odgovarajući niz P_k važi $P_{n-1}=b$, $Q_{n-1}=d$.
Determinanta sistema (3) je $D=ad-bc=1$

(S) $ax+by=P_{n-2}$, $cx+dy=Q_{n-2}$ i rašireno sistema(S) je, koristeći (6)

$x_o = P_{n-2}\cdot d - Q_{n-2}\cdot b = P_{n-2}\,Q_{n-1} - Q_{n-2}\,P_{n-1} = 1$

$y_p = a\cdot Q_{n-2} - c\cdot P_{n-2}$. Tada

$$a=-y_o\,P_{n-1}+P_{n-2},\quad c=-y_o\,Q_{n-1}+Q_{n-2}$$

a to prema (4) znači da je

$$\frac{a}{c} = q_o + \cfrac{1}{-a_1 + \ddots + \cfrac{1}{-a_n}}\quad ,\quad i\ P_n=a,\ Q_n=c$$

Takodje prema (4) sledi

$$\frac{P_{n+1}}{Q_{n+1}} = q_o + \cfrac{1}{-q_1 + \ddots + \cfrac{1}{-q_n + \frac{1}{z}}} \qquad i\ \frac{P_{n+1}}{Q_{n+1}} = \frac{z\cdot P_{n-1}+P_{n-2}}{z\cdot Q_{n-1}+Q_{n-2}} = \frac{za+b}{cz+d}$$

c) Neka je $M_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in Z \ \wedge\ (ad-bc)=1 \right\}$

i neka je $\varphi: M_2 \longrightarrow M$ preslikavanje $\varphi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{az+b}{cz+d}$

Lako se pokazuje da je φ homomorfizam. Jezgro za φ je skup matrica $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $(ad-bc=1)$ koje se preslikavaju u z. Dakle, $\frac{az+b}{cz+d} \equiv z$, odakle $c=0$, $b=0$, $d=a$. Zbog $ad-bc=1$, tj. $ad=1$, sledi $a=d=1$ ili $a=d=-1$.
Prema tome $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ predstavlja normalnu podgrupu N, za koju je $M_2/N \simeq M$.

2.7. Neka su $H,F \lhd G$ i $H \simeq F$. Dokazati da ne mora biti $G/H \simeq G/F$.

Rešenje: Neka je $G=Z$, $H=2Z$, $F=3Z$. Za njih važi $2Z \simeq 3Z$ $(\simeq Z)$.
Medjutim, $Z/2Z \simeq C_2$, $Z/3Z \simeq C_3$, ali $C_2 \neq C_3$

2.8. Dokazati da u opštem slučaju iz $G/H \simeq G/F$ ne sledi $H \simeq F$.

Rešenje: Neka je $G=D_4$ (v.zad. 1.4.), $H=\{e,a,a^2,a^3\}$, $F=\{e,b,a^2,a^2b\}$.
Ispunjeno je $G/H \simeq G/F \simeq C_2$, dok $H \neq F$ (H je ciklična grupa a F nije).

2.9. Dokazati da iz $|H| = |F|$ ne sledi obavezno $H \simeq F$.

Rešenje: Neka je $H=C_4$, $F=V$ (Klein-ova grupa). Za njih važi $|H| = |F|$ ali nije $H \simeq F$.

2.10. Dokazati da postoji prirodan broj n, $n \geqslant 2$ i nije prost, takav da važi

$|H| = |F| = n \Rightarrow H \simeq F$, za sve H,F.

Rešenje: Nadjimo prvo neke prirodne brojeve za koje tvrdjenje važi. Napr. ako je n=15, tada $|H| = 15 \Rightarrow H \simeq C_{15}$ *pa* $|H| = |F| = 15 \Rightarrow H \simeq F$. *Slično, tvrdjenje važi i za n=33, n=35, n=51,... itd.*

Naime, ako je n=pq gde je $p < q$, $p \nmid q-1$, *tada:* $|H| = n \Rightarrow H \simeq C_n$ *(v.zad. 8.2.15)*

Postavlja se pitanje koliko ima takvih brojeva. Dokazuje se (v.zad. 13.1.39) da ima beskonačno mnogo parova prostih brojeva (p,q) takvih da: $p < q$, $q \neq_p 1$.

2.11. Odrediti sledeće količničke grupe:

a) S_3/C_3 b) S_3/S_3' c) C_{12}/C_4 d) $(Z,+)/(nZ,+)$ $(n \in N)$

Rešenje: a) $S_3/C_3 \simeq C_2$ *b)* $S_3/S_3' \simeq C_2$ *c)* $C_{12}/C_4 \simeq C_3$.

d) U aditivnoj grupi celih brojeva, podgrupe $nZ = \{nk \mid k \in Z\}$ *su normalne (jer je (Z,+) Abel-ova grupa). U količničkoj grupi (Z,+)/(nZ,+) sabiranje je odredjeno sa*

$$(m+nZ) + (k+nZ) = m+k+nZ$$

Odnosno, $(Z,+)/(nZ,+) \simeq Z_n$, *gde je* Z_n *grupa* **iz z. 2.2.2.**

2.12. Dokazati da je količnička grupa G/N Abel-ova akko N sadrži komutant G'.

Rešenje: G/N *je Abel-ova grupa* $\iff (\forall a,b \in G)(Na)^{-1}(Nb)^{-1}(Na)(Nb) = N$

$\iff (\forall a,b \in G)Na^{-1}b^{-1}ab = N \iff (\forall a,b \in G)a^{-1}b^{-1}ab \in N$

2.13. U ovom zadatku opisuje se trojstvo: kongruencija - normalna podgrupa - homomorfizam.

Neka je G grupa, f homomorfizam G u grupu G_1, ε izomorfizam $G/\ker f$ i G_1, $H \lhd G$ i ρ kongruencija u G. Uvedimo sledeće oznake

$N(\rho) = \{x \in G \mid x \rho e\}$

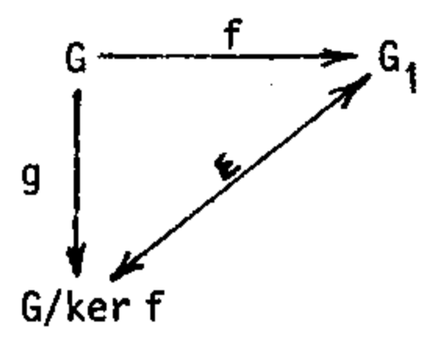
$N(f) = \ker f$

$\sigma(H)$ je relacija: $x\sigma(H)y \overset{def}{\iff} xy^{-1} \in H$

$\sigma(f)$ " " $x\sigma(f)y \overset{def}{\iff} f(x)=f(y)$ $(x,y \in G)$

$g(H)$ je kanonsko preslikavanje $G \to G/H$

$g(\rho)$ " " " $G \to G/\rho$



a) Dokazati da je

1° $N(\sigma(H))=H$ 4° $\varepsilon \cdot g(N(f))=f$

2° $\sigma(N(\rho))=\rho$ 5° $\sigma(g(\rho))=\rho$

3° $N(g(H))=H$ 6° $\varepsilon \cdot g(\sigma(f))=f$

b) Dokazati

1° $(\forall H)(\exists \rho)H = N(\rho)$ 4° $(\forall \rho)(\exists f)\rho = \sigma(f)$

2° $(\forall H)(\exists f)H = N(f)$ 5° $(\forall f)(\exists H)f = \varepsilon \cdot g(H)$

3° $(\forall \rho)(\exists H)\rho = \sigma(H)$ 6° $(\forall f)(\exists \rho)f = \varepsilon \cdot g(\rho)$

Rešenje: a) 1° $N(\sigma(H))=\{x\in G \mid x\sigma(H)e\}=\{x\in G \mid xe^{-1}\in H\}=H$

2° $x(\sigma(N(\rho)))y \Leftrightarrow xy^{-1}\in N(\rho) \Leftrightarrow xy^{-1}\in\{x\in G \mid x\rho e\} \Leftrightarrow xy^{-1}\rho e \Leftrightarrow x\rho y$

3° $N(g(H))=\ker g(H)=\{x\in G \mid g(x)=H\}=\{x\in G \mid g(x)=xH\}$;

dakle, $x\in \ker g(H)$ akko $H=xH$, tj. (prema zad. 2.3.7) akko $x\in H$.

Odavde, $N(g(H))=H$.

b) 1° Svakoj normalnoj podgrupi H (grupe G) pridružuje se relacija $\sigma(H)$ za koju je $x\sigma(H)y \Leftrightarrow xy^{-1}\in H$, $(x,y\in G)$. Prema a)1° je $N(\sigma(H))=H$.

2° podgrupi H se pridružuje preslikavanje g(H), za koje (prema a)3°) važi $N(g(H))=H$

3° relaciji ρ se pridružuje $N(\rho)$ za koju je (prema a)2°) $\sigma(N(\rho))=\rho$

2.14. Naći sve homomorfne likove sledećih grupa:

a) Klein-ove grupe V b) S_3 c) C_{12}

Rešenje: a) Prvi način. Za nalaženje svih homomorfnih likova date grupe G primenjujemo sledeći postupak: odrede se sve normalne podgrupe H grupe G i odgovarajuće količničke grupe G/H; prema teoremi o homomorfizmu dobijene grupe su homomorfni likovi grupe G.

$V=\{e,a,b,ab\}$. Normalne podgrupe su: $\{e\}$, V, C_2.

Dakle, sve homomorfne slike grupe G izomorfne su jednoj od grupa: V, $\{e\}$, C_2.

Drugi način. Uočavaju se elementi grupe G i njihovi redovi. Prema zad. 2.46 redovi elemenata f(a) (f je homomorfizam) su delioci odgovarajućih redova elemenata a, $a\in G$. Znajući kog reda mogu biti elementi iz f(G), razmatraju se svi mogući slučajevi.

Elementi grupe V su sledećih redova: $r(e)=1$, $r(a)=2$, $r(b)=2$, $r(ab)=2$.

Prema tome, elementi f(x) iz f(V) su reda 1 ili 2. Slučajevi:

- *svi elementi iz V se preslikavaju u e_1, $e_1\in f(V)$; homomorfni lik je $G_1=\{e_1\}$*
- *$f(a)=e_1$, $f(b)=c$; ako je $r(c)=1$, slučaj se svodi na gornji; zato neka je $r(c)=2$. Dalje, $f(ab)=f(a)f(b)=c$, pa je homomorfni lik $G_2=\{e_1,c\}=C_2$*
- *$f(a)=d$, $f(b)=e_1$; slučaj se svodi na prethodni*
- *$f(a)=f(b)=c$; tada $f(ab)=c^2=e_1$, tj. $G_2=C_2$*
- *$f(a)=c$, $f(b)=d$; $f(ab)=cd$, $r(c)=2$, $r(d)=2$, pa je f izomorfizam. Dakle, $G_3=V$*

2.15. Naći sve endomorfizme grupa iz zadatka 2.14.

Rešenje: b) Elementi grupe S_3 su: $I=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ i $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$. Uvedimo oznake

$$a=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \quad i \quad b=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}.$$

Tada je $S_3=\{a,a^2,ab,ab^2,b,b^2\}$ gde je ispunjeno $a^2=I$, $b^3=I$, $ba=ab^2$

Homomorfizme $S_3 \to S_3$ *odredjujemo tako što odredimo sva preslikavanja* $f=\begin{pmatrix} a & b \\ \bar{a} & \bar{b} \end{pmatrix}$ *za koja je* $\bar{a}^2=I$, $\bar{b}^3=I$, $\bar{b}\bar{a}=\bar{a}\bar{b}^2$. *Uslov* $\bar{a}^2=I$ *daje sledeće mogućnosti izbora slike* $\bar{a}$: $\bar{a} \in \{a, a^2, ab, ab^2\}$ *(jer, ako je* $\bar{a}=ab$, *tada* $\bar{a}^2=abab=aab^2b=I$, *itd., dok ako je* $\bar{a}=b^2$ *tada* $\bar{a}^2 \neq I$, *itd.).*

Takodje, $\bar{b}^3=I$ *ako je* $\bar{b} \in \{b, b^2, a^2\}$.

Postoji, dakle, 12 mogućnosti, od kojih su, zbog $\bar{b}\bar{a}=\bar{a}\bar{b}^2$, *endomorfizmi:*

$f_1=\begin{pmatrix} I & a & b & b^2 & ab & ab^2 \\ I & a & b & b^2 & ab & ab^2 \end{pmatrix}$ $f_1(a)=a,\ f_1(b)=b$

$f_2=\begin{pmatrix} I & a & b & b^2 & ab & ab^2 \\ I & a & b^2 & b & ab^2 & ab \end{pmatrix}$ $f_2(a)=a,\ f_2(b)=b^2$

$f_3=\begin{pmatrix} I & a & b & b^2 & ab & ab^2 \\ I & a & I & I & a & a \end{pmatrix}$ $f_3(a)=a,\ f_3(b)=I$

$f_4=\begin{pmatrix} I & a & b & b^2 & ab & ab^2 \\ I & I & I & I & I & I \end{pmatrix}$ $f_4(a)=I,\ f_4(b)=I$

$f_5=\begin{pmatrix} I & a & b & b^2 & ab & ab^2 \\ I & ab & I & I & ab & ab \end{pmatrix}$ $f_5(a)=ab,\ f_5(b)=I$

$f_6=\begin{pmatrix} I & a & b & b^2 & ab & ab^2 \\ I & ab & b & b^2 & ab^2 & a \end{pmatrix}$ $f_6(a)=ab,\ f_6(b)=b$

$f_7=\begin{pmatrix} I & a & b & b^2 & ab & ab^2 \\ I & ab & b^2 & b & a & ab^2 \end{pmatrix}$ $f_7(a)=ab,\ f_7(b)=b^2$

$f_8=\begin{pmatrix} I & a & b & b^2 & ab & ab^2 \\ I & ab^2 & b & b^2 & a & ab \end{pmatrix}$ $f_8(a)=ab^2,\ f_8(b)=b$

$f_9=\begin{pmatrix} I & a & b & b^2 & ab & ab^2 \\ I & ab^2 & b^2 & b & ab & a \end{pmatrix}$ $f_9(a)=ab^2,\ f_9(b)=b^2$

$f_{10}=\begin{pmatrix} I & a & b & b^2 & ab & ab^2 \\ I & ab^2 & I & I & ab^2 & ab^2 \end{pmatrix}$ $f_{10}(a)=ab^2,\ f_{10}(b)=I$

2.16. U cikličnoj grupi C_{15} data je relacija $\rho=\{(a^7,a^2),(a^3,a^8)\}$.
Odrediti minimalnu kongruenciju $\rho^\sim$ koja sadrži ρ i odrediti grupu $C_{15}/\rho^\sim$.

Rešenje: $C_{15}=\{e,a,a^2,a^3,\ldots,a^{14}\}$, $(a^{15}=e)$.

Dopunjavamo relaciju ρ *do minimalne kongruencije* $\rho^\sim$ *na sledeći način:*
izvrši se prvo dopuna do refleksivne relacije, tj. do relacije za koju je $(\forall x \in C_{15})x\rho^\sim x$. *Zatim se vrši dopuna do relacije koja je simetrična, tranzitivna i saglasna sa operacijom* $\cdot$ *u grupi* C_{15}, *primenjujući sledeća pravila:*

$$(S)\ \frac{x\rho^\sim y}{y\rho^\sim x},\quad (T)\ \frac{x\rho^\sim y,\ y\rho^\sim z}{x\rho^\sim z},\quad (S')\ \frac{x\rho^\sim y}{xz\rho^\sim yz},\quad (S'')\ \frac{x\rho^\sim y}{zx\rho^\sim zy}$$

U datom slučaju, dopunjena relacija $\rho^\sim$ *je*

$$\rho^\sim = \{(a^i,a^j) \mid i,j \in \{0,1,2,\ldots,14\} \wedge i =_5 j\}$$

Dakle, $C_{15}/\rho^\sim \simeq C_5$.

2.17. Neka je G multiplikativna grupa svih nesingularnih matrica reda n sa elementima iz polja F, i neka je F* multiplikativna grupa elemenata iz F različitih od 0. Dokazati da je preslikavanje $\det : G \to F^*$ homomorfizam.

Rešenje: Koristiti $\det(AB)=\det(A)\det(B)$.

2.18.Dokazati da je homomorfizam $f : G \to H$, 1-1 preslikavanje akko $\ker f = \{e\}$.

Rešenje: ($\Rightarrow$) $f(e) = e$, *pa je* $\ker f = \{e\}$.

($\Leftarrow$) *Neka su* $a,b \in G$ *i neka je* $f(a)=f(b)$; *tada* $f(ab^{-1})=f(a)f(b)^{-1}=e$, *tj.* $ab^{-1} \in \ker f$. *Kako je* $\ker f = \{e\}$, *to je* $a=b$.

2.19.Neka je grupa G generisana skupom S i neka su $f,g : G \to H$ homomorfizmi. Dokazati : $f \restriction S = g \restriction S \Rightarrow f = g$.

Rešenje: Ako je grupa G generisana skupom S, tada

$$(\forall a \in G)(\exists n \in N)(\exists s_1,\dots,s_n \in S)(\exists k_1,\dots,k_n \in Z)\ a = s_1^{k_1}\dots s_n^{k_n}.$$

Otuda, za $a \in G$ *i* $s_1,\dots,s_n \in S$, $k_1,\dots,k_n \in Z$

$$f(a)=f(s_1^{k_1}\dots s_n^{k_n})=f(s_1^{k_1})\dots f(s_n^{k_n})=f(s_1)^{k_1}\dots f(s_n)^{k_n}$$

$$=g(s_1)^{k_1}\dots g(s_n)^{k_n}=g(s_1^{k_1})\dots g(s_n^{k_n})=g(s_1^{k_1}\dots s_n^{k_n})=g(a)\ .$$

2.20.Neka su G_1 i G_2 izomorfne grupe. Dokazati:

a) $|G_1| = |G_2|$ b) $\mathrm{Aut}\, G_1 \simeq \mathrm{Aut}\, G_2$ c) $\mathrm{Inn}\, G_1 \simeq \mathrm{Inn}\, G_2$

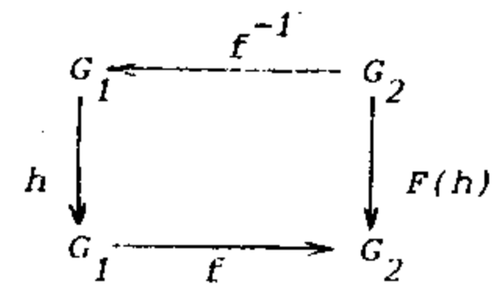
d) Kardinalni broj skupa svih izomorfizama G_1 u G_2 jednak je kardinalnom broju skupa $\mathrm{Aut}\, G_1$.

Rešenje: Neka je $f : G_1 \to G_2$ *izomorfizam.*

b) Preslikavanje

$$F : \mathrm{Aut}\, G_1 \to \mathrm{Aut}\, G_2$$

definisano sa $F(h) = f^{-1} \circ h \circ f$ *je izomorfizam.*



2.21.Dokazati da je $\mathrm{Inn}\, G \simeq G/Z(G)$.

Rešenje: Preslikavanje $F : G \to Sym(G)$ *(Sym(G) je simetrična grupa svih 1-1 i* <u>*na*</u> *preslikavanja* ***skupa G)definisano sa***

$$F(g)(x) = g^{-1}xg$$

je homomorfizam i $\ker F = Z(G)$ *(v.zad. 2.26.)*

2.22.Dokazati da su sledeće grupe izomorfne:

a) Multiplikativna grupa svih n-tih korena iz 1 i grupa $Z_n = (\{0,1,\dots,n-1\},+_n)$

b) Aditivna grupa svih polinoma po x sa koeficijentima iz Z, i $(Q^+,\cdot)$

c) $(R,+)$ i $(R^+,\cdot)$

Rešenje: a) Obe grupe su ciklične, istog reda n.

b) Neka je $p_0,p_1,p_2,\dots$ *niz svih prostih brojeva. Svaki pozitivni racionalni broj q pretstavlja se na jedinstven način u obliku*

$$q=p_0^{a_0}\ p_1^{a_1}\ \dots\ p_k^{a_k}$$ *za neki* $k \in N$ *i neke cele brojeve* $a_0,a_1,\dots,a_k$.

Preslikavanje

$$f(a_0 + a_1x + \dots + a_kx^k) = p_0^{a_0}\ p_1^{a_1}\ \dots\ p_k^{a_k}$$

$k\in N$, $a_0,\dots,a_k\in Z$ je izomorfizam grupa $(Z[x],+)$ i $(Q^+,\cdot)$.

c) Preslikavanje $f:R\to R^+$ definisano sa $f(x)=2^x$ ostvaruje traženi izomorfizam.

2.23. Dokazati da je

a) $(R,+)\simeq(C,+)/(R,+)$, b) $(Q^+,\cdot)\simeq(Q',\cdot)/C_2$ ($Q'=Q\setminus\{0\}$, Q^+ je skup pozitivnih racionalnih brojeva)

c) $(C',\cdot)\simeq(C,+)/(Z,+)$, ($C'=C\setminus\{0\}$)

2.24. Dokazati da je dijedarska grupa D_n izomorfna grupi

a) $G_1=\left\langle \begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}\alpha&0\\0&\alpha^{-1}\end{pmatrix}\right\rangle$, $\alpha=e^{2\pi i/n}$

b) $G_2=\left(\left\{\begin{pmatrix}\pm1&a\\0&1\end{pmatrix}\mid a\in Z_n\right\},\cdot\right)$

Rešenje: $D_n=\langle a,b;\ a^n=1,\ b^2=1,\ (ab)^2=1\rangle$ *(.videti definiciju grupe D_n).*

Označimo $A=\begin{pmatrix}\alpha&0\\0&\alpha^{-1}\end{pmatrix}$, $B=\begin{pmatrix}0&1\\1&0\end{pmatrix}$.

Za njih važi:

$$B^2=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad A^n=\begin{pmatrix}\alpha^n&0\\0&\alpha^{-n}\end{pmatrix}=\begin{pmatrix}e^{2\pi i}&0\\0&e^{-2\pi i}\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad (AB)^2=\begin{pmatrix}1&0\\0&1\end{pmatrix}.$$

Traženo preslikavanje je $F:D_n\to G_1$, gde je $F(a)=A$, $F(b)=B$

(jer G_1 ima $2n$ elemenata).

2.25. Dokazati da je za dijedarske grupe D_n, $n\geq3$, ispunjeno sledeće:

a) ako je n neparan broj, tada je $Z(D_n)=\{1\}$

b) ako je n paran broj, tada

1° $|Z(D_n)|=2$ 2° $D_n/Z(D_n)\simeq D_{n/2}$, za $n\geq6$ 3° $D_4/Z(D_4)\simeq C_2\times C_2$

Rešenje: Grupa D_n je reda $2n$; elementi su oblika

$$a^ib^j,\quad \text{gde je } i=0,1,\dots,n-1\ ;\ j=0,1\ .$$

Dakle, elementi centra $Z(D_n)$ su oblika a^k ili a^kb, gde je $k=0,1,\dots,n-1$.

Neposrednom proverom utvrđujemo da u centru mogu biti samo elementi oblika a^k, i da je

$$a^k(a^ib)=(a^ib)a^k \quad \text{akko} \quad a^{i+k}=a^{i-k} \quad (\text{jer je } ba=a^{-1}b),\ \text{tj.}\ a^k=a^{-k}.$$

Odavde, $2k=n$.

Odnosno, za n neparno je $Z(D_n)=\{1\}$, a za n parno $Z(D_n)=\{1,a^{n/2}\}$.

2.26. Neka je $\sigma_x:G\to G$ unutrašnji automorfizam grupe G. Dokazati:

a) $\sigma_x\in\operatorname{Aut}G$ b) $H\leq G\wedge(\forall x\in G)\sigma_x(H)=H\iff H\trianglelefteq G$ c) $\sigma_x^n=\sigma_{x^n}$

d) $r(\sigma_x)\leqslant r(x)$, gde je $r(\sigma_x)$ red σ_x u grupi $\operatorname{Aut}G$

e) ako je $f:G\to\operatorname{Aut}G$ preslikavanje definisano sa $f(x)=\sigma_x$, dokazati da je f homomorfizam i da je $\ker f=Z(G)$ ($Z(G)$ - centar grupe G)

f) neka je $a^x=\sigma_x(a)$; dokazati: ako je $f:G\to G$ homomorfizam, tada je

$$f(a^x)=f(a)^{f(x)}$$

Rešenje: a) $\sigma_x(a)=x^{-1}ax$, $\sigma_x(b)=x^{-1}bx$, $\sigma_x(ab)=x^{-1}abx=x^{-1}axx^{-1}bx=\sigma_x(a)\sigma_x(b)$, *odnosno,* σ_x *je homomorfizam.*

Takodje, svaki element $g\in G$ *je slika u odnosu na ovo preslikavanje, jer* $g=x^{-1}(xgx^{-1})x$. *Kako je još i* $x^{-1}ax=x^{-1}bx$ *akko* $a=b$, σ_x *je automorfizam (za sve* $x\in G$).

b) Podgrupa H je normalna akko $(\forall x\in G)Hx=xH$ *tj. akko* $(\forall x\in G)H=x^{-1}Hx$. *S druge strane,* $x^{-1}Hx$ *je lik podgrupe H u odnosu na preslikavanje* σ_x.

c) Zbog asocijativnosti množenja preslikavanja, dokazujemo tvrdjenje za

n=2: $\sigma_x^2(a)=(\sigma_x\circ\sigma_x)(a)=\sigma_x(\sigma_x(a))=\sigma_x(x^{-1}ax)=x^{-1}x^{-1}axx=(x^2)^{-1}ax^2=\sigma_{x^2}(a)$

d) Ako je $r(x)=n$, *tada je prema prethodnom*

$$(\sigma_x)^n=\sigma_{x^n}=\sigma_e=I \text{ tj. } r(\sigma_x)\leqslant r(x)$$

e) $f: G\to \mathrm{Aut}\,G$, $f(x)=\sigma_x$

$$f(xy)=\sigma_{xy}=\sigma_x\sigma_y=f(x)f(y) \quad \text{jer}$$

$$\sigma_{xy}(a)=(xy)^{-1}a(xy)=y^{-1}(x^{-1}ax)y=\sigma_y(\sigma_x(a)=(\sigma_x\sigma_y)(a)$$

$\ker f=\{x\in G \mid \sigma_x=I\}$

$\sigma_x=I \Leftrightarrow (\forall a\in G)x^{-1}ax=a \Leftrightarrow (\forall a\in G)ax=xa \Leftrightarrow x\in Z(G)$,

f) $f: G\to G$, $f(xy)=f(x)f(y)$. *Stoga*

$$f(a^x)=f(x^{-1}ax)=f(x^{-1})f(a)f(x)=f(x)^{-1}f(a)f(x)=f(a)^{f(x)}.$$

2.27.Ako je $|G|\geqslant 3$, dokazati da G ima netrivijalan automorfizam.

Rešenje: Pretpostavimo prvo da G nije komutativna grupa. Neka je element $a\in G$, *takav da za neki x iz G bude* $ax\neq xa$. *Tada je* σ_a *jedan netrivijalni automorfizam grupe G.*

Neka je sada G Abel-ova grupa. Za nju postoje dve mogućnosti:

1° postoji bar jedan element a u G za koji je $r(a)>2$; *u ovom slučaju je jedan netrivijalan automorfizam* $f(x)=x^{-1}$;

2° svi elementi u G su reda 2 ; tada je grupa $\underline{G}=(G,+)$ *Abel-ova. Pri tom je G vektorski prostor nad poljem* $\underline{Z}_2=(Z_2, +_2, \cdot_2, 0, 1)$. *Kako je* $|G|\geqslant 3$ *i* $|Z_2|=2$, *to je* $\dim(G)\geqslant 2$, *pa baza za G nad* $\underline{Z}_2$ *ima bar dva elementa. Neka je f jedna permutacija baze, različita od identične. Tada je endomorfizam h prostora G koji proširuje f, jedan netrivijalni automorfizam grupe (G,+).*

2.28.Za sledeće grupe, odrediti grupe automorfizama:

a) S_3 b) V c) $(Z,+)$

Rešenje: a) Opisujemo jedan način odredjivanja grupe Aut G.

$\underline{S}_3=\langle a,b;\ a^3=e,\ b^2=e,\ ab=ba^2\rangle$, *tj.* $S_3=\{e,a,a^2,b,ba,ba^2\}$.

Automorfizam f grupe S_3 *je potpuno odredjen slikama f(a) i f(b) njenih ge-*

neratornih elemenata. Kako je uvek $f(e)=e$, zbog $a^3=e$, $b^2=e$ je $r(f(a))=3$ i $r(f(b))=2$. U grupi S_3 elementi reda 3 su a i a^2, a elementi reda 2 : b,ba, ba^2. Postoje dakle sledeće mogućnosti:

$$f(a)\in\{a,a^2\}\ ,\quad f(b)\in\{b,ba,ba^2\}\ .$$

Svako od ovih preslikavanja se produžava do automorfizma:

$$f_1=\begin{pmatrix} e & a & a^2 & b & ba & ba^2\\ e & a & a^2 & b & ba & ba^2\end{pmatrix}=I$$

$$f_2=\begin{pmatrix} e & a & a^2 & b & ba & ba^2\\ e & a & a^2 & ba & ba^2 & b\end{pmatrix}$$

$$f_3=\begin{pmatrix} e & a & a^2 & b & ba & ba^2\\ e & a & a^2 & ba^2 & a & ba\end{pmatrix}$$

$$f_4=\begin{pmatrix} e & a & a^2 & b & ba & ba^2\\ e & a^2 & a & b & ba^2 & ba\end{pmatrix}$$

$$f_5=\begin{pmatrix} e & a & a^2 & b & ba & ba^2\\ e & a^2 & a & ba & b & ba^2\end{pmatrix}$$

$$f_6=\begin{pmatrix} e & a & a^2 & b & ba & ba^2\\ e & a^2 & a & ba^2 & ba & b\end{pmatrix}$$

Kako je $f_2^3=I$, $f_4^2=I$, $f_2 f_4=f_4 f_2^2$, sledi $\mathrm{Aut}\,S_3\simeq S_3$

b) $\mathrm{Aut}\,V\simeq S_3$

c) $\mathrm{Aut}(Z,+)\simeq C_2$

2.29. Ispitati koje se od sledećih osobina prenose sa grupe G na grupu Aut G :

a) konačnost b) beskonačnost c) komutativnost d) nekomutativnost e) biti grupa bez centra

Rešenje: a) Ako je $|G|=n$ tada je $\mathrm{Aut}\,G<S_n$, pa je $|\mathrm{Aut}\,G|=k$, $k\leqslant n!$

b) Ako je G beskonačna grupa, Aut G ne mora biti beskonačna. Na primer $\mathrm{Aut}\,C_\infty\simeq C_2$

c) Aut G Abel-ove grupe G ne mora biti Abel-ova. Na primer $G=\langle a,b,\ a^2=e,b^2=e,ab=ba\rangle$ je Klein-ova četvorna grupa (dakle Abel-ova) ali $\mathrm{Aut}\,G\simeq S_3$ nije Abel-ova.

d) Grupa G može biti nekomutativna, dok je Aut G komutativna.

e) Neka je G grupa bez centra, tj. grupa u kojoj je e jedini element komutativan sa svim elementima grupe. Pretpostavimo da Aut G ima netrivijalan centar, f; dakle $(\exists a\in G)f(a)\neq a$.

Iz $(\forall g\in\mathrm{Aut}\,G)fg=gf$ sledi $f\sigma_a=\sigma_a f$ gde je $\sigma_a\in Inn\,G$. Odavde, za proizvoljni element $x\in G$ je

$(\sigma_a f)(x)=(f\sigma_a)(x)$, tj. $f(a^{-1}xa)=a^{-1}f(x)a$, odnosno

$$f(a)^{-1}f(x)f(a)=a^{-1}f(x)a,\quad \text{jer je } f\in\mathrm{Aut}\,G\ .$$

Ako x prodje sve elemente grupe G, s obzirom da je $f\in\mathrm{Aut}\,G$, i f(x) prodje sve njene elemente. Prema tome, a i f(a) odredjuju isti unutrašnji automorfizam: $(\forall x\in G)\sigma_a(x)=\sigma_{f(a)}(x)$, tj. $(\forall x\in G)a^{-1}xa=f(a)^{-1}\ldots(a)$,

odnosno $(\forall x \in G) xaf(a)^{-1} = af(a)^{-1}x$.

Dakle, element $af(a)^{-1}$, *koji je različit od e, pripada centru grupe G, suprotno pretpostavci. Stoga je* $\mathrm{Aut}\, G$ *takodje bez centra.*

2.30. Naći primere neizomorfnih grupa čije su grupe automorfizama izomorfne.

Rešenje: Prema zad.1.48 je $\mathrm{Aut}\, S_3 \cong S_3$ *i* $\mathrm{Aut}\, V \cong S_3$, *a* $S_3 \not\cong V$.
Takodje je $\mathrm{Aut}\, C_3 \cong C_2$ *i* $\mathrm{Aut}\, C_\infty \cong C_2$, *a* $C_2 \not\cong C_\infty$.

2.31. Dokazati da je H maksimalna normalna podgrupa u G akko je G/H prosta grupa.

Rešenje: Podgrupa H je maksimalna normalna podgrupa grupe G ako ne postoji normalna podgrupa N takva da je $H < N \lhd G$.
Netrivijalna grupa G je prosta ako ne sadrži pravu normalnu podgrupu.
($\Rightarrow$*) Kako su sve podgrupe (pa i normalne) grupe G/H oblika A/H , gde je* $H < A < G$, *i kako je* $A/H \lhd G/H$ *akko* $A \lhd G$ *(teorema o korespodenciji), to iz maksimalnosti normalne podgrupe H u G, sledi da G/H nema pravih normalnih podgrupa.*
($\Leftarrow$*) Ako H nije maksimalna normalna podgrupa u G, nego postoji podgrupa N,* $N \lhd G$ *tako da* $H < N$, *tada u G/H postoji normalna podgrupa; to je podgrupa N/H, suprotno pretpostavci da je G/H prosta.*

2.32. Navesti primer grupe koja nema (pravu) maksimalnu podgrupu.

Rešenje: Deljive grupe nemaju maksimalnu podgrupu
Takve su napr. grupe $(Q,+)$, $(R,+)$, $(C,+)$, $(R^+,\cdot)$.

2.33. Neka je $a \in G$ $(a \neq e)$. Dokazati: postoji maksimalna normalna podgrupa N grupe G tako da $a \notin N$.

Rešenje: Uočimo skup $\mathcal{H}$ *svih normalnih podgrupa H grupe G za koje* $a \notin H$ *(takve podgrupe postoje u G; jedna je napr.* $\{e\}$, *jer* $a \neq e$*).*
Neka je $\mathcal{L} = \{H_i \mid i \in I\}$ *lanac podgrupa iz* $\mathcal{H}$ *u odnosu na inkluziju (tj. za sve* $i,j \in I$ *je* $H_i \subseteq H_j$ *ili* $H_j \subseteq H_i$*) i neka je* $L = \bigcup_{i \in I} H_i$. *Tada je* $L < G$ *(v.zad. 1.4.9.). Štaviše, važi i* $L \lhd G$, *jer je za proizvoljni* $x \in G$:

$$x^{-1}Lx = x^{-1}(\bigcup_{i \in I} H_i)x = \bigcup_{i \in I} x^{-1}H_i x = \bigcup_{i \in I} H_i = L$$

Prema tome svaki lanac elemenata iz $\mathcal{H}$ *ima gornju granicu. Koristeći Zornovu lemu zaključujemo da postoji maksimalni element u* $\mathcal{H}$.

2.34. Dokazati da u svakoj grupi G postoji podgrupa maksimalna u skupu svih komutativnih podgrupa grupe G.

Rešenje: Uočiti skup $\mathcal{K}$ *svih komutativnih podgrupa u G. Dalje, analogno prethodnom zadatku.*

2.35.Dokazati da sve normalne podgrupe grupe G čine mrežu.

Rešenje: Videti zadatke 1.9. i 1.12.

2.36.Neka je $H<G$ i neka je $Core(H) = \bigcap_{\sigma\in Inn\, G} \sigma(H)$. Dokazati:

a) $Core(H)\lhd G$ b) $Core(H)<H$

c) $N\lhd G \wedge N<H \Rightarrow N<Core(H)$, tj. Core(H) je najveća podgrupa grupe H koja je normalna u G

d) ako je $|G:H| = n$, tada je broj n! deljiv brojem $|G:Core(H)|$ (n! teorema)

e) ako je $H<G$ konačnog indeksa, tada postoji $N\lhd G$, $N<H$ i N je konačnog indeksa u G

Rešenje: a) $Core(H)<G$:

kako je $H<G$ i $\sigma\in Inn\, G$, to je i $\sigma(H)<G$; prema zadatku 2.3.8. je i $\bigcap_{\sigma\in Inn\, G} \sigma(H)<G$.

$Core(H)\lhd G$:

neka je τ proizvoljni unutrašnji automorfizam; tada je

$$\tau(\bigcap_{\sigma} \sigma(H)) = \bigcap_{\sigma} \tau\cdot\sigma(H)$$

(jer je τ 1-1 preslikavanje). Dalje, preslikavanje $F_\tau : Inn\, G \to Inn\, G$ odredjeno sa $F_\tau(\sigma) = \tau\cdot\sigma$ je 1-1 i <u>na</u>, pa je $\bigcap_{\sigma} \tau\,\sigma(H) = \bigcap_{\sigma} \sigma(H)$.

Odavde, $(\forall\tau\in Inn\, G)\,\tau(Core(H)) = Core(H)$.

b) $\bigcap_{\sigma} \sigma(H) \subseteq I(H)$, gde je I identičko preslikavanje, i $I(H)=H$, (primetimo da je $I\in Inn\, G$)

c) Neka je $N\lhd G$ i $N<H$. Tada: $\sigma(N)\subseteq\sigma(H)$ za svako σ iz $Inn\, G$.

Zbog $\sigma(N)=N$ je dakle $N\subseteq\sigma(H)$, tj. $N\subseteq\bigcap_{\sigma}\sigma(H)$

d) Videti zadatak 8.1.17.

e) Ako je H konačnog indeksa u G, tada je, prema d) Core(H) takodje konačnog indeksa u G i $Core(H)\lhd G$.

2.37.Ako je $Z(p^\infty)$ Prüfer-ova grupa, dokazati: $Z(p^\infty)\simeq Z(q^\infty)\Longleftrightarrow p=q$.

Rešenje: ($\Rightarrow$) Neka je h izomorfizam grupa $Z(p^\infty)$ i $Z(q^\infty)$. Uočimo element $a\in Z(p^\infty)$ za koji je $a^p=1$, $a\neq 1$. Takav a postoji jer je

$$Z(p^\infty) = \{x\in C \mid (\exists n\in N)x^{p^n}=1\}$$

Neka je $h(a)=b$. Otuda, zbog $1=h(1)=h(a^p)=h(a)^p=b^p$, je $b^p=1$.

Dalje, za neki n je $b^{q^n}=1$. Ako je $p\neq q$, tada su p i q^n uzajamno prosti; stoga, za neke cele brojeve x,y je $xp+yq^n=1$. Otuda

$$b=b^1=b^{xp+yq^n}=(b^p)^x(b^{q^n})^y=1\cdot 1=1$$

što je kontradikcija, jer je $b\neq 1$. Dakle, $p=q$.

2.38.Ako je $N \lhd G$ i $N < \Phi(G)$, dokazati da je $\Phi(G/N) = \Phi(G)/N$.

Rešenje: M je maksimalna podgrupa grupe G akko je $\bar{M}=M/N$ maksimalna podgrupa grupe G/N.

Zaista: kako $N < \Phi(G)$, a $\Phi(G) < M$, to je $N < M$, pa je $M/N < G/N$ za svaku maksimalnu podgrupu M iz G. Prema teoremi o korespodenciji, za podgrupe H i K grupe G (koje sadrže N) je ispunjeno: $H < K$ akko $H/N < K/N$, odakle sledi gornje tvrdjenje.

Presek svih maksimalnih podgrupa $\bar{M}$ u G/N je $\Phi(G/N)$. Njoj odgovara podgrupa u G koja je presek svih maksimalnih podgrupa u G, tj. $\Phi(G)$. Dakle,

$$\Phi(G/N) = \Phi(G)/N \ .$$

2.39.Ako je $H < G$, dokazati da je grupa $N(H)/C(H)$ izomorfna nekoj podgrupi grupe Aut H.

Rešenje: Preslikavanje $F : N(H) \to \mathrm{Aut}\, H$ *definisano sa*

$$F(g) = \sigma_g \ , \text{ gde je } g \in N(H), \quad \sigma_g(x) = g^{-1}xg \quad (x \in H)$$

je očigledno homomorfizam.

$$\ker F = \{g \mid g \in N(H) \wedge F(g)=I\} = \{g \mid g \in N(H) \wedge (\forall x \in H) g^{-1}xg = x\}$$
$$= \{g \mid g \in N(H) \wedge (\forall x \in H) xg = gx\} = C(H)$$

(jer je $C(H) \lhd N(H)$ - v.zad 1.15.b)).

Dakle, $N(H)/C(H) \simeq F(N(H))$, $F(N(H) < \mathrm{Aut}\, H$.

3.3. KARAKTERISTIČNE I POTPUNO INVARIJANTNE PODGRUPE

Medju normalnim podgrupama grupe G, koje su invarijantne u odnosu na svaki unutrašnji automorfizam te grupe, izdvajaju se one koje su invarijantne u odnosu na *svaki* automorfizam grupe G, odnosno u odnosu na svaki njen endomorfizam.

3.1.*Definicija: Podgrupa H grupe G je karakteristična u G ako je*

$$(\forall f \in \mathrm{Aut}\, G)\ f(H) \subseteq H \ .$$

Skup svih karakterističnih podgrupa grupe G označava se sa Char(G). Lako se dokazuje da je uslov $f(H) \subseteq H$ za karakteristične podgrupe ekvivalentan uslovu $f(H) = H$. Zaista, neka je $f \in \mathrm{Aut}\, G$ i $H' = f(H)$. Kako je H karakterisitčna, to je $H' \subseteq H$, pa $H = f^{-1}(H') \subseteq f^{-1}(H)$, tj. $H \subseteq f^{-1}(H)$. Kako je $f^{-1} \in \mathrm{Aut}\, G$, sledi $f^{-1}(H) \subseteq H$; dakle $H = f^{-1}(H)$, tj. $H = f(H)$.

3.2.*Definicija: Podgrupa H grupe G je potpuno invarijantna u G ako je*

$$(\forall f \in \mathrm{End}\, G)\ f(H) \subseteq H \ .$$

Skup svih potpuno invarijantnih podgrupa grupe G označava se sa Inv(G). U zadacima 3.1,3.4,3.6. je dokazano koje su od važnijih podgrupa, o kojima je bilo reči u ovom i prethodnom poglavlju, katakteristične, odnosno potpuno invarijantne.

Prema definicijama 1.1., 3.1. i 3.2. očigledno je da važi

$$Inv(G) \leqq Char(G) \leqq \mathcal{N}(G) .$$

U opštem slučaju, ove relacije su prave.Naime, postoje normalne podgrupe koje nisu karakteristične (zad.3.2.) i karakteristične koje nisu potpuno invarijantne (zad. 3.5.);

O komutantu grupa, izvodu grupe i uopštenjima (viši komutant - i-ta izvedena grupa) videti poglavlje 9.

PRIMERI I ZADACI

3.1.Dokazati da su karakteristične sledeće podgrupe grupe G:

a) Z(G) b) svaki viši komutant $G^{(i)}$)i=1,2,...)

c) Frattini-eva podgrupa $\Phi(G)$

Rešenje: a) $Z(G)=\{x \mid x\in G \wedge (\forall y\in G)xy=yx\}$, $f\in Aut\,G$. *Tada* $f(xy)=f(yx)$ *za sve* $x\in Z(G)$, $y\in G$, *tj.* $f(x)f(y)=f(y)f(x)$. *Kako je* $\{f(y) \mid y\in G\}=G$, *to i* $f(x)\in Z(G)$. *Dakle,* $f(Z(G))\prec Z(G)$.

b) ***Prema z. 3.4. a). Videti takodje z. 9.2.1. g).***

c) Neka je $f\in Aut\,G$. *Prema teoremi o korespodenciji, M je maksimalna podgrupa u G akko je f(M) maksimalra podgrupa u f(G).*

3.2.Dokazati da je A×{1} normalna podgrupa u grupi G = A×B, ali ne mora biti karakteristična u G.

Rešenje: U grupi G=AxB je, prema zad. 5.1.3. , $Ax\{1\}\lhd G$. *Ako je* $f\in Aut\,G$, *tada nije uvek* $f(Ax\{1\})\prec Ax\{1\}$.

Primer: G=AxA i $f(x,y)=(y,x)$.

3.3.Ako je H karakteristična podgrupa u F, i $F\lhd G$, dokazati da je $H\lhd G$.

Rešenje: Kako je $\sigma_x(F)=F$ *za svako* $x\in G$ $(\sigma_x\in Inn\,G)$, σ_x *odredjuje automorfizam grupe F. Prema pretpostavci je* $(\forall f\in Aut\,F)f(H)=H$, *pa je i* $\sigma_x(H)=H$, *tj.* $H\lhd G$.

3.4.Dokazati da su potpuno invarijantne sledeće podgrupe grupe G:

a) svaki viši komutant $G^{(i)}$ (i=1,2,...)

b) $H=\langle g^n \mid g\in G\rangle$, $n\in N$ c) $H=\langle g \mid g\in G \wedge r(g)<\infty\rangle$

Rešenje: a) Neka je f endomorfizam grupe G. Tada je

$$f(a^{-1}b^{-1}ab)=f(a)^{-1}f(b)^{-1}f(a)f(b) \quad tj. \quad f([a,b])=[f(a),f(b)] ,$$

pa $f(G')\prec G'$. Dakle, $G'\in Inv(G)$.

Kako je $G''=(G')'$, to je $G''\in Inv(G')$, a prema zad. 3.7. je $G''\in Inv(G)$, itd.

b) Ako je $f\in End\,G$ i $g\in G$, tada je $f(g^n)=(f(g))^n$.

c) Ako je $h\in H$, tada postoji $n\in N$, tako da je $h^n=1$. Neka je $f\in End\,G$.

$f(h)^n=f(h^n)=f(1)=1$, pa $f(h)\in H$

3.5. Dokazati da Z(G) nije uvek potpuno invarijantna podgrupa u G.

Rešenje: Neka je G grupa matrica, definisana u zad.1.18.b) i neka je n=2.
Dalje, neka je f proizvoljno preslikavanje $G\to F\setminus\{0\}$ sa svojstvom

$$f(AB)=f(A)+f(B)\qquad (A,B\in G)\qquad (*)$$

Tada je $\psi: G\to G$ definisano sa $\psi(A)=\begin{pmatrix}1 & f(A)\\ 0 & 1\end{pmatrix}$ endomorfizam grupe G. Neka je $C=\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}$, $a\in F$, proizvoljni element centra Z(G). Tada je $\psi(C)=\begin{pmatrix}1 & f(C)\\ 0 & 1\end{pmatrix}$, tj. $\psi(C)\notin Z(G)$, jer $f(c)\neq 0$.
U stvari, za f je dovoljno izabrati preslikavanje $G\to F$ sa svojstvom (*) takvo da nije za sve $C\in Z(G)$ ispunjeno $f(C)=0$.
Primer: neka je F polje Q racionalnih brojeva i f preslikavanje $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\to k$, gde je $ad-bc=\frac{p}{q}2^k$, $k\in Z$, a p i q su neparni brojevi.

3.6. Dokazati da su sve podgrupe ciklične grupe potpuno invarijantne.

Rešenje: Neka je $G=\langle a\rangle$ ciklična grupa, $H=\langle a^k\rangle$ njena podgrupa, i $f\in End\,G$.
Tada je $f(a)=a^m$ i $f(a^k)=f(a)^k=(a^m)^k=(a^k)^m$, tj. $f(H)\prec H$.

3.7. Dokazati da su svojstva karakterističnosti i potpune invarijantnosti u grupi, tranzitivna, tj.

a) $H\in Char(K)\wedge K\in Char(G)\Longrightarrow H\in Char(G)$

b) $H\in Inv(K)\wedge K\in Inv(G)\Longrightarrow H\in Inv(G)$

Rešenje: a) Neka je $f\in Aut\,G$ i $H\prec K\prec G$, tada $f(K)=K$, tj. $f\restriction_K\in Aut\,K$.
No, po pretpostavci, za svako $g\in Aut\,K$ je $g(H)=H$, pa je i $f(H)=H$.
b) Slično kao pod a)

3.8. Ako su H i K karakteristične (potpuno invarijantne) podgrupe grupe G, tada je $[H,K]$ karakteristična (potpuno invarijantna) u G. Dokazati.

3.9. Ako su H_i, $i\in I$ karakteristične (potpuno invarijantne) podgrupe grupe G, tada je i $\bigcap_{i\in I} H_i$ karakteristična (potpuno invarijantna) u G.

Rešenje: Predpostavka : $(\forall f\in End\,G)(\forall i\in I)f(H_i)\prec H_i$. Tada

$$a\in\bigcap_{i\in I}H_i\Longrightarrow(\forall i\in I)a\in H_i\Longrightarrow(\forall f\in End\,G)(\forall i\in I)f(a)\in H_i$$
$$\Longrightarrow(\forall f\in End\,G)f(a)\in\bigcap_{i\in I}H_i$$

Odnosno, $f(\bigcap_{i\in I}H_i)\prec\bigcap_{i\in I}H_i$

3.10. Ako su H_i, $i \in I$ karakteristične (potpuno invarijantne) podgrupe grupe G, tada je i $\langle \bigcup_{i\in I} H_i \rangle$ karakteristična (potpuno invarijantna) u G. Dokazati.

Rešenje: Elementi grupe $\langle \bigcup_{i\in I} H_i \rangle$ *su oblika* $h_{i_1} h_{i_2} \ldots h_{i_k}$, $h_{i_j} \in H_{i_j}$. *Ako je* $f \in End\, G$ *tada*

$$f(h_{i_1} h_{i_2} \ldots h_{i_k}) = f(h_{i_1}) f(h_{i_2}) \ldots f(h_{i_k}) = h'_{i_1} h'_{i_2} \ldots h'_{i_k} = h$$

gde su $h'_{i_j} = f(h_{i_j})$ *iz* H_{i_j} *jer* $f(H_{i_j}) \leq H_{i_j}$. *Dakle,* $h \in \langle \bigcup_{i\in I} H_{i_j} \rangle$

3.11. Neka je H jedina podgrupa reda n u grupi G. Dokazati da je $H \in Char(G)$.

Rešenje: Neka je $H \leq G$ *takva da je* $|H| = n$. *Tada je* $|f(H)| = n$, *za sve* $f \in Aut\, G$. *Kako je H jedina podgrupa reda n u G, to je* $(\forall f \in Aut\, G) f(H) = H$.

3.12. Dokazati da su $\mathcal{N}(G)$, Char(G) i Inv(G) kompletne mreže.

Rešenje: $\mathcal{N}(G)$ *u odnosu na operacije* $\cap$ *i* $\langle \ldots \cup \ldots \rangle$ *je mreža (v. zad. 1.35. Ona je kompletna, jer za svaki neprazan skup S normalnih podgrupa za G, postoje podgrupe* $\inf S = \bigcap \{H \mid H \in S\}$, $\sup S = \langle \bigcup \{H \mid H \in S\} \rangle$ *(v. zadatke 1. 9 i 1.12). Najmanji element ove mreže je jedinična podgrupa I, a najveći sama grupa G. Na osnovu zadataka 3.9. i 3.10, Char(G) i Inv(G) su takodje kompletne mreže* $(f(I) = I,\ f(G) \leq G$ *za svaki* $f \in End\, G)$.

Napomena: Mreža $\mathcal{N}(G)$ *je i* <u>*modularna*</u>, *tj. za sve normalne podgrupe grupe G za koje je* $B \leq A$, *važi*

$$A \cap (BC) = B(A \cap C)$$

(prema zad. 1.12. $\langle B \cup C \rangle = BC$, ako su $B, C \in \mathcal{N}(G)$).

Kako su podmreže modularne mreže, takodje modularne, sledi da su Char(G) i Inv(G) modularne mreže.

4. GRUPE PERMUTACIJA

U drugom poglavlju napomenuto je da su grupe permutacija prvi primeri grupa, ali isto tako i apstraktnih algebarskih struktura uopšte. Zato nije neobično da se savremeni pojam grupe odvojio od grupa permutacija nakon dugog perioda. Danas, teorija grupa permutacija predstavlja mali deo savremene teorije grupa.

Ipak, vredno je spomenuti da postoje bar dva ozbiljna razloga zašto su ove grupe ostale važan deo savremene teorije grupa.

Prvi razlog se odnosi na njihovu primenljivost u odredjenim situacijama. Naime, kad god se proučavaju svojstva simetrija nekih objekata sa konačnim opisom, grupe permutacija se javljaju kao prirodan algebarski model za opis tih osobina. Jedan primer te vrste smo upoznali; to je dijedarska grupa D_n, grupa simetrije pravilnog n-tougla.

Drugi razlog je *univerzalnost* grupa simetrije, s obzirom da se svaka grupa predstavlja kao neka grupa permutacija. Cayley-eva teorema kazuje upravo to, da je *svaka* grupa izomorfna nekoj grupi permutacija.

4.1. GRUPA S_n

Svako preslikavanje $f : X \xrightarrow[1-1]{na} X$ nepraznog skupa X naziva se *permutacijom* skupa X. Kako je proizvod bijekcija takodje bijekcija, i inverzna funkcija bijekcije je bijekcija, sledi da skup svih permutacija skupa X čini grupu u odnosu na slaganje funkcija.

1.1. Definicija: Simetrična grupa nepraznog skupa X je grupa $\underline{S}_X = (S_X, \circ, I_X)$ *gde je* S_X *skup svih permutacija skupa X,* $\circ$ *slaganje funkcija, a* I_X *je identička funkcija skupa X.*

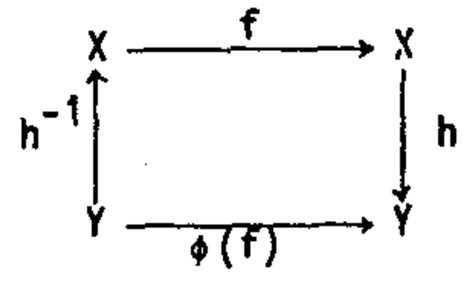
Za grupu $\underline{S}_X$ koristi se i oznaka Sym(X). I ubuduće, simbol S_X označava grupu $\underline{S}_X$ ali i njen domen.

Simbol S_n označava grupu S_X za $X = \{1,2,\ldots,n\}$. Dakle, $|S_n| = n!$.

1.2. Teorema: $|X| = |Y| \Rightarrow S_X \simeq S_Y$.

Dokaz: Neka su X,Y neprazni skupovi iste kardinalnosti. Tada postoji preslikavanje $h : X \xrightarrow[1-1]{na} Y$. Neka je preslikavanje $\phi : S_X \to S_Y$ definisano sa

$(\forall f \in S_X)\ \phi(f) = h^{-1} \circ f \circ h$.



Implikacija $f \in S_X \Rightarrow \phi(f) \in S_X$ važi
s obzirom da je proizvod bijekcija takodje bijekcija. Takodje je

$$\phi(f \circ g) = (h^{-1} \circ f \circ h) \circ (h^{-1} \circ g \circ h) = \phi(f) \circ \phi(g) ,$$

tj. ϕ je homomorfizam.
Dalje, ϕ ima inverznu bijekciju $\psi : S_Y \to S_X$, gde $\psi : g \longmapsto h \circ g \circ h^{-1}$, pa je ϕ 1-1 i na. Dakle, $\phi : S_X = S_Y$. ▼

Prema prethodnoj teoremi, algebarske osobine grupe S_X su u potpunosti odredjene brojem elemenata skupa X. Dakle, za svaki konačni skup X važi $S_X \cong S_{|X|}$.

1.3. *Definicija: Podgrupa $G < S_X$, naziva se grupom permutacija nad skupom X. Ako je $G < S_n$, tada je G grupa permutacija stepena n.*

Permutacija $f \in S_n$ je *ciklus dužine k*, u oznaci $f=(i_1 i_2 \ldots i_k)$, ako je $f(i_1)=i_2$, $f(i_2)=i_3$,..., $f(i_{k-1})=i_k$, $f(i_k)=i_1$, gde su $i_1, i_2, \ldots, i_k$ različiti elementi iz $\{1,2,\ldots,n\}$, i ako je $f(x)=x$ za $x \in \{1,2,\ldots,n\} \setminus \{i_1, i_2, \ldots, i_k\}$. Ciklus dužine 2 **naziva se *transpozicijom*.**

Permutacije f i g iz S_X su *disjunktne* ako

$$(\forall x \in X)(f(x) \neq x \Rightarrow g(x) = x)$$

Drugim rečima, svaki x koji se preslikava u neki **element skupa** X jednom permutacijom, ostaje fiksiran u odnosu na drugu permutaciju.

Prema zadatku 1.11. svaka permutacija f konačnog skupa može se predstaviti na jedinstven način kao proizvod disjunktnih ciklusa. Ovakvo predstavljanje permutacije f naziva se *ciklusnom dekompozicijom* te permutacije.

Primeri i zadaci

1.1. Odrediti elemente simetrične grupe S_X ako je
a) $X = \{a,b\}$, b) $X = \{1,2,3\}$, c) $X = Z$

Rešenje: a) Permutacije skupa X su $I = \begin{pmatrix} a & b \\ a & b \end{pmatrix}$, $f = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ *; one, očigledno, čine grupu reda 2.*

b) Sve permutacije skupa X su

$$I=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad f_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad f_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

$$f_3=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad f_4=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\quad f_5=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

U odnosu na množenje preslikavanja, one čine grupu reda 6.

c) Elementi ove grupe su sva preslikavanja $f: Z \xrightarrow[1-1]{na} Z$ *i čine beskonačnu simetričnu grupu kardinalnosti* $2^{\aleph_0}$.

1.2.Izračunati $f\circ g$, $g\circ f$, f^{-1}, $(f\circ g)^{-1}$ ako je

$$f=\begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix},\quad g=\begin{pmatrix}1&2&3&4&5\\2&3&5&1&4\end{pmatrix}$$

Rešenje:

$$f\circ g=\begin{pmatrix}1&2&3&4&5\\1&2&4&3&5\end{pmatrix},\quad g\circ f=\begin{pmatrix}1&2&3&4&5\\5&2&3&4&1\end{pmatrix},$$

$$f^{-1}=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix},\quad (f\circ g)^{-1}=\begin{pmatrix}1&2&3&4&5\\1&2&4&3&5\end{pmatrix}$$

1.3.Dokazati: Ako je $n\leq m$ tada se S_n utapa u S_m.

Rešenje: Preslikavanje $\begin{pmatrix}1&2&\dots&n\\a_1&a_2&\dots&a_n\end{pmatrix}\longmapsto\begin{pmatrix}1&2&\dots&n&n+1&\dots&m\\a_1&a_2&\dots&a_n&n+1&\dots&m\end{pmatrix}$

(gde $a_1,\dots,a_n\in\{1,\dots,n\}$*) je jedno utapanje grupe* S_n *u grupu* S_m.

1.4.Napisati tablice za sledeće grupe permutacija:

a) S_2 , b) S_3 , c) S_4 , d) Aut S_3

Rešenje: a) S_2:

$\circ$	I	f
I	I	f
f	f	I

gde su I,f kao u zadatku 1.1.a)

b) Koristeći oznake iz zadatka 1.1.b), tablica za S_3 *je sledeća*

$\circ$	I	f_1	f_2	f_3	f_4	f_5
I	I	f_1	f_2	f_3	f_4	f_5
f_1	f_1	I	f_4	f_5	f_2	f_3
f_2	f_2	f_3	I	f_1	f_5	f_4
f_3	f_3	f_2	f_5	f_4	I	f_1
f_4	f_4	f_5	f_1	I	f_3	f_2
f_5	f_5	f_4	f_3	f_2	f_1	I

Napomena: Grupa S_3 *može se predstaviti i na sledeći način. Uvedimo oznake* $a=f_3$, $b=f_1$, $e=I$; *preostali elementi iz* S_3 *su:* a^2, ba, ba^2. *Neposrednom proverom možemo ustanoviti da važi:*

$$a^3=e,\ b^2=e,\ ab=ba^2 \qquad (*)$$

Svaka grupa generisana elementima a,b koji zadovoljavaju ove jednakosti izomorfna je grupi S_3. *Dakle* $S_3=\langle a,b;\ a^3=e, b^2=e, ab=ba^2\rangle$.

c) Koristeći ciklusno izražavanje, v. 2. odeljak, elementi grupe S_4 **su**

$$I=\begin{pmatrix}1234\\1234\end{pmatrix},\quad f_1=\begin{pmatrix}1234\\1243\end{pmatrix}=(34),\quad f_2=\begin{pmatrix}1234\\1324\end{pmatrix}=(23),\quad f_3=\begin{pmatrix}1234\\1342\end{pmatrix}=(234)$$

$$f_4=\begin{pmatrix}1234\\1423\end{pmatrix}=(243),\quad f_5=\begin{pmatrix}1234\\1432\end{pmatrix}=(24),\quad f_6=\begin{pmatrix}1234\\2134\end{pmatrix}=(12),\quad f_7=(^{1234})=(12)(34)$$

$$f_8=\begin{pmatrix}1234\\2314\end{pmatrix}=(123),\quad f_9=\begin{pmatrix}1234\\2341\end{pmatrix}=(1234),\ f_{10}=\begin{pmatrix}1234\\2413\end{pmatrix}=(1243),\ f_{11}=\begin{pmatrix}1234\\2431\end{pmatrix}=(124)$$

$$f_{12}=\begin{pmatrix}1234\\3124\end{pmatrix}=(132),\quad f_{13}=\begin{pmatrix}1234\\3142\end{pmatrix}=(1342),\ f_{14}=\begin{pmatrix}1234\\3214\end{pmatrix}=(13),\quad f_{15}=\begin{pmatrix}1234\\3241\end{pmatrix}=(134)$$

$$f_{16}=\begin{pmatrix}1234\\3412\end{pmatrix}=(13)(24),\ f_{17}=\begin{pmatrix}1234\\3421\end{pmatrix}=(1324),\ f_{18}\begin{pmatrix}1234\\4123\end{pmatrix}=(1432),\ f_{19}=\begin{pmatrix}1234\\4132\end{pmatrix}=(142)$$

$$f_{20}=\begin{pmatrix}1234\\4213\end{pmatrix}=(143),\quad f_{21}=\begin{pmatrix}1234\\4231\end{pmatrix}=(14),\ f_{22}=\begin{pmatrix}1234\\4312\end{pmatrix}=(1423),\ f_{23}=\begin{pmatrix}1234\\4321\end{pmatrix}=(14)(23)$$

tada, npr. $f_6 \circ f_{14}=\begin{pmatrix}1234\\2134\end{pmatrix}\circ\begin{pmatrix}1234\\3214\end{pmatrix}=\begin{pmatrix}1234\\3124\end{pmatrix}=(132)$.

d) $Aut\ S_3 \cong S_3$.

1.5.Ako je $f\in S_n$, dokazati da je $f^{n!}=I$.

Rešenje: Kako je $|S_n|=n!$ *i* $f\in S_n$, *prema Lagrange-ovoj teoremi*

$$r(f)\ |\ n!\ .$$

1.6.Odrediti broj $r_2^{(n)}$ elemenata reda 2 u grupi S_n.

Rešenje: Neka je $f\in S_n$ *i* $r(f)=2$. *Permutaciji f pridružimo sledeću relaciju* $\sim_f$:

$$x \sim_f y \iff (y=x \vee y=f(x))$$

Kako je f reda 2, $\sim_f$ *je relacija ekvivalencije. Klase ekvivalencije su, očigledno, jednočlani i dvočlani skupovi. Dakle, relaciji* $\sim_f$ *odgovara sledeće razbijanje skupa* $X=\{1,2,\ldots,n\}$:

$$\{A_i \mid i=1,2,\ldots,m\}\cup\{B_j \mid j=1,2,\ldots,k\}$$

gde su A_i *jednočlani a* B_j *dvočlani skupovi, i gde je* $m+2k=n$. *Dalje, neka je* $A=A_1\cup A_2\cup\ldots\cup A_m$. *Primetimo da je za* $x\in A$ *uvek* $f(x)=x$, *a za* $x\in B_j$, $B_j=\{a,b\}$, *važi* $f(a)=b$ *i* $f(b)=a$.

Prema tome, broj $r_2^{(n)}$ *elemenata reda 2 u* S_n *jednak je broju razbijanja*

skupa X oblika $\{A\}\cup\{B_j \mid j=1,\dots,k\}$, gde je $k>1$ i $|B_j|=2$. Skup $B=B_1\cup\dots\cup B_k$ gde je $|B|=2k$ moguće je izdvojiti iz skupa X na $\binom{n}{2k}$ načina. Ako sa t_k označimo broj razbijanja skupa B od $2k$ elemenata na dvočlane skupove, tada je

$$r_2^{(n)} = \sum_{0<2k\leq n}\binom{n}{2k}t_k \ .$$

Lako se utvrdjuje da je $t_{k+1}=(2k+1)t_k$, odakle je $t_k=1\cdot 3\cdots(2k-1)=(2k-1)!!$, $(k>1)$. Dakle

$$r_2^{(n)} = \sum_{0<2k<n}\binom{n}{2k}(2k-1)!!$$

1.7.Odrediti broj elemenata reda p (p - prost broj) u grupi S_n.

Rešenje: Pretpostavimo da je $p>3$, jer je slučaj $p=2$ rešen u predhodnom zadatku. I ovde dokazujemo da svaka permutacija reda p odredjuje razbijanje skupa $\{1,2,\dots,n\}$ oblika $\{A\}\cup\{B_i \mid i=1,\dots,m\}$ gde je $|B_i|=p$, $B_i=\{a,f(a),\dots,f^{p-1}(a)\}$, $A=\{x \mid x<n\wedge f(x)=x\}$, $pm+|A|=n$. Takodje, svako razbijanje ovoga tipa odredjuje jednu permutaciju reda p.

Analogno prethodnom zadatku izvodi se da je traženi broj jednak

$$r_p^{(n)} = \sum_{p\leq pm\leq m}\binom{n}{pm}(p-1)!^m\, t_{pm}$$

gde je t_{pm} broj razbijanja skupa od pm elemenata na podskupove od p elemenata. Kako za t_{pm} važi

$$t_{pm+p}=\left[1+\binom{p}{1}\binom{pm}{1}+\dots+\binom{p}{k}\binom{pm}{k}\right]t_{pm} \quad \text{gde je } k=\frac{p-1}{2}$$

to je

$$t_{(m+1)p}=\prod_{0\leq j\leq m}\left(\sum_{0\leq i\leq\frac{p-1}{2}}\binom{p}{i}\binom{pj}{i}\right) \ .$$

Dakle, $$r_p^{(n)}=\sum_{pm\leq k}\binom{n}{pm}(p-1)!^m\prod_{0\leq j\leq m-1}\left(\sum_{0\leq i\leq k}\binom{p}{i}\binom{pj}{i}\right)$$

Primer za $p=3$:

$$r_3^{(n)}=\sum_{3\leq 3m<n}2^m\binom{n}{3m}\prod_{0\leq j\leq m-1}(9j+1),$$

tj. $r_3^{(3)}=2$, $r_3^{(4)}=8$, $r_3^{(5)}=20$, itd.

1.8.Odrediti broj transpozicija t_n skupa od n elemenata $(n\in N)$.

Rešenje: U skupu X od n elemenata, svaka dva medjusobno različita elementa $a,b\in X$ odredjuju tačno jednu transpoziciju $(a\ b)$. Kako je $(a\ b)=(b\ a)$, to je $t_n=\binom{n}{2}$.

1.9.Ako su f i g disjunktne permutacije, tada je $fg=gf$. Dokazati.

1.10.Ciklusi $(i_1\ i_2\dots i_k)$ i $(j_1\ j_2\dots j_1)$ su disjunktni akko je

$\{i_1,i_2,\ldots,i_k\}\cap\{j_1,j_2,\ldots,j_1\}=\emptyset$. Dokazati.

Rešenje: Dve permutacije f i g su disjunktne akko $(\forall x\in X)(f(x)=x\vee g(x)=x)$

1.11. Neka je X konačan skup i $f\in S_X$. Dokazati:

a) Relacija $x\rho y\Leftrightarrow(\exists i\in Z)(f^i(x)=y)$, $(x,y\in X)$

je relacija ekvivalencije skupa X; odrediti klase ekvivalencije.

b) f se može jedinstveno (do na raspored ciklusa) predstaviti kao proizvod disjunktnih ciklusa.

Rešenje: a) $x\rho x$ *jer* $f^0(x)=x \quad (f^0\equiv I)$;

$x\rho y\Rightarrow(\exists i\in Z)f^i(x)=y\Rightarrow(\exists i\in Z)x=f^{-i}(y)\Rightarrow(\exists j\in Z)x=f^j(y)\Rightarrow y\rho x$;

$x\rho y\wedge y\rho u\Rightarrow(\exists i\in Z)f^i(x)=y\wedge(\exists j\in Z)f^j(y)=u\Rightarrow(\exists i,j\in Z)f^j(f^i(x))=u$

$\Rightarrow(\exists i,j\in Z)f^{i+j}(x)=u\Rightarrow(\exists k\in Z)f^k(x)=u\Rightarrow x\rho u$.

Klase ekvivalencije su:

$$C_x=\{y\mid x\rho y\}=\{f^i(x)\mid i\in Z\}=\{x,f(x),f^2(x),\ldots,f^{-1}(x),\ldots\}\ .$$

Kako je X konačan skup, u skupu $\{x,f(x),\ldots,f^{-1}(x),\ldots\}$ *nisu svi elementi različiti, tj. postoje nenegativni brojevi m i l takvi da je*

$$f^m(x)=f^l(x)\quad (m>l),\quad \text{odnosno}\quad f^{m-l}(x)=x\ .$$

Neka je k najmanji ***pozitivan broj takav da je*** $f^k(x)=x$. ***Tada je***

$$f^{-1}(x)=f^{-1}(f^k(x))=f^{k-1}(x),\quad f^{-2}(x)=f^{-2}(f^k(x))=f^{k-2}(x),\ldots\ .$$

Dakle, $C_x=\{x,f(x),f^2(x),\ldots,f^{k-1}(x)\}$.

Napomena: navedene klase ekvivalencije nazivaju se orbitama permutacije f.

b) X je konačan skup, pa za dato $f\in S_X$, *gornja relacija razbija X na konačno mnogo klasa ekvivalencije, tj. orbita* $C_1,C_2,\ldots,C_n$. *Svakoj orbiti* $C_i=\{x,f(x),\ldots,f^j(x)\}$ *može se pridružiti ciklus* $cy(C_i)=(x\ f(x)\ f^2(x)\ldots f^j(x))$, *(ostali elementi su fiksirani). Kako su orbite disjunktne i pokrivaju ceo skup X, ovako dobijeni ciklusi su disjunktni i*

$$f=cy(C_1)cy(C_2)\ldots cy(C_n)\ .$$

Jedinstvenost: neka su $\alpha_1,\alpha_2,\ldots,\alpha_i,\beta_1,\beta_2,\ldots,\beta_j$ *ciklusi takvi da je* $f=\alpha_1\alpha_2\ldots\alpha_i=\beta_1\beta_2\ldots\beta_j$. *Za svaki* $x\in X$ *za koji je* $f(x)\neq x$, *postoje k,l* $(1\leqslant k\leqslant i,\ 1\leqslant l\leqslant j)$ *tako da je* $f(x)=\alpha_k(x)=\beta_l(x)$.

Kako je $(\forall n\in N)\alpha_k^n(x)=\beta_l^n(x)$, *sledi* $\alpha_k=\beta_l$.

1.12. Sledeće permutacije predstaviti kao proizvod disjunktnih ciklusa:

a) $\begin{pmatrix}1&2&3&4&5&6&7\\3&4&1&7&6&5&2\end{pmatrix}$, b) $\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}$, c) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&5&8&7&9&2&1&3&6\end{pmatrix}$

Rešenje: a) $C_1=\{1,f(1),f^2(1),\ldots\}=\{1,3\}=C_3$, *pa je* $cy(C_1)=(1\ 3)$.

Slično, $C_2=\{2,4,7\}=C_4=C_7$, $cy(C_2)=(2\ 4\ 7)$,

$C_5=\{5,6\}=C_6$, $cy(C_5)=(5\ 6)$.

Dakle, $f=(1\ 3)(2\ 4\ 7)(5\ 6)$.

b) $(1\ 2\ 4)(3\ 5)$.

c) $(1\ 4\ 7)(2\ 5\ 9\ 6)(3\ 8)$.

1.13.Dokazati da je red permutacije $f\in S_n$ jednak najmanjem zajedničkom sadržaocu redova disjunktnih ciklusa kojima se ta permutacija predstavlja.

Rešenje: Neka je $f=\alpha_1\alpha_2\ldots\alpha_k$, *gde su* α_i $(i=1,\ldots,k)$ *disjunktni ciklusi, i neka je* $f^m=I$. *Tada*

$$f^m=(\alpha_1\alpha_2\ldots\alpha_k)^m=\alpha_1^m\alpha_2^m\ldots\alpha_k^m$$

jer elementi $\alpha_1,\ldots,\alpha_k$ *komutiraju. S obzirom da su stepeni disjunktnih ciklusa takodje disjunktni, to je*

$$f^m=I \Leftrightarrow (\forall i\in\{1,\ldots,k\})\alpha_i^m=I ,$$

odakle neposredno sledi: $(\forall i\in\{1,\ldots,k\})r(\alpha_i)\mid m$.

Dakle, $m=NZS(r(\alpha_1),\ldots,r(\alpha_k))$.

1.14.Ako su $f,g\in S_n$ i ako je $f=(i_1\ldots i_k)\ldots(j_1\ldots j_1)$ **ciklusna** dekompozicija permutacije f, dokazati da je

$$gfg^{-1}=(g(i_1)g(i_2)\ldots g(i_k))\ldots(g(j_1)g(j_2)\ldots g(j_1))$$

ciklusna dekompozicija permutacije gfg^{-1}.

Rešenje: U cikličnoj dekompoziciji $f=(i_1\ldots i_k)\ldots(j_1\ldots j_1)$ *uočimo proizvoljni element i, neposredno naredni u ovoj dekompoziciji je f(i). Slike elemenata i i f(i) u odnosu na permutaciju g su g(i) i gf(i).*

Koristeći činjenicu da je

$$gf(i)=gfg^{-1}g(i)$$

zaključujemo da je u cikličnoj dekompoziciji permutacije gfg^{-1}, *iza elementa g(i) neposredno naredni,(tj. njegova slika), upravo element gf(i), što je i trebalo dokazati.*

1.15.Odrediti cikličnu dekompoziciju permutacije gfg^{-1} ako je

a) $g=\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}$, $f=(1\ 2)(3\ 4)$,

b) $g=(a\ c\ d)(e\ f)$, $f=(a\ d\ e)(b)(c)$.

Rešenje: Koristeći prethodni zadatak je:

a) $gfg^{-1} = (3\ 1)(4\ 2)$

b) $gfg^{-1} = (c\ a\ f)(b)(d)$, *tj.* $gfg^{-1} = (c\ a\ f)$.

1.16.Odrediti red ciklusa $(i_1\ i_2\ \dots\ i_k)$.

Rešenje: Red ciklusa $(i_1\ i_2\ \dots\ i_k)$ *je* k.

1.17.Dokazati da se sve permutacije iz S_n mogu predstaviti kao proizvod transpozicija.

Rešenje: Koristeći zad. 1.11., dovoljno je dokazati da je svaki ciklus proizvod transpozicija. Zaista,

$$(1\ 2\ 3\ \dots\ k) = (1\ 2)(1\ 3)\dots(1\ k)\ .$$

1.18.Sledeće permutacije predstaviti proizvodom transpozicija

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 5 & 4 \end{pmatrix}$, b) $(1\ 4\ 3)(2\ 5)$, c) $(2\ 3\ 6)(1\ 5\ 4)^{-1}$.

Rešenje: a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 5 & 4 \end{pmatrix} = (1\ 3\ 2)(4\ 6) = (1\ 3)(1\ 2)(4\ 6)$.

b) $(1\ 4)(1\ 3)(2\ 5)$.

c) $(2\ 3)(2\ 6)(1\ 4)(1\ 5)$.

1.19.Dokazati da je grupa S_3 generisana sa dva elementa. Da li je generisana jednim elementom?

Rešenje: Videti zad. **1.17.**

1.20.Dokazati da je grupa S_n generisana sledećim ciklusima:

a) $(1\ 2)$, $(1\ 3)$,..., $(1\ n)$, b) $(1\ 2\ \dots\ n-1)$,$(n-1,n)$, c) $(1\ 2)$,$(1\ 2\dots n)$

Rešenje: Koristeći zad. 1.5., dovoljno je dokazati da se navedenim ciklusima može predstaviti proizvoljna transpozicija (a b).

a) $(a\ b) = (1\ a)(1\ b)(1\ a)$

b) $c_1 = (1\ 2\ \dots\ n-1)$, $c_2 = (n-1\ \ n)$, $c_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 \\ n-1 & 1 & 2 & \dots & n-2 \end{pmatrix}$

Svaku transpoziciju (a b) je moguće predstaviti kao

$$(a\ b) = (n\ a)(n\ b)(n\ a)\ .$$

Kako je $(n\ m) = c_1^{-m} c_2 c_1^{-m}$, *biće*

$$(a\ b) = c_1^{-a} c_2 c_1^{a} c_1^{-b} c_2 c_1^{b} c_1^{-a} c_2 c_1^{a}\ .$$

1.21.Dokazati da je podgrupa grupe S_4, generisana elementima $(1\ 2\ 3\ 4)$ i $(2\ 4)$ dijedarska grupa D_4.

Rešenje: Ako je $a=(1\ 2\ 3\ 4)$ *i* $b=(2\ 4)$, *tada* $r(a)=4$, $r(b)=2$ *i* $ab=ba^3$, *tj važe strukturne jednakosti grupe* D_4 *(videti uvodni deo odeljka 2.2.).*

4.2. GRUPA A_n

Funkcija parnosti je preslikavanje P sa domenom S_n definisano sledećom formulom

$$P(f) = \prod_{i<j} \frac{f(j)-f(i)}{j-i} \qquad (f \in S_n) .$$

Koristeći osobine ove funkcije moguće je izvršiti klasifikaciju permutacija skupa {1,2,...,m}, a njeno najvažnije svojstvo iskazano je sledećim tvrdjenjem.

2.1.Teorema: (i) $(\forall f \in S_n)\ P(f) \in \{1,-1\}$

(ii) Preslikavanje P je homomorfizam grupe S_n na grupu $(\{1,-1\},\cdot,1)$.

Dokaz: (i) Neka je $S = \{(i,j) \mid 1 < i < j < n\}$ i neka je za $f \in S_n$ preslikavanje $g : S \to S$ definisano sa

$$g(i,j) = \begin{cases} (f(i),f(j)), & f(i) < f(j) \\ (f(j),f(i)), & f(j) < f(i) \end{cases} , \quad \text{gde } (i,j) \in S.$$

Neposredno se proverava da je $g \in Sym(S)$. Dalje, uvedimo funkciju a sa domenom S: $a_s = |j-i|$ gde $s \in S$ i $s=(i,j)$. Tada, prema 1.3.12. i s obzirom da je $a_{g(s)} = |f(j)-f(i)|$ imamo

$$\prod_{i<j} |j-i| = \prod_{s \in S} a_s = \prod_{s \in S} a_{g(s)} = \prod_{i<j} |f(j)-f(i)| ;$$

dakle, $P(f) \in \{1,-1\}$.

(ii) Neka su f,g proizvoljni elementi iz S_n.

$$P(f\circ g) = \prod_{i<j} \frac{(f\circ g)(j)-(f\circ g)(i)}{j-i} = \prod_{i<j} \frac{f(g(j))-f(g(i))}{j-i} =$$

$$= \prod_{i<j} \frac{f(g(j))-f(g(i))}{g(j)-g(i)} \cdot \frac{g(j)-g(i)}{j-i} = \prod_{i<j} \frac{f(g(j))-f(g(i))}{g(j)-g(i)} \cdot \prod_{i<j} \frac{g(j)-g(i)}{j-i}$$

$$= \prod_{(k,l)\in S_1} \frac{f(g(l))-f(g(k))}{g(l)-g(k)} \cdot \prod_{(k,l)\in S_2} \frac{f(g(l))-f(g(k))}{g(l)-g(k)} \cdot P(g)$$

gde je

$$S_1 = \{(i,j) \mid i < j < n,\ g(i) < g(j)\}$$
$$S_2 = \{(i,j) \mid i < j < n,\ g(i) > g(j)\}$$

$$= \prod_{(k,l)\in S_1} \frac{f(g(l))-f(g(k))}{g(l)-g(k)} \cdot \prod_{(k,l)\in S_2} \frac{f(g(k))-f(g(l))}{g(k)-g(l)} \cdot P(g)$$

Kako je preslikavanje $\phi : (i,j) \longmapsto (g(i),g(j))$ skupa X^2 u X^2, gde je $X=\{1,2,...,n\}$, 1-1 i na, to je dalje

$$= \prod_{(i,j)\in \phi(S_1)} \frac{f(j)-f(i)}{j-i} \cdot \prod_{(i,j)\in \phi(S_2)} \frac{f(j)-f(i)}{j-i} \cdot P(g) = \prod_{i<j} \frac{f(j)-f(i)}{j-i} \cdot P(g) = P(f)P(g)$$

Permutacija $f \in S_n$ je *parna* ukoliko je $P(f)=1$. Ako je $P(f)=-1$, f se naziva *neparnom* permutacijom. Ova terminologija je u vezi sa brojem inverzija permutacije. Naime, ako je $f \in S_n$, par $(i,j) \in S$ (S je skup uveden u teoremi 2.1.) čini *inverziju* u permutaciji f akko $f(j) < f(i)$. Neka je $\alpha(i,j)=1$ ako (i,j) čini inverziju, inače $\alpha(i,j)=0$. Tada očigledno $f(j)-f(i) = (-1)^{\alpha(i,j)}|f(j)-f(i)|$, pa prema izvodjenju u teoremi 2.1. neposredno nalazimo

$$\prod_{i<j} (f(j)-f(i)) = \prod_{i<j} (-1)^{\alpha(i,j)}|f(j)-f(i)| = (-1)^{i(f)}\prod_{i<j} |f(j)-f(i)|$$
$$= (-1)^{i(f)}\prod_{i<j} (j-i) ;$$

dakle,

$$P(f) = (-1)^{i(f)} \text{ , gde je } i(f) \text{ broj inverzija permutacije } f.$$

Skup svih parnih permutacija iz S_n označavamo sa A_n. Kako je

$$f \in A_n \Leftrightarrow P(f)=1 \Leftrightarrow f \in \ker P \text{ ,}$$

to je $A_n = \ker P$. Dakle, važi sledeća

2.2.*Teorema:* $A_n \lhd S_n$.

2.3.*Definicija:* *Grupa A_n je alternirajuća grupa skupa $\{1,2,\ldots,n\}$.*

Jednu od najvažnijih osobina grupe A_n kazuje sledeća

2.4.*Teorema:* *Ako je $n \geqslant 5$ tada je A_n prosta grupa.*

Za dokaz videti zad. 2.15.

Primeri i zadaci

2.1.Za sledeće permutacije f odrediti $P(f)$:

a) $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, b) $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, c) $f = (1\ 3\ 4)(2\ 5)$

Rešenje: a) $P(f) = \prod_{i<j} \frac{f(j)-f(i)}{j-i} = \frac{f(3)-f(2)}{3-2} \cdot \frac{f(3)-f(1)}{3-1} \cdot \frac{f(2)-f(1)}{2-1}$

$$= \frac{1-2}{3-2} \cdot \frac{1-3}{3-1} \cdot \frac{2-3}{2-1} = (-1)(-1)(-1) = -1$$

b) $P(f) = 1$

c) $P(f) = -1$.

2.2.Dokazati: $(\forall f \in S_n)\ P(f^{-1}) = P(f)$.

Rešenje: $P(f^{-1}) = P(f)^{-1}$, *pa kako je* $P(f) \in \{1,-1\}$, *to* $P(f)^{-1} = P(f)$.

2.3.Neka je $H = \{f \in A_n \mid f(1)=1\}$. Dokazati da je $H \leqslant A_n$ i odrediti $|H|$.

Rešenje: Ako je $f \in H$, $f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & a_2 & a_3 & \dots & a_n \end{pmatrix}$, *tada je* $g = \begin{pmatrix} 2 & 3 & \dots & n \\ a_2 & a_3 & \dots & a_n \end{pmatrix}$ *permutacija skupa* $\{2,3,\dots,n\}$ *i broj inverzija u f jednak je broju inverzija u g, tj. g je parna permutacija skupa* $\{2,3,\dots,n\}$. *Dakle,* $H = A_{n-1}$, *pa* $|H| = \frac{(n-1)!}{2}$ $(n > 2)$.

2.4. Dokazati da u S_n važi:

a) Proizvod dve permutacije jednake parnosti je parna permutacija,

b) Proizvod parne i neparne permutacije je neparna permutacija,

c) Konjugovane permutacije su jednake parnosti.

Rešenje: a) $(\forall f,g \in S_n)(\forall \varepsilon \in \{1,-1\})(P(f)=\varepsilon \wedge P(g)=\varepsilon \Rightarrow P(f\cdot g)=\varepsilon\cdot\varepsilon=1)$

b) $(\forall f,g \in S_n)(\forall \varepsilon \in \{1,-1\})(P(f)=\varepsilon \wedge P(g)=-\varepsilon \Rightarrow P(f\cdot g)=\varepsilon(-\varepsilon)=-1)$

c) $(\forall f,g \in S_n)P(g^{-1}fg) = P(g^{-1})P(f)P(g) = P(f)P(g^{-1}g) = P(f)P(I) = P(f)$

2.5. Ispitati parnost sledećih permutacija:

a) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 2 & 5 & 6 & 1 & 4 \end{pmatrix}$, c) $(1\ 2)$,

d) Proizvoljne transpozicije (i j), e) $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ n & n-1 & n-2 & \dots & 1 \end{pmatrix}$,

f) $\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 4 & 3 & \dots & \end{pmatrix}$

Rešenje: a) <u>*I način:*</u> $P(f) = \prod_{i<j} \frac{f(j)-f(i)}{j-i} = \frac{f(3)-f(2)}{3-2}\ \frac{f(3)-f(1)}{3-1}\ \frac{f(2)-f(1)}{2-1}$

$= \frac{1-3}{3-2}\ \frac{1-2}{3-1}\ \frac{3-2}{2-1} = 1$

<u>*II način:*</u> *Pomoću broja inverzija date permutacije.*

U ovom primeru parovi (1,3), (2,3) čine inverziju; dakle, i(f)=2, tj. $P(f)=(-1)^{i(f)}=1$, *pa je f parna permutacija.*

b) $P(f)=(-1)^{12}=1$, *tj. f je parna permutacija.*

c) Transpozicija (1 2) je neparna, jer je i((1 2))=1, tj. P((1 2))=-1.

d) Neka je f proizvoljna permutacija iz S_n. *Tada* $f^{-1}(1\ 2)f = (f(1)\ \ f(2))$,

jer $f^{-1}(1\ 2)f = \begin{pmatrix} f(1) & f(2) & \dots \\ 1 & 2 & \dots \end{pmatrix}\begin{pmatrix} 1 & 2 & \dots \\ 2 & 1 & \dots \end{pmatrix}\begin{pmatrix} 1 & 2 & \dots \\ f(1) & f(2) & \dots \end{pmatrix}$.

Uzimajući za f, redom, sve permutacije iz S_n, *vrednosti f(1) i f(2) dobijaju sve vrednosti iz skupa* $\{1,\dots,n\}$.

Drugim rečima, proizvoljna transpozicija (i j) konjugovana je transpoziciji (1 2). Prema zad. 2.4.c) je P(i j) = P(1 2), tj. sve transpozicije su neparne.

e) $f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ n & n-1 & n-2 & \dots & 1 \end{pmatrix}$, $i(f)=(n-1)+(n-2)+\dots+2+1 = \frac{n(n-1)}{2}$

tj. $P(f) = (-1)^{\frac{n(n-1)}{2}}$.

f) $P(f) = (-1)^{\left[\frac{n}{2}\right]}$ *(*$[a]$ *je celobrojni deo broja a)*.

2.6. Dokazati da je permutacija $f \in S_n$ parna (neparna) akko je proizvod parnog (neparnog) broja transpozicija.

Rešenje: Svaka permutacija f može se predstaviti proizvodom transpozicija (zad. 1.17.)

$$f = t_1 \cdot t_2 \cdot \ldots \cdot t_k \qquad (*)$$

Prema teoremi 2.1. je $P(f) = P(t_1)P(t_2)\ldots P(t_k) = (-1)^k$.

Napomena: Predstavljanje (*) proizvodom transpozicija nije jedinstveno. Moguće je, na primer, transpoziciju (i j) predstaviti i na sledeće načine

$$(i\ j) = (1\ i)(1\ j)(1\ i) \qquad (i \neq 1,\ j \neq 1)$$

$$(i\ j) = (k\ 1)(1\ k)(i\ j) \qquad (\text{za proizvoljne } k, l \in X)$$

itd. Medjutim, $(\forall f \in S_n) P(f) = 1 \vee P(f) = -1$, *odnosno parnost permutacije f je jedinstveno odredjena tom permutacijom. Dakle, broj k iz (*), za fiksirano f, ili je uvek paran ili uvek neparan.*

2.7. Predstaviti kao proizvod transpozicija i ispitati parnost sledećih permutacija:

a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$, b) (1 5 2 3 4), c) (1 3 4 7 6 8)(2 5 9) .

Rešenje: a) $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (1\ 4\ 2\ 3) = (1\ 4)(1\ 2)(1\ 3)$, *tj.* $P(f) = (-1)^3 = -1$

b) $f = (1\ 5\ 2\ 3\ 4) = (1\ 5)(1\ 2)(1\ 3)(1\ 4)$, *tj.* $P(f) = (-1)^4 = 1$

c) $f = (1\ 3)(1\ 4)(1\ 7)(1\ 6)(1\ 8)(2\ 5)(2\ 9)$, $P(f) = (-1)^7 = -1$.

2.8. Dokazati da je ciklus dužine k paran akko je k neparan broj.

Rešenje: S obzirom da je $(i_1\ i_2 \ldots i_k) = (i_1\ i_2)\ldots(i_1\ i_k)$, *tj. ciklus dužine k jednak je proizvodu k-1 transpozicije, sledi*

$$P(i_1 \ \ldots \ i_k) = 1 \Leftrightarrow k \in 2N + 1$$

2.9. Neka je S_n grupa svih permutacija nad skupom od n elemenata.

a) Ispitati da li je skup svih neparnih permutacija iz S_n, podgrupa u S_n

b) Odrediti red grupe A_n i njen indeks u S_n .

Rešenje: a) Skup B svih neparnih permutacija iz S_n *ne čini grupu u odnosu na slaganje preslikavanja. Zaista, jedinični element* $I \in S_n$ *je parna permutacija, tj.* $I \notin B$. *Takodje nije ispunjen ni uslov zatvorenosti grupne operacije. Proizvod dve neparne permutacije je parna permutacija.*

b) $|S_n : A_n| = |S_n / A_n| = 2$. *Iz* $|S_n| = |A_n| \cdot |S_n : A_n|$ *sledi* $|A_n| = \frac{n!}{2}$

2.10. Opisati grupe: a) A_3 , b) A_4

Rešenje: a) U zadatku 1.4.b) data je tablica za grupu S_3. Od navedenih 6 permutacija parne su: I, $f_3=(1\ 2\ 3)$, $f_4=(1\ 3\ 2)$. Tablica za grupu A_3 je

•	I	f_3	f_4
I	I	f_3	f_4
f_3	f_3	f_4	I
f_4	f_4	I	f_3

Iz tablice neposredno zaključujemo: $A_3 \simeq C_3$; $C_3=\{e,a,a^2\}$, $a=f_4$, $a^2=f_3$.

b) A_4 je reda 12 i sastoji se od sledećih permutacija (oznake su kao u zadatku 1.4.c):

I , $f_3=\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$, $f_4=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$, $f_7=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$,

$f_8=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$, $f_{11}=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$, $f_{12}=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$, $f_{15}=\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}$,

$f_{16}=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$, $f_{19}=\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$, $f_{20}=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$, $f_{23}=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$.

Tablica za A_4:

	I	f_3	f_4	f_7	f_8	f_{11}	f_{12}	f_{15}	f_{16}	f_{19}	f_{20}	f_{23}
I	I	f_3	f_4	f_7	f_8	f_{11}	f_{12}	f_{15}	f_{16}	f_{19}	f_{20}	f_{23}
f_3	f_3	f_4	I	f_{12}	f_{16}	f_{15}	f_{19}	f_{23}	f_{20}	f_7	f_8	f_{11}
f_4	f_4	I	f_3	f_{19}	f_{20}	f_{23}	f_7	f_{11}	f_8	f_{12}	f_{16}	f_{15}
f_7	f_7	f_{11}	f_8	I	f_4	f_3	f_{20}	f_{19}	f_{23}	f_{15}	f_{12}	f_{16}
f_8	f_8	f_7	f_{11}	f_{15}	f_{12}	f_{16}	I	f_3	f_4	f_{20}	f_{23}	f_{19}
f_{11}	f_{11}	f_8	f_7	f_{20}	f_{23}	f_{19}	f_{15}	f_{16}	f_{12}	I	f_4	f_3
f_{12}	f_{12}	f_{15}	f_{16}	f_3	I	f_4	f_8	f_7	f_{11}	f_{23}	f_{19}	f_{20}
f_{15}	f_{15}	f_{16}	f_{12}	f_8	f_{11}	f_7	f_{23}	f_{20}	f_{19}	f_3	I	f_4
f_{16}	f_{16}	f_{12}	f_{15}	f_{23}	f_{19}	f_{20}	f_3	f_4	I	f_8	f_{11}	f_7
f_{19}	f_{19}	f_{23}	f_{20}	f_4	f_3	I	f_{16}	f_{12}	f_{15}	f_{11}	f_7	f_8
f_{20}	f_{20}	f_{19}	f_{23}	f_{11}	f_7	f_8	f_4	I	f_3	f_{16}	f_{15}	f_{12}
f_{23}	f_{23}	f_{20}	f_{19}	f_{16}	f_{15}	f_{12}	f_{11}	f_8	f_7	f_4	f_3	I

2.11. Dokazati da se parnost permutacija iz S_n ne očuvava, u opštem slučaju, homomorfizmom $f : S_n \to S_m$.

Rešenje: Kako je za svaku permutaciju $f=\begin{pmatrix}1&2&\dots&n\\i_1&i_2&\dots&i_n\end{pmatrix}$ iz S_n, tačno jedna od permutacija

$$\begin{pmatrix}1&2&\dots&n&n+1&n+2\\i_1&i_2&\dots&i_n&n+1&n+2\end{pmatrix},\quad \begin{pmatrix}1&2&\dots&n&n+1&n+2\\i_1&i_2&\dots&i_n&n+2&n+1\end{pmatrix}$$

iz S_{n+2} parna, možemo definisati sledeće preslikavanje $F : S_n \to A_{n+2}$

$$F\begin{pmatrix}1&2&\dots&n\\i_1&i_2&\dots&i_n\end{pmatrix}=\begin{pmatrix}1&2&\dots&n&n+1&n+2\\i_1&i_2&\dots&i_n&a&b\end{pmatrix}$$

gde je $a=n+1,\ b=n+2$ *ako je* $P(f)=1$

$a=n+2,\ b=n+1$ *ako je* $P(f)=-1$ $\qquad (i_1,\ldots,i_n \in \{1,\ldots,n\})$.

F je preslikavanje skupa S_n *u skup* A_{n+2}, *i za njega očigledno važi*

$$F(f_1 \circ f_2) = F(f_1)\cdot F(f_2)\ .$$

Dakle, homomorfizmom F se ne očuvava parnost permutacija iz S_n.

2.12. Dokazati da je grupa A_n $(n \geq 3)$ generisana sledećim ciklusima:
$(1\ 2\ 3),\ (1\ 2\ 4),\ldots,(1\ 2\ n)$.

Rešenje: Prema zad. 2.6., svaka transpozicija (a b) iz A_n *je proizvod transpozicija oblika (1 k), gde je* $k \in \{2,3,\ldots,n\}$. *Takodje, svaka parna permutacija* $f \in A_n$ *je proizvod parnog broja transpozicija. Dakle, svaka permutacija iz* A_n *se može predstaviti proizvodom parova oblika (1 a)(1 b), gde je* $a \neq b$. *Dovoljno je stoga predstaviti (1 a)(1 b) navedenim ciklusima (1 2 3), (1 2 4),...,(1 2 n).*

Za $a=2$ *je* $(1\ 2)(1\ b) = (1\ 2\ b)$;

za $b=2$ *je* $(1\ a)(1\ 2) = (1\ a\ 2) = (1\ 2\ a)^2$;

za $a,b > 2$ *je* $(1\ a)(1\ b) = (1\ a\ b) = (1\ 2\ b)(1\ 2\ a)(1\ b\ 2)$

$$= (1\ 2\ b)(1\ 2\ a)(1\ 2\ b)^2.$$

2.13. Ako grupa G, $G < S_X$, sadrži bar jednu neparnu permutaciju, dokazati da sve parne permutacije iz G obrazuju normalnu podgrupu indeksa 2 u G.

Rešenje: Neka je f neparna permutacija iz G, i neka je H skup svih parnih permutacija u G. Kako $I \in H$, *proizvod parnih je parna permutacija, i permutacija inverzna parnoj je parna, to je* $H < G$.

Dokažimo da je $H \lhd G$. *Uočimo razlaganje G po desnim razredima podgrupe H:*

$$H,\ Hf,\ Hg,\ldots \qquad (f,g \in G)\ .$$

Očigledno je $H \neq Hf$ *jer je* $P(f)=-1$, *a* $(\forall h \in H)P(h)=1$.

Ispitajmo razrede oblika Hg, gde je g proizvoljna neparna permutacija iz G. Kako je $P(f\circ g^{-1})=1$, *to* $f\circ g^{-1} \in H$, *tj.* $Hf = Hg$. *Odnosno,* $G = H \cup Hf$, *ili* $|G:H| = 2$, *odakle sledi da je* $H \lhd G$.

2.14. Dokazati da A_4 nije prosta[1] grupa.

Rešenje: Treba dokazati da A_4 *ima pravu (tj. različitu od* A_4 *i jedinične grupe* $\{1\}$*) normalnu podgrupu. Uočimo sledeći podskup permutacija iz* A_4:
$N = \{I, f_7, f_{16}, f_{23}\}$, *gde je, prema oznakama iz zadatka 2.10.*

$$f_7=(1\ 2)(3\ 4),\quad f_{16}=(1\ 3)(2\ 4),\quad f_{23}=(1\ 4)(2\ 3).$$

Dokažimo da je $\underline{N}=(N,\circ)$ *normalna podgrupa u* A_4. *Prema zad. 2.10.b) važi:*

[1] Grupa *G* je prosta ukoliko nema pravih normalnih podgrupa.

$\circ$	I	f_7	f_{16}	f_{23}
I	I	f_7	f_{16}	f_{23}
f_7	f_7	I	f_{23}	f_{16}
f_{16}	f_{16}	f_{23}	I	f_7
f_{23}	f_{23}	f_{16}	f_7	I

odakle se neposredno zaključuje da je $N < A_4$.

Neka je g *proizvoljna permutacija iz* S_4. *Tada*

$$gf_7g^{-1} = g(1\ 2)(3\ 4)g^{-1} = (g(1)\ \ g(2))(g(3)\ \ g(4)),$$
$$gf_{16}g^{-1} = g(1\ 3)(2\ 4)g^{-1} = (g(1)\ \ g(3))(g(2)\ \ g(4)),$$
$$gf_{23}g^{-1} = g(1\ 4)(2\ 3)g^{-1} = (g(1)\ \ g(4))(g(2)\ \ g(3)).$$

Kako je g *permutacija i kako su* f_7, f_1, f_{23} *jedine tri permutacije iz* S_4 *oblika* $(i\ j)(k\ l)$, *gde je* $\{i,j,k,l\} = \{1,2,3,4\}$, *to svaka od parnih permutacija* gf_7g^{-1}, $gf_{16}g^{-1}$, $gf_{23}g^{-1}$ *pripada N. Dakle, N sadrži elemente* I, f_7, f_{16}, f_{23} *i sve njima konjugovane elemente, u odnosu na grupu* S_4. *Otuda,* $N \lhd S_4$, *koristeći zad. 3.1.3. je* $N \lhd A_4$.

2.15. Dokazati da je A_n $(n \neq 4)$ prosta grupa.

Rešenje: Grupe A_1, A_2 *i* A_3 *su proste. Za grupu* A_4 *dokazali smo u prethodnom zadatku da nije prosta. Ispitujemo slučaj* $n \geqslant 5$.

Neka je $N \lhd A_n$; *tada postoje dve mogućnosti: 1° N sadrži bar jedan element koji je ciklus dužine 3, 2° N ne sadrži ciklus dužine 3.*

1° Neka je $\alpha \in N$, *gde je* $\alpha = (a_1\ a_2\ a_3)$. *Dovoljno je dokazati da N sadrži i sve ostale cikluse dužine 3, odakle* $A_n = N$ *(zad. 2.12.).*

Proizvoljni ciklus $\pi = (x\ y\ z)$ *dužine 3 se može predstaviti*

$$\pi = \begin{pmatrix} x & y & z \\ a_1 & a_2 & a_3 \end{pmatrix}\begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix}\begin{pmatrix} a_1 & a_2 & a_3 \\ x & y & z \end{pmatrix}$$

Ako je $\beta = \begin{pmatrix} a_1 & a_2 & a_3 \\ x & y & z \end{pmatrix}$ *parna permutacija, tada* $\pi \in N$, *jer je* π *konjugovana sa* α. *Neka je* β *neparna. Kako je* $n \geqslant 5$, *postoje elementi* $a_4, a_5 \leqslant 5$ *različiti medjusobno i različiti od* a_1, a_2, a_3. *Ciklus* $(a_4\ a_5)$ *je neparan (zad. 2.5.d)), pa je permutacija* $\beta_1 = (a_4\ a_5)$ *parna. Iz* $\pi = \beta_1^{-1}\alpha\beta_1$ *sledi takodje* $\pi \in N$.

2° Neka je $\gamma = c_1c_2\ldots c_k$ (c_i *su ciklusi) proizvoljni element podgrupe N. Postoje sledeće mogućnosti:*

(a1) bar jedan od c_i $(i=1,\ldots,k)$ *je dužine veće od 3,*

(a2) svi c_i $(i=1,\ldots,k)$ *su dužine 2 ili 3,*

(a3) svi c_i $(i=1,\ldots,k)$ *su dužine 2.*

(a1) Neka je jedan od ciklusa iz γ dužine veće od 3. Kako disjunktni ciklusi komutiraju, može se uzeti $\gamma = c_1 c$, gde je $d(c_1) \geq 4$, a sa c je označen proizvod preostalih ciklusa. Neka je $c_1 = (a_1\ a_2\ a_3\ \dots\ a_j)$.

Ako $(a_1\ a_2\ a_3\ \dots\ a_j)\, c \in N$, tada za

$$\delta = (a_1\ a_2\ a_3)^{-1}\gamma(a_1\ a_2\ a_3) = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_j \\ a_4 & a_3 & a_1 & \dots & a_2 \end{pmatrix} c$$

$\delta \in N$, jer $(a_1\ a_2\ a_3) \in A_n$ ($(a_1\ a_2\ a_3) = (a_1\ a_2)(a_1\ a_3)$). Kako je

$$\gamma^{-1}\delta = \begin{pmatrix} a_2 & a_3 & a_4 & \dots & a_1 \\ a_1 & a_2 & a_3 & \dots & a_j \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_j \\ a_4 & a_3 & a_1 & \dots & a_2 \end{pmatrix} c^{-1}c = (a_1\ a_2\ a_4),$$

to i $\gamma^{-1}\delta \in N$, tj. N sadrži ciklus dužine 3, što je u kontradikciji sa 2°.

(a2) Svi c_i $(i=1,\dots,k)$ iz γ su dužine 2 ili 3. Ako je samo jedan od njih, napr. c_j $(1 < j < k)$, dužine 3, tada je $\gamma^2 = c_j$ (jer je za sve transpozicije τ ispunjeno $\tau^2 = I$), tj. slučaj je sveden na 1°. Neka su stoga, bar dva ciklusa iz γ dužine 3, tj. $\gamma = c_1 c_2 c$, gde je $c_1 = (a_1\ a_2\ a_3)$, $c_2 = (b_1\ b_2\ b_3)$, a c je proizvod ostalih ciklusa iz γ. Tada permutacije

$$\delta = (a_3\ b_1\ b_2)^{-1}\gamma(a_3\ b_1\ b_2) \quad i$$

$$\gamma\delta = (a_1\ a_2\ a_3)(b_1\ b_2\ b_3)c(a_1\ a_2\ b_1)(a_3\ b_3\ b_2) = (a_1\ b_1\ a_3\ a_2\ b_3)c$$

pripadaju N. Time je slučaj sveden na (a1).

(a3) $\gamma = (a_1\ a_2)(b_1\ b_2)c$. Element $\alpha = (a_2\ b_1\ b_2)^{-1}\gamma(a_2\ b_1\ b_2)\gamma^{-1} = (a_1\ b_2)(a_2\ b_1)$ je iz N. Neka je $d \neq a_1, a_2, b_1, b_2$; tada je

$\beta = (a_1\ b_2\ d)^{-1}\alpha(a_1\ b_2\ d)$ u N. Odavde i $\beta\alpha = (a_1\ b_2\ d)$ pripada N, čime je *slučaj sveden na 1°.*

2.16. Dokazati: a) Grupa A_4 nema podgrupu reda 6

b) Grupa A_5 nema podgrupu reda 20 (tj. ne važi obrat Lagrange-ove teoreme).

Rešenje: b) Neka grupa A_5 ima podgrupu H reda 20; tada je

$$n = |A_5 : H| = 3, \text{ jer je } |A_5| = 60.$$

Prema zad. 3.7., postoji normalna podgrupa N u H čiji je ondeks k deljiv indeksom n grupe H i deli broj n!. Drugim rečima, u A_5 postoji normalna podgrupa indeksa k za koji važi: $3 \mid k$ i $k \mid 6$. Odavde, k=3 ili k=6. To je medjutim, suprotno činjenici da je A_5 prosta grupa.

2.17. Dokazati da je A_n $(n > 4)$ jedina prava normalna podgrupa grupe S_n.

Rešenje: Neka je $N \lhd S_n$; prema teoremi 2.3. je $A_n \lhd S_n$, pa je i $N \cap A_n \lhd S_n$. Kako je A_n za $n > 4$ prosta grupa, to je

1° $N \cap A_n = E$ ili 2° $N \cap A_n = A_n$.

1° Neka je $N \cap A_n = E$ i $N \neq E$; to znači da N sadrži bar jednu neparnu permu-

taciju iz S_n. Prema zad. 2.13., podgrupa E sastavljena od parnih permutacija iz N je indeksa 2 u N. Odnosno, $|N|=2$.
Kako je S_n primitivna grupa (v.zad. 3.22.), to je N tranzitivna (v.zad. 3.24.), pa je njen red $|N|$ deljiv sa n (v.zad. 3.15.). Medjutim, 2 nije deljivo sa n jer je $n>4$, pa ovaj slučaj nije moguć.
2° Ako je $N\cap A_n = A_n$, to znači $N \supseteq A_n$. Kako je $N \neq S_n$, a $|S_n : A_n| = 2$, sledi da je $N = A_n$.

2.18. Dokazati da su grupe S_n i A_n ($n>4$) grupe bez centra. Ispitati posebno slučajeve $n \leqslant 4$.

Rešenje: Za grupu G kažemo da je bez centra, ako se centar Z(G) sastoji samo od jediničnog elementa. Ranije je već dokazano da je $Z(G) \lhd G$ i Z(G) je Abel-ova grupa. Kako je A_n prosta grupa za $n>4$, to je i $Z(A_n)=E$ ili $Z(A_n)=A_n$. Medjutim, A_n nije Abel-ova grupa, pa je $Z(A_n)=E$. Dalje, grupa S_n ima A_n kao jedinu pravu normalnu podgrupu (v.zad. 2.17.), pa je i $Z(S_n)=E$.

2.19. Odrediti komutant grupe: a) A_n ($n>4$), b) S_n ($n>4$).

Rešenje: a) A_n je prosta grupa, pa je $A_n'=E$ ili $A_n'=A_n$. Za $n>4$ A_n nije Abel-ova grupa, pa je $A_n' = A_n$.
b) Jedine normalne podgrupe u S_n su S_n, A_n i E. Da je $S_n' \neq E$ sledi iz toga što S_n ($n>4$) nije Abel-ova grupa. Takodje, $S_n' \neq S_n$, jer je $S_n/A_n \simeq C_2$, a C_2 je Abel-ova grupa, pa je (v.zad. 3.1.2.) $S_n' \lhd A_n$. Stoga je $S_n' = A_n$.

4.3. PERMUTACIJSKA REPREZENTACIJA GRUPA

U poglavlju o grupoidima dokazali smo da je svaka semigrupa izomorfna nekoj semigrupi funkcija (v. teoremu 1.3.2.). Cayley-eva teorema kazuje da se za ove funkcije mogu izabrati permutacije.

3.1. Teorema (Cayley): Svaka grupa izomorfna je nekoj grupi permutacija.

Dokaz: Neka je $(G,\cdot,1)$ grupa i neka je za svaki $a \in G$ preslikavanje p_a definisano sa $p_a : x \longmapsto ax$. S obzirom da u G važi zakon kancelacije, p_a je 1-1. Takodje, za svaki $y \in G$ jednačina $p_a(x)=y$ ima rešenje po x, $x=a^{-1}y$; dakle, $p_a \in Sym(G)$.
Prema prethodnom, za preslikavanje $\phi : a \longmapsto p_a$ važi $\phi : G \to Sym(G)$.
Dokazujemo da je ϕ utapanje grupe G u grupu Sym(G). Za $a,b,x \in G$ imamo

$\phi(a\cdot b)(x) = (ab)x = a(bx) = p_a(p_b(x)) = (p_a \circ p_b)(x) = (\phi(a)\circ\phi(b))(x)$,
pa kako je $x \in G$ proizvoljan, sledi $\phi(ab) = \phi(a)\circ\phi(b)$, tj. ϕ je homomorfizam.
Ako je $\phi(a)=\phi(b)$ onda $p_a=p_b$; dakle $p_a(1)=p_b(1)$, tj. a=b. Stoga, ϕ je 1-1. ▼

3.2. *Posledica: Svaka konačna grupa G izomorfna je nekoj konačnoj podgrupi grupe S_n, gde je $|G| = n$.*

Napomena: U algebarskoj notaciji slaganja funkcija uzima se $p_a : x \longmapsto xa$, jer tada $p_{ab} = p_a p_b$.
Postoje razna uopštenja Cayley-eve teoreme. Jedno od njih dato je u zad.3.5.

3.3. *Definicija: Homomorfizam grupe G u simetričnu grupu S_X naziva se permutacijskom reprezentacijom G na X ili dejstvom grupe G na skup X. Kardinalni broj X je stepen te reprezentacije.*

Cayley-evom teoremom se, dakle, opisuje jedna posebna reprezentacija, ostvarena izomorfizmom..
O dejstvu grupa biće više reči u poglavlju o konačnim grupama.

3.4. *Definicija: Grupa permutacija G, $G<S_X$, je tranzitivna ako je ispunjeno*

$$(\forall x,y \in X)(\exists f \in G) f(x) = y \ .$$

Grupa G je k-tostruko tranzitivna ako za proizvoljne dve k-torke $(a_1,\ldots,a_k)$, $(b_1,\ldots,b_k)$ različitih elemenata iz X, postoji f iz G tako da je $f(a_i) = b_i$ $(i=1,\ldots,k)$.

Ako je $|X| = n$, tada je, očigledno, $k < n$.

3.5. *Definicija: Grupa G $(G<S_X)$ je regularna ako je tranzitivna i ako je*

$$(\forall x \in X)\ \{f \in G \mid f(x) = x\} = \{I\} \ .$$

Neka je G tranzitivna grupa permutacija nad skupom X (tj. $G<S_X$).
Pravi podskup A skupa X (tj. $A \subsetneq X$) za koji je ispunjeno
(i) $|A| > 1$, (ii) $(\forall f \in G)(f(A) = A \vee f(A) \cap A \neq \emptyset)$
je *blok A grupe G.*
Primetimo da uslov (ii) zadovoljava svaki podskup $A \subseteq X$ za koji je $|A| = 1$, kao i sam skup X. Otuda uslovi da A bude pravi podskup i da je $|A| > 1$.

3.6. *Definicija: Tranzitivna grupa permutacija G je primitivna ako nema blokova.*

Primeri i zadaci

3.1. Dokazati posledicu 3.2.

Rešenje: Neka je $\phi : G \to Sym(G)$ utapanje iz Cayley-eve teoreme i neka je $\psi : Sym(G) \to S_n$ izomorfizam koji, prema teoremi 1.2., postoji. Tada je preslikavanje $\psi \circ \phi : G \to S_n$ utapanje.

3.2. Za sledeće grupe odrediti izomorfne grupe permutacija:
a) $(\{1,-1,i,-i\},\cdot)$, b) C_3, c) C_5, d) D_3, e) $V = C_2 \times C_2$, f) A_3, g) A_4

Rešenje: Za date grupe treba odrediti izomorfizam opisan u dokazu Cayley-eve teoreme.

a) Svakom elementu iz G pridružujemo preslikavanja iz S_4:

$$f_1 = \begin{pmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{pmatrix} = I, \quad f_{-1} = \begin{pmatrix} 1 & -1 & i & -i \\ 1(-1) & (-1)(-1) & i(-1) & (-i)(-1) \end{pmatrix} = (1\ -1)(i\ -i)$$

$$f_i = \begin{pmatrix} 1 & -1 & i & -i \\ 1i & (-1)i & ii & (-i)i \end{pmatrix} = (1\ i\ -1\ -i)$$

$$f_{-i} = \begin{pmatrix} 1 & -1 & i & -i \\ 1(-i) & (-1)(-i) & (-i)i & (-i)(-i) \end{pmatrix} = (1\ -i\ -1\ i)\ .$$

Odnosno, grupa G izomorfna je sledećoj podgrupi grupe S_4:

$$\{I, (1\ 2)(3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}$$

b) C_3 je izomorfna podgrupi $\{I, (1\ 2\ 3), (1\ 3\ 2)\}$.

3.3. Odrediti jednu permutacijsku reprezentaciju trećeg stepena za grupu C_2.

Rešenje: Rešenje je bilo kakav homomorfizam $h : C_2 \to S_3$. Na primer

$$1 \longmapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad a \longmapsto \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

3.4. Za sledeće grupe odrediti po nekoliko permutacijskih reprezentacija različitog stepena: a) C_3, b) C_n, c) D_4 .

3.5. Neka je G grupa koja ima podgrupu H konačnog indeksa. Dokazati da postoji grupa permutacija homomorfna grupi G, takva da je jezgro tog homomorfizma normalna podgrupa N u G, maksimalna medju onima koje se sadrže u H.

Rešenje: Neka je H podgrupa indeksa n u G, i neka su $x_1, \ldots, x_n$ predstavnici razlaganja grupe G na razrede po H. Svakom elementu $a \in G$ pridružujemo preslikavanje

$$f_a = \begin{pmatrix} Hx_1 & Hx_2 & \ldots & Hx_n \\ Hx_1a & Hx_2a & \ldots & Hx_na \end{pmatrix}$$

koje je, očigledno, permutacija skupa desnih razreda grupe G po podgrupi H. Preslikavanje $F : a \to f_a$ je traženi homomorfizam. Zaista,

$f_{ab} = \begin{pmatrix} Hx_1 & Hx_2 & \dots & Hx_n \\ Hx_1ab & Hx_2ab & \dots & Hx_nab \end{pmatrix} = \begin{pmatrix} Hx_1a & \dots & Hx_na \\ Hx_1a & \dots & Hx_na \end{pmatrix} \begin{pmatrix} Hx_1a & \dots & Hx_na \\ Hx_1ab & \dots & Hx_nab \end{pmatrix} = f_a \circ f_b$

Neka je N maksimalna normalna podgrupa grupe G koja se sadrži u H, tj. $N = \bigcap_{x \in G} \{x^{-1}hx \mid h \in H\}$ *i neka je M jezgro homomorfizma F.*

Tada

$$a \in N \Rightarrow (\forall x \in G) xax^{-1} \in N \Rightarrow (\forall x \in G) xax^{-1}xx^{-1} \in H$$

$$\Rightarrow (\forall x \in G) Hxax^{-1}x = Hx \Rightarrow (\forall x \in G) Hxa = Hx \Rightarrow f_a = I \Rightarrow N \subseteq M \ ;$$

$$a \in M \Rightarrow f_a = I \Rightarrow (\forall x \in G) Hxa = Hx \Rightarrow (\forall x \in G) xax^{-1} \in H \Rightarrow (\forall x \in G)(\exists h \in H) xax^{-1} = h$$

$$\Rightarrow (\forall x \in G)(\exists h \in H) a = x^{-1}hx \Rightarrow a \in \bigcap_{x \in G} \{x^{-1}hx \mid h \in H\} \Rightarrow a \in N$$

3.6. Dokazati da se prosta grupa koja sadrži pravu podgrupu indeksa n, može potopiti u S_n.

Rešenje: Neka je G prosta grupa, $H < G$ *i* $|G : H| = n$. *Prema prethodnom zadatku, postoji homomorfizam* $F : G \to S_n$ *za koji je* $\ker F = \bigcap_{x \in G} x^{-1}Hx$. *Kako je G prosta grupa,* $\ker F$ *je* $\{1\}$ *ili G. Zbog* $\ker F < H < G$, *sledi* $\ker F = \{1\}$, *tj. F je utapanje.*

3.7. Svaka podgrupa H konačnog indeksa n u grupi G, sadrži normalnu podgrupu N konačnog indeksa k u G koji je deljiv brojem n a koji deli broj n!.Dokazati.

Rešenje: Videti n! teoremu iz poglavlja o konačnim grupama.

3.8. Dokazati da je S_n, za $n \geq 3$ $(n \neq 6)$ savršena[1] grupa.

3.9. Neka je A skup kvadratnih matrica takvih da se u svakoj vrsti i koloni nalazi tačno jedna 1, a svi ostali elementi su 0. Dokazati:

a) $(A, \cdot)$ je grupa i $(A, \cdot) \simeq S_n$

b) Svaka konačna grupa izomorfna je nekoj grupi matrica.

Rešenje: a) Neka je $\underline{e} = (e_1, e_2, \dots, e_n)$ *jedna baza prostora* $\mathcal{R}^n$ *i neka je* $\mathcal{F}$ *skup svih linearnih operatora ovog prostora koji permutuju bazu* $\underline{e}$. *Matrične reprezentacije operatora iz* $\mathcal{F}$ *u bazi* $\underline{e}$ *imaju upravo oblik opisan u zadatku. I obratno, svaka od tih matrica odredjuje jedan operator koji permutuje bazu* $\underline{e}$. *Kako* $F_1, F_2 \in \mathcal{F} \Rightarrow F_1 \circ F_2 \in \mathcal{F}$, *to je* $(\mathcal{F}, \circ) = (A, \cdot)$. *Preslikavanje* $f : \mathcal{F} \to S_n$ *definisano sa*

$$f(F) = p \quad \text{gde je} \quad F = \begin{pmatrix} e_1 & e_2 & \dots & e_n \\ e_{p(1)} & e_{p(2)} & \dots & e_{p(n)} \end{pmatrix}$$

---

[1] Grupa G je *savršena* ako je bez centra i svaki njen automorfizam je unutrašnji.

je izomorfizam, pa je $S_n \simeq (\mathcal{F}, \circ)$. *Odavde sledi* $(A,\cdot) \simeq S_n$.

b) Prema Cayley-evoj teoremi, svaka konačna grupa G od n elemenata izomorfna je nekoj grupi permutacija S, gde je $S < S_n$. *Dakle,* $G \simeq S$, $S < S_n$ *i* $S_n \simeq (A,\cdot)$; *odnosno, G se (izomorfno) utapa u* $(A,\cdot)$.

3.10. Dokazati da je za $n > 3$ $(n \neq 6)$: a) $\mathrm{Aut}\, A_n \simeq S_n$, b) $\mathrm{Aut}\, S_n \simeq S_n$.

3.11. Ispitati da li su sledeće grupe tranzitivne:

a) S_n, b) A_n, c) $G = \{I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Rešenje: a) Kako S_n *sadrži sve permutacije skupa* $X = \{1,\ldots,n\}$, *to za proizvoljni par* (i,j) *postoji* f *iz* S_n *tako da je* $f(i)=j$; *takva permutacija je napr. transpozicija* $(i\ j)$.

Štaviše, S_n *je n-tostruko tranzitivna, jer za proizvoljne n-torke* $(i_1,\ldots,i_n)$, $(j_1,\ldots,j_n)$ *različitih elemenata iz X, postoji* $f \in S_n$ *tako da je*

$$f = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix} .$$

b) A_n *je primitivna grupa; ona je pri tom i (n-2)-struko tranzitivna.*

Zaista, uočimo dve (n-2)-ke različitih elemenata $(i_1,i_2,\ldots,i_{n-2})$, $(j_1,j_2,\ldots,j_{n-2})$, *i sledeće dve permutacije:*

$$\begin{pmatrix} i_1 & i_2 & \cdots & i_{n-2} & i_{n-1} & i_n \\ j_1 & j_2 & \cdots & j_{n-2} & j_{n-1} & j_n \end{pmatrix}, \quad \begin{pmatrix} i_1 & i_2 & \cdots & i_{n-2} & i_{n-1} & i_n \\ j_1 & j_2 & \cdots & j_{n-2} & j_n & j_{n-1} \end{pmatrix}$$

gde su i_{n-1}, i_n *odnosno* j_{n-1}, j_n *preostala dva elementa iz X. Očigledno je uvek jedna od ove dve permutacije parna, tj. iz* A_n.

c) Grupa G jeste tranzitivna, jer za svaki od parova (i,j), $(i,j \in \{1,2,3,4\})$ *postoji* $f \in G$ *tako da* $f(i)=j$. *Naime, permutacije iz G su proizvodi transpozicija* $(i\ j)$ *nad skupom* $\{1,2,3,4\}$.

3.12. Odrediti sve tranzitivne grupe permutacija nad skupovima:

a) $\{1,2,3\}$, b) $\{1,2,3,4\}$.

Rešenje: a) Postoje dve, neizomorfne tranzitivne grupe.

b) Ima ukupno 9 tranzitivnih grupa, medju kojima ima i izomorfnih.

3.13. Ispitati da li se svojstvo tranzitivnosti grupe permutacija prenosi izomorfizmom.

Rešenje: Uočimo sledeće dve grupe G_1 *i* G_2 *reda 4:*

$$G_1 : \quad f_1 = I, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \quad f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \quad f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$G_2 : \quad g_1 = I, \quad g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad g_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad g_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Preslikavanje $F: G_1 \to G_2$ gde je $F(f_i)=g_i$ $(i=1,2,3,4)$ je, očigledno, izomorfizam. Ispitajmo sada tranzitivnost svake od ovih grupa.
Kako za par (2,3) ne postoji preslikavanje f_i $(i=1,\ldots,4)$ sa svojstvom $f_i(2)=3$, grupa G_1 nije tranzitivna.
S druge strane, grupa G_2 jeste tranzitivna (v.zad. 3.11.c)).
Dakle, svojstvo tranzitivnosti nije algebarsko, tj. ne prenosi se izomorfizmom.

3.14. Dokazati da je grupa G, $G<S_n$, za koju je $n < |G|$, tranzitivna, akko je podgrupa $G_1 = \{f \in G \mid f(1)=1\}$ svih permutacija iz G koje ostavljaju element 1 nepromenjenim, indeksa n u G.

Rešenje: ($\Rightarrow$) Neka je grupa G tranzitivna. Stoga, za parove (1,1),(1,2), ...,(1,n) elemenata iz $X=\{1,2,\ldots,n\}$, postoje permutacije $g_1,g_2,\ldots,g_n$ iz G $(G<S_n)$ za koje je $g_i(1)=i$ $(i=1,\ldots,n)$. Dokažimo sada da skup razreda

$$G_1g_1, G_1g_2, \ldots, G_1g_n \qquad (1)$$

čini razlaganje grupe G (na desne razrede) po podgrupi G_1. Kako elementi iz G_1 zadržavaju 1 nepromenjenom, to elementi iz G_1g_j preslikavaju 1 u j $(1 \leq j \leq n)$. Stoga su svi razredi iz (1) medjusobno različiti. Neka je, dalje, f proizvoljni element iz G, i neka je $f(1)=k$ $(1 < k < n)$. Tada $g_k^{-1}(f(1)) = g_k^{-1}(k) = 1$, tj. $g_k^{-1} \circ f \in G_1$, odakle, prema zad. 2.3.7. $f \in G_1g_k$. Dakle, $|G : G_1| = n$.
($\Leftarrow$) Neka je $|G : G_1| = n$ i neka je

$$G_1f_1, G_1f_2, \ldots, G_1f_n \qquad (2)$$

razlaganje grupe G po podgrupi G_1. Kako za razrede iz (2) važi

$$i \neq j \Rightarrow G_1f_i \neq G_1f_j \qquad (1 \leq i,j \leq n)$$

to permutacije $f_1,\ldots,f_n$ preslikavaju element 1 u različite elemente iz X. Zaista,

$$f_i(1)=f_j(1) \Rightarrow (f_j^{-1} \circ f_i)(1)=1 \Rightarrow f_j^{-1} \circ f_i \in G_1 \overset{①}{\Rightarrow} G_1f_i=G_1f_j$$

① *prema zad. 2.3.7.*

Neka je sada (k,l) proizvoljni par elemenata iz X i neka su f′ i f″ permutacije iz $\{f_1,f_2,\ldots,f_n\}$ za koje je $f'(i)=k$, $f''(1)=l$. Tada $(f'' \circ (f')^{-1})(k)=l$. Dakle, G je tranzitivna grupa.

<u>Napomena:</u> *Podgrupa G_1 naziva se stabilizatorom elementa 1. Slično se definiše stabilizator G_a proizvoljnog elementa $a \in X$: $G_a = \{f \in G \mid f(a)=a\}$.*
Tvrdjenje ovog zadatka može se dokazati koristeći proizvoljni G_a, $a \in X$.

3.15. Neka je G, $G<S_n$, tranzitivna grupa. Dokazati da je broj $|G|$ deljiv sa n.

Rešenje: Prema zad. 3.14. tranzitivna grupa G, $G<S_n$, sadrži podgrupu G_1 indeksa n. Stoga je, koristeći Lagrange-ovu teoremu $|G|$ deljiv sa n.

3.16. Dokazati da je red k-tostruko tranzitivne grupe G, $G<S_n$, deljiv brojem $n(n-1)...(n-k+1)$.

Rešenje: Uočiti podgrupu H grupe G koja ostavlja k elemenata iz $\{1,...,n\}$ nepromenjenim. Slično kao u zad. 3.14. dokazati da je H indeksa $n(n-1)...(n-k+1)$ u G, odakle neposredno izvodimo traženu deljivost.

3.17. Tranzitivna grupa permutacija G je k-tostruko tranzitivna ($k>2$), akko je za svako $a\in X$, grupa $G_a=\{f\in G \mid f(a)=a\}$ svih permutacija iz G koje ostavljaju element a nepromenjenim, (k-1)-struko tranzitivna nad skupom $X\setminus\{a\}$ ($G<S_X$). Dokazati.

3.18. Dokazati da je tranzitivna Abel-ova grupa permutacija G, regularna.

Rešenje: Neka je G, $G<S_X$ tranzitivna, tj. $(\forall a,b\in X)(\exists f\in G)f(a)=b$. Tada

$$G_b=\{g\in G \mid g(b)=b\}=\{g\in G \mid g(f(a))=f(a)\}=G_{f(a)}=$$

$$\{g\in G \mid (f^{-1}\circ g\circ f)(a)=a\}\overset{①}{=}\{g\in G \mid (g\circ f^{-1}\circ f)(a)=a\}=G_a$$

① G je Abel-ova grupa

Dakle, za svako fiksirano b, G_b ostavlja nepromenjenim a, gde je a proizvoljni element iz X. Odavde, $(\forall a\in X)G_a=I$.

3.19. Dokazati da je regularna grupa G, $G<S_n$, reda n.

Rešenje: Neka je G, $G<S_n$, regularna grupa. Koristeći zad. 3.14. podgrupa $G_a=\{f\in G \mid f(a)=a\}$, $(a\in\{1,...,n\})$ je indeksa n u G; dakle, $|G|=|G_a|\cdot|G:G_a|$. Kako je $(\forall a)|G_a|=1$, sledi $|G|=n$.

3.20. Ako je G, $G<S_n$, ciklična grupa permutacija, i ako je generator grupe G ciklus dužine n, tada je G regularna grupa. Dokazati.

3.21. Dokazati da je svaka dvostruko tranzitivna grupa G, primitivna.

Rešenje: Neka je A proizvoljni podskup od X koji sadrži bar dva različita elementa a i b, i neka $c\notin A$. Prema pretpostavci, postoji f iz G tako da je $f(a)=a$ i $f(b)=c$, tj. A nije blok u G.

3.22. Ispitati primitivnost sledećih grupa permutacija:

a) S_n, b) A_n, c) $G_1=\{I,(1\ 2\ 3\ 4),(1\ 3)(2\ 4),(1\ 4\ 3\ 2)\}$,

d) $G_2=\{I,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$.

Rešenje: a) Svaki pravi podskup $A \subsetneq \{1,\ldots,n\}$, permutacije iz S_n preslikavaju u sve moguće podskupove reda $|A|$. Dakle, ne postoji ni jedan blok u S_n. Dalje, S_n je tranzitivna grupa (v.zad. 3.11.), odakle sledi i njena primitivnost.

b) Videti zadatke 3.11. i 3.21.

c) Uočimo podskup $A = \{1,3\}$ skupa $\{1,2,3,4\}$ i odredimo $f(a)$ za sve $f \in G_1$, gde je $G_1 : I,\ f_1=(1\ 2\ 3\ 4),\ f_2=(1\ 3)(2\ 4),\ f_3=(1\ 4\ 3\ 2)$.

Kako je $I(A)=A$, $f_1(A)=\{2,4\}$, $f_2(A)=\{1,3\}$, $f_3(A)=\{2,4\}$, skup $\{1,3\}$ je blok grupe G_1 (videti uvodni deo ovog odeljka). Otuda, G_1 nije primitivna grupa.

d) Grupa G_2 nije primitivna, jer je svaki dvočlani podskup skupa $\{1,2,3,4\}$ blok za G_2.

3.23. Dokazati da je tranzitivna grupa permutacija G, koja je prostog stepena, tj. $G < S_p$, primitivna.

Rešenje: Dokažimo pre svega da su sledeći uslovi ekvivalentni uslovima (i) i (ii) iz definicije bloka A u grupi G. Naime,

$$(A \text{ je blok u } G) \Leftrightarrow (|A| > 1 \wedge (\forall f \in G)(f(A)=A \vee f(A) \cap A = \emptyset)$$
$$\Leftrightarrow (|A| > 1 \wedge (\forall g,h \in G)(g(A)=h(A) \vee g(A) \cap h(A) = \emptyset)$$

Zaista,

$$(\forall g,h \in G)(g(A)=h(A) \vee g(A) \cap h(A) = \emptyset)$$
$$\Leftrightarrow (\forall g,h \in G)((h^{-1} \circ g)(A)=(h^{-1} \circ h)(A) \vee h^{-1}(g(A) \cap h(A))=h^{-1}(\emptyset))$$
$$\Leftrightarrow (\forall g,h \in G)((h^{-1} \circ g)(A)=A \vee (h^{-1} \circ g)(A) \cap A=\emptyset)$$
$$\Leftrightarrow (\forall f \in G)(f(A)=A \vee f(A) \cap A=\emptyset)$$

Dakle, ako je A blok, tada su elementi iz skupa $\{f(A) \mid f \in G\}$ disjunktni medjusobno. Kako je G tranzitivna grupa, $G < S_X$, to je $X = \bigcup_{f \in G} f(A)$. Otuda, broj $|A|$ deli broj $|X|$. No, po pretpostavci $|X|$ je prost broj, odnosno G nema blokova. Stoga je grupa G primitivna.

3.24. Svaka prava normalna podgrupa N primitivne grupe permutacija G, je tranzitivna. Dokazati.

Rešenje: Neka je $N \lhd G$ $(N \neq E,\ N \neq G)$, $G < S_X$. Ako N nije tranzitivna, onda $(\exists a,b \in X)\ \neg(\exists f \in N) f(a)=b$, tj. $(\exists a,b \in X)(\forall f \in N) f(a) \neq b$. Dakle, za neko $c \in X$ postoji skup $C = \{f(c) \mid f \in N\}$, $C \subseteq X$, $C \neq X$. Lako se pokazuje da je C blok za grupu G, suprotno pretpostavci da je G primitivna grupa.

3.25. Dokazati da je tranzitivna grupa permutacija G, primitivna, akko je $G_a = \{f \in G \mid f(a)=a\}$ maksimalna podgrupa grupe G, za svako $a \in X$.

3.26. Neka je S_F skup svih permutacija skupa $\{1,2,\ldots,n\}$ u odnosu na koje je funkcija $F : R^n \to R$ (R - skup realnih brojeva) invarijantna[1]. Dokazati da je $S_F < S_n$[2].

Rešenje: $f,g \in S_F \Rightarrow f \circ g \in S_F$ *jer* $F(x_{f(g(1))},\ldots,x_{f(g(n))}) = F(x_{g(1)},\ldots,x_{g(n)}) = F(x_1,\ldots,x_n)$;

$I \in S_F$;

$f \in S_F \Rightarrow f^{-1} \in S_F$ *jer* $F(x_1,\ldots,x_n) = F(x_{f(f^{-1}(1))},\ldots,x_{f(f^{-1}(n))}) = F(x_{f^{-1}(1)},\ldots,x_{f^{-1}(n)})$;

dakle, $(S_F,\circ)$ *je grupa, tj.* $S_F < S_n$.

3.27. Odrediti grupe sledećih funkcija:

a) $f(x,y,z) = x+y+z$, b) $f(x,y,z) = x^2+y^2+z^2$, c) $f(x,y,z)=(x-y)(y-z)(z-x)$

d) $f(x,y,z)=xy+yz+zx$, e) $f(x_1,\ldots,x_n)=\sum_{i=1}^{n} x_i$, f) $f(x_1,\ldots,x_n)=\prod_{i=1}^{n} x_i$

g) $f(x_1,\ldots,x_n)=\sum_{1<i<j<n} x_i x_j$

Rešenje: a) $f(x,y,z)=f(x,z,y)=f(y,x,z)=f(y,z,x)=f(z,x,y)=f(z,y,x)$,

odnosno, f je invarijantna u odnosu na sve permutacije iz S_3, *pa je* $S_F = S_3$.

b) $S_F = S_3$

c) Funkcija $f(x,y,z)=(x-y)(y-z)(z-x)$ *je invarijantna samo u odnosu na permutacije I,* $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ *iz* S_3, *tj.*

$f(x,y,z)=f(y,z,x)=f(z,x,y)$, *dok je* $f(x,y,z)=-f(x,z,y)=-f(y,x,z)=-f(z,y,x)$:

Kako su navedene permutacije, očigledno, parne, to je $S_F = A_3$.

d) $S_F = S_3$, *e)* $S_F = S_n$, *f)* $S_F = S_n$, *g)* $S_F = S_n$.

---

[1] Funkcija $F : R^n \to R$ je *invarijantna* u odnosu na permutaciju $f \in S_n$ ako je $F(x_1,x_2,\ldots,x_n) = F(x_{f(1)},x_{f(2)},\ldots,x_{f(n)})$.

[2] Grupa $(S_F,\circ)$ se naziva *grupom funkcije F.*

5. DIREKTAN PROIZVOD

Direktan proizvod grupoida je definisan u 1. poglavlju. Ta definicija se prirodno prenosi i na grupe, ali u ovom slučaju sa mogućnošću uvodjenja nekih novih pojmova i definicija. Naime, u vezi sa direktnim proizvodom grupa razmatraćemo dve vrste problema:

(1) Problem konstrukcije nove grupe iz datih

(2) Problem razlaganja date grupe (na podgrupe).

U svim slučajevima glavnu ulogu imaju direktan proizvod (unutrašnji i spoljašnji) i suma grupa.

5.1. DIREKTAN PROIZVOD GRUPA

Razlikujemo *spoljašnji* i *unutrašnji* proizvod grupa.

Neka je $\{(G_i,\cdot_i,1_i) \mid i\in I\}$ familija grupa i neka je $G=\prod_{i\in I} G_i$. Dakle, G je skup svih funkcija f sa domenom I takvih da za svaki $i\in I$, $f(i)\in G_i$.

Dalje, neka je na G definisana operacija $\cdot$ na sledeći način:

ako su $f,g\in G$ tada $h=f\cdot g \Leftrightarrow (\forall i\in I)h(i)=f(i)\cdot g(i)$.

Najzad, neka je konstanta $1\in G$ odredjena sa $(\forall i\in I)1(i)=1_i$.

Prema zadatku 1.4.6.c) algebarska struktura $\underline{G}=(G,\cdot;1)$ je monoid. Ako je $f\in G$, neka je $g\in G$ definisana sa $g(i)=f(i)^{-1}$ $(i\in I)$. Tada $(f\cdot g)(i)=f(i)\cdot g(i)=1_i$, tj. $f\cdot g=1$; dakle, $\underline{G}$ je grupa. Za ovako odredjenu grupu $\underline{G}$ koristi se oznaka $\underline{G}=\prod_{i\in I}\underline{G}_i$.

1.1. *Definicija:* *Neka je $\underline{G}_i$ $(i\in I)$ familija grupa. Grupa $\prod_{i\in I}\underline{G}_i$ je direktni spoljašnji proizvod grupa $\underline{G}_i$.*

Grupa $\underline{G}_i$ naziva se direktnim faktorom grupe $\underline{G}$.

Ako je I konačan skup od n elemenata, umesto $\prod_i \underline{G}_i$ upotrebljavamo i oznaku $\underline{G}_1\times\underline{G}_2\times\ldots\times\underline{G}_n$. Dakle, u ovom slučaju funkcija $f\in\prod_i G_i$ identifikovana je sa n-torkom $(f(1),\ldots,f(n))$.

Ako su grupe $\underline{G}_i$ medjusobno jednake, recimo $(\forall i\in I)\underline{G}_i=\underline{K}_i$, tada je $\underline{K}^I=\prod_i \underline{G}_i$, odnosno u konačnom slučaju $(|I|=n)$, $\underline{K}^n=\underline{G}_1\times\ldots\times\underline{G}_n$.

Neka su $\underline{G}_i$ $(i\in I)$ grupe i $\underline{G}=\prod_i \underline{G}_i$. Pod *i-tom projekcijom grupe* $\underline{G}$ podrazumeva se preslikavanje $\pi_i : G \to G_i$ takvo da je $(\forall f\in G)\pi_i(f) = f(i)$. Tada je $\pi_i : \underline{G} \to \underline{G}_i$ homomorfizam jer za $f,g\in G$ važi

$$\pi_i(f\cdot g)=(f\cdot g)(i)=f(i)\cdot_i g(i) =\pi_i(f)\cdot_i \pi_i(g)$$

(videti takodje zadatak 1.4.5.c)).

Na primer, ako je $\underline{G}=\underline{G}_1\times\underline{G}_2$, tada $\pi_1 : \underline{G} \to \underline{G}_1$ i $\pi_1(x,y)=x$; slično, $\pi_2 : \underline{G} \to \underline{G}_2$ i $\pi_2(x,y)=y$.

Ako je $H\leq\prod_i \underline{G}_i$, s obzirom da je π_i homomorfizam, prema zadatku 1.4.11. važi $\pi_i(\underline{H})<\underline{G}_i$; $\pi_i(H)$ se naziva *projekcijom podgrupe* $\underline{H}$.

Primetimo da proizvod grupa $\underline{G}=\prod_i \underline{G}_i$ sadrži izomorfnu kopiju svake grupe $\underline{G}_i$. Naime, preslikavanje $\phi : G_i \to \prod_i G_i$, $\phi : a \longmapsto f_a$ $(a\in G)$, $f_a(j) = \begin{cases} a, & j=i \\ 1_j, & j\neq i \end{cases}$ je utapanje grupe $\underline{G}_i$ u $\underline{G}$. Tako, ako je $\underline{G}=\underline{G}_1\times\underline{G}_2$ onda $\underline{G}_1\times\{1_2\}<\underline{G}$ i $\underline{G}_1\times\{1_2\}\simeq\underline{G}_1$.

1.2. *Definicija:* *Grupa* $\underline{G}=(G,\cdot,1)$ *je unutrašnji proizvod svojih podgrupa* $\underline{H}_1,\underline{H}_2,\ldots,\underline{H}_n$ *akko*

(i) $(\forall i\leq n)\ \underline{H}_i\lhd\underline{G}$,

(ii) Grupa $\underline{G}$ *je generisana skupom* $H_1\cup\ldots\cup H_n$, *tj.* $\underline{G}=\langle H_1,\ldots,H_n\rangle$,

(iii) $(\forall i\leq n)H_i\cap\langle H_1,\ldots,H_{i-1},H_{i+1},\ldots,H_n\rangle=\{1\}$.

Sledeće tvrdjenje daje osnovnu vezu izmedju spoljašnjeg i unutrašnjeg proizvoda grupa.

1.3. *Teorema:* *(i) Ako je grupa* $\underline{G}$ *unutrašnji proizvod svojih podgrupa* $\underline{H}_1,\ldots,\underline{H}_n$ *tada* $\underline{G}\simeq\underline{H}_1\times\ldots\times\underline{H}_n$,

(ii) Ako je $\underline{G}=\underline{G}_1\times\ldots\times\underline{G}_n$ *tada je* $\underline{G}$ *unutrašnji proizvod svojih podgrupa* $\underline{H}_i=\pi_i(G)$.

Dokaz: (i) Neka je $\underline{G}$ unutrašnji proizvod grupa $\underline{H}_1,\ldots,\underline{H}_n$. Tada prema zadatku 1.6. važi:

(a) $i\neq j\wedge a\in H_i\wedge b\in H_j \Rightarrow ab=ba$,

(b) Svaki element $g\in G$ se jedinstveno predstavlja proizvodom $g=h_1h_2\ldots h_n$, $h_i\in H_i$ $(i=1,\ldots,n)$.

Dakle, preslikavanje $\psi : H_1\times\ldots\times H_n \to G$ definisano sa $\psi : (h_1,\ldots,h_n) \longmapsto h_1\ldots h_n$ je prema (b) 1-1 i na.

Dalje, za $h=(h_1,\ldots,h_n)$ i $k=(k_1,\ldots,k_n)$, gde $h,k\in H_1\times\ldots\times H_n$, važi

$$\psi(h\cdot k)=\psi(h_1\cdot k_1,\ldots,h_n\cdot k_n)=(h_1k_1)\ldots(h_nk_n)\overset{①}{=}(h_1\ldots h_n)(k_1\ldots k_n)=\psi(h)\psi(k).$$

① prema (a)

Dakle, ψ je 1-1 homomorfizam grupe $\underline{H}_1\times\ldots\times\underline{H}_n$ na $\underline{G}$, tj. izomorfizam.

(ii) Uslovi (i),(ii) i (iii) definicije 1.2. se neposredno proveravaju. ▼

S obzirom na prethodnu teoremu, ako je $\underline{G}$ direktan unutrašnji proizvod grupa $\underline{H}_1,\ldots,\underline{H}_n$, takodje se koristi oznaka $\underline{G}=\underline{H}_1\times\ldots\times\underline{H}_n$. I u ovom slučaju moguće je uvesti preslikavanja $\pi_i : G \to H_i$ $(i=1,\ldots,n)$, gde za $g\in G$, $g=h_1\ldots h_n$, $h_i\in H_i$ $(i\leqslant n)$, $\pi_i(g)=h_i$. Funkcija π_i je homomorfizam grupe $\underline{G}$ na $\underline{H}_i$. Primetimo da je $\pi_i \restriction H_i$ identička funkcija skupa H_i.
Nadalje ćemo najčešće, umesto $\underline{G}=\prod_i \underline{G}_i$, pisati samo $G=\prod_i G_i$.

Primeri i zadaci

1.1.Dokazati da je direktan proizvod grupa takodje grupa.

1.2.Dokazati da je za proizvoljne grupe G_i, $i\in I$, ispunjeno:
a) $G_1\times G_2 \simeq G_2\times G_1$, b) $(G_1\times G_2)\times G_3 \simeq G_1\times(G_2\times G_3)$,
c) Ako je $G=\prod_{i\in I} G_i$ i ako je $(\forall i\in I)\ G_i=\prod_{j\in J_i} H_{ij}$, tada $G\simeq \prod_{\substack{i\in I\\ j\in J_i}} H_{ij}$

Rešenje: a) Preslikavanje $f : G_1\times G_2 \to G_2\times G_1$ odredjeno sa $f((a,b))=(b,a)$ je izomorfizam.

b) Navedeni izomorfizam ostvaruje preslikavanje $f : (G_1\times G_2)\times G_3 \to G_1\times(G_2\times G_3)$ definisano sa $f((a,b),c)=(a,(b,c))$.

1.3.Neka je $G=G_1\times G_2$ i $x_1\in G_1$, $x_2\in G_2$. Ako su preslikavanja f_1,f_2,p_1,p_2 definisana na sledeći način
$f_1(x_1)=(x_1,e_2)$, $f_2(x_2)=(e_1,x_2)$, $p_1(x_1,x_2)=x_1$, $p_2(x_1,x_2)=x_2$
(e_1 i e_2 su jedinični elementi u G_1 i G_2), dokazati:
a) f_i je homomorfizam $G_i \to G_1\times G_2$, $(i=1,2)$
p_i je homomorfizam $G_1\times G_2 \to G_i$, $(i=1,2)$
b) $f_i(G_i)\lhd G_1\times G_2$, $(i=1,2)$, c) $G_1\times G_2=f_1(G_1)f_2(G_2)$,
d) $f_1(G_1)\cap f_2(G_2)=E$ (E - jedinična grupa).

Rešenje: a) Neka su $a,b\in G_1$ i $c,d\in G_2$. Tada
$f_1(ab)=(ab,e_2)=(a,e_2)(b,e_2)=f_1(a)f_1(b)$,
$p_1((a,c)(b,d))=p_1(ab,cd)=ab=p_1(a,c)p_1(b,d)$.
Slično za f_2,p_2.
b) $f_i(G_i)$ (za $i=1,2$) je podgrupa grupe $G_1\times G_2$. Zaista, napr. za $i=1$ važi:
za sve $x_1,y_1\in G_1$ je $(x_1,e_2)(y_1,e_2)=(x_1y_1,e_2)$;
(e_1,e_2) je jedinični element grupe $f_1(G_1)$;
za element (x_1,e_2) inverzni je (x_1^{-1},e_2) .

Dalje, $f_1(G_1) \lhd G_1 \times G_2$:

$$(x,y)^{-1}(x_1,e_2)(x,y)=(x^{-1}x_1,y^{-1})(x,y)=(x^{-1}x_1x,e_2)\in f_1(G_1).$$

c) Svaki element (x,y) *iz* $G_1 \times G_2$ *može se napisati u obliku*

$$(x,y)=(x,e_2)(e_1,y)=f_1(x)f_2(y).$$

d) Neka je $(x,y)\in f_1(G_1)\cap f_2(G_2)$ *; tada*

$(\exists x_1\in G_1)(x,y)=(x_1,e_2)\wedge(\exists y_2\in G_2)(x,y)=(e_1,y_2)$. *Odavde,* $x=e_1$, $y=e_2$.

1.4.Ako je $A \lhd G$, $B \lhd G$, $G=AB$, $A\cap B=\{1\}$, dokazati:

a) $(\forall a\in A)(\forall b\in B)ab=ba$, b) $G \cong A \times B$.

Rešenje: a) Uočimo element $a^{-1}b^{-1}ab$ *iz G, gde je* $a\in A$, $b\in B$. *Kako su A i B normalne podgrupe, to je* $a^{-1}b^{-1}a\in B$, *tj.* $(a^{-1}b^{-1}a)b\in B$, *i* $b^{-1}ab\in A$, *tj.* $a^{-1}(b^{-1}ab)\in A$. *Zbog* $A\cap B=\{1\}$ *je* $a^{-1}b^{-1}ab=1$, *tj.* $ab=ba$.

b) Kao u dokazu teoreme 1.3.(i).

1.5.Ako je $G=A \times B$, onda je $B \cong G/A$. Dokazati.

Rešenje: Podgrupe A i B su normalne u G. Prema teoremi o izomorfizmu je $B/(B\cap A) \cong AB/A$. *Kako je* $A\cap B=\{1\}$ *i* $AB=G$, *to je* $B \cong G/A$.

1.6.Dokazati: grupa G je direktan proizvod svojih podgrupa $H_1,H_2,\ldots,H_n$ akko je

(a) Ako je $i\neq j$ i $a\in H_i$, $b\in H_j$, tada $ab=ba$,

(b) Svaki element $g\in G$ se *jedinstveno* predstavlja proizvodom $g=h_1h_2\ldots h_n$, $h_i\in H_i$ $(i=1,\ldots,n)$.

Rešenje: ($\Rightarrow$) *Neka je* $G=H_1 \times H_2 \times \ldots \times H_n$, *tj. neka su ispunjeni uslovi (i), (ii) i (iii) definicije 1.2.*

(a) Neka je $i\neq j$, $a\in H_i$, $b\in H_j$, *i* $A=H_i$, $B=H_j$. *Dalje kao u zadatku 1.4.a).*

(b) Koristeći (ii), za svaki $g\in G$ *postoje* $h_{i_j}\in H_{i_j}$, $i_j\in\{1,\ldots,n\}$ *takvi da je* $g=h_{i_1}h_{i_2}\ldots h_{i_k}$. *Prema dokazanom pod (a) je* $g=h_1h_2\ldots h_n$ $(h_i\in H_i)$. *Dokazujemo jedinstvenost ovog razlaganja.*

Ako je $g=h_1h_2\ldots h_n$ *i* $g=k_1k_2\ldots k_n$, $(k_i\in H_i)$, *gde je za neko j* $(1\leqslant j\leqslant n)$ $h_j\neq k_j$, *izaberimo takvo i* $(1\leqslant i\leqslant n)$ *da je* $h_i\neq k_i$ *i* $h_j=k_j$ *za* $j=i+1,\ldots,n$. *Tada* $h_1\ldots h_i=k_1\ldots k_i$, *tj.* $h_i=h_{i-1}^{-1}\ldots h_1^{-1}k_1\ldots k_i$. *Ako označimo* $s_1=h_j^{-1}k_j$ $(j=1,\ldots,i-1)$ *prema (a) je* $h_i=k_is_1\ldots s_{i-1}$, *tj.* $k_i^{-1}h_i=s_1\ldots s_{i-1}$. *Kako je* $k_i^{-1}h_i\in H_i$, *a* $s_1,\ldots,s_{i-1}\in\langle H_1,\ldots,H_{i-1}\rangle$, *prema (iii) je* $k_i^{-1}h_i=1$, *tj.* $h_i=k_i$ *za sve* $i\in\{1,\ldots,n\}$.

($\Leftarrow$) *Neka su ispunjeni uslovi (a) i (b) zadatka. Tada:*

(i) Neka je $h\in H_i$ *i g proizvoljni element iz G. Prema (b) je* $g=h_1h_2\ldots h_n$. *Dokažimo da je* $g^{-1}hg\in H_i$.

$$g^{-1}hg=h_n^{-1}\ldots h_i^{-1}\ldots h_1^{-1}hh_1\ldots h_i\ldots h_n=h_n^{-1}\ldots h_2^{-1}hh_1^{-1}h_1\ldots h_n=$$
$$h_n^{-1}\ldots h_i^{-1}hh_i\ldots h_n$$

(ovde je i-1 puta primenjen uslov (a): $h_k^{-1}h=hh_k^{-1}$, k=1,...,i-1).
Element $h_j^{-1}hh_i$ je iz H_i ; narednih n-i puta primenjujemo (a) na sledeći način: $h_k^{-1}(h_i^{-1}hh_i)=(h_i^{-1}hh_i)h_k^{-1}$ $(k=i+1,\ldots,n)$.
Tako dobijamo $g^{-1}hg=h_i^{-1}hh_i$, *odnosno* $H_i\triangleleft G$.

(ii) Kako je, prema (b), svaki $g\in G$ predstavljiv proizvodom $g=h_1\ldots h_n$, $h_i\in H_i$, to je G generisana podgrupama $H_1,\ldots,H_n$.
(iii) Neka je $a\in H_i\cap\langle H_1,\ldots,H_{i-1},H_{i+1},\ldots,H_n\rangle$; tada, koristeći (a), postoje $h_j\in H_j$ $(j\neq i)$ tako da je $a=h_1h_2\ldots h_{i-1}h_{i+1}\ldots h_n$, i postoji $h_i\in H_i$ tako da je $a=h_i$. Odavde, zbog (b), a=1.

1.7.Proveriti tablicu

×	C_1	C_2	C_3
C_1	C_1	C_2	C_3
C_2	C_2	V	C_6
C_3	C_3	C_6	G

gde su C_k ciklične grupe reda k, V je Klein-ova četvorna grupa, a G je grupa $G=\langle a,b;\ a^3=1,b^3=1,ab=ba\rangle$.

Rešenje: $C_2\times C_2=V$ *. Zaista, ako je $C_2=\{1,a\}$, tada $C_2\times C_2=\{(1,1),(1,a),(a,1),(a,a)\}$. Svi elementi ove grupe (različiti od jedinice) su reda 2. Kako postoje samo dve (neizomorfne) grupe reda 4 - ciklična C_4 i Klein-ova V (v.zad. 8.2.3.), to je $C_2\times C_2\simeq V$.*
$C_2\times C_3\simeq C_6$, jer ako je a generator grupe C_2 i b je generator grupe C_3, onda je (a,b) generator grupe $C_2\times C_3$.

1.8.Neka je $G=A\times B$ i neka su $a\in A$, $b\in B$ takvi da je r(a)=n, r(b)=m. Dokazati da je r(a,b)=NZS(m,n).

1.9.Odrediti redove elemenata (a,b), (a^2,b), (a,b^2) u grupi $G=C_3\times C_4$, gde je $C_3=\langle a\rangle$, $C_4=\langle b\rangle$. Koji od ovih elemenata generišu grupu G?

Rešenje: Grupa $C_3\times C_4$ je ciklična grupa reda 12 (v.zad. 6.1.12.). Zbog $a^3=1$, $b^4=1$, važi: (a,b) je reda 12; (a^2,b) je reda 12; (a,b^2) je reda 6.
Element (a,b) je generator grupe G:

$$(a,b)^n=(a^i,b^j),\ \text{gde je } i\in\{0,1,2\},\ j\in\{0,1,2,3\}$$
$$(\ i\equiv n(\mathrm{mod}\ 3)\ ,\ j\equiv n(\mathrm{mod}\ 4)\ )$$

Element (a^2,b) je takodje generator grupe G, jer je $(a,b)=(a^2,b)^5$.

1.10.Dokazati da je grupa $G=A\times B$ Abel-ova akko su obe grupe A i B Abel-ove.

Rešenje: Neka su $a_1,a_2\in A$; $e,b_1,b_2\in B$. *Tada*

$$(a_1,e)(a_2,e)=(a_1a_2,e)=(a_2,e)(a_1,e)=(a_2a_1,e)$$

odakle $a_1a_2=a_2a_1$. *Slično,* $b_1b_2=b_2b_1$.

Obratno, $(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2)=(a_2a_1,b_2b_1)=(a_2,b_2)(a_1,b_1)$.

1.11.Dokazati da je $S_3\times C_2\simeq D_6$.

Rešenje: Neka su a,b generatori grupe S_3 *takvi da* $a^3=b^2=1$, $ba=ab^2$, *i neka je c generator grupe* C_2. *Dalje, za* $x=ac$, $y=b$ *važi* $r(x)=6$, $r(y)=2$, $yx=bac=a^2bc=a^2cb=(ac)^5b=x^5y$, *što znači da x,y zadovoljavaju strukturne jednakosti za grupu* D_6; *dakle,* $D_6\simeq S_3\times C_2$.

1.12.Ako je $G=A\times B$ i $C<A$, $D<B$, dokazati da je $CD\simeq C\times D$.

Rešenje: Zbog $C\cap D\subseteq A\cap B$ *je* $C\cap D=\{1\}$, *pa je prema zad. 1.4.,* $CD\simeq C\times D$.

1.13.Ako je $|G|\leqslant 10$ i G je proizvod netrivijalnih grupa, dokazati da je G Abel-ova grupa.

Rešenje: Neka je $|G|\leqslant 10$ *i* $G=H\times F$, *gde je* $|H|\geqslant 2$, $|F|\geqslant 2$. *Odavde,* $|H|\leqslant 5$ *i* $|F|\leqslant 5$, *tj. H i F su Abel-ove grupe. Prema zadatku 1.10. i G je Abel-ova grupa.*

1.14.Neka je $D=\{(g,g,\ldots,g)\mid g\in G\}$ [1] podgrupa grupe G^n. Dokazati:

a) $D\simeq G$, b) $D\lhd G^n$ akko je G Abel-ova grupa.

Rešenje: a) Preslikavanje $f: D\to G$ *definisano sa* $f(g,\ldots,g)=g$ *je izomorfizam.*

b) Ako je G Abel-ova grupa, i G^n *je Abel-ova, pa su sve podgrupe grupe* G^n *normalne u* G^n. *Obratno, neka je* $D\lhd G^n$ *i* $g,h\in G$. *Tada je*

$$(h,1,\ldots,1)^{-1}(g,g,\ldots,g)(h,1,\ldots,1)=(h^{-1}gh,g,\ldots,g)$$

element D. Otuda $h^{-1}gh=g$, *tj.* $gh=hg$.

1.15.Ako je G (unutrašnji) direktni proizvod grupa A i B, onda je svaka normalna podgrupa N podgrupe A, normalna i u G. Dokazati.

Rešenje: Neka je $N\lhd A$, *tj.* $(\forall a\in A)a^{-1}Na=N$. *Neka je, dalje,* $g\in G$; *kako je* $G=A\times B$, *to je* $g=ab$ *za neke* $a\in A$, $b\in B$. *Tada* $g^{-1}Ng=b^{-1}a^{-1}Nab=b^{-1}Nb$.
Kako je $(\forall a\in A)(\forall b\in B)ab=ba$, *to je* $Nb=bN$, *pa je* $g^{-1}Ng=b^{-1}bN=N$, *tj.* $N\lhd G$.

---

[1] Grupa D je tzv. *dijagonala* direktnog stepena G^n.

1.16.Odrediti sve podgrupe sledećih grupa: a) $C_3 \times C_4$, b) $C_p \times C_p$ (p - prost broj)-

1.17.Ako je $A \simeq C$, $B \simeq D$, tada je $A \times B = C \times D$. Dokazati.

Rešenje: Neka su $f : A \to C$, $g : B \to D$ izomorfizmi. Preslikavanje $h : A \times B \to C \times D$, definisano sa $h((a,b))=(f(a),g(b))$, gde su $a \in A$, $b \in B$, je izomorfizam ovih grupa.

1.18.Ako je $A \times B = A \times C$, da li je uvek $B = C$?

Rešenje: Prema zadatku 1.5. je $B \simeq C$, ali ne mora biti $B = C$.

1.19.Ako je $A \times B \simeq C \times D$ i ako je $A \simeq C$, tada ne mora biti $B \simeq D$. Dokazati.

Rešenje: Neka je $A = \prod_{i \in N} G_i$, gde su sve grupe G_i jednake cikličnoj grupi C_2 (N je skup prirodnih brojeva), zatim $B=C_2$, $C=(\prod_{i \in N} G_i) \times C_2$ i $D=\{1\}$. Tada je $A \simeq C$, $A \times B \simeq C \times D$, i $B \neq D$.

1.20.Da li grupa $A \times B$ može biti izomorfna grupi A? Šta ako su grupe A i B konačne?

Rešenje: Neka su A i B grupe navedene u dokazu prethodnog zadatka. Za njih važi:

$$(\prod_{i \in N} G_i) \times C_2 \simeq \prod_{i \in N} G_i \text{ , odnosno } A \times B \simeq A.$$

Ako su A i B konačne netrivijalne grupe, tada navedeni izomorfizam nije moguć, jer je $|A \times B| = |A| \cdot |B|$, tj. $|A \times B| \neq |A|$ i $|A \times B| \neq |B|$.

1.21.Neka je $G=A \times B$ i neka su π_1 i π_2 projekcijska preslikavanja grupe G redom na podgrupe A i B. Ako je $H \prec G$, dokazati da je

a) $A \cap H \lhd \pi_1(H)$, $B \cap H \lhd \pi_2(H)$, b) $\pi_1(H)/(A \cap H) \simeq \pi_2(H)/(B \cap H)$.

Rešenje: a) Projekcije $\pi_1 : G \to A$ i $\pi_2 : G \to B$ su homomorifzmi čije su restrikcije: $\pi_1 \restriction A = \pi_2 \restriction B = I$ (I - identičko preslikavanje) (1)
Kako je $A \lhd G$ to je $A \cap H \lhd G$, odakle $A \cap H \lhd H$. Koristeći zad. 3.2.3. odavde je $\pi_1(A \cap H) \lhd \pi_1(H)$, odnosno, zbog (1), $A \cap H \lhd \pi_1(H)$.
Slično, $B \cap H \lhd H$, $\pi_2(B \cap H) \lhd \pi_2(H)$, $B \cap H \lhd \pi_2(H)$.
b) Preslikavanje definisano sa $\phi : \pi_1(H) \to \pi_2(H)/(B \cap H)$, je homomorfizam čije je jezgro $A \cap H$. Tada tvrdjenje sledi prema Teoremi o homomorfizmu.
Pokazuje se da se preslikavanje ϕ može uvesti na sledeći način

$$\phi(a)=b(B \cap H), \text{ gde je } a \in \pi_1(H), \text{ a } b \in B \text{ takav da } ab \in H.$$

1.22.Neka je G netrivijalna grupa. Dokazati da grupa $G \times G$ ima netrivijalan automorfizam.

Rešenje: Preslikavanje $\phi : G \times G \to G \times G$ definisano sa $\phi(x,y) = (y,x)$ je jedan (netrivijalni) automorfizam.

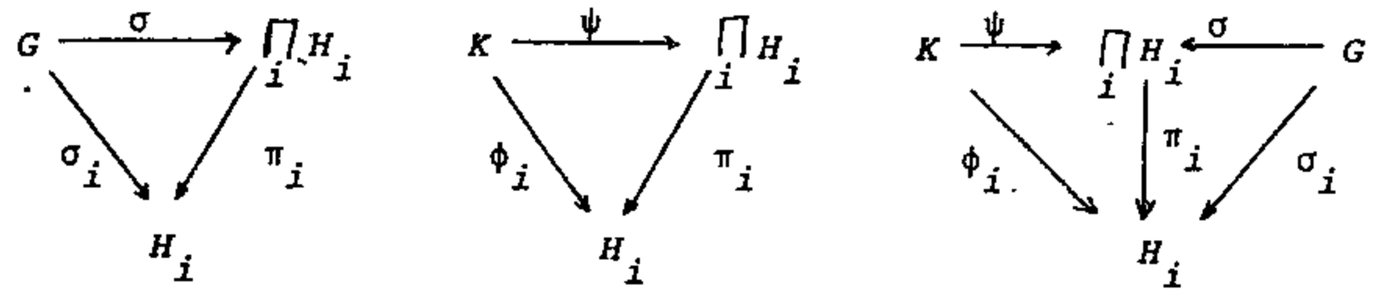
Sledeći zadatak daje još jedan opis, dakle i moguću novu definiciju, direktnog proizvoda grupa. Ova definicija prenosi se i na druge algebarske strukture i od značaja je ukoliko se koristi teorija kategorija u teoriji grupa.

1.23. Neka je $\{H_i \mid i \in I\}$ familija grupa. Dokazati da su sledeći uslovi ekvivalentni za grupu G:

(i) $G \simeq \prod_i H_i$

(ii) Postoje homomorfizmi $\sigma_i : G \to H_i$ $(i \in I)$ sa osobinom:
ako je K proizvoljna grupa i ako su $\phi_i : K \to H_i$ homomorfizmi, onda postoji tačno jedan homomorfizam $\phi : K \to G$ takav da za svaki $i \in I$, $\sigma_i \circ \phi = \phi_i$.

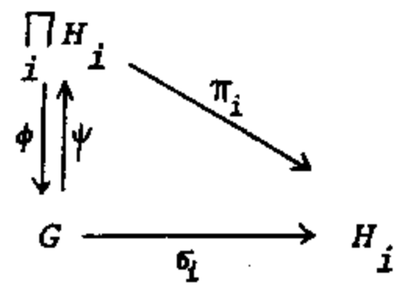
Rešenje: ($\Rightarrow$) Neka je $\sigma : G \to \prod_i H_i$ izomorfizam i neka su $\sigma_i (i \in I)$ homomorfizmi definisani jednakostima $\sigma_i = \pi_i \circ \sigma$. Dalje, ako su $\phi_i : K \to H_i$



(1) (2) (3)

homomorfizmi, onda je preslikavanje $\psi : K \to \prod_i H_i$, definisano sa $\psi(x)(i) = \phi_i(x)$ takodje homomorfizam i dijagram (2) komutira.
Preslikavanje $\phi : K \to G$ definisano je sa $\phi = \sigma^{-1} \circ \psi$.

($\Leftarrow$) Neka su ispunjeni uslovi iskaza (ii). Tada postoji preslikavanje $\phi : \prod_i H_i \to G$ takvo da za svaki $i \in I$ važi $\sigma_i \circ \phi = \pi_i$. Dalje, prema dokazu za ($\Rightarrow$), postoji $\psi : G \to \prod_i H_i$ tako da za svaki $i \in I$ važi $\pi_i \circ \psi = \sigma_i$.



Neka je $f \in \prod_i H_i$. Tada za svaki $i \in I$ važi $(\pi_i \circ \psi \circ \phi)(f) = (\sigma_i \circ \phi)(f) = \pi_i(f)$, dakle

$$\psi \circ \phi = I_G \qquad (1)$$

Dalje, $\sigma_i \circ \phi \circ \psi = \pi_i \circ \psi = \sigma_i$, pa iz uslova jedinosti sledi

$$\phi \circ \psi = I_G \qquad (2)$$

Iz (1) i (2) sledi da je $\phi : \prod_i H_i \to G$ izomorfizam.

5.2. DIREKTNA SUMA GRUPA

Kao i u slučaju direktnog proizvoda razlikujemo spoljašnju i unutrašnju *direktnu sumu* grupa.

2.1. *Definicija: Spoljašnja direktna suma grupa* G_i $(i \in I)$, *u oznaci* $\sum_{i\in I} G_i$, *je podgrupa grupe* $\prod_{i\in I} G_i$ *koju čine one funkcije* f *iz* $\prod_{i\in I} G_i$ *za koje je* $f(i)=1_i$ *osim za konačno mnogo* i *iz* I.

Ako je I konačan skup ili su sve grupe G_i, osim konačno mnogo njih, trivijalne, tada je $\prod_{i\in I} G_i = \sum_{i\in I} G_i$ (v.zad. 2.2.).

2.2. *Definicija: Grupa* G *je unutrašnja direktna suma svojih podgrupa* H_i, $(i \in I)$ *ako je:*

(i) $(\forall i \in I) H_i \lhd G$

(ii) $G = \langle H_i \mid i \in I \rangle$

(iii) $(\forall i \in I) H_i \cap \langle H_j \mid j \in I \wedge j \neq i \rangle = \{1\}$.

Odavde sledi (v.zad. 2.3.) da je svaki element $g \in G$ moguće jedinstveno (do na redosled množioca) predstaviti proizvodom *konačnog* broja elemenata iz nekih podgrupa G_i.

Napomena: Unutrašnji direktni proizvod beskonačne familije podgrupa grupe G nije moguće analogno definisati. Primećujemo da uopštavanje unutrašnjeg direktnog proizvoda iz definicije 1.2. na beskonačni slučaj, vodi do beskonačne unutrašnje sume.

Dualno projekciji π_i uvodi se *kanonsko utapanje* $\varepsilon_j : G_j \to \sum_i G_i$ $(j \in I)$, gde za $a \in G_j$ $\varepsilon_j(a) : i \longmapsto a$ ako $j=i$, $\varepsilon_j(a) : i \longmapsto 1_i$ za $j \neq i$. Neposredno se proverava da je ε_j utapanje grupe G_j u grupu $\sum_i G_i$.

Primeri i zadaci

2.1. Dokazati da je $\sum_{i\in I} G_i$ grupa (u smislu definicije 2.2.).

2.2. Neka je I konačan skup i neka je $G = \prod_{i\in I} G_i$, $H = \sum_{i\in I} G_i$. Dokazati da je $G \simeq H$.

Rešenje: Ako je $G = \prod_{i=1}^{n} G_i$, *tj. I je konačan skup, tada su elementi* $g \in G$ *oblika* $g=(a_1,a_2,\ldots,a_n)$, $a_i \in G_i$ $(i=1,\ldots,n)$. *Po definiciji, to su i elementi direktne sume.*

2.3.Dokazati da je $G = \sum_{i\in I} G_i$ akko je ispunjeno sledeće:

(a) Za $i\neq j$, $a\in G_i$, $b\in G_j$ je $ab=ba$

(b) Svaki (nejedinični) element $g\in G$ se na jedinstven način predstavlja *konačnim* proizvodom $g=a_{i_1}a_{i_2}\ldots a_{i_k}$, gde je $a_{i_j}\in G_{i_j}$, i_j su različiti medjusobno i $a_{i_j}\neq 1$.

Rešenje: Videti zadatak 1.6.

2.4.Neka je I prebrojiv skup i neka su G_i, $i\in I$ prebrojive grupe. Dokazati da je $\mathrm{card}(\prod_{i\in I} G_i) = 2^{\aleph_0}$, dok je $\mathrm{card}(\sum_{i\in I} G_i) = \aleph_0$.

Rešenje: Videti zadatak 1.4.27.

2.5.Neka je G grupa čiji su svi elementi (različliti od jedinice) reda 2. Dokazati da je G direktna suma cikličnih grupa C_2.

Rešenje: Grupa G je vektorski prostor nad dvočlanim poljem $\underline{Z}_2 = (Z_2, +_2, \cdot_2, 0, 1)$. Ako je $B = \{a_i \mid i\in I\}$ baza ovog prostora i $H_i = \langle a_i\rangle$ $(i\in I)$, tada $G = \sum_i H_i$ i $(\forall i\in I) H_i \cong C_2$

2.6.Neka je $G = \sum_{i\in I} H_i$ gde je $(\forall i\in I) H_i \neq \{1\}$. Dokazati

$$((\forall N \lhd G)(\exists J\subseteq I)\, N = \sum_{j\in J} H_j) \Rightarrow (\forall i\in I)\, H_i \text{ je prosta grupa .}$$

Rešenje: Uočimo proizvoljnu grupu H_α iz skupa $\{H_i \mid i\in I\}$. Ako ona nije prosta, postoji prava podgrupa A, $A\lhd H_\alpha$; prema zad. 1.15. je $A\lhd G$. Kako je

$$H_\alpha \cap \langle H_i \mid i\in I,\ i\neq\alpha\rangle = \{1\} \quad (\text{jer je } G = \sum_{i\in I} H_i),\ \text{to je i}$$

$$A \cap \langle H_i \mid i\in I,\ i\neq\alpha\rangle = \{1\}.$$

Kako je po pretpostavci A direktna suma nekih podgrupa H_j, to preostaje da je $A = H_\alpha$ ili $A = \{1\}$. Dakle, H_α je prosta grupa.

2.7.Rešiti zadatak 3.12. ako se "direktni proizvod" u uslovu zadatka zameni sa "direktna suma".

Rešenje: a), b), c) i e) kao kod direktnog proizvoda.

d) Za razliku od direktnog proizvoda, direktna suma očuvava svojstvo periodičnosti svojih direktnih sabiraka.

Zaista, neka je $G = \sum_{i\in I} G_i$, gde su G_i periodične grupe, i neka je $g\in G$. Prema zad. 2.3. postoji prirodni broj k i $a_{i_j}\in G_{i_j}$ $(j=1,\ldots,k)$ tako da je $g=a_{i_1}a_{i_2}\ldots a_{i_k}$. Neka su $r_1, r_2, \ldots, r_k$ (konačni) redovi elemenata $a_{i_1}, a_{i_2}, \ldots, a_{i_k}$. Tada je

$$g^{r_1 r_2\ldots r_k} = (a_{i_1}a_{i_2}\ldots a_{i_k})^{r_1 r_2\ldots r_k} = a_{i_1}^{r_1\ldots r_k}\ldots a_{i_k}^{r_1\ldots r_k} = 1$$

pa je red elementa g manji ili jednak broju $r_1 r_2 \ldots r_k$, *tj. konačan je.*

2.8. Neka je u=v zakon koji važi na grupama G_i, $i \in I$. Dokazati da taj zakon važi i na grupama $\prod_{i \in I} G_i$, $\sum_{i \in I} G_i$.

Rešenje: Videti zadatak 1.4.5.

2.9. Neka je G skup svih preslikavanja $f : \omega \to \{0,1\}$ takvih da je počev od nekog broja i : $(\forall j \geqslant i) f(j)=0$. Neka je u G definisana operacija + na sledeći način : $(f+g)(i) = f(i) +_2 g(i)$ ($+_2$ je sabiranje po modulu 2). Dokazati:

a) (G,+) je Abel-ova grupa

b) $G \simeq \sum_{i < \omega} G_i$, gde su G_i izomorfne grupi C_2

c) $G = \langle f_1, f_2, \ldots \rangle$ gde je $f_i(j) = \begin{cases} 1, & \text{za } i=j \\ 0, & \text{za } i \neq j \end{cases}$

d) Za svaku funkciju f iz G postoje jedinstvene funkcije $g_1, g_2, \ldots, g_n$ iz $\{f_1, f_2, \ldots\}$ takve da je $f = g_1 + g_2 + \ldots + g_n$.

2.10. Dokazati da je grupa G direktna suma prostih grupa akko je potpuno razloživa [1].

Rešenje: ($\Rightarrow$ *) Neka je* $G = \sum_{i \in I} H_i$, *gde su* H_i *proste grupe, i neka je* $N \lhd G$. *Dokaz se izvodi u dva koraka. Pokazuje se prvo da postoji maksimalni podskup M skupa podgrupa* $S = \{H_i \mid i \in I\}$ *za koji postoji u G podgrupa vida* $N + \sum_{H \in M} H$ [2]. *Zatim se dokazuje da je* $G = N + \sum_{H \in M} H$.

1° Za dokaz prvog koraka koristimo Zorn-ovu lemu. Treba, dakle, konstruisati neprazan delimično uredjen (u odnosu na relaciju $\subseteq$ *) skup* $\mathcal{R}$ *podskupova iz S, čiji svaki lanac C ima gornju medju u* $\mathcal{R}$. *Za* $\mathcal{R}$, *prirodno, biramo skup svih podskupova T iz S za koje je* $M + \sum_{H \in T} H < G$. *Skup* $\mathcal{R}$ *je neprazan, jer* $\emptyset \in \mathcal{R}$ *(zbog* $N < G$).

Neka je C proizvoljni lanac iz $\mathcal{R}$; *tada je* $Q = \bigcup_{T \in C} T$ *gornja medja za C.*

Dokažimo da $Q \in \mathcal{R}$, *tj. da postoji podgrupa* $N + \sum_{H \in Q} H$.

- Grupa $F_1 = \sum_{H \in Q} H$ *postoji i normalna je u G. Stoga ako označimo sa* $F_2 = \langle N, F_1 \rangle$, *imamo* $N \lhd F_2$, $F_1 \lhd F_2$.

---

1) Videti naredni odeljak.

2) Napomena: Spoljašnja direktna suma podgrupa H_j ($j \in J$) grupe G ne mora biti potopiva u G. Na primer, u grupi $G = C_2 \times C_2$, podgrupe $A = \langle a \rangle$, $B = \langle b \rangle$, $C = \langle ab \rangle$ ispunjavaju sledeće uslove : $G = ABC$, $A \cap B = B \cap C = C \cap A = \{1\}$; medjutim, $A \times B \times C$ nije podgrupa u G (jer je $|G| = 4$, a $|A \times B \times C| = 8$).

- Dalje je $N \cap F_1 = \{1\}$. Zaista, ako postoji h, $h \in N \cap F_1$, gde je h konačan proizvod elemenata iz podgrupa H, $(H \in Q)$, to znači da u Q postoji konačno mnogo grupa $H_1, H_2, \ldots, H_k$ takvih da je $N \cap \langle H_1, \ldots, H_k \rangle \neq \{1\}$. Podgrupe $H_1, \ldots, H_k$ pripadaju nekom podskupu P iz lanca C, tj. postoji suma $N + \sum_{H \in P} H$. Odavde, $N \cap \langle H \mid H \in P \rangle = \{1\}$, što je u kontradikciji sa $N \cap \langle H_1, \ldots, H_k \rangle \neq \{1\}$. Dakle, $F_2 = N + \sum_{H \in Q} H$ postoji. Možemo sada primeniti Zorn-ovu lemu, po kojoj $\mathcal{R}$ ima maksimalni element. Neka je to skup podgrupa M $(M \subseteq S)$.

2° Prema prethodnom, grupa $F = N + \sum_{H \in M} H$ postoji. Dokažimo da je $G = F$. Neka je, naprotiv, F prava podgrupa u G, tj. postoji podgrupa $\bar{H}$ iz S za koju nije $\bar{H} \cap F = \bar{H}$, već je $\bar{H} \cap F \prec \bar{H}$. Kako je $\bar{H}$ prosta grupa, to je $\bar{H} \cap F = \{1\}$. Odavde bi, zbog $\bar{H} \lhd \langle \bar{H}, F \rangle$ i $F \lhd \langle \bar{H}, F \rangle$ sledilo da postoji podgrupa $\bar{H} + F = N + \sum_{H \in M \cup \{\bar{H}\}} H$ suprotno pretpostavci o maksimalnosti skupa M. Dakle,

$$G = N + \sum_{H \in M} H, \text{ tj. grupa } G \text{ je potpuno razloživa.}$$

($\Leftarrow$) Neka je G potpuno razloživa grupa i neka je S skup svih normalnih prostih podgrupa u G. Kao u koraku 1°, primenom Zorn-ove leme, dokazuje se da postoji maksimalni podskup T iz S za koji postoji podgrupa $\sum_{H \in T} H$. Kako je G potpuno razloživa, to postoji podgrupa K takva da je $G = K + \sum_{H \in T} H$. Dokazujemo da je $K = \{1\}$.

Pretpostavimo suprotno, da je K netrivijalna podgrupa u G. Tada za K možemo da zaključimo sledeće:

- K nije prosta grupa, jer je T maksimalni skup prostih podgrupa za koje $\sum_{H \in T} H$ postoji; postoji, dakle, podgrupa L', $L' \lhd K$.
- K je potpuno razloživa grupa. Zaista, $L' \lhd K$ pa je $L' \lhd G$. Kako je G potpuno razloživa, postoji podgrupa M' u G takva da je $G = L' + M'$. Otuda, $K = L' + (M' \cap K)$.
- K nema prostu normalnu podgrupu. Ako bi postojala prosta grupa $L_1, L_2 \lhd K$ tada, prema gornjem, $K = L_1 + L_2$, tj. postoji podgrupa $\sum_{H \in T \cup \{L_1\}} H$ suprotno pretpostavci o maksimalnosti skupa T.

Slično, za svaku normalnu podgrupu L u K važi sledeće:

$$\begin{array}{l} L \text{ nije prosta, potpuno je razloživa} \\ \text{i nema prostu normalnu podgrupu} \end{array} \qquad (*)$$

Konstruisaćemo jednu posebnu podgrupu L u K, tako da gornja pretpostavka $K \neq \{1\}$ dovodi do kontradikcije. Neka je L minimalna normalna podgrupa u K koja sadrži neki fiksirani element x $(x \neq 1)$ iz K (tj. L je normalno zatvorenje $[x]_K$ elementa x u K). Kontradikciju dobijamo tako što pokazujemo da postoji prava normalna podgrupa $\tilde{M} \lhd L$ koja sadrži x.

Ako je $L = [x]_K$ tada zbog $(*)$ postoji M_1 tako da je $K = L + M_1$. Odavde,

$[x]_K = [x]_L$, tj. $L = [x]_L$.

Rastavimo grupu L (prema (*)) na $L = A_1 + B_1$. *Za* B_1, *dalje, važi svojstvo analogno (*), tj.* B_1 *rastavljamo na* $B_1 = A_2 + B_2, \ldots$, *itd., i*

$$L > A_1 + A_2 + \ldots + A_n + \ldots$$

Tada za grupu $C = \sum_{1 \le i} A_i$ *važi* $C \lhd L$, *pa postoji D tako da* $L = C + D$. *Zbog jednostavnijeg zapisa elemenata iz L, označimo* $D = A_0$, *tj.* $L = \sum_{0 \le i} A_i$.

Kako je $x \in L$, *to postoji konačno mnogo podgrupa* $A_{i_1}, A_{i_2}, \ldots, A_{i_n}$ *(v.zad. 2.3.) tako da je* $x = a_{i_1} a_{i_2} \ldots a_{i_n}$, $(a_{i_j} \in A_{i_j}$, $j=1,\ldots,n)$. *No tada* $x \in \bar{M}$, *gde je* $\bar{M} = \langle A_{i_1}, \ldots, A_{i_n} \rangle$ *i* $\bar{M}$ *je prava normalna podgrupa u L.*

2.11. Iskazati i dokazati tvrdjenje odgovarajuće tvrdjenju u zadatku 1.23.

5.3. RAZLAGANJE GRUPA

3.1. *Definicija: Grupa G je* razloživa *u direktan proizvod ako postoje prave podgrupe A i B tako da je* $G = A \times B$. *Podgrupe A i B su* direktni činioci *grupe G. Ako takve podgrupe ne postoje, grupa je* nerazloživa *u direktan proizvod.*

Prema ovoj definiciji, *razloživost* u tekstovima zadataka uvek znači razloživost u direktan proizvod svojih *netrivijalnih* podgrupa.

Svojstvo razloživosti je pravo svojstvo grupa; odnosno, postoje razložive i nerazložive grupe. To ilustruju zadaci 3.1. - 3.6.

Razlaganje, inače, nije uvek jedinstveno odredjeno. U nekim posebnim slučajevima činioci su bliže opisani, a u nekim su odredjeni do na izomorfizam .

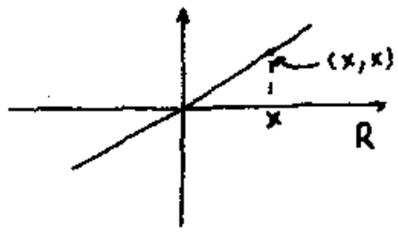
3.2. *Definicija: Grupa G je* potpuno razloživa *u direktan proizvod ako je svaka normalna podgrupa N grupe G, direktan činilac te grupe.*

Zadatak 2.10. daje potreban i dovoljan uslov potpune razloživosti grupe G.

Jedno uopštenje direktnog proizvoda je *pod-direktni* proizvod grupa.

3.3. *Definicija: Podgrupa H direktnog proizvoda grupa* $\prod_i G_i$ *je* pod-direktni proizvod *grupa* G_i *ako za svaki* $i \in I$, $\pi_i(H) = G_i$

3.4. *Primer: Neka je* $H = \{(x,x) \mid x \in R\}$ *(simetrala prvog i trećeg kvadranta realne ravni). Tada je* $H \prec R^2$, *gde*



$\underline{R} = (R,+,0)$ i $\pi_1(H)=\pi_2(H)=R$, tj. H je pod-direktni proizvod grupa $\underline{R},\underline{R}$.

Ako je H podgrupa iz $G_1 \times G_2$, onda je H očigledno pod-direktan proizvod svojih projekcija $\pi_1(H)$ i $\pi_2(H)$. Primer iz zadatka 3.18 pokazuje da ne mora uvek biti $H = \pi_1(H) \times \pi_2(H)$. Jedan uslov da H bude direktan proizvod svojih projekcija $\pi_1(H)$ i $\pi_2(H)$ je dat u zadatku 3.19.

Primeri i zadaci

3.1. Dokazati: a) Grupa C_6 je razloživa u direktan proizvod svojih podgrupa
b) Grupa S_3 nije razloživa u direktan proizvod.

Rešenje: a) Prema zadatku 1.7., $C_6 \simeq C_2 \times C_3$.
b) Grupa S_3 je reda 6, tj. prema teoremi Lagrange-a može imati samo podgrupe reda 2 i 3. Odnosno, jedine moguće (netrivijalne) podgrupe grupe S_3 su C_2 i C_3. Medjutim, $C_2 \times C_3 \simeq C_6$, a $C_6 \neq S_3$, pa se S_3 ne može razložiti u direktan proizvod svojih podgrupa.

3.2. Sledeće grupe razložiti u direktan proizvod (svojih pravih podgrupa):
a) $(C,+)$ (C - skup kompleksnih brojeva), b) $(Q^*, \cdot)$,
c) $(R^*,\cdot)$, d) $(C^*,\cdot)$ (Q^*, R^* i C^* su redom skupovi svih racionalnih, realnih i kompleksnih brojeva različitih od nule),
e) $(V,+)$, gde je V vektorski prostor dimenzije n ($n \geq 1$) nad poljem F.

Rešenje: a) Neka je $Re = \{x+i\cdot 0 \mid x \in R\}$ i $Im = \{0+i\cdot y \mid y \in R\}$, gde je R skup realnih brojeva. Očigledno je $Re \lhd C$, $Im \lhd C$, $Re \cap Im = \{0\}$,
$C = \langle Re, Im \rangle$, jer $x+iy=(x+i0)+(0+iy)$. Odavde,

$$C \simeq Re \times Im \quad (tj.\ C \simeq (R,+) \times (R,+))$$

b) $(Q^*,\cdot) \simeq (Q^+,\cdot) \times C_2$ (Q^+ je skup svih pozitivnih racionalnih brojeva)
c) $(R^*,\cdot) \simeq (R^+,\cdot) \times C_2$ (R^+ je skup svih pozitivnih realnih brojeva)
d) $(C^*,\cdot) \simeq (R^+,\cdot) \times G$ gde je $G = \{z \mid z \in C^* \wedge |z| = 1\}$
e) $(V,+) \simeq (F,+)^n$

3.3. Razložiti u direktan proizvod grupu $\underline{G} = (G,\cdot_k)$, gde je G skup prirodnih brojeva manjih od k, uzajamno prostih sa k, a $\cdot_k$ množenje po modulu k, ako je
a) k=15, b) k=21 .

Rešenje: a) $G \simeq C_2 \times C_4$, b) $G \simeq C_6 \times C_2$.

3.4. Ako je $G = G_1 \times G_2 \times \ldots \times G_n$ i preslikavanje $f : G \to H$ je izomorfizam, dokazati da je $H = f(G_1) \times f(G_2) \times \ldots \times f(G_n)$.

Rešenje: Dokaz izvodimo koristeći zadatak 1.6.

1° Neka je $i\neq j$ i $a\in G_i$, $b\in G_j$. Tada : $f(a)f(b) \overset{①}{=} f(ab) \overset{②}{=} f(ba) \overset{①}{=} f(b)f(a)$

① f je homomorfizam

② ab=ba jer su G_i i G_j direktni činioci za G

2° Dokažimo još da se svaki element h iz H jedinstveno predstavlja proizvodom $h=f(g_1)f(g_2)\dots f(g_n)$, $g_i\in G_i$ $(i=1,\dots,n)$.

Neka je $g\in G$ i $f(g)=h$. Kako je $G=G_1\times G_2\times\dots\times G_n$, tada $g=g_1g_2\dots g_n$, tj. $f(g)=f(g_1)f(g_2)\dots f(g_n)$. Ako je $f(g)=f(g_1')f(g_2')\dots f(g_n')$, tada

$$f(g_1)f(g_2)\dots f(g_n)=f(g_1')f(g_2')\dots f(g_n') \text{ , tj.}$$

$$f(g_1g_2\dots g_n)=f(g_1'g_2'\dots g_n') \text{ odakle } g_1g_2\dots g_n=g_1'g_2'\dots g_n' \text{ ,}$$

jer je f izomorfizam. Zbog jedinstvenosti predstavljanja elemenata iz G, odavde je $g_i=g_i'$ $(i=1,2,\dots,n)$.

3.5. Ispitati razloživost u direktan proizvod sledećih grupa:

a) $C_\infty=(Z,+)$, b) Grupa reda p^2 (p je prost broj) ,

c) C_{p^n} (p je prost broj), d) $(Q,+)$ (Q - skup racionalnih brojeva).

Rešenje: a) Ako je $C_\infty\cong A\times B$, tada su prema zadatku 1.5., A i B homomorfni likovi grupe C_∞, tj. A i B su ciklične grupe (v. teoremu 6.1.4.).Ako je bar jedna od grupa A,B konačna, onda $A\times B$ ima nejedinični element konačnog reda; dakle, i C_∞ ima nejedinični element konačnog reda, što nije tačno. Dakle, $A\cong C_\infty$, $B\cong C_\infty$, tj. $C_\infty\cong C_\infty\times C_\infty$, što prema zadatku 7.2.17. nije tačno.

b) Neka je G grupa reda p^2. Prema zad. 8.1.3. postoje tačno dve neizomorfne grupe reda p^2 - ciklična C_{p^2} i $C_p\times C_p$. Dakle, ako je G ciklična grupa, ona nije razloživa u direktan proizvod. Ako G nije ciklična, tada $G\cong C_p\times C_p$

c) Ako je $C_{p^n}\cong A\times B$, gde A i B nisu trivijalne grupe, onda za neki $k<n$, $p^k=\max(|A|,|B|)$, i redovi grupa A,B su stepeni broja p.Otuda, za svaki element g grupe $A\times B$ je $r(g)\leq p^k$, pa je onda i za svaki element c grupe C_{p^n} $r(c)\leq p^k$. To je kontradikcija, jer generator a grupe C_{p^n} je reda p^n, a $p^n>p^k$.

d) Ako je $(Q,+)\cong A\times B$, tada je A grupa sa deljenjem i svaki $x\in A$ je beskonačnog reda. Odnosno, $A\cong Q$. Slično, $B\cong Q$. Medjutim, $Q\not\cong Q\times Q$, jer su Q,Q^2 vektorski prostori nad poljem racionalnih brojeva i $\dim Q=1$, $\dim Q^2=2$, stoga, Q nije razloživa u direktan proizvod.

3.6. Dokazati da su sledeće grupe nerazložive u direktan proizvod svojih podgrupa: a) K (grupa kvaterniona), b) Konačne grupe prostog reda, c) Grupe sa najviše jednom (pravom) normalnom podgrupom.

Rešenje: a) K nije razloživa, jer bi inače bila komutativna.

b),c) Da bi grupa G bila razloživa u direktan proizvod k podgrupa (k > 1), neophodno je da ima bar k normalnih podgrupa.

3.7. Ako je $G = A \times B$ i $A < H < G$, dokazati da je $H = A \times (B \cap H)$.

3.8. Ako je $G = H \times F$ i $H_1 \lhd H$, $F_1 \lhd F$, dokazati da je:

a) $H_1 \times F_1 \lhd G$, b) $G/(H_1 \times F_1) \simeq (H/H_1) \times (F/F_1)$.

Rešenje: Neka su f i h prirodni homomorfizmi $f : F \mapsto F/F_1$, $h : H \to H/H_1$.

Preslikavanje $g : G \to (H/H_1) \times (F/F_1)$ definisano sa $g(x,y)=(h(x),f(y))$ je homomorfizam. Pri tome je $\ker g = H_1 \times F_1$, odakle, $H_1 \times F_1 \lhd G$.

Preslikavanje $\phi : (H_1 \times F_1)(x,y) \longmapsto (H_1x, F_1y)$ gde $x \in H$, $y \in F$ jeste izomorfizam grupa $G/(H_1 \times F_1)$ i $(H/H_1) \times (F/F_1)$.

3.9. Neka je $N \lhd G$, gde je $G = A \times B$. Tada je N Abel-ova grupa ili je presek N sa jednom od podgrupa A,B netrivijalan. Dokazati.

Rešenje: Tvrdjenje $N \lhd A \times B \Rightarrow$ (N je Abel-ova grupa) $\vee$ ($N \cap A \neq \{1\} \vee N \cap B \neq \{1\}$) dokazujemo na sledeći način:

$$(N \lhd A \times B) \wedge (N \cap A = \{1\} \wedge N \cap B = \{1\}) \Rightarrow (N \text{ je Abel-ova grupa}).$$

Neka su x,y proizvoljni elementi iz N; kako su $x,y \in A \times B$, to postoje a i b ($a \in A$, $b \in B$) takvi da je $y=ab$. Tada

$$x^{-1}y^{-1}xy = x^{-1}b^{-1}a^{-1}xab = x^{-1}b^{-1}xx^{-1}a^{-1}xab .$$

$N \lhd G$ pa $a^{-1}xa \in N$, tj. $x^{-1}a^{-1}xa \in N$; $A \lhd G$ pa $x^{-1}a^{-1}x \in A$, tj. $x^{-1}a^{-1}xa \in A$.

Odavde, zbog pretpostavke $N \cap A = \{1\}$, je $x^{-1}a^{-1}xa = 1$.

Slično, $b^{-1}xb \in N$, tj. $x^{-1}b^{-1}xb \in N$, i $x^{-1}b^{-1}x \in B$, tj. $x^{-1}b^{-1}xb \in B$, (jer je $B \lhd G$), odakle zbog $N \cap B = \{1\}$ sledi $x^{-1}b^{-1}xb = 1$.

Dakle, $x^{-1}y^{-1}xy = x^{-1}b^{-1}x(x^{-1}a^{-1}xa)b = 1$, tj. $xy = yx$.

3.10. Ako su A i B konačne Abel-ove grupe uzajamno prostih redova, dokazati

$$\text{Aut}(A \times B) \simeq \text{Aut}(A) \times \text{Aut}(B) .$$

3.11. Neka su $M_1, M_2, \ldots, M_n$ minimalne normalne podgrupe[1] grupe G. Dokazati da postoji podskup $\{i_1, i_2, \ldots, i_m\}$ skupa $\{1,2,\ldots,n\}$, $1 \leq m \leq n$, tako da je

$$M_1M_2\ldots M_n = \prod_{j=1}^{n} M_{i_j}$$

---

[1] Prava normalna podgrupa M grupe G je *minimalna* akko ne sadrži nijednu drugu pravu normalnu podgrupu te grupe.

Rešenje: Uočimo skup P svih podskupova $\{j_1,j_2,\ldots,j_k\}$ *skupa* $\{1,2,\ldots,n\}$ $1 \leqslant k \leqslant n$, *za koje je*

$$M_{j_1} M_{j_2} \ldots M_{j_k} = M_{j_1} \times M_{j_2} \times \ldots \times M_{j_k}$$

Skup P je neprazan (jer $\{i\} \in P$, $i=1,\ldots,n$*) i konačan. Neka je* m $(1 \leqslant m \leqslant n)$ *najveći kardinalni broj skupova iz P, i neka je* $\{i_1,i_2,\ldots,i_m\}$ *jedan od skupova (ako ih ima više) kardinalnosti m. Za ovaj skup važi*

$$M_{i_1} M_{i_2} \ldots M_{i_m} = M_{i_1} \times M_{i_2} \times \ldots \times M_{i_m} \qquad (1)$$

Uvedimo oznake $M = M_1 M_2 \ldots M_n$, $N = \prod_{j=1}^{n} M_{i_j}$. *Da bismo dokazali da je* $M = N$ *pretpostavimo, suprotno, da postoji* i, $i \in \{1,\ldots,n\}$ *tako da je* $M_i \not\subseteq N$ *(jer je, očigledno,* $N < M$*). Pri tom je* i *različito od svakog* $i_1,i_2,\ldots,i_m$. *Kako je* $N \lhd G$, *to je* $N \cap M_i = \{1\}$ *(jer bi inače* $N \cap M_i$ *bila normalna podgrupa, suprotno pretpostavci o minimalnosti* M_i*).*

Dakle, $\langle N, M_i \rangle = NM_i$ *i* $NM_i = N \times M_i$. *Odnosno, zbog (1)*

$$M_{i_1} M_{i_2} \ldots M_{i_m} M_i = M_{i_1} \times M_{i_2} \times \ldots \times M_{i_m} \times M_i$$

suprotno pretpostavci o maksimalnosti m.

3.12. Ispitati koja od sledećih svojstava p ispunjavaju uslov:

Ako je grupa G razloživa u direktan proizvod grupa sa svojstvom p, tada je i G sa svojstvom p.

a) Biti konačna grupa, b) Abel-ova, c) ciklična, d) periodična, e) grupa sa deljenjem [1)]

Rešenje: Neka je $G = \prod_{i \in I} G_i$.

a) Neka je $(\forall i \in I)|G_i| < \infty$. *Ako je I konačan skup, tada je* $|G| < \infty$. *To, medjutim, ne važi u opštem slučaju, kada je I beskonačan skup, pa se direktnim proizvodom svojstvo konačnosti ne prenosi.*

b) Svojstvo "biti Abel-ov" ispunjava uslov zadatka (v.zad. 1.10.).

c) Cikličnost se ne prenosi direktnim proizvodom, kao što pokazuje jednostavan primer u zadatku 1.7. ($C_3 \times C_3$ *nije ciklična grupa),*

d) Neka je $G = \prod_{n \in N} C_n$, *gde je* $C_n = \langle a_n \rangle$ *ciklična grupa reda n. Element* $g=(a_1,a_2,\ldots,a_n,\ldots)$ *iz G nije konačnog reda, pa se svojstvo periodičnosti takodje ne prenosi beskonačnim direktnim proizvodom.*

e) Dokazujemo da za svaki element $(a,b) \in G_1 \times G_2$ *i za svaki prirodni broj* n *postoji* $(x,y) \in G_1 \times G_2$ *tako da je* $(x,y)^n=(a,b)$. *Po pretpostavci, jednačine* $x^n=a$, $y^n=b$ *imaju rešenja* x_o *i* y_o *tim redom u grupama* G_1 *i* G_2. *Tada*

[1)] Grupa G je *grupa sa deljenjem* (ili potpuna grupa) ako za sve $g \in G$ i sve $n \in N$, jednačina (po x) $x^n=g$ ima rešenje u G.

$$(x_o,y_o)^n = (x_o^n, y_o^n) = (a,b) \ .$$

Dakle, deljivost se prenosi direktnim proizvodom.

3.13. Odrediti potrebne i dovoljne uslove da sledeće grupe budu razložive u direktan proizvod:

a) Ciklične grupe, b) Grupe reda pq (p,q su prosti brojevi).

Rešenje: a) potreban i dovoljan uslov za razloživost ciklične grupe je da red te grupe bude konačan (v.zad. 3.5.a)) i da je jednak proizvodu dva uzajamno prosta broja (v.zad. 6.2.3.a)

b) Potreban i dovoljan uslov za razloživost je da grupa bude Abel-ova (v.zad. 8.2.15.).

3.14. Dokazati da je centar (komutant) direktnog proizvoda jednak direktnom proizvodu centara (komutanata) činilaca.

Rešenje: Neka je $G = A \times B$. *Tada*

$$(a,b) \in Z(G) \Leftrightarrow (\forall x \in A)(\forall y \in B)(x,y)(a,b) = (a,b)(x,y)$$
$$\Leftrightarrow (\forall x \in A)(\forall y \in B)(xa,yb) = (ax,by) \Leftrightarrow (\forall x \in A)(\forall y \in B)(xa=ax \wedge yb=by)$$
$$\Leftrightarrow (a \in Z(A) \wedge b \in Z(B) \Leftrightarrow (a,b) \in Z(A) \times Z(B)$$

Dalje, $[G,G] = \{(a,b)^{-1}(c,d)^{-1}(a,b)(c,d) \mid (a,b),(c,d) \in G\}$
$$= \{(a^{-1}c^{-1}ac, b^{-1}d^{-1}bd) \mid a,c \in A;\ b,d \in B\}$$
$$= \{(x,y) \mid x \in [A,A],\ y \in [B,B]\}$$
$$= [A,A] \times [B,B]$$

3.15. Dokazati da je normalna podgrupa H direktni činilac grupe G akko postoji homomorfizam $f : G \to H$ za koji je $(\forall x \in H) f(x) = x$.

Rešenje: ($\Rightarrow$ *) Neka postoji grupa K takva da je* $G = H \times K$. *Tada je preslikavanje* $f(g)=h$, *gde je* $g=hk$ $(h \in H,\ k \in K)$ *homomorfizam* $G \to H$ *i* $f \restriction H = I$.

($\Leftarrow$ *) Neka postoji homomorfizam* $f : G \to H$ *takav da* $(\forall x \in H) f(x) = x$, *i neka je* $K = \ker f$. *Kako je* $K \lhd G$, $H \lhd G$ *i* $K \cap H = \{1\}$ *(jer iz* $x \in K \cap H$ *sledi* $f(x)=1$ *i* $f(x)=x$, *tj.* $x=1$*), to je* $\langle K,H \rangle = K \times H$.

Dokažimo još da K i H generišu celu grupu G. Neka je g proizvoljni element iz G, označimo $f(g)=h$. *Tada za element* $h^{-1}g$ *iz G važi*

$$f(h^{-1}g) = \underset{①}{f(h^{-1})} \underset{②}{f(g)} = h^{-1}h = 1$$

① *f je homomorfizam*

② *jer* $h^{-1} \in H$

Dakle, $h^{-1}g \in K$, *tj. postoji* $k \in K$ *tako da je* $h^{-1}g=k$, *odnosno* $g=hk$. *Prema tome,* $\langle K,H \rangle = G$.

3.16.Ako je $G = A \times B$, dokazati : $\Phi(G) < \Phi(A) \times \Phi(B)$ [1].

Rešenje: Neka su M i N redom maksimalne podgrupe grupa A i B. Tada su $A \times N$ *i* $B \times M$ *maksimalne podgrupe grupe G, pa je*

$$\Phi(G) < A \times N < A \times \Phi(B) \quad i \quad \Phi(G) < B \times M < B \times \Phi(A) .$$

Odavde, $\Phi(G) < (A \times \Phi(B)) \cap (B \times \Phi(A))$, *tj.* $\Phi(G) < \Phi(A) \times \Phi(B)$.

3.17.Neka grupa G ispunjava bar jedan od sledeća dva svojstva:

1° Za svaki rastući niz normalnih podgrupa od G

$$A_1 \lhd A_2 \lhd \ldots \lhd A_n \lhd A_{n+1} \lhd \ldots$$

postoji broj k tako da je $A_k = A_{k+1} = A_{k+2} = \ldots$

2° Za svaki opadajući niz normalnih podgrupa od G

$$B_1 \rhd B_2 \rhd \ldots \rhd B_n \rhd N_{n+1} \rhd \ldots$$

postoji broj m tako da je $B_m = B_{m+1} = B_{m+2} = \ldots$ [2]

Dokazati da je tada G direktan proizvod konačnog broja nerazloživih grupa.

Rešenje: Pretpostavimo, obrnuto, da G nije (konačan) direktan proizvod nerazloživih grupa. Pokažimo zatim da pod tom pretpostavkom ne može biti ispunjen nijedan uslov lanaca.

Grupa G, dakle, nije nerazloživa (jer bi, inače, tvrdjenje bilo ispunjeno). Neka je G razloživa na konačno mnogo direktnih činilaca (beskonačni proizvod uvek možemo predstaviti konačnim, napr. $\prod_{i=1} H_i = (\prod_{i=1} H_i) \times F$ *gde je* $F = \prod_{i=n+1} H_i$ *). Tada u G sigurno postoji direktni činilac* G_1 *koji takodje nije (konačan)proizvod nerazloživih grupa (jer ako bi svi činioci bili direktni proizvodi konačnog broja nerazloživih grupa, takva bi bila i grupa G). Predstavimo G u obliku :* $G = G_1 \times H_1$.

Slično, u G_1 *postoji pravi direktni činilac* G_2, $G_1 = G_2 \times H_2$ *takav da* G_2 *nije (konačan) direktan proizvod nerazloživih grupa, itd. Naime, imamo da je*

$G = G_1 \times H_1$, $\quad G = G_2 \times H_2 \times H_1$, $\quad G = G_3 \times H_3 \times H_2 \times H_1, \ldots$

odnosno, lanci

$$G > G_1 > G_2 > \ldots$$
$$H_1 < H_1 \times H_2 < H_1 \times H_2 \times H_3 < \ldots$$

su beskonačni, suprotno pretpostavci zadatka.

---

[1] *Frattini-eva podgrupa* $\Phi(G)$ *grupe G* je presek svih maksimalnih podgrupa iz G, ako G ima maksimalnih podgrupa; inače je $\Phi(G)=G$. Primetimo da je $\Phi(G)$ karakteristična podgrupa grupe G.

[2] Drugim rečima, grupa G zadovoljava bar jedan uslov lanaca (videti uvodni deo 8-og poglavlja).

3.18. Ispitati da li je svaka podgrupa direktnog proizvoda, direktan proizvod svojih projekcija (na direktne činioce).

Rešenje: Neka je $H \prec G_1 \times G_2$ *: prema definiciji 3.3. H je uvek pod-direktni proizvod svojih projekcija, tj.* $H \prec \pi_1(H) \times \pi_2(H)$. *Navodimo primer kada je* $H \neq \pi_1(H) \times \pi_2(H)$.
U grupi $G \times G$ *uočimo podgrupu* $D = \{(g,g) \mid g \in G\}$; *tada je* $\pi_1(D) = G$, $\pi_2(D) = G$. *Očigledno je D pod-direktni proizvod u grupi* $G \times G$. *Prema zadatku 1.14.* $D \simeq G$, *pa kako nije uvek* $G \times G \simeq G$, *to D u opštem slučaju nije direktan proizvod svojih projekcija.*

3.19. Ako je $G = A \times B$ i $H \prec G$, dokazati da je

$$H = (A \cap H) \times (B \cap H) \Leftrightarrow (\pi_1(H) = A \cap H) \wedge (\pi_2(H) = B \cap H) .$$

Rešenje: ($\Rightarrow$) *Neka je* $H = (A \cap H) \times (B \cap H)$. *Kako je* $\pi_1(A \times B) = A$, *to je i* $\pi_1(H) = A \cap H$, *i slično* $\pi_2(H) = B \cap H$.
($\Leftarrow$) *Kako je* $A \cap H \lhd H$, $B \cap H \lhd H$ *i* $(A \cap H) \cap (B \cap H) = \{1\}$ *(jer je* $A \cap B = \{1\}$*),* to je

$$(A \cap H) \times (B \cap H) \prec H \qquad (1)$$

Dalje je, prema definiciji 3.3.

$$H \prec \pi_1(H) \times \pi_2(H) \qquad (2)$$

Ako je $\pi_1(H) = A \cap H$, *tada je prema zad. 1.20. i* $\pi_2(H) = B \cap H$, *i obratno, pa iz (1) i (2) sledi* $H = (A \cap H) \times (B \cap H)$.

3.20. Neka je $G = A \times B$ konačna grupa za koju je $(|A|,|B|)=1$. Tada je svaka podgrupa H iz G direktan proizvod svojih projekcija na činioce A i B.

Rešenje: Ako je $(|A|,|B|)=1$, *tada je i* $(|A_1|,|B_1|)=1$ *za proizvoljne podgrupe* $A_1 \prec A$, $B_1 \prec B$. *Stoga je, zbog* $\pi_1(H) \prec A$, $\pi_2(H) \prec B$

$$(|\pi_1(H)|,|\pi_2(H)|)=1 \qquad (1)$$

Koristeći zad. 1.20. važi $\pi_1(H)/(A \cap H) \simeq \pi_2(H)/(B \cap H)$.
Kako su grupe $\pi_1(H)/(A \cap H)$ *i* $\pi_2(H)/(B \cap H)$ *konačne, jednakih redova, tj.* $\dfrac{|\pi_1(H)|}{|A \cap H|} = \dfrac{|\pi_2(H)|}{|B \cap H|}$, *zbog (1) je* $\dfrac{|\pi_1(H)|}{|A \cap H|} = \dfrac{|\pi_2(H)|}{|B \cap H|} = 1$, *odakle sledi* $\pi_1(H)=A \cap H$, $\pi_2(H)=B \cap H$. *Prema zad. 3.19. je* $H = \pi_1(H) \times \pi_2(H)$.

3.21. Neka su N_i $(i \in I)$ normalne podgrupe grupe G i neka je $N = \bigcap_{i \in I} N_i$. Dokazati da je grupa G/N izomorfna pod-direktnom proizvodu grupa G/N_i $(i \in I)$.

Rešenje: Neka je preslikavanje $\phi : G \longrightarrow \prod_{i \in I} G/N_i$, *definisano sa* $\phi(x)(i) = N_i x$. *Tada je* ϕ *homomorfizam čije je jezgro N, pa tvrdjenje sledi prema Teoremi o homomorfizmu.*

6. C I K L I Č N E G R U P E

Klasa cikličnih grupa je, u izvesnom smislu, klasa najjednostavnijih grupa. Ali , one predstavljaju važan primer grupa, s obzirom da se mnoge druge grupe mogu izgraditi od cikličnih, primenom odredjenih konstrukcija. Na primer, u sledećem poglavlju dokazaćemo da je svaka Abel-ova grupa na jednostavan način izgradjena od nekih svojih cikličnih podgrupa. Otuda, ovaj odeljak se može smatrati uvodnim za naredno poglavlje o Abel-ovim grupama.

6.1. DEFINICIJA I OSOBINE

1.1.Definicija: Grupa G je ciklična ako je G generisana jednim elementom.

Dakle, grupa G je ciklična ako za neki $a \in G$ važi $G = \langle a \rangle$. Element a se naziva *generatorom* grupe G.

1.2. Primeri: 1° $\underline{Z}_n = (\{0,1,\ldots,n-1\},+_n,0)$, *gde je* $+_n$ *sabiranje po modulu n, je ciklična grupa.*

Zaista, prema 2.2.2. $\underline{Z}_n$ *je Abel-ova grupa reda n. Dalje, za* $i \in Z_n$ *važi* $i=\underbrace{1+1+\ldots+1}_{(i\ puta)} = \underbrace{1+_n 1+_n \ldots +_n 1}_{(i\ puta)}$ *; dakle* $Z_n = \langle 1 \rangle$.

2° Aditivna grupa celih brojeva, $\underline{Z} = (Z,+,0)$.

Prethodnim primerima obezbedjena je egzistencija cikličnih grupa. Ovi primeri kazuju i nešto više:

Za svaki prirodan broj n, postoji grupa reda n.

Ipak, cikličnih grupa nema mnogo:

1.3.Teorema: Ciklične grupe istog reda su izomorfne.

Dokaz: Neka je $|G| = |H| = n > 2$. Prema zad. 1.1., za neke $a \in G$, $b \in H$ je $G = \{e,a,a^2,\ldots,a^{n-1}\}$, $H = \{e,b,b^2,\ldots,b^{n-1}\}$, e je jedinični element grupe G i e´ je jedinica grupe H. Preslikavanje $f : G \to H$ odredjeno jednakošću $f(a^i)=b^i$ $(0 \leqslant i \leqslant n-1)$ je dobro definisano. Kako za $0 \leqslant i < j \leqslant n-1$ $a^i \neq a^j$, $b^i \neq b^j$, to je f 1-1 i na. Dokazujemo da je f homomorfizam. Neka su $x,y \in G$. Za neke $0 \leqslant i, j \leqslant n-1$ je $x=a^i$, $y=a^j$.

Slučaj $i+j \leq n-1$: $f(xy) = f(a^i a^j) = f(a^{i+j}) = b^{i+j} = b^i b^j = f(a^i)f(a^j) = f(x)f(y)$.
Slučaj $i+j \geq n$: neka je $i+j = n+k$. Tada $0 < k \leq n-1$, $a^n = e$, $b^n = e'$ i

$f(xy) = f(a^i a^j) = f(a^{i+j}) = f(a^{n+k}) = f(a^n a^k) = f(ea^k) = f(a^k) = b^k = e'b^k = b^n b^k = b^{n+k} = b^{i+j} = b^i b^j = f(a^i)f(a^j) = f(x)f(y)$.

Neka su G, H beskonačne ciklične grupe. Prema zad. 1.2. za generatore $a \in G$, $b \in H$ važi $G = \{a^n \mid n \in Z\}$, $H = \{b^n \mid n \in Z\}$. Preslikavanje $f : G \to H$ određeno jednakošću $f(a^n) = b^n$, $n \in Z$, je dobro definisano i predstavlja jedan izomorfizam grupa G i H, što je lako proveriti.▼

Dakle, primerom 1.2. su do na izomorfizam opisane *sve* ciklične grupe. Neke druge strukturne osobine cikličnih grupa kazuju sledeća tvrdjenja.

1.4. *Teorema: Homomorfna slika ciklične grupe je ciklična grupa.*

Dokaz: Neka je G ciklična grupa, a generator ove grupe i h homomorfizam iz G na grupu H. Tada $H = \langle h(a) \rangle$.▼

1.5. *Teorema: Podgrupa ciklične grupe je takodje ciklična grupa.*

Dokaz: Neka je G ciklična grupa i $H \leq G$. Ukoliko je $|H| = 1$, tada $H = \langle 1 \rangle$. Pretpostavimo $|H| > 2$. Tada postoji prirodan broj k takav da $a^k \in H$; neka je k najmanji prirodan broj $(k > 0)$ za koji je $a^k \in H$.
Dokazujemo da je a^k generator grupe H. Neka je $h \in H$; tada za neki $n \in Z$, $h = a^n$. Neka su $\alpha \in Z$, $i \in N$ takvi da $n = \alpha k + i$, $0 \leq i < k$; tada $h = a^{k\alpha} a^i$, $a^k \in H$. Otuda $a^i \in H$, jer $a^i = h(a^{k\alpha})^{-1}$. Kako je $0 \leq i < k$, $a^i \in H$, prema izboru prirodnog broja k sledi da je $i = 0$. Dakle, $h = a^{\alpha k}$, tj. a^k generiše H.▼

Primeri i zadaci

1.1. Neka je G ciklična grupa reda n i $a \in G$ generator grupe G. Dokazati:
$(\forall x \in G)(\exists_1 i \in \{0,1,\ldots,n-1\})\ x = a^i$, tj. $G = \{1, a, a^2, \ldots, a^{n-1}\}$ i za $0 \leq i < j \leq n-1$ je $a^i \neq a^j$.

Rešenje: Neka je $G = \langle a \rangle$ i $|G| = n$. Dalje, neka je $x \in G$. Tada za neki $m \in Z$ $x = a^m$. Neka su $k \in Z$, $i \in \omega$ takvi da $m = kn + i$, $i \leq n-1$. Tada $a^m = a^{kn+i} = (a^n)^k a^i = 1 \cdot a^i = a^i$ budući da je $n = |G|$, pa prema tome i $a^n = 1$. Otuda je $G = \{a^i \mid 0 \leq i \leq n-1\}$. Preslikavanje $f : \{0,1,\ldots,n-1\} \to G$ definisano sa $f(i) = a^i$ je na, pa kako je $|G| = |\{0,1,\ldots,n-1\}| = n$, to je f 1-1, tj.

$0 \leq i < j \leq n-1 \Rightarrow a^i \neq a^j$.

1.2. Neka je G beskonačna ciklična grupa i $a \in G$ generator grupe G. Dokazati:
$(\forall x \in G)(\exists_1 n \in Z)\ x = a^n$.

1.3.Dokazati da je svaka grupa prostog reda ciklična.

Rešenje: Neka je $a \in G$, $a \neq 1$; tada $r(a) \mid |G|$ pa kako je $|G|$ prost broj, $r(a)=|G|$. Otuda $G = \langle a \rangle$.

1.4.Neka je $n \in N$ i $X = \{x \in C \mid x^n = 1\}$. Dokazati da je $(X,\cdot)$ ciklična grupa. Odrediti bar jedan generator ove grupe.

Rešenje: Kako $x^n=1 \wedge y^n=1 \Rightarrow (xy)^n=1$, $x^n=1 \Rightarrow 1/x^n=1$ i $1 \in X$, sledi da je $(X,\cdot)$ Abel-ova grupa. Neka je $a=\cos(2\pi/n)+i\sin(2\pi/n)$. Tada $a^n=1$ pa $a \in X$. Dalje, za $0 \leqslant i < j \leqslant n-1$ je $a^i \neq a^j$ i takodje $a^i \in X$, dakle $|X| \geqslant n$.
S druge strane, jednačina $x^n=1$ ima n rešenja u polju kompleksnih brojeva, odakle $|X| \leqslant n$. Prema prethodnom $|X| = n$ i $X = \langle a \rangle$.

1.5.Koje su od grupa navedenih tablicama u zadatku 2.2.3. ciklične?

Rešenje: Grupe date tablicama b),e) su ciklične. Generatori ovih grupa su redom, recimo, a, h_1.

1.6.Neka je n prirodan broj i $nZ = \{nx \mid x \in Z\}$. Dokazati: $nZ \lhd Z$ i Z/nZ je ciklična grupa reda n. Navesti tablicu grupe $Z/4Z$.

Rešenje: Neka su $nx, ny \in nZ$. Tada $nx-ny=n(x-y)$, pa $(nx-ny) \in Z$. Otuda, prema zad. 2.3.1. $nZ < Z$. Kako je Z Abel-ova grupa, to je $nZ \lhd Z$.
Grupa Z/nZ je homomorfna slika grupe Z u odnosu na kanonski homomorfizam $k : Z \to Z/nZ$, pa je prema teoremi 1.4. Z/nZ ciklična grupa. Kako za svaki $m \in Z$ postoje $k \in Z$, $i \in \{0,1,\ldots,n-1\}$ takvi da $m=nk+i$, to za razred $nZ+m$ važi $nZ+m = nZ+i$, dakle $|Z/nZ| \leqslant n$. S druge strane, ako je $0 \leqslant i, j \leqslant n-1$ (može se pretpostaviti $i < j$), tada iz $nZ+i = nZ+j$ sledi $(j-i) \in nZ$, tj. $n \mid j-i$, odnosno $i=j$. Prema tome $|Z/nZ| \geqslant n$, dakle $|Z/nZ| = n$. Prema teoremi 1.3. sledi $Z/nZ \cong Z_n$.

Tablica za Z/nZ je:

+	4Z	4Z+1	4Z+2	4Z+3
4Z	4Z	4Z+1	4Z+2	4Z+3
4Z+1	4Z+1	4Z+2	4Z+3	4Z
4Z+2	4Z+2	4Z+3	4Z	4Z+1
4Z+3	4Z+3	4Z	4Z+1	4Z+2

1.7.Neka su H i G konačne ciklične grupe. Dokazati: ako $|H| \mid |G|$ tada je H homomorfna slika grupe G. Da li važi i obrat ovog tvrdjenja?

Rešenje: Neka je $G = \langle a \rangle$, $H = \langle b \rangle$, $|G| = m$, $|H| = n$ i $m=kn$ $(k \in N)$. Preslikavanje $f : G \to \langle a^k \rangle$ odredjeno jednakošću $f(a^i)=a^{ki}$ je homomorfizam koji je <u>na</u>. Grupa $\langle a^k \rangle$ je ciklična reda n, dakle $\langle a^k \rangle = H$, pa je H homomorfna slika grupe G.

Obrat važi, jer, ako je $f : G \overset{na}{\to} H$, *tada* $H = G/\ker f$ *pa zbog* $|H| = |G : \ker f|$ *i* $|G : \ker f| \mid |G|$ *sledi da* $|H|$ *deli* $|G|$.

1.8. Dokazati da je svaka ciklična grupa homomorfna slika grupe $(Z,+)$.

Rešenje: Neka je G ciklična grupa. Pretpostavimo da je G beskonačna, tada je G prebrojiva pa su G i Z istog reda, dakle prema teoremi 1.3. $G \simeq Z$. *Pretpostavimo da je* $|G| = n$, $n \in N$. *Grupa* Z/nZ *je ciklična reda n (zad.1.6.) pa postoji izomorfizam* $f : Z/nZ \to G$ *(teorema 1.3.). Neka je* $k : Z \to Z/nZ$ *kanonski homomorfizam; tada je* $h = fk$ *homomorfizam iz Z na G.*

1.9. Dokazati da je svaka ciklična grupa izomorfna jednoj od grupa Z_n ili grupi Z.

Rešenje: Prema teoremi 1.3.

1.10. Odrediti Aut Z .

Rešenje: Jedini generatori grupe Z su 1 i -1. Ako je $f \in \mathrm{Aut}\, Z$, *tada f prevodi generator grupe Z u generator grupe Z, dakle* $|\mathrm{Aut}\, Z| \leqslant 2$. *S druge strane, preslikavanja* $i(x)=x$, $j(x)=-x$, $x \in Z$, *su automorfizmi grupe Z pa* $\mathrm{Aut}\, Z = \{i,j\}$.

1.11. Odrediti sve podgrupe i grupu automorfizama grupe C_{15}.

Rešenje: Neka je $C_{15} = \{e,a,a^2,\ldots,a^{14}\}$. *Ako je* $H \prec G$, *prema Lagrange-ovoj teoremi* $|H| \mid 15$, *tj.* $|H| \in \{1,3,5,15\}$. *Otuda:*
ako je $|H|=1$, *tada* $H=\{e\}$; *ako je* $|H|=3$, *tada je* $H=\{e,a^5,a^{10}\}$;
ako je $|H|=5$, *tada* $H=\{e,a^3,a^6,a^9,a^{12}\}$; *ako je* $|H|=15$, *tada* $H=G$.

Prema zad. 2.2. grupa C_{15} *ima* $\phi(15)=8$ *automorfizama. Svaki je određen slikom generatora a. Otuda, postoje jedinstveni automorfizmi* $f_1, f_2, \ldots, f_8$ *takvi da* $f_1(a)=a$, $f_2(a)=a^2$, $f_3(a)=a^4$, $f_4(a)=a^7$, $f_5(a)=a^8$, $f_6(a)=a^{11}$, $f_7(a)=a^{13}$, $f_8(a)=a^{14}$. *Tako, za*

$$f=f_5=\begin{pmatrix} e & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 & a^8 & a^9 & a^{10} & a^{11} & a^{12} & a^{13} & a^{14} \\ e & a^8 & a & a^9 & a^2 & a^{10} & a^3 & a^{11} & a^4 & a^{12} & a^5 & a^{13} & a^6 & a^{14} & a^7 \end{pmatrix}$$

imamo: $f(a)=a^8$, $f(a^2)=f(a)f(a)=a^8a^8=a^{16}=a$ $f(a^3)=f(a)f(a^2)=a^8a=a^9$ *itd.*

1.12. Dokazati da je $C_m \times C_n$ ciklična grupa akko su m i n uzajamno prosti. Da li je za neki $n \in N$ grupa $Z \times C_n$ ciklična?

Rešenje: Osim za n=1 grupa $Z \times C_n$ *nije ciklična budući da je* $Z \times C_n$ *beskonačna grupa i za generator a grupe* C_n, *element (0,a) je reda n, dok beskonačna ciklična grupa nema elemenata konačnog reda, osim jediničnog.*

1.13. Dokazati da je svaka netrivijalna konačno generisana podgrupa aditivne

grupe racionalnih brojeva ciklična i beskonačna.

Rešenje: Dokaz izvodimo indukcijom po k, broju generatora podgrupe $H<(Q,+)$. *Slučaj k=2: neka je* $H=\langle m_1/n_1, m_2/n_2 \rangle$ *gde su* m_1, m_2 *celi,* n_1, n_2 *pozitivni celi brojevi i bar jedan od* m_1, m_2 *je različit od 0. Element h grupe H je oblika* $h=xm_1/n_1 + ym_2/n_2$, *tj.* $h = (xm_1n_2 + ym_2n_1)/n_1n_2$. *Neka je* $d = NZD(n_1, n_2)$, $n_1=dn_1'$, $n_2=dn_2'$, $n_1n_2=dn$, $m = NZD(m_1n_2', m_2n_1')$ *i* $m_1n_2'=mr$, $m_2n_1'=ms$. *Tada* $h = (xr + ys)\cdot(m/n)$, *gde su r,s uzajamno prosti celi brojevi. Kako Diofantovska jednačina* $xr + ys=z$ *ima rešenje po x,y za ma koji* $z \in Z$, *to je* $H = \{z\cdot(m/n) \mid z \in Z\}$, *tj.* $H= \langle m/n \rangle$.

Pretpostavimo da tvrdjenje važi za k. Dokazujemo da važi za k+1. Neka je $H= \langle a_1, \ldots, a_k, a_{k+1} \rangle$, $a_i \in Q$ *i neka je* $K= \langle a_1, \ldots, a_k \rangle$. *Tada* $H= \langle K, a_{k+1} \rangle$ *i prema induktivnoj hipotezi, za neki* $a \in Q$ *je* $K= \langle a \rangle$. *Otuda,* $H= \langle a, a_{k+1} \rangle$, *pa prema prethodnom (slučaj k=2), za neki* $b \in Q$ *je* $H= \langle b \rangle$.

1.14. Neka je $K \leq Z(G)$. Dokazati: a) $K \trianglelefteq G$, b) Ako je G/K ciklična grupa tada je G komutativna.

Rešenje: a) Budući da svaki element iz K komutira sa svakim iz G, to je $K \trianglelefteq G$.

b) Neka je G/K generisana elementom Kc i pretpostavimo da je $|G/K|=k$. *Tada je* $\{K, Kc, \ldots, Kc^{k-1}\}$ *skup razreda podgrupe K. Otuda za* $a \in G$ *postoje* $n \in K$, $i \leq k-1$ *tako da* $a=nc^i$. *Neka su a,b bilo koji elementi grupe G. Tada za odgovarajuće* n_1, n_2, i, j *važi* $ab=n_1c^in_2c^j=n_1n_2c^ic^j$, *pa zbog* $n_1, n_2 \in Z(G)$:

$$ab = n_2n_1c^jc^i = n_2c^jn_1c^i = ba \ .$$

Sličan je dokaz i u slučaju kada je G/K beskonačna grupa.

1.15. Neka je G nekomutativna grupa. Dokazati da G/Z(G) nije ciklična.

Rešenje: Videti prethodni zadatak.

1.16. Dokazati da grupa automorfizama nekomutativne grupe G nije ciklična.

Rešenje: Neka je G nekomutativna grupa i $F : G \to \mathrm{Aut}\, G$ *preslikavanje odredjeno jednakošću* $F(a)=\sigma_a$. *Tada je F homomorfizam i* $\ker F = Z(G)$. *Prema Prvoj teoremi o izomorfizmu postoji utapanje* $f : G/Z(G) \xrightarrow[1-1]{} \mathrm{Aut}\, G$. *Otuda postoji* $H < \mathrm{Aut}\, G$ *tako da* $H \cong G/Z(G)$. *Prema zad. 1.15.* $G/Z(G)$ *nije ciklična, pa ni H nije ciklična grupa. Ako je* $\mathrm{Aut}\, G$ *ciklična grupa, tada je i H kao podgrupa ove grupe takodje ciklična, što je u kontradikciji sa prethodnim. Prema tome* $\mathrm{Aut}\, G$ *nije ciklična grupa.*

1.17. Ukoliko je G ciklična grupa, tada je G najviše prebrojiv skup. Dokazati.

Rešenje: Videti zadatak 1.2.

1.18.Dokazati da je svaka grupa reda 15 ciklična.

Rešenje: Videti zadatak 8.2.11.

1.19.Neka je $Z(p^\infty)$ p-Prüfer-ova grupa. Dokazati da je:

a) $Z(p^\infty) = \bigcup_{n\in\omega} G_i$, gde su G_i ciklične grupe i $G_0 < G_1 < G_2 < \ldots$

b) Svaka prava podgrupa grupe $Z(p^\infty)$ je konačna i ciklična .

c) Da li je $Z(p^\infty)$ ciklična grupa?

Rešenje: Budući da je $\underline{Z}(p^\infty) \simeq (\{x \in C \mid (\exists n \in \omega)\ x^{p^n} = 1\}, \cdot)$, gde je C skup kompleksnih brojeva, uzećemo da je $Z(p^\infty) = \{x \in C \mid (\exists n \in \omega)\ x^{p^n} = 1\}$.

a) Neka je $G_n = \{x \in C \mid x^{p^n} = 1\}$. G_n je ciklična grupa reda p^n, $G_0 < G_1 < G_2 < \ldots$ i $Z(p^\infty) = \bigcup_{n\in\omega} G_n$.

b) Neka je $H < Z(p^\infty)$. Dokazujemo da važi jedan od sledeća dva slučaja:

1° Za neki $n \in \omega$ je $H < G_n$ (G_n su ciklične grupe odredjene u a)); dakle, H je ciklična, ili 2° $H = Z(p^\infty)$.

Pretpostavimo da ne važi 1°. Tada za svaki $n \in \omega$, $H \cap (G_{n+1} \setminus G_n) \neq \emptyset$. Neka su $a_n \in H$ takvi da $a_n \in G_n \setminus G_{n-1}$ $(n > 1)$, tj. $a_n^{p^n} = 1$ i za $k < n$ $a_n^{p^k} \neq 1$. Neka je $K < Z(p^\infty)$ generisana elementima $a_1, a_2, \ldots$. Kako $a_1, a_2, \ldots \in H$ to $K < H$. Dokazujemo da za svaki $n \in \omega$, $G_n \subseteq K$. Grupa G_n je ciklična reda p^n pa $r(a_n) \mid p^n$. Otuda $r(a_n) \in \{1, p, p^2, \ldots, p^n\}$. Po pretpostavci, za sve $k < n$ je $a_n^{p^k} \neq 1$, stoga $r(a_n) = p^n$. Prema tome, $G_n = \langle a_n \rangle$ pa kako $a_n \in K$ to $G_n \subseteq K$. Otuda $\bigcup_{n\in\omega} G_n \subseteq K \subseteq H$ pa kako je $Z(p^\infty) = \bigcup_{n\in\omega} G_n$, sledi $Z(p^\infty) = H$.

c) $Z(p^\infty)$ je beskonačan skup dok su svi elementi grupe $Z(p^\infty)$ konačnog reda. Otuda $Z(p^\infty)$ nije ciklična grupa.

1.20.Svaka multiplikativna konačna podgrupa polja kompleksnih brojeva C je ciklična. Dokazati.

Rešenje: Ako je $H < (C \setminus \{0\}, \cdot)$ i $|H| = n$, tada $H = \{x \in C \mid x^n = 1\}$.

1.21.Opisati konačno generisane podgrupe aditivne grupe realnih brojeva.

1.22.Dokazati da svaka nekomutativna grupa G ima bar 4 unutrašnja automorfizma.

Rešenje: Ako G nije komutativna tada $G/Z(G)$ nije ciklična (v.zad. 1.15.). S druge strane $G/Z(G) \simeq Inn\, G$. Prema tome $|Inn\, G| \geq 4$.

1.23.Dokazati: ako je G konačna ciklična grupa, $H_1, H_2 < G$ i $|H_1| = |H_2|$, tada je $H_1 = H_2$.

Rešenje: Neka je $C_n = \langle a \rangle$ i $H_1 = \langle a^i \rangle$, $|H_1| = k$. Tada $ik = n$, tj. $i = n/k$. Otuda, ako je $H_2 = \langle a^j \rangle$, $|H_2| = k$, tada je $j = n/k$ pa $H_1 = H_2 = \langle a^i \rangle$.

6.2. EULER-OVA FUNKCIJA

Koristeći osobine cikličnih grupa mogu se izvesti svojstva raznih aritmetičkih funkcija. To se naročito odnosi na Euler-ovu funkciju $\phi(n)$ (prema velikom švajcarskom matematičaru L.Euler-u, 1707-1783).

2.1. *Definicija: Ako je $n \geq 2$ tada je $\phi(n)$ broj prirodnih brojeva uzajamno prostih sa n i manjih od n ; $\phi(1)=1$.*

Dakle, $\phi(2)=1$, $\phi(3)=2$, $\phi(12)=4$.

U najvažnije osobine ove funkcije spada njena *multiplikativnost.*

2.2. *Teorema: Ako su prirodni brojevi m i n uzajamno prosti, tada*

$$\phi(mn) = \phi(m)\phi(n) \ .$$

Za dokaz videti zadatak 2.3.

U poglavlju o brojevima razmatraju se osobine ove i drugih aritmetičkih funkcija, i to primenjujući razultate teorije grupa.

Primeri i zadaci

2.1. Dokazati: a) Element $a^k \in C_n$ je generator grupe C_n akko su k i n uzajamno prosti brojevi

b) Broj generatora grupe C_n jednak je $\phi(n)$.

Rešenje: a) Neka je $C_n = \langle a \rangle$, $C_n = \{e,a,a^2,\ldots,a^{n-1}\}$ i $k<n$. Lako se pokazuje da je $C_n = \langle a^k \rangle$ akko $a \in \langle a^k \rangle$. Dalje,

$$a \in \langle a^k \rangle \Leftrightarrow (\exists x \in N)a^{kx}=a \Leftrightarrow (\exists x \in N)kx \equiv 1 \pmod n \Leftrightarrow (\exists x,y \in N)kx-ny=1$$
$$\Leftrightarrow (k,n)=1$$

(Diofantovska jednačina $kx+ny=1$ ima rešenje akko $(k,n)=1$).

b) Prema prethodnom, broj različitih generatora grupe C_n je $\phi(n)$.

2.2. Dokazati da je $\mathrm{Aut}\, C_n \simeq (G,\cdot_n)$, gde je $G=\{i<n \mid i \in N \ \ (i,n)=1\}$, i $\cdot_n$ je množenje prirodnih brojeva po modulu n. Odavde izvesti $|\mathrm{Aut}\, C_n| = \phi(n)$.

Rešenje: Neka je za $(i,n)=1$, f_i funkcija definisana sa $f_i(x)=x^i$, $x \in C_n$.

Dokazujemo da je $f_i \in \mathrm{Aut}\, C_n$.

f_i je homomorfizam: $f_i(xy)=(xy)^i=x^iy^i=f_i(x)f_i(y)$, jer je C_n komutativna, dakle važi $(xy)^i=x^iy^i$.

f_i je 1-1: neka je $b \in \ker f_i$; tada $b^i=e$. Neka je $C_n=\langle a \rangle$; tada postoji k,

$k<n$ takav da je $b=a^k$. Otuda $a^{ki}=e$, tj. $ki\equiv 0 (\mathrm{mod}\, n)$, pa $n \mid k$; stoga $k=0$ pa je $b=a^0=e$. Prema tome $\ker f_i=\{e\}$, tj. f_i je 1-1.

Dalje, kako je C_n konačan skup i $f_i : C_n \to C_n$ je 1-1, to je f_i na.

Prema prethodnom $f_i \in \mathrm{Aut}\, C_n$.

Uvedimo preslikavanje $F : G \to \mathrm{Aut}\, C_n$ jednakošću $F(i)=f_i$, $i \in G$. Dokažimo da je F izomorfizam grupa G i $\mathrm{Aut}\, C_n$.

F je homomorfizam: $F(i\cdot j)(x)=f_{ij}(x)=x^{ij}=(x^j)^1=(f_i \cdot f_j)(x)$, pa $F(ij)=f_i \circ f_j = F(i)\circ F(j)$.

F je 1-1: neka je $F(i)=F(j)$; tada $(\forall x \in C_n) x^i=x^j$ pa $a^i=a^j$, odakle sledi $i\equiv j (\mathrm{mod}\, n)$. Budući da je $0 \leqslant i, j < n$ to $i=j$.

F je na: neka je $f \in \mathrm{Aut}\, C_n$, $f(a)=a^m$; tada postoji k, $k<n$ takav da $f(a^k)=a$ (jer f je na), pa $f(a)^k=a$, tj. $a^{mk}=a$. Otuda $mk\equiv 1 (\mathrm{mod}\, n)$, odakle, $(m,n)=1$ (Diofantovska jednačina $mx+ny=1$ ima rešenje!) pa $F(m)=f_m=f$

Kako je $\mathrm{Aut}\, C_n \cong (G, \cdot_n)$, $|G|=\phi(n)$, to $|\mathrm{Aut}\, C_n| = \phi(n)$.

2.3. Dokazati: a) $C_m \times C_n \simeq C_{mn}$ akko su m,n uzajamno prosti brojevi,

b) Ako su m,n uzajamno prosti brojevi tada je $\phi(mn)=\phi(m)\phi(n)$.

c) Ako je $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ razlaganje broja n na proste faktore, tada je

$$\phi(n) = n(1-p_1^{-1})(1-p_2^{-1})\ldots(1-p_k^{-1})$$

Rešenje: a) ($\Rightarrow$) Neka je $C_{mn} \simeq C_m \times C_n$; tada postoje podgrupe $H,K < C_{mn}$ takve da je $H \simeq C_m$, $K \simeq C_n$ i $H \cap K = \langle e \rangle$. Neka je $C_{mn} = \langle a \rangle$; tada postoje $b \in H$, $c \in K$ takvi da $a=bc$. Elementi $a^m, a^{2m}, \ldots, a^{(n-1)m}$ su medjusobnó različiti, dok sa druge strane $a^m=c^m$, $a^{2m}=(c^m)^2, \ldots, a^{(n-1)m}=(c^m)^{n-1}$ budući da je $b^m=e$, pa je c^m generator grupe K. Otuda je i c generator grupe K, pa kako je $|K|=n$ to je prema zad. 2.1. $(m,n)=1$.

($\Leftarrow$) Pretpostavimo $(m,n)=1$ i neka je $C_m = \langle a \rangle$, $C_n = \langle b \rangle$; tada

$$C_m \times C_n = \{(a^i, b^j) \mid 0 \leqslant i \leqslant m-1,\ 0 \leqslant j \leqslant n-1\}.$$

Dokazujemo da je $C_m \times C_n$ ciklična grupa sa generatorom (a,b). Neka su e_1, e_2 jedinični elementi redom grupa C_m, C_n. Tada

$$(ab)^{mn}=(a^{mn}, b^{mn})=(e_1^n, e_2^m)=(e_1, e_2).$$

Ako je $(a,b)^r=(e_1,e_2)$, $r>0$, tada $(a,b)^r=(a^r,b^r)=(e_1,e_2)$, tj. $a^r=e_1$, $b^r=e_2$. Odavde $m \mid r$, $n \mid r$ i kako je $(m,n)=1$ sledi $mn \mid r$, tj. $mn \leqslant r$. Dakle (a,b) je generator grupe $C_m \times C_n$, tj. $C_m \times C_n$ je ciklična, reda mn.

b) Neka je $(m,n)=1$; tada $C_{mn}=C_m \times C_n$, odnosno postoje $H,K<G$ takve da $H \simeq C_m$, $K \simeq C_n$, $C_{mn}=HK$, $H \cap K = \langle e \rangle$. Prema prethodnom delu zadatka lako je videti da važi $H=\langle b \rangle \wedge K=\langle c \rangle \Leftrightarrow C_{mn}=\langle bc \rangle$ $(b \in H,\ c \in K)$.

Otuda, $|\{x \mid x \text{ je generator grupe } H\}| \cdot |\{x \mid x \text{ je generator grupe } K\}| = |\{x \mid x \text{ je generator grupe } C_{mn}\}|$, *tj.* $\phi(mn)=\phi(m)\phi(n)$.

c) Prema prethodnom, lako je videti da je

$$C_n = C_{p_1^{\alpha_1}} \times C_{p_2^{\alpha_2}} \times \ldots \times C_{p_k^{\alpha_k}}$$

i

$$\phi(n) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\ldots\phi(p_k^{\alpha_k}) .$$

Dalje, neka je p prost broj. Tada su brojevi manji ili jednaki p^{α}, *koji nisu uzajamno prosti sa* p^{α}, *oblika pm, gde* $m < p^{\alpha-1}$. *Otuda njih ima* $p^{\alpha-1}$, *pa* $\phi(p^{\alpha}) = p^{\alpha}-p^{\alpha-1}$, *stoga*

$$\phi(n) = (p_1^{\alpha_1}-p_1^{\alpha_1-1})(p_2^{\alpha_2}-p_2^{\alpha_2-1})\ldots(p_k^{\alpha_k}-p_k^{\alpha_k-1}) = n\prod_{i=1}^{k}(1-p_i^{-1}).$$

Napomena: Ovaj zadatak može se rešiti koristeći stav o razlaganju konačnih Abel-ovih grupa (videti poglavlje o Abel-ovim grupama).

2.4. Dokazati: ako je G ciklična grupa reda n, tada je broj različitih podgrupa ove grupe jednak broju delilaca broja n.

Rešenje: Videti zad. 1.23.

2.5. (K.F.Gauss) Dokazati da za Euler-ovu funkciju $\phi(n)$ važi $\sum_{k|n} \phi(k) = n$.

Rešenje: Pretpostavimo: $k \mid n$. *Prema zad. 1.23. postoji podgrupa* A_k *grupe* C_n *koja je ciklična i reda k. Prema teoremi 1.5. to su i jedine podgrupe grupe* C_n. *Neka je* S_k *skup generatora grupe* A_k. *Ako je* $i \neq j$ *tada* $S_i \cap S_j = \emptyset$, *jer ukoliko bi bilo* $a \in S_i \cap S_j$ *tada bi element a generisao grupe različitih redova i,j, što je kontradikcija. Svaki* $a \in C_n$ *generiše jednu od grupa* A_i, *pa je* $C_n = \bigcup_i S_i$ *i* $n = \sum_{k|n} |S_k|$. *Kako je* $|C_k|=k$ *to je* $|S_k|=\phi(k)$, *dakle* $n = \sum_{k|n} \phi(k)$.

2.6. Neka je i prirodan broj uzajamno prost sa n. Dokazati da je $i^{\phi(n)} \equiv 1 \pmod n$.

Rešenje: Red grupe $G = (\{i < n \mid (i,n)=1\}, \cdot_n)$, *gde je* $\cdot_n$ *množenje po modulu n, je* $\phi(n)$. *Otuda* $(\forall x \in G)\ x^{\phi(n)} = 1$.

7. ABEL-OVE GRUPE

Upoznali smo mnogobrojne primere Abel-ovih (ili komutativnih) grupa, pa se već iz te činjenice moglo naslutiti da ove algebarske strukture čine značajnu klasu grupa. Razmatranja Abel-ovih grupa su specifičnog karaktera; naime, najveći deo odnosi se na klasifikaciju ovih grupa. Tako, pokazuje se na primer, da se konačne Abel-ove grupe, za razliku od nekomutativnih, veoma jednostavno opisuju; to kazuje stav o reprezentaciji konačno generisanih grupa (videti odeljak 7.3.). Otuda, netrivijalan deo ove teorije odnosi se uglavnom na beskonačne Abel-ove grupe . Jedan stav reprezentacije za Abel-ove grupe sa deljenjem biće i ovde izložen (videti odeljak 7.4.).

S obzirom na posebnost problema koji se razmatraju u okviru ove teorije, tehnika i pristup izučavanju ovih grupa su takodje specifični, pa otuda teorija Abel-ovih grupa čini jednu zasebnu oblast teorije grupa. Zainteresovani čitalac se podrobnije može upoznati sa ovom teorijom u [8].

7.1. ADITIVNA NOTACIJA. PRIMERI

U slučaju Abel-ovih grupa koristi se naročito obeležavanje, tzv. *aditivna notacija*. Naime, za jezik Abel-ovih grupa uzima se $L=\{+,-,0\}$, gde je: + simbol binarne operacije, - simbol unarne operacije i 0 simbol konstante. Dakle, svaka Abel-ova grupa je vida $\underline{A}=(A,+,-,0)$ i pri tom $\underline{A}$ zadovoljava aksiome: $(x+y)+z=x+(y+z)$, $x+y=y+x$, $x+(-x)=0$, $x+0=x$.

Nazivi pojmova ostaju isti kao i ranije, ali sada se svuda umesto reči "proizvod" dosledno koristi reč "zbir".

Tako, prevodi izraza 1, $x\cdot y$, x^{-1}, $x\cdot y^{-1}$, x^n, $X\cdot y$, $X\cdot Y$ sada izgledaju redom: 0, $x+y$, $-x$, $x-y$, nx, $X+y$, $X+Y$.

Ova nova notacija u potpunosti je opravdana sledećim tvrdjenjem.

1.1. Teorema: Neka je $\underline{A}$ Abel-ova grupa i neka su n,m celi brojevi. Tada za sve $x,y\in A$ važi:

(i) Ako je $n>0$ tada $nx=\underbrace{x+x+\ldots+x}_{n}$; ako je $n<0$ tada $nx=-|n|x$,

(ii) $(n+m)x=nx+mx$, (iii) $(nm)x=n(mx)$, (iv) $-(nx)=(-n)x$,

(v) $1\cdot x=x$, (vi) $n(x+y)=nx+ny$.

Dokaz: Tvrdjenja (i) - (vi) slede prema teoremi 2.1.2. Iskaz (vi) očigledno je ekvivalentan sledećem tvrdjenju:

> Neka je i ceo broj; tada je u svakoj komutativnoj grupi $(G,\cdot)$ preslikavanje $\phi: x \longmapsto x^i$ endomorfizam grupe $\underline{G}$. (*)

Zaista, indukcijom po i dokazuje se da važi $(xy)^i = x^i y^i$, $i \in \omega$. Navodimo dokaz za induktivni prelaz sa i na i+1. Neka je ispunjeno $(xy)^i = x^i y^i$. Tada

$$(xy)^{i+1} \underset{①}{=} (xy)^i (xy) \underset{②}{=} x^i y^i xy = x^i xy^i y = x^{i+1} y^{i+1}.$$

① *prema induktivnoj hipotezi*

② prema komutativnosti grupe G

Ako je $i=-j$, $j \in N$, tada

$$(xy)^i = (xy)^{-j} \underset{③}{=} ((xy)^j)^{-1} = (x^j y^j)^{-1} = (y^j)^{-1}(x^j)^{-1} = y^i x^i = x^i y^i$$

③ koristeći tvrdjenje za prirodne brojeve.

Suma grupa u slučaju Abel-ovih grupa ima naročito važnu ulogu (za razliku od nekomutativnih grupa), s obzirom da većina stavova o razlaganju ovih grupa sadrži upravo pojam sume. Ako su K,H podgrupe Abel-ove grupe $\underline{A}$ *tada, prema već uvedenoj simbolici,* $K+H=\{k+h \mid k \in K, h \in H\}$. *Primetimo da je za zbir podgrupa uvek ispunjeno* $K+H < A$ *(jer je svaka podgrupa komutativne grupe komutativna).*

1.2. $\underline{Definicija}$*: Neka je A Abel-ova grupa i neka su* $K,H < A$.

(i) $\mathbf{0}$ *je trivijalna podgrupa grupe A, tj.* $\mathbf{0}=\{0\}$.

(ii) Ako je $K \cap H = \mathbf{0}$, *tada je* $K+H$ $\underline{suma}$ *grupa K,H i označava se sa* $K \dot{+} H$

Kao i do sada $\sum_i K_i$ označava sumu grupa K_i u smislu definicija 5.2.1.-2. Navodimo najvažnije primere Abel-ovih grupa.

1.3. $\underline{Primeri}$*: 1° Svaka ciklična grupa* C_n *je Abel-ova grupa. Dakle, svaka grupa* Z_n *je Abel-ova grupa, kao i aditivna grupa celih brojeva Z.*

2° Svaka Prüfer-ova grupa $Z(p^\infty)$ *(p je prost broj) je Abel-ova grupa.*

3° Aditivne grupe racionalnih, realnih i kompleksnih brojeva su komutativne. Za njih u ovom odeljku koristimo redom oznake Q, R, C.

Klasa Abel-ovih grupa je *varijete* tj. zatvorena je za osnovne algebarske konstrukcije, kao što kazuje sledeća

1.4. $\underline{Teorema}$*: (i) Direktan proizvod Abel-ovih grupa je Abel-ova grupa,*

(ii) Homomorfna slika Abel-ove grupe je Abel-ova grupa,

(iii) Podgrupa Abel-ove grupe je Abel-ova grupa.

Dokaz: Videti zadatak 1.4.5.

Najzad, od koristi mogu biti sledeća tvrdjenja iz linearne algebre.

1.5.*Teorema:* *1° Ako su $\underline{V}$, $\underline{W}$ vektorski prostori nad istim poljem F, onda*

$$\underline{V} \cong \underline{W} \Leftrightarrow \dim \underline{V} = \dim \underline{W} .$$

2° Ako je $(V,+)$ vektorski prostor nad poljem $(F,+,\cdot,0,1)$ i $\dim \underline{V}=k$, tada

$$(V,+) = \sum_{i\in I} \underline{A}_i \ , \ gde \ |I|=k \ \ i \ \ (\forall i \in I)\, \underline{A}_i \cong (F,+) .$$

Primeri i zadaci

1.1.Dokazati: Grupa G je Abel-ova akko je preslikavanje $f: x \mapsto x^{-1}$ automorfizam grupe G.

Rešenje: $(\Rightarrow)$ $f(xy)=(xy)^{-1}=y^{-1}x^{-1}=x^{-1}y^{-1}=f(x)f(y)$, *tj. f je homomorfizam. kako je* $f(f(x))=x$, *to je f 1-1 i na, dakle,* $f\in \mathrm{Aut}\, G$.

$(\Leftarrow)$ *Neka je* $f\in \mathrm{Aut}\, G$ *i* $x,y\in G$. *Tada* $xy=f(f(x))f(f(y))=f(f(x)f(y))=(x^{-1}y^{-1})^{-1}=(y^{-1})^{-1}(x^{-1})^{-1}=yx$, *tj. G je komutativna.*

1.2.Neka je G konačna grupa i $f\in \mathrm{Aut}\, G$ za koji važi:
$f^2=I$ (I je identičko preslikavanje skupa G) i $(\forall x\in G)(f(x)=x \Rightarrow x=e)$.
Dokazati da je G Abel-ova grupa.

Rešenje: Neka je $g : G \to G$ *preslikavanje definisano sa* $g(x)=x^{-1}f(x)$. *Preslikavanje g je 1-1. Zaista, ako je* $g(x)=g(y)$ *tada* $x^{-1}f(x)=y^{-1}f(y)$, *pa* $yx^{-1}=f(yx^{-1})$, *odakle* $yx^{-1}=1$, *tj.* $x=y$. *Kako je G konačan skup to je g takodje na. Prema tome* $(\forall y\in G)(\exists x\in G)x^{-1}f(x)=y$. *Neka je* $a\in G$ *proizvoljan i* $b\in G$ *takav da* $b^{-1}f(b)=a$. *Tada* $f(b)=ba$ *odakle* $b=f(f(b))=f(ba)=f(b)f(a)=baf(a)$, *tj.* $b=baf(a)$. *Otuda* $f(a)=a^{-1}$. *Prema prethodnom,* $(\forall x\in G)f(x)=x^{-1}$, *pa je* $x \mapsto x^{-1}$ *automorfizam grupe G. Prema tome G je Abel-ova grupa.*

1.3.Neka je G grupa generisana a) elementima a,b, b) skupom S.
Dokazati: a) $ab=ba \Rightarrow$ G je Abel-ova grupa,
b) $(\forall x,y\in S)(xy=yx) \Rightarrow$ G je Abel-ova grupa.

Rešenje: a) Neka je $ab=ba$. *Tada takodje* $a^{-1}b=ba^{-1}$, $ab^{-1}=b^{-1}a$, $a^{-1}b^{-1}=b^{-1}a^{-1}$. *Dalje, indukcijom po* $n,m\in N$ *dokazuje se* $a^m b^n=b^n a^m$. *Otuda, koristeći gornje jednakosti i* $a^{-n}=(a^{-1})^n$ *dobija se*

$$(\forall m,n\in Z)a^m b^n=b^n a^m \ . \qquad (1)$$

Kako je svaki $x\in G$ *oblika* $x=a^{\alpha_1}b^{\beta_1}a^{\alpha_2}b^{\beta_2}\ldots a^{\alpha_n}b^{\beta_n}$, $\alpha_i,\beta_i\in Z$, *koristeći*

(1) dobija se da je svaki $x\in G$ oblika $x=a^{\alpha}b^{\beta}$ $(\alpha,\beta\in Z)$. Otuda za $x,y\in G$, $x=a^{\alpha}b^{\beta}$, $y=a^{\lambda}b^{\mu}$ je $xy=a^{\alpha}b^{\beta}a^{\lambda}b^{\mu}=b^{\beta}a^{\alpha}a^{\lambda}b^{\mu}=b^{\beta}a^{\lambda}a^{\alpha}b^{\mu}=\ldots=a^{\lambda}b^{\mu}a^{\alpha}b^{\beta}=yx$.

b) Primetimo da za svaki $x\in G$ postoje $a_1,a_2,\ldots,a_n\in S$ i $\alpha_1,\alpha_2,\ldots,\alpha_n\in\{-1,1\}$ tako da je $x=a_1^{\alpha_1}a_2^{\alpha_2}\ldots a_n^{\alpha}$ i kao u prethodnom slučaju za sve $\alpha,\beta\in\{-1,1\}$, $a,b\in S$ je $a^{\alpha}b^{\beta}=b^{\beta}a^{\alpha}$.

1.4.Ako je G Abel-ova grupa i K podgrupa grupe G, tada je K normalna podgrupa grupe G. Dokazati.

1.5.Neka je G Abel-ova grupa, $K<G$ i $k:G\to G/K$ prirodni homomorfizam. Dalje, neka je $S<G$ za koju su ispunjeni uslovi:

1° $G/K=\{k(s)\mid s\in S\}$, 2° $(\forall s,s'\in S)(s\neq s'\Rightarrow k(s)\cap k(s')=\emptyset)$.

a) Dokazati da postoji izomorfizam $f:(G/K)\times K\simeq G$,

b) Kontraprimerom pokazati da ne važi za proizvoljne Abel-ove grupe G,K implikacija $K<G\Rightarrow G\simeq(G/K)\times K$.

Rešenje: a) Preslikavanje $f:K\times(G/K)\to G$ definisano sa $f(x,k(s))=x+s$ je izomorfizam. Zaista,

f je homomorfizam: $f((x,k(s))+(x',k(s')))=f(x+x',k(s)+k(s'))=$ $f(x+x',k(s+s'))$. Kako je $s+s'\in S$, to

$f(x+x',k(s+s'))=(x+x')+(s+s')=(x+s)+(x'+s')=f(x,k(s))+f(x',k(s'))$.

f je na: Neka je $a\in G$; tada postoji $s\in S$ takav da je $k(a)=k(s)$. Otuda, $k(a-s)=0$ pa $a-s\in\ker k$. Kako je $K=\ker k$, postoji $x\in K$ takav da $a-s=x$. Otuda $a=x+s$, tj. $a=f(x,k(s))$, pa $a\in Im(f)$.

f je 1-1: Neka je $f(x,k(s))=f(x',k(s'))$. Otuda $x+s=x'+s'$. Stoga $x-x'=s'-s$, dakle $s'-s\in K$. Odavde je $k(s'-s)=0$, tj. $k(s)=k(s')$. Prema uslovu 2° onda je $s=s'$, pa i $x=x'$.

b) Kontraprimer: $Z\times(Q/Z)\not\simeq Q$. Zaista, element $a=(0,k(1/2))$ je reda 2, jer $2a=(0,2k(1/2))=(0,k(1))=0$. S druge strane, $k(1/2)\neq 0$, pa $a\neq 0$. Medjutim, aditivna grupa racionalnih brojeva nema elemenata reda 2.

1.6.Neka su G i K komutativne grupe u kojima su svi elementi, osim neutralnog, reda p, gde je p prost broj. Dokazati:

a) $|G|=|K|\Rightarrow G\simeq K$, b) $|G|<\infty$ $(\exists n\in N)|G|=p^n$,

c) Ukoliko je p=2, u pretpostavci se uslov komutativnosti može izostaviti,

d) Neka je $X=\{y\subseteq\omega\mid y$ je konačan$\}$ i $Y=X\cup\{y\subseteq\omega\mid\omega-y$ je konačan$\}$. Ako je $+$ simetrična razlika skupova, dokazati da su $(X,+)$ i $(Y,+)$ komutativne grupe i odrediti bar jedan izomorfizam ovih grupa.

Rešenje: $(G,Z_p,\cdot)$ je vektorski prostor, gde je $Z_p=(\{0,1,\ldots,p-1\},+_p,\cdot_p,0,1)$

polje, a za $\alpha \in Z_p$, $x \in G$, $\alpha \cdot x = x+x+\ldots+x$ (α *puta). Ako je G konačna grupa, tada je G konačno dimenzioni prostor nad* Z_p, *recimo* $dim(G)=n$. *Prema poznatom stavu iz linearne algebre, prostor* $(G,Z_p,\cdot)$ *je izomorfan vektorskom prostoru* $(Z_p^n,Z_p,\cdot)$. *Ako je pak* $|G|=\infty$, *tada je* $dim(G)=|G|$, *tačnije* $(G,Z_p,\cdot) \simeq \sum_{i<k} R_i$, *gde je* $R_i=(Z_p,Z_p,\cdot)$ *i* $k=|G|$. *Otuda,*

a) Ako $|G|=|K|=n$, $n \in N$, *tada* $G \simeq K \simeq Z_p^m$ *za neki* $m \in N$. *Ako* $|G|=|K|=\infty$, *tada* $G \simeq K \simeq \sum_{i<k} R_i$.

b) Ako je $|G|<\infty$, *prema prethodnom* $G \simeq (Z_p,+_p)^n$ *za neki* $n \in N$, *pa je* $|G|=|Z_p|^n=p^n$.

c) Ako je p=2, tada $(\forall x \in G)x^2=1$ *(u multiplikativnoj notaciji). No tada je G Abel-ova grupa, budući da iz* $(xy)^2=1$ *sledi* $(xy)(xy)=1$, $xy=y^{-1}x^{-1}$; *stoga* $xy=yx$ *jer je* $x^{-1}=x$ *ekvivalentno sa* $x^2=1$.

d) Neka su $x,y \in X$. *Tada* $x+y=(x-y) \cup (y-x)$. *Otuda, kako su x,y konačni, i* $x+y$ *je konačan. Dalje,* $(x-y) \cup (y-x) \subseteq \omega$, *dakle* $(x+y) \in X$. *Simetrična razlika skupova je asocijativna, pa kako je* $x+x=\emptyset$ *i* $\emptyset \in X$, $(X,+)$ *je grupa čiji su svi elementi reda 2. Slično se dokazuje da je* $(Y,+)$ *grupa. Kako je* $|X|=|Y|$, *prema a) je* $(X,+) \simeq (Y,+)$.

Neka su $a_0=\{0\}$, $a_1=\{1\}$, $a_2=\{2\},\ldots$. *Lako je videti da je grupa* $(X,+)$ *generisana elementima* $a_0,a_1,\ldots$, *dok je* $(Y,+)$ *generisana elementima* $\omega,a_0,a_1,\ldots$. *Za svaki* $x \in X-\{\emptyset\}$ *postoji* $n<\omega$ *i jedinstveni, medjusobno različiti elementi* $a_{i_1},a_{i_2},\ldots,a_{i_n}$ *takvi da* $x=a_{i_1}+a_{i_2}+\ldots+a_{i_n}$. *Slično, za svaki* $y \in Y-\{\emptyset\}$ *postoje jedinstveni, medjusobno različiti elementi* $b_{j_1},b_{j_2},\ldots,b_{j_m} \in \{\omega,a_0,a_1,\ldots\}$ *takvi da* $y=b_{j_1}+b_{j_2}+\ldots+b_{j_m}$. *Koristeći ove činjenice, preslikavanje*

$$f = \begin{pmatrix} a_o & a_1 & a_2 & \cdots \\ \omega & a_0 & a_1 & \ldots \end{pmatrix}$$

proširuje se do jedinstvenog izomorfizma $h: (X,+) \tilde{+} (Y,+)$.

Preciznije, za $x \in X$ $h(x)=\{s-1 \mid s \in x\}$ *ako* $0 \in x$, *inače* $h(x)=\omega+\{s-1 \mid s \in x, s \neq 0\}$.

Recimo, $h(\{0,1,3\})=h(\{0\})+h(\{1\})+h(\{3\})=\omega+\{0\}+\{2\}=\omega-\{0,2\}$.

1.7. Grupa H je prosto proširenje grupe G, u oznaci $H=G(c)$, ukoliko je $G<H$ i postoji $c \in H$ tako da je H najmanja podgrupa ma koje grupe K koja sadrži $G \cup \{c\}$; drugim rečima $K<H \wedge G \cup \{c\} \subseteq K \Rightarrow K=H$.

Dokazati: a) $G(c) = \langle G,c \rangle$,

b) $\langle G,c_1,c_2 \rangle = (G(c_1))(c_2) = (G(c_2))(c_1)$, gde je za neku grupu H, $G<H$ i $c_1,c_2 \in H$,

c) $\langle G,c_1,\ldots,c_n \rangle = \langle G,c_1,\ldots,c_{n-1} \rangle (c_n)$ $(n>1)$,

d) Ukoliko je $\underline{G} = (G,+)$ Abel-ova grupa, tada je $G(c)=\{mc+g \mid m \in Z,\ g \in G\}$.

Rešenje: d) Lako je proveriti da je $K=\{mc+g \mid m\in Z,\ g\in G\}$ *podgrupa grupe* G *i da je* $c\in K$. *S druge strane, za* $g\in G$ *i* $m\in Z$, $mc+g\in G(c)$, *tj.* $K\subseteq G(c)$. *Prema tome* $G(c)=K$.

1.8. Dokazati: Svaka podgrupa Abel-ove grupe G generisane sa najviše n elemenata, takodje je **generisana sa najviše n generatora.**

Rešenje: Dokaz izvodimo indukcijom po n, broju generatora grupe G. Za n=1 grupa G je ciklična, pa tvrdjenje sledi na osnovu teoreme 6.1.5. Neka je $G=\langle g_1,\dots,g_n\rangle$ *i pretpostavimo da je za n-1* $(n\geq 2)$ *tvrdjenje tačno. Dalje, neka je* $H<G$ *i* $x\in H$. *Tada za neke* $m_1,\dots,m_n\in Z$, $x=g_1^{m_1}\dots g_n^{m_n}$. *Ako je za svaki* $x\in H$ *odgovarajući* $m_1=0$, *tada* $H<\langle g_2,g_3,\dots,g_n\rangle$ *pa po induktivnoj hipotezi tvrdjenje sledi. Zato pretpostavimo da je za neki* $x\in H$ *odgovarajući* m_1 *uvek* $\neq 0$, *tj.* $(\forall m_1,\dots,m_n\in Z)(x=g_1^{m_1}\dots g_n^{m_n} \Rightarrow m_1\neq 0)$. *Kako je takodje* $x^{-1}\in H$, *može se u prethodnoj formuli pretpostaviti da je* $m_1>0$. *Prema tome postoji najmanji prirodan broj* $m>0$ *i brojevi* $m_2,\dots,m_n\in Z$ *takvi da* $g_1^{m}\,g_2^{m_2}\dots g_n^{m_n}\in H$. *Dalje, neka je y bilo koji element iz H. Tada* $y=g_1^{j_1}\dots g_n^{j_n}$ *za neke* $j_1,\dots,j_n\in Z$. *Dokazujemo da m deli* j_1. *Neka je* $j_1=mq+r$, $0\leq r<m$. *Tada za* $a=g_1^{m}\,g_2^{m_2}\dots g_n^{m_n}$, $y(a^q)^{-1}\in H$, *pa kako je* $y(a^q)^{-1}=g_1^{r}\dots$ *i* $0\leq r<m$, *prema izboru broja m sledi r=0. Otuda,* $y=a^q g_2^{r_2}\dots g_n^{r_n}$ *za neke* $r_2,\dots,r_n\in Z$. *Prema prethodnom* $H=\langle a,K\rangle$ *gde* $K=H\cap\langle g_2,\dots,g_n\rangle$. *Prema induktivnoj hipotezi K je generisana sa n-1 generatorom (jer* $K<\langle g_2,\dots,g_n\rangle$*), neka su to* $c_1,\dots,c_{n-1}$. *Otuda je* $H=\langle a,c_1,\dots,c_{n-1}\rangle$.

1.9. Dokazati da je $Z^n=\sum_{i=1}^{n} Z_i$, gde je $Z_i\simeq \underline{Z}$, $\underline{Z}=(Z,+)$.

Rešenje: Neka su $a_i\in Z^n$ *odredjeni sa* $a_1=(1,0,0,\dots,0)$, $a_2=(0,1,0,\dots,0)$, $\dots$, $a_n=(0,0,\dots,0,1)$. *Tada*

$$Z^n=\langle a_1\rangle\dot{+}\langle a_2\rangle\dot{+}\dots\dot{+}\langle a_n\rangle=\sum_{i=1}^{n} Z_i,\ \text{gde } Z_i=\langle a_i\rangle.$$

Elementi a_i *su beskonačnog reda pa su grupe* Z_i *beskonačne ciklične, tj.* $Z_i\simeq(Z,+)$.

1.10. Neka je G Abel-ova grupa generisana elementima $g_1,g_2,\dots,g_n$. Dokazati da je G homomorfna slika grupe Z^n.

Rešenje: Neka je $\underline{G}=(G,+)=\langle g_1,\dots,g_n\rangle$ *i* $h: Z^n\to G$ *definisano sa* $h(x_1,\dots,x_n)=x_1g_1+\dots+x_ng_n$. *Kako je* $G=\{x_1g_1+\dots+x_ng_n \mid x_1,\dots,x_n\in Z\}$ *jer je G generisana elementima* $g_1,\dots,g_n$, *to je h <u>na</u> preslikavanje; neposredno se proverava da je h homomorfizam iz* Z^n *na G.*

Napomena: Kako je $Z^n=\sum_{i=1}^{n} Z_i$, $Z_i\simeq Z$, *to je G takodje homomorfna slika grupe* $\sum_{i=1}^{n} Z_i$.

1.11. Neka su A,B Abel-ove grupe i $G=A \dot{+} B$. Ako su $A_1 < A$ i $B_1 < B$, dokazati:
a) $A_1 + B_1 < G$, b) $A_1 + B_1 = A_1 \dot{+} B_1$, c) $G/(A_1 + B_1) = (A/A_1) \dot{+} (B/B_1)$.

Rešenje: b) $A_1 \cap B_1 \subseteq A \cap B = \emptyset$.

c) Neka su $f: A \to A/A_1$, $g: B \to B/B_1$ *kanonski homomorfizmi i* $k: G \to A/A_1 \dot{+} B/B_1$ *preslikavanje definisano na sledeći način: ako je* $x \in A+B$ *tada postoje jedinstveni* $a \in A$, $b \in B$ *takvi da* $x=a+b$. *Tada* $k(x)=f(a)+g(b)$. *Preslikavanje k je homomorfizam grupe G na* $A/A_1 \dot{+} B/B_1$ *i* $\ker k = A_1 + B_1$. *Prema Teoremi o homomorfizmu je* $G/(A_1 + B_1) = A/A_1 \dot{+} B/B_1$.

1.12. Odrediti $\mathrm{Aut}\,\underline{Q}^n$ gde je $\underline{Q} = (Q,+,0)$.

Rešenje: Grupa $\underline{Q}^n$ *je vektorski prostor nad poljem racionalnih brojeva* $(Q,+,\cdot)$ *dimenzije n. Svi automorfizmi grupe* $\underline{Q}^n$ *su upravo linearni 1-1 operatori pomenutog vektorskog prostora. Otuda,* $\mathrm{Aut}\,\underline{Q}^n \simeq (M,\cdot)$, *gde je M skup regularnih matrica nad Q reda n.*

1.13. Dokazati da za $n \neq m$ $(n,m \in N)$ grupe Q^n, Q^m nisu medjusobno izomorfne.

Rešenje: Ako je $Q^n \simeq Q^m$ *tada su* Q^n *i* Q^m *izomorfni kao vektorski prostori nad poljem racionalnih brojeva, pa je* $n=\dim(Q^n)=\dim(Q^m)=m$.

1.14. Dokazati da je $\underline{R} \simeq \underline{C}$, gde je $\underline{R}$ aditivna grupa realnih brojeva a $\underline{C}$ aditivna grupa kompleksnih brojeva.

Rešenje: Grupe (R,+) i (C,+) su vektorski prostori nad poljem racionalnih brojeva Q i to iste dimenzije $c=2^{\aleph_0}$. *Prema poznatom stavu iz linearne algebre sledi da su ovi vektorski prostori izomorfni, pa su izomorfne i grupe* $\underline{R}$ *i* $\underline{C}$.

1.15. Dokazati da aditivna grupa racionalnih brojeva nije izomorfna sumi dveju netrivijalnih grupa.

Rešenje: Ako su $K,H < Q$, *tada* $K \neq 0 \wedge H \neq 0 \Rightarrow K \cap H \neq 0$.

Familija podskupova X_i skupa X $(i \in I)$ naziva se *lokalnim pokrivačem* ukoliko je $\bigcup_i X_i = X$ i za sve $i,j \in I$ postoji $k \in I$ takav da $X_i \cup X_j \subseteq X_k$. Na primer, skup svih konačnih (prebrojivih) podskupova skupa X čini jedan lokalni pokrivač skupa X. Kažemo da grupa G *ima lokalno svojstvo* ϕ akko postoji lokalni pokrivač $\{G_i \mid i \in I\}$ grupe G, gde $(\forall i \in I) G_i < G$ i svaka od grupa G_i ima svojstvo ϕ. Sledeći zadaci odnose se na ovaj pojam.

1.16. Dokazati da je svaka grupa G lokalno konačno generisana.

Rešenje: Familija $\{H \mid H < G$ *i H je konačno generisana*$\}$ *čini jedno lokalno*

pokrivanje grupe G.

1.17.Dokazati: ako je grupa G lokalno Abel-ova, onda je G Abel-ova.

1.18.Dokazati da su aditivna grupa racionalnih brojeva Q i Prüfer-ova grupa $Z(p^\infty)$ (p je prost broj) lokalno ciklične.

Rešenje: Svaka konačno generisana podgrupa racionalnih brojeva Q je ciklična (v.zad. 6.1.13.), pa tvrdjenje sledi prema 1.16.
Prema zad. 6.1.19. postoji niz cikličnih grupa $A_0 < A_1 < \ldots$ *tako da* $Z(p^\infty) = \bigcup_n A_n$.

1.19.Dokazati: a) Svaka Prüfer-ova grupa $Z(p^\infty)$ je lokalno konačna,
b) Aditivna grupa racionalnih brojeva nije lokalno konačna.

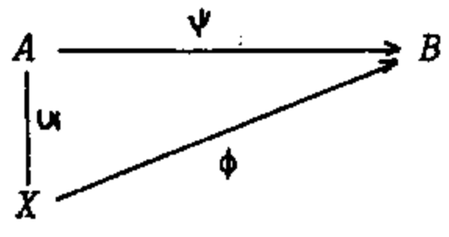
Rešenje: a) Za $Z(p^\infty)$ videti prethodni zadatak.
b) Svaka podgrupa grupe Q je beskonačna.

1.20.Neka su A i B Abel-ove grupe i Hom(A,B) skup svih homomorfizama iz A u B. Dokazati da je $(\mathrm{Hom}(A,B),+,\underline{0})$ grupa, gde je $(\forall x\in A)(f+g)(x)=f(x)+g(x)$, $(f,g\in \mathrm{Hom}(A,B))$ i $(\forall x\in A)\underline{0}(x)=0_B$.

7.2. SLOBODNE ABEL-OVE GRUPE

U prethodnom odeljku pokazali smo (zad. 1.10.) da grupa Z^n ima zanimljivo svojstvo *univerzalnosti*; naime, *svaka* Abel-ova grupa generisana skupom od n elemenata jeste homomorfna slika ove grupe. Pored ovog, grupa Z^n ima i neka druga interesantna svojstva, koja ćemo upoznati u ovom odeljku.

2.1.*Definicija: Neka je A Abel-ova grupa i $X\subseteq A$. Grupa A je slobodna Abel-ova grupa sa skupom slobodnih generatora X akko za svaku Abel-ovu grupu B, svako preslikavanje $\phi: X \to B$ ima proširenje do homomorfizma $\psi : A \to B$.*



Sledećom teoremom se utvrdjuje egzistancija slobodnih Abel-ovih grupa, kao i njihov tačan opis.

2.2.*Teorema: Neka je $A = \sum_{i\in I} A_i$ Abel-ova grupa, gde za svaki $i\in I$, $A_i \cong Z$ i $A_i = \langle a_i \rangle$. Tada je A slobodna Abel-ova grupa sa skupom slobodnih generatora $\{a_i \mid i\in I\}$.*

Dokaz: Za svaki $a \in \sum_{i \in I} A_i$ postoje jedinstven prirodan broj n, jedinstveni $a_{i_1},\ldots,a_{i_n}$ i jedinstveni celi brojevi $x_1,\ldots,x_n$ tako da

$$a = x_1 a_{i_1} + \ldots + x_n a_{i_n}$$

(videti zadatke 5.2.3. i 5.1.6.).
Koristeći ovu činjenicu, svako preslikavanje $\phi : \{a_i \mid i \in I\} \to B$ ima jedinstveno proširenje do homomorfizma $\psi : \sum_i A_i \to B$. Proširenje ψ odredjeno je sa $\psi(a) = x_1\phi(a_{i_1}) + \ldots + x_n\phi(a_{i_n})$. Dakle, $\sum_i A_i$ je slobodna Abel-ova grupa.

2.3.Primer: Prema prethodnom dokazu, ako su elementi a_i iz Z^n odredjeni sa $a_1=(1,0,\ldots,0)$, $a_2=(0,1,0,\ldots,0)$,..., $a_n=(0,\ldots,0,1)$, tada oni čine skup slobodnih generatora grupe Z^n; dakle, Z^n je slobodna Abel-ova grupa sa n slobodnih generatora.

2.4.Definicija: Neka je G Abel-ova grupa, $X,Y \subseteq G$ i $a \in G$.

(i) Skup X je nezavisan akko za svakih n različitih elemenata $x_1,\ldots, x_n \in X$ i cele brojeve $k_1,\ldots,k_n$ važi

$$k_1x_1 + k_2x_2 + \ldots + k_nx_n = 0 \Rightarrow k_1x_1=0 \wedge k_2x_2=0 \wedge \ldots \wedge k_nx_n=0 .$$

(ii) Element a je zavisan od skupa X akko postoje celi brojevi $k_0,k_1,\ldots,k_n$ i $x_1,\ldots,x_n \in X$ tako da važi

$$k_0a + k_1x_1 + \ldots + k_nx_n = 0 .$$

(iii) Skup Y je zavisan od skupa X akko je svaki $y \in Y$ zavisan od skupa X.

Neki primeri nezavisnih skupova dati su u zadatku 2.4.

Kao što se kod vektorskih prostora uvodi dimenzija, imajući u vidu pojam nezavisnosti na sličan način se kod Abel-ovih grupa uvodi pojam *ranga*.

2.5.Definicija: Ako je S maksimalan nezavisan konačan podskup Abel-ove grupe A bez torzije, tada je rang A = S . Ukoliko u A ne postoji konačan maksimalno nezavisan podskup, tada je rang A = ∞.

U zadatku 2.7. dokazuje se da je koncept ranga dobro definisan za grupe bez torzije. Podsećamo da je grupa A bez torzije ukoliko nema elemenata konačnog reda, tj. $(\forall x \in A \setminus \{0\})(\forall n \in N) nx \neq 0$.

Primeri i zadaci

2.1. Neka je G Abel-ova grupa generisana elementima $g_1, g_2, \ldots, g_n$ sa svojstvom: za svaku komutativnu grupu H, svako preslikavanje $h : \{g_1, \ldots, g_n\} \to H$ ima homomorfno proširenje $f : G \to H$. Dokazati da je $G = Z^n$.

Rešenje: Neka su $a_i \in Z^n$, $1 \leqslant i \leqslant n$, odredjeni kao u primeru 2.3.; neka je zatim $h(g_i) = a_i$, $1 \leqslant i \leqslant n$ i $f : G \to Z^n$ homomorfizam koji proširuje h. Tada je f izomorfizam ovih grupa.

2.2. Neka je G Abel-ova grupa slobodno generisana svakim od skupova X,Y. Ako je X konačan skup, dokazati da je tada i skup Y konačan.

Rešenje: Ako je G slobodno generisana konačnim skupom $X = \{g_1, \ldots, g_n\}$, tada G ima najviše prebrojivo mnogo endomorfizama. Zaista, za svako preslikavanje $h : \{g_1, \ldots, g_n\} \to G$ postoji najviše jedan homomorfizam $f : G \to G$ koji proširuje h. Kako je G prebrojiv skup, ovakvih preslikavanja h, dakle i samih endomorfizama f, ima najviše prebrojivo mnogo.
Dalje, ako Y slobodno generiše G, onda se svaka permutacija skupa Y proširuje do automorfizma grupe G; dakle, ako bi Y bio beskonačan skup, onda $|Aut\, G| = 2^{|Y|} \geqslant 2^{\aleph_0} > \aleph_0$, što je u kontradikciji sa uslovom da G ima najviše prebrojivo mnogo automorfizama. Dakle, Y je konačan.

2.3. Neka je $G = \langle a_1 \rangle \dot{+} \langle a_2 \rangle \dot{+} \ldots \dot{+} \langle a_n \rangle$ direktna suma beskonačnih cikličnih grupa i neka su $m_2, \ldots, m_n \in Z$. Dokazati da je $G = \langle b \rangle \dot{+} \langle a_2 \rangle \dot{+} \ldots \dot{+} \langle a_n \rangle$, gde je $b = a_1 + m_2 a_2 + \ldots + m_n a_n$.

Rešenje: Dokazujemo da za svaki $x \in G$ postoji jedinstveno predstavljanje

$$x = \alpha_1 b + \alpha_2 a_2 + \ldots + \alpha_n a_n \quad (\alpha_i \in Z) \qquad (1)$$

Kako je G generisana elementima $a_1, \ldots, a_n$ to postoje $\beta_1, \ldots, \beta_n \in Z$ takvi da

$$x = \beta_1 a_1 + \beta_2 a_2 + \ldots + \beta_n a_n \ . \qquad (2)$$

Ukoliko važi uslov (1), onda $x = \alpha_1 a_1 + (\alpha_1 m_2 + \alpha_2) a_2 + \ldots + (\alpha_1 m_n + \alpha_n) a_n$, pa je dovoljno dokazati da sistem jednačina

$$\alpha_1 = \beta_1 \ , \quad \alpha_1 m_2 + \alpha_2 = \beta_2 \ , \ldots , \quad \alpha_1 m_n + \alpha_n = \beta_n$$

ima rešenje po $\alpha_1, \alpha_2, \ldots, \alpha_n$. Rešenja ovog sistema su: $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2 - \beta_1 m_2$, $\ldots$, $\alpha_n = \beta_n - \beta_1 m_n$.
Jedinstvenost reprezentacije (1) sledi na osnovu jedinstvenosti predstavljanja (2).

2.4. Dokazati da su sledeći skupovi elemenata nezavisni u Z^3:
a) $\{(1,0,0),(0,1,0),(0,0,1)\}$, b) $\{(1,0,0),(1,1,0),(1,1,1)\}$,

c) $\{(1,0,0),(1,3,4),(3,2,3)\}$, d) $\{(1,0,0),(1,2,0),(1,2,3)\}$.
Koji od navedenih skupova generišu celu grupu Z^3?

Rešenje: b) Neka su $x,y,z \in Z$ takvi da $x(1,0,0)+y(1,1,0)+z(1,1,1)=(0,0,0)$. Tada $(x+y+z,y+z,z)=(0,0,0)$, odakle $x=0$, $y=0$, $z=0$.

Skupovi pod a), b) i c) generišu grupu Z^3, dok skup pod d) ne generiše, budući da nije svaki $(a,b,c) \in Z^3$ predstavljiv u obliku

$$(a,b,c)=x(1,0,0)+y(1,2,0)+z(1,2,3), \quad x,y,z \in Z .$$

2.5.Dokazati da je relacija zavisnosti tranzitivna, tj. ako su X,Y,Z podskupovi Abel-ove grupe G i ako X zavisi od Y i Y zavisi od Z, tada X zavisi od Z.

2.6.(Steinitz-ova teorema o zameni nezavisnih skupova): Neka je G Abel-ova grupa bez torzije i $A=\{a_1,\ldots,a_m\}$ nezavisan podskup od G. Dalje, neka je $B=\{b_1,\ldots,b_n\}$ podskup od G takav da A zavisi od B. Tada $n \geqslant m$ i B zavisi od $A \cup C$, gde je $C \subseteq B$ i $|C|=n-m$.

Rešenje: Dokaz izvodimo indukcijom po m, broju elemenata skupa A.
Slučaj $m=1$. Tada $A=\{a_1\}$, pa kako je $n \in N$, to $n \geqslant m$. Dalje, kako a_1 zavisi od B, za neke $x,x_1,\ldots,x_n \in Z$, $xa_1=x_1b_1+\ldots+x_nb_n$ i $xa_1 \neq 0$ .Otuda sledi da nisu svi $x_i=0$, pa za neki i, $x_i \neq 0$. Tada B zavisi od $\{a_1\} \cup (B \setminus \{b_i\})$. Očigledno $|B \setminus \{b_i\}|=n-1$ i $B \setminus \{b_i\} \subseteq B$.

Pretpostavimo da tvrdjenje važi za m. Dokazujemo da važi za m+1.
Neka je $A=\{a_1,\ldots,a_{m+1}\}$ nezavisan skup koji zavisi od B. Tada $\{a_1,\ldots,a_m\}$ zavisi od B pa po indukcijskoj hipotezi $n \geqslant m$ i za neki $D \subseteq B$, B zavisi od $\{a_1,\ldots,a_m\} \cup D$ i $|D|=n-m$. Dalje, a_{m+1} zavisi od B, B zavisi od $\{a_1,\ldots,a_m\} \cup D$, tj. za neke $x,x_1,\ldots,x_m,y_1,\ldots,y_s \in Z$, $xa_{m+1} \neq 0$ i $xa_{m+1}=x_1a_1+\ldots+x_ma_m+y_1d_1+\ldots+y_sd_s$, gde $D=\{d_1,\ldots,d_s\}$. Tada za neki i, $y_id_i \neq 0$ jer bi inače A bio zavisan skup. Neka je $C=D \setminus \{d_i\}$. Tada $\{a_1,\ldots,a_m\} \cup D$ zavisi od $\{a_1,\ldots,a_m\} \cup C$, pa prema tranzitivnosti relacije zavisnosti, B zavisi od $\{a_1,\ldots,a_m\} \cup C$. Kako $C \subseteq D \subseteq B$ to $C \subseteq B$ i $|C|=|D|-1=(n-m)-1=n-(m+1)$.

2.7.Neka su S,T maksimalni konačni nezavisni skupovi Abel-ove grupe G bez torzije. Tada $|S|=|T|$. Dokazati.

Rešenje: Ako su S i T maksimalni nezavisni skupovi grupe G, tada S zavisi od T, pa prema Steinitz-ovoj teoremi $|S| \geqslant |T|$. Slično, $|T| \geqslant |S|$ i stoga $|S|=|T|$.

2.8.Neka su X,Y skupovi slobodnih generatora slobodne Abel-ove grupe G, tako da svaki od X,Y generiše G. Ako je bar jedan od X,Y konačan, dokazati da

je $|X|=|Y|=\operatorname{rang} G$.

Rešenje: Videti prethodna dva zadatka.

2.9.Dokazati da u svakoj Abel-ovoj grupi postoji maksimalan nezavisan skup.

Rešenje: Neka je $X=\{S\subseteq G \mid S$ *je nezavisan u* $G\}$. *Ako je* S_i $(i\in I)$ *lanac skupova iz* X, *tada je* $S=\bigcup_{i\in I} S_i$ *takodje iz* X *(tj. nezavisan skup u* G*). Prema Zorn-ovoj lemi postoji* $S\in X$ *koji je maksimalan u odnosu na* $\subseteq$.

2.10.Da li svaki maksimalni nezavisni podskup slobodne Abel-ove grupe G generiše G?

Rešenje: U zadatku 2.4.d) naveden je skup koji je maksimalno nezavisan, ali ne generiše Z^3.

2.11.Neka su A i B Abel-ove grupe bez torzije. Dokazati da je

$$\operatorname{rang}(A\times B)=\operatorname{rang}(A\dot{+}B)=\operatorname{rang}A+\operatorname{rang}B\ .$$

Rešenje: Neka su $\{a_1,\ldots,a_m\}$ *i* $\{b_1,\ldots,b_n\}$ *maksimalni nezavisni skupovi redom u grupama A i B. Dokazujemo da je* $S=\{a_1,\ldots,a_m,b_1,\ldots,b_n\}$ *nezavisan skup grupe* $A\dot{+}B$. *Neka su* x_i,y_i *celi brojevi takvi da* $x_1a_1+\ldots+x_ma_m+y_1b_1+\ldots+y_nb_n=0$. *Tada* $x_1a_1+\ldots x_ma_m=-y_1b_1-\ldots-y_nb_n$, *pa kako je* $A\cap B=\mathbf{0}$ *i* $(x_1a_1+\ldots+x_ma_m)\in A$, $(y_1b_1+\ldots+y_nb_n)\in B$, *to* $x_1a_1+\ldots+x_ma_m=-y_1b_1-\ldots-y_nb_n=0$, *odakle* $x_i=y_i=0$ $(i=1,2,\ldots)$.
Prema prethodnom S je nezavisan skup. Neka je $c\in A\dot{+}B$. *Tada za neke elemente* $a\in A$, $b\in B$, $c=a+b$ *i zbog maksimalne nezavisnosti postoje* $x,y,x_i,y_i\in Z$ *tako da* $xa=x_1a_1+\ldots+x_ma_m$, $yb=y_1b_1+\ldots+y_nb_n$ $(x,y\neq 0)$. *Otuda* $xy\neq 0$ *i*
$xyc=y(xa)+x(yb)=yx_1a_1+\ldots+yx_ma_m+xy_1b_1+\ldots+xy_nb_n$.
Prema prethodnom $\operatorname{rang}(A\dot{+}B)=m+n=\operatorname{rang}A+\operatorname{rang}B$.

2.12.Odrediti rang sledećih grupa: a) Z^n , b) $(Q,+)$, c) $(Q\setminus\{0\},\cdot)$, d) $(R,+)$, e) $(R\setminus\{0\},\cdot)$, f) $(C\setminus\{0\},\cdot)$.

Rešenje: a) $\operatorname{rang} Z=1$, *pa prema prethodnom zadatku* $\operatorname{rang} Z^n=\operatorname{rang}(Z\dot{+}\ldots\dot{+}Z)=\operatorname{rang} Z+\ldots+\operatorname{rang} Z=n$.
b) $\operatorname{rang}(Q,+)=1$, *c)* $\operatorname{rang}(Q\setminus\{0\},\cdot)=\infty$, *d)* $\operatorname{rang}(R,+)=\infty$.

2.13.Neka je G Abel-ova grupa konačno generisana sa n slobodnih generatora. Ako je $H<G$ tada postoje slobodni generatori $c_1,c_2,\ldots,c_n\in G$ i prirodni brojevi $u_1,u_2,\ldots,u_n$ takvi da je $H=\langle u_1c_1,u_2c_2,\ldots,u_nc_n\rangle$. Dokazati.

Rešenje: Dokaz se izvodi indukcijom po n, broju slobodnih generatora grupe G.

Slučaj n=1. Kako je G slobodna Abel-ova grupa generisana jednim elementom, to je G beskonačna ciklična, tj. $G \cong Z$. Otuda, H je kao podgrupa ciklične grupe takodje ciklična, pa za neki $n \in N$, $H = \langle na \rangle$, gde je a generator za G.

Pretpostavimo da tvrdjenje važi za n-1 ($n \geq 2$). Dokazujemo da važi za n. Neka je $h \in H$ i $\{a_1,\ldots,a_n\}$ jedan skup generatora grupe G. Tada za neke

$$x_1,\ldots,x_n \in Z \qquad h = x_1a_1 + \ldots + x_na_n \ . \qquad (1)$$

Kako je $-h \in H$, to ako postoji $h \in H$ za koji je $x_1 \neq 0$, to u H postoji h za koji je odgovarajući $x_1 > 0$. Dalje, primetimo da svaki skup slobodnih generatora grupe G ima n (=rang G) elemenata.

Neka je $u \geq 1$ najmanji prirodan broj takav da za neki skup slobodnih generatora $a_1,\ldots,a_n$ grupe G i neke $x_1,\ldots,x_n \in Z$ i neki $h \in H$ važi (1) za $x_1 = u$ (takav u postoji, inače $H = 0$). Dokazujemo da u deli $x_2,\ldots,x_n$.
Neka je $x_2 = mu + r$, $0 \leq r < m$. Tada

$$h = ua_1 + (mu+r)a_2 + x_3a_3 + \ldots + x_na_n = ra_2 + u(a_1 + ma_2) + x_3a_3 + \ldots + x_na_n.$$

Elementi $a_2, a_1 + ma_2, a_3, \ldots, a_n$ čine jedan skup slobodnih generatora grupe G (v.zad.2.3.), pa prema izboru broja u, r=0. Prema tome, u deli x_2. Slično, u deli $x_3,\ldots,x_n$. Otuda za neke $y_2,\ldots,y_n$, h=uc gde
$c = a_1 + y_2a_2 + \ldots + y_na_n$.

Neka je $g = z_1a_1 + \ldots + z_na_n$, $z_i \in Z$, bilo koji element iz H. Dokazujemo da u deli z_1. Neka je $z_1 = mu + r$, $0 \leq r < m$. Tada $g - mh \in H$ i takodje za neke $z_i' \in Z$ $g - mh = ra_1 + z_2'a_2 + \ldots + z_n'a_n$. Prema izboru broja u, r=0. Dakle, $g - mh = z_2'a_2 + \ldots + z_n'a_n$ tj. $g \in \langle h, a_2,\ldots,a_n \rangle$. Otuda $H = \langle h, K \rangle$ gde $K = H \cap \langle a_2,\ldots,a_n \rangle$. Prema induktivnoj hipotezi, budući da je $\langle a_2,\ldots,a_n \rangle$ slobodna Abel-ova grupa sa slobodnim generatorima $a_2,\ldots,a_n$, $K = \langle u_2c_2,\ldots, u_nc_n \rangle$, gde su $c_2,\ldots,c_n$ slobodni generatori grupe $\langle a_2,\ldots,a_n \rangle$ a $u_i \in \omega$. Otuda $K = \langle uc, u_2c_2,\ldots,u_nc_n \rangle$ i prema zad. 2.3., $c, c_2,\ldots,c_n$ čine jedan skup slobodnih generatora grupe G.

2.14. Dokazati da je svaka podgrupa konačno generisane slobodne Abel-ove grupe, takodje **slobodna Abel-ova grupa.**

Rešenje: Ako je G slobodna Abel-ova grupa i $H < G$, prema prethodnom zadatku postoje slobodni generatori $c_1,\ldots,c_n$ grupe G i celi brojevi $m_1,\ldots,m_n$ tako da je $H = \langle m_1c_1,\ldots,m_nc_n \rangle$. Tada neposredno sledi $H = \langle m_1c_1 \rangle \dot{+} \ldots \dot{+}$ $\langle m_nc_n \rangle$ i svaka grupa $\langle m_ic_i \rangle$ izomorfna je jednoj od grupa 0, Z .
Dakle, $H \cong Z^k$ za neki $k \leq n$.

2.15. Dokazati da je svaka podgrupa grupe Z^2 trivijalna ili izomorfna jednoj od grupa Z, Z^2 .

Rešenje: Ako je $H<Z^2$, *za neke slobodne generatore* a_1,a_2 *grupe* Z^2 *i neke* $n_1,n_2\in\omega$ *je* $H=<n_1a_1,n_2a_2>$ *(videti prethodni zadatak). Otuda, ako* n_1, $n_2=0$ *onda* $H=0$; *ako* $n_1=0$, $n_2\neq 0$, *tada* $H=<n_2a_2>\simeq Z$; *ako* $n_1,n_2\neq 0$ *tada* $H=<n_1a_1>\dot{+}<n_2a_2>\simeq Z^2$

2.16. Opisati podgrupe grupe Z^n .

Rešenje: Svaka podgrupa H grupe Z^n *izomorfna je trivijalnoj ili jednoj od grupa* Z^i $(1\leqslant i\leqslant n)$.

2.17. Dokazati da za $n\neq m$ $(n,m\in N)$ grupe Z^n i Z^m nisu medjusobno izomorfne.

Rešenje: Ako $Z^m\simeq Z^n$ *tada* $m=rang\, Z^m=rang\, Z^n=n$.

7.3. KONAČNO GENERISANE ABEL-OVE GRUPE

Već smo napomenuli da konačno generisane Abel-ove grupe imaju jednostavnu strukturu. Naime, važi sledeći stav o razlaganju ovih grupa.

3.1. *Teorema: Svaka konačno generisana Abel-ova grupa izomorfna je direktnom proizvodu cikličnih grupa.*

Dokaz: Neka je Abel-ova grupa G generisana elementima $g_1,\ldots,g_n$. Grupa Z^n je slobodna Abel-ova sa n slobodnih generatora, pa postoji homomorfizam $h: Z^n \to G$. Neka je $H=\ker h$. Prema zad. 2.13. za neke slobodne generatore $a_1,\ldots,a_n$ grupe Z^n i $m_1,\ldots,m_n\in\omega$ važi $H=<m_1a_1,\ldots,m_na_n>$. Otuda $H\simeq A_1\dot{+}\ldots\dot{+}A_n$ gde $A_i=<m_ia_i>$ i $A_i<B_i$, $Z_i=<a_i>$, $Z^n=B_1\dot{+}\ldots\dot{+}B_n$. Prema Teoremi o homomorfizmu $G\simeq Z^n/\ker h$, tj. $B\simeq(B_1\dot{+}\ldots\dot{+}B_n)/(A_1\dot{+}\ldots\dot{+}A_n)$. Kako je $(B_1\dot{+}\ldots\dot{+}B_n)/(A_1\dot{+}\ldots\dot{+}A_n)\simeq B_1/A_1\dot{+}\ldots\dot{+}B_n/A_n$ (v.zad. 1.11.), $B_i/A_i\simeq Z/m_iZ=C_{m_i}$ $(C_0=C_\infty)$, to $G\simeq C_{m_1}\dot{+}\ldots\dot{+}C_{m_n}\simeq C_{m_1}\times\ldots\times C_{m_n}$ ▼

Koristeći aditivnu notaciju ova teorema ima sledeći preizraz:

3.2. *Posledica: Svaka konačno generisana Abel-ova grupa A jednaka je konačnoj (unutrašnjoj) sumi nekih cikličnih grupa.*

Dakle $A\simeq\sum_{i<k}A_i$, gde je svaka grupa A_i izomorfna nekoj od grupa Z, Z_n $(n\in N)$. U slobodnijoj notaciji pišemo $A=\sum_{i\leqslant r}Z_{n_i}\dot{+}Z^m$.

3.3. *Posledica: Svaka konačna Abel-ova grupa izomorfna je konačnom proizvodu cikličnih grupa.*

Dokaz: Primetimo da je svaka konačna grupa takodje konačno generisana. ▼

Neka je A Abel-ova grupa. Prema teoremi 3.1. postoje ciklične grupe

C_{n_i} , i=1,...,k tako da $A \simeq C_{n_1} \times \ldots \times C_{n_k} \times C_\infty^m$. Neka je $n_1 = q_1^{\alpha_1} \ldots q_m^{\sigma_m}$ razlaganje prirodnog broja n_1 na proste faktore. Prema zad. 6.2.3.a), $C_{n_1} \simeq C_{q_1^{\sigma_1}} \times \ldots \times C_{q_m^{\sigma_m}}$. Dakle, postoji niz prostih brojeva $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_k$ i niz prirodnih brojeva $\alpha_1, \ldots, \alpha_k$ većih od nule tako da

$A \simeq C_{p_1^{\alpha_1}} \times C_{p_2^{\alpha_2}} \times \ldots \times C_{p_k^{\alpha_k}} \times C_\infty^m$ ili,u aditivnoj notaciji

$$A \simeq Z_{p_1^{\alpha_1}} + Z_{p_2^{\alpha_2}} + \ldots + Z_{p_k^{\alpha_k}} + Z^m \ .$$

Dokazaćemo da su za svaku konačno generisanu Abel-ovu grupu A brojevi $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$, m jedinstveno odredjeni. Prethodno, podsetimo da je za svaki ceo broj n, preslikavanje $\phi : x \longmapsto nx$ homomorfizam grupe A (videti teoremu 1.1.f)). Za ovaj homomorfizam, $nA = \phi(A)$, dakle $nA = \{nx \mid x \in A\}$. Koristeći svojstva homomorfizama imamo:

3.4. <u>Lema</u>: *Neka su A,B Abel-ove grupe i $n \in Z$. Tada*

(i) $nA < A$, $n(A+B) = nA + nB$,

Ako su p,q različiti prosti brojevi i $\alpha, \beta \in N$, tada

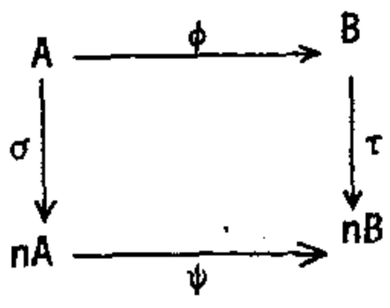
(ii) $pZ_{p^\alpha} \simeq Z_{p^{\alpha-1}}$; *ako je* $\beta > \alpha$ *tada* $p^\beta Z_{p^\alpha} = Z_{p^{\beta-\alpha}}$; *za* $\alpha < \beta$ $p^\beta Z_{p^\alpha} = 0$,

(iii) $pZ \simeq Z$, *opštije* $p^\alpha Z \simeq Z$,

(iv) $qZ_{p^\alpha} \simeq Z_{p^\alpha}$, *opštije* $q^\beta Z_{p^\alpha} \simeq Z_{p^\alpha}$,

(v) $A \simeq B \Rightarrow nA = nB$.

Dokaz: Dokažimo, recimo, tvrdjenje (v).



Neka je $\phi : A \xrightarrow{\simeq} B$ i $\sigma : x \longmapsto nx$, $x \in A$;
$\tau : x \longmapsto nx$, $x \in B$. Kako za $x,y \in A$ važi
$nx=ny \Rightarrow \phi(nx)=\phi(nx) \Rightarrow n\phi(x)=n\phi(y)$,
jer je ϕ homomorfizam, to je $\psi : nA \to nB$,
gde $\psi(nx)=n\phi(x)$, $x \in A$, dobro definisano. Dalje, ψ je 1-1 jer
$\psi(nx)=\psi(ny) \Rightarrow n\phi(x)=n\phi(y) \Rightarrow \phi(nx)-\phi(ny)=0 \Rightarrow \phi(nx-ny)=0 \Rightarrow nx=ny$,
jer je ϕ izomorfizam. Najzad,
$\psi(nx+ny)=\psi(n(x+y))=n\phi(x+y)=n(\phi(x)+\phi(y))=n\phi(x)+n\phi(y)$
tj. ψ je homomorfizam 1-1 i <u>na</u> ; dakle, ψ je izomorfizam. ▼

Neka su

$$A = Z_{p_1^{\alpha_1}} \dot{+} \ldots \dot{+} Z_{p_m^{\alpha_m}} \dot{+} Z^s \ , \quad A = Z_{q_1^{\beta_1}} \dot{+} \ldots \dot{+} Z_{q_n^{\beta_n}} \dot{+} Z^t$$

<u>dva</u> razlaganja konačno generisane Abel-ove grupe A, gde su $p_1 \leqslant \ldots \leqslant p_m$, $q_1 \leqslant \ldots \leqslant q_n$ prosti brojevi.

Neka je $u = p_1^{\alpha_1} \ldots p_m^{\alpha_m} q_1^{\beta_1} \ldots q_n^{\beta_n}$. Koristeći prethodnu lemu imamo

$$uA = uZ_{p_1^{\alpha_1}} \dot{+} \ldots \dot{+} uZ_{p_m^{\alpha_m}} + uZ^s = 0 \dot{+} \ldots \dot{+} 0 \dot{+} Z^s = Z^s \ ,$$

i slično, $uA \simeq Z^t$.

Dakle, $Z^s \simeq Z^t$, pa prema zad. 2.17., s=t.

Kako je u grupi A , $(Z_{p_1^{\alpha_1}} \dot{+} \ldots \dot{+} Z_{p_m^{\alpha_m}}) \cap Z^s = 0$, to

$A/Z^S \simeq Z_{p_1^{\alpha_1}} \dot{+} \ldots \dot{+} Z_{p_m^{\alpha_m}}$, i slično $A/Z^S \simeq Z_{q_1^{\beta_1}} \dot{+} \ldots \dot{+} Z_{q_n^{\beta_n}}$. Dakle,

$$Z_{p_1^{\alpha_1}} \dot{+} \ldots \dot{+} Z_{p_m^{\alpha_m}} \simeq Z_{q_1^{\beta_1}} \dot{+} \ldots \dot{+} Z_{q_n^{\beta_n}} \qquad (1)$$

Ako je $p_1 \neq q_1, \ldots, q_n$, tada za $u = q_1^{\beta_1} \ldots q_n^{\beta_n}$, iz poslednje jednakosti prema lemi 3.4. i

$$u(Z_{p_1^{\alpha_1}} \dot{+} \ldots \dot{+} Z_{p_m^{\alpha_m}}) \simeq Z_{p_1^{\alpha_1}} \dot{+} \ldots$$

$$u(Z_{q_1^{\beta_1}} \dot{+} \ldots \dot{+} Z_{q^{\beta}}) \simeq \boldsymbol{0} \dot{+} \ldots \dot{+} \boldsymbol{0}$$

nalazimo $Z_{p^{\alpha_1}} + \ldots \simeq \boldsymbol{0}$, što je očigledna kontradikcija.
Dakle, $p_1 \in \{q_1, \ldots, q_n\}$. Ponavljajući postupak za ostale p_i i sve q_j, sledi

$$\{p_1, \ldots, p_m\} = \{q_1, \ldots, q_n\} , \qquad (2)$$

Sada, neka je v proizvod onih članova iz skupa $\{p_1, \ldots, p_m\}$ koji se razlikuju od p_1. Tada, prema lemi 3.4. važi za neke λ_i, μ_j i $p = p_1$

$$v(Z_{p_1^{\alpha_1}} \dot{+} \ldots \dot{+} Z_{p_m^{\alpha_m}}) \simeq Z_{p^{\lambda_1}} \dot{+} \ldots \dot{+} Z_{p^{\lambda_k}}$$

$$v(Z_{p_1^{\beta_1}} \dot{+} \ldots \dot{+} Z_{p_m^{\beta_m}}) \simeq Z_{p^{\mu_1}} \dot{+} \ldots \dot{+} Z_{p^{\mu_r}}$$

pa prema (1) i (2) sledi

$$Z_{p^{\lambda_1}} \dot{+} \ldots \dot{+} Z_{p^{\lambda_k}} \simeq Z_{p^{\mu_1}} \dot{+} \ldots \dot{+} Z_{p^{\mu_r}} . \qquad (3)$$

Formula (3) može se napisati u obliku

$$L \simeq D \qquad (3')$$

gde $L = L_1 \dot{+} Z^a_{p^\lambda}$, $D = D_1 \dot{+} Z^b_{p^\mu}$ i za svaki član $Z_{p^{\lambda_i}}$ sume L_1 važi $\lambda_i < \lambda$, i slično za D. Otuda, ako je $\lambda < \mu$ onda $p^\lambda L \simeq \boldsymbol{0}$, $p^\lambda D \simeq p^\lambda D_1 \dot{+} Z^b_{p^{\mu-\lambda}} \neq \boldsymbol{0}$, što je u kontradikciji sa (3´). Dakle, $\lambda \geqslant \mu$ i slično $\mu \geqslant \lambda$, pa $\lambda = \mu$. Odavde i (3´) nalazimo prema lemi 3.4.

$$p^{\mu-1} L \simeq p^{\lambda-1} D \text{ , pa } p^{\lambda-1} L_1 \dot{+} p^{\lambda-1} Z^a_{p^\lambda} \simeq p^{\lambda-1} D_1 \dot{+} p^{\lambda-1} Z^b_{p_\lambda}$$

Kako je $p^{\lambda-1} L_1 \simeq \boldsymbol{0}$, $p^{\lambda-1} D_1 \simeq \boldsymbol{0}$, sledi $Z^a \simeq Z^b$, tj. a=b. Otuda sledi $L/Z^a_{p^\lambda} \simeq L_1$, $D/Z^a_{p^\lambda} \simeq D_1$, jer u D $Z^a_{p^\lambda} = Z^b_{p^\lambda}$ i $L_1 \simeq D_1$. Ponavljajući postupak sada sa L_1, D_1, nalazimo m=n i $\alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n$.

3.5. *Definicija: Neka je* $A = Z_{p_1^{\alpha_1}} \dot{+} \ldots \dot{+} Z_{p_n^{\alpha_n}} \dot{+} Z^m$ *razlaganje konačno generisane Abel-ove grupe A,* $p_1, \ldots, p_n$ *su prosti brojevi i* $p_1 \leqslant \ldots \leqslant p_n$, $0 < \alpha_1 \leqslant \ldots \leqslant \alpha_n$, $m > 0$. *Tada se n+1-orka* $(p_1^{\alpha_1}, \ldots, p_n^{\alpha_n}, m)$ *naziva* tipom *grupe A.*

Prema prethodnom izvodjenju imamo:

3.6. *Teorema: Dve konačno generisane Abel-ove grupe su izomorfne akko imaju iste tipove.*

Primeri i zadaci

3.1.Odrediti do na izomorfizam sve Abel-ove grupe reda: a) 100 , b) 1000 .

Rešenje: a) $C_2^2 \times C_5^2$, $C_4 \times C_5^2$, $C_2^2 \times C_{25}$, $C_4 \times C_{25}$.

3.2.Neka su p,q,r različiti prosti brojevi. Odrediti broj neizomorfnih Abel-ovih grupa reda p, p^2, p^3, pq, pq^2, pqr .

Rešenje: Ako je napr. $r(G)=p^3$ *, G je izomorfna jednoj od grupa* C_p^3 , C_{p^3} , $C_p \times C_{p^2}$.

3.3.Neka je F formula oblika u=v gde su u,v termi jezika Abel-ovih grupa. Dokazati da su sledeći uslovi ekvivalentni:

a) F važi u svim Abel-ovim grupama , b) F važi u $\underline{Z}$,

c) F važi u svim konačnim Abel-ovim grupama ,

d) F važi u svim cikličnim grupama ,

e) F važi u svim konačnim cikličnim grupama , f) F važi u (Q,+) ,

g) F važi u svim cikličnim grupama reda p^n, $n \in N$, p je prost broj .

Rešenje: (b $\Rightarrow$ *a) Neka F važi u* $\underline{Z}$*; tada za svaki* $n \in N$*, F važi u* Z^n *(v.zad. 1.4.5.). Otuda F važi i u svakoj homomorfnoj slici grupe* Z^n*, pa prema tome i u svakoj konačno generisanoj Abel-ovoj grupi . Stoga F važi u svim Abel-ovim grupama (v.zad. 1.4.21.).*

(c $\Rightarrow$ *b) Neka F važi u svim konačnim Abel-ovim grupama. Dalje, neka je* T_{Ab} *teorija Abel-ovih grupa (tj. skup aksioma za Abel-ove grupe) i neka je*

$$T = T_{Ab} \cup \{c \neq 0,\ 2c \neq 0,\ 3c \neq 0, \ldots\} \cup \{F\}.$$

Kako je svako konačan podskup teorije T neprotivurečan, tj. ima model, to prema stavu kompaktnosti i T ima model $\underline{G}$*. Neka je* $a \in G$ *interpretacija simbola konastante c. Podgrupa* $\langle a \rangle$ *je beskonačna ciklična i F važi u* $\langle a \rangle$ *budući da* $\langle a \rangle < G$*. Otuda F važi u* $\underline{Z}$*, jer* $\langle a \rangle \cong Z$.

(e $\Rightarrow$ *c) Koristiti stav dekompozicije za konačne Abel-ove grupe (v. teoremu 3.6.).*

3.4.Dokazati da za svaki term $t(x_1,\ldots,x_n)$ jezika Abel-ovih grupa postoje jedinstveni celi brojevi $m_1,\ldots,m_n$ tako da jednakost $t=m_1x_1+\ldots+m_nx_n$ važi u svim Abel-ovim grupama ($x_1,\ldots,x_n$ su različite promenljive).

Uputstvo: Dokaz se može izvesti, na primer, indukcijom po dužini terma t.

3.5.Neka je F kao u zadatku 3.3. Ako F važi u beskonačno mnogo grupa prostog reda, dokazati da F važi u svim Abel-ovim grupama.

Uputstvo: Videti rešenje zadatka 3.3., deo (c $\Rightarrow$ *b) .*

3.6.Neka je F kao u zadatku 3.3. Dokazati da postoji prirodan broj n_F tako da važi: ako F važi u svim Abel-ovim grupama čiji je red manji ili jednak n_F, tada F važi u svim Abel-ovim grupama.

Rešenje: Ako za neku formulu F ne postoji $n_F \in N$, tada bi F važila u svim konačnim Abel-ovim grupama, dok sa druge strane F ne bi važila u svim Abel-ovim grupama, što je u kontradikciji sa zad. 3.3.

3.7.Neka je G konačna Abel-ova grupa i $H \prec G$. Tada je G/H izomorfna podgrupi grupe G. Dokazati.

3.8.Neka je θ preslikavanje čiji je domen klasa konačnih grupa i koje zadovoljava uslov: $\sum_{H \prec G} \theta(H) = |G|$. (*)

Dokazati:

a) Postoji jedinstveno preslikavanje θ sa svojstvom (*) ,

b) Ako je C_n ciklična grupa reda n, tada $\theta(C_n) = \phi(n)$, gde je ϕ Euler-ova funkcija ,

c) Ako G nije Abel-ova grupa, tada $\theta(G) = 0$.

Rešenje: a) θ je induktivno definisano formulom

$$\theta(G) = |G| - \sum_{H \lneq G} \theta(H) .$$

b) Dokaz koji dajemo je indukcijom po broju elemenata ciklične grupe G. Pretpostavimo da tvrdjenje važi za sve ciklične grupe reda manjeg od n, i $n=|G|$. Kako je $\theta(G) = n - \sum_{H \neq G} \theta(H)$ i koristeći da za svaki k koji deli n postoji tačno jedna (i to ciklična) podgrupa od G, imamo, prema induktivnoj hipotezi, $\theta(G) = n - \sum_{k \mid n, k \neq n} \phi(k)$. Prema zad. 6.2.5 sledi $\theta(G) = \phi(k)$.

3.9.Dokazati ,da su medju Abel-ovim grupama proste samo ciklične reda 1 ili p (p je prost broj).

Rešenje: Prema teoremi 3.1. i zadatku 6.2.3'.a).

3.10.Dokazati da ima tačno prebrojivo mnogo tipova izomorfizama konačno generisanih Abel-ovih grupa, tj. svaki skup $\mathcal{F}$ neizomorfnih, konačno generisanih Abel-ovih grupa je prebrojiv.

Rešenje: Prema stavu o reprezentaciji konačno generisanih Abel-ovih grupa, za svaku grupu $A \in \mathcal{F}$ postoji konačan niz cikličnih grupa $A_1, \ldots, A_n$ tako da $A \approx \sum_i A_i$. S druge strane, cikličnih grupa ima tačno prebrojivo mnogo, dakle $\mathcal{F}$ ima najviše onoliko grupa koliko ima konačnih nizova cikličnih grupa. Ovih ima prebrojivo mnogo, pa $|\mathcal{F}| \leq \aleph_0$.

3.11. Dokazati da je Abel-ova grupa A konačno generisana akko svaka familija podgrupa od A ima maksimalan element u odnosu na inkluziju.

Rešenje: ($\Rightarrow$) *Neka je A konačno generisana Abel-ova grupa i pretpostavimo da postoji familija* $\mathcal{F}$ *podgrupa od A koja nema maksimalni element. Tada postoji prebrojiv niz podgrupa* $A_0 \lneq A_1 \lneq \ldots$ *grupe A. Neka su* $a_0 \in A_0$, $a_1 \in A_1 \setminus A_0$, $a_2 \in A_2 \setminus A_1, \ldots$ *i neka je* $B = \langle a_0, a_1, \ldots \rangle$. *Kako je B podgrupa konačno generisane grupe A, prema zad. 1.8. B je takodje konačno generisana; recimo, neka je* $B = \langle b_1, \ldots, b_n \rangle$. *Kako je za svaki* $i \leqslant n$, $b_i \in \langle a_0, a_1, \ldots \rangle$ *to za* b_i *postoji term t i konstante* $a_0, a_1, \ldots, a_k$ *tako da* $b_i = t(a_0, \ldots, a_k)$, *dakle* $b_i \in \langle a_0, \ldots, a_k \rangle$. *Otuda, postoji prirodan broj m takav da* $b_0, \ldots, b_n$ *pripadaju* $\langle a_0, \ldots, a_m \rangle$, *pa* $B \subseteq \langle a_0, \ldots, a_m \rangle \subseteq A_m$. *Ali,* $a_{m+1} \in B$, *pa* $a_{m+1} \in A_m$ što je u kontradikciji sa pretpostavkom $a_{m+1} \in A_{m+1} \setminus A_m$.

($\Leftarrow$) *Ako grupa A nije konačno generisana, tada postoji prebrojiv niz elemenata* $a_0, a_1, \ldots$ *iz A tako da* $B = \langle a_0, a_1, \ldots \rangle$ *takodje nije konačno generisana. Neka je* $\mathcal{F} = \{A_i \mid i \in \omega\}$, *gde* $A_0 = \langle a_0 \rangle$, $A_1 = \langle a_0, a_1 \rangle, \ldots$ *Kako je* $B = \bigcup_{i \in \omega} A_i$, *i B nije konačno generisana, to* $\mathcal{F}$ *nema maksimalni element.*

3.12. Neka je A konačna Abel-ova grupa. Dokazati da postoje ciklične grupe $B_1, B_2, \ldots, B_n$ tako da važi $A = B_1 \times B_2 \times \ldots \times B_n$ i za svaki $i < n$ $|B_i|$ deli $|B_{i+1}|$.

Rešenje: Prema teoremi 3.6. A je proizvod nekih grupa $A_1, A_2, \ldots, A_m$ *vida*

$$A_1 = C_{p_1^{\alpha_{11}}} \times C_{p_1^{\alpha_{21}}} \times \ldots \times C_{p_1^{\alpha_{k_1 1}}}$$

$$A_2 = C_{p_2^{\alpha_{12}}} \times C_{p_2^{\alpha_{22}}} \times \ldots \times C_{p_2^{\alpha_{k_2 2}}}$$

$$\vdots$$

$$A_m = C_{p_m^{\alpha_{1m}}} \times C_{p_m^{\alpha_{2m}}} \times \ldots \quad C_{p_m^{\alpha_{k_m m}}}$$

gde su C_n *ciklične grupe reda n,* $p_1, \ldots, p_m$ *prosti brojevi i* $0 < \alpha_{1i} \leqslant \alpha_{2i} \leqslant \ldots \leqslant \alpha_{k_i i}$. *Neka je* $n = \max_{i<m} k_i$. *S obzirom da je* C_1 *trivijalna grupa i* $G \times C_1 \cong G$, *to postoji matrica* $\|\beta_{ij}\|_{n \times m}$ *tako da*

$$A_1 = C_{p_1^{\beta_{11}}} \times C_{p_1^{\beta_{21}}} \times \ldots \times C_{p_1^{\beta_{n1}}}$$

$$A_2 = C_{p_2^{\beta_{12}}} \times C_{p_2^{\beta_{22}}} \times \ldots \times C_{p_2^{\beta_{n2}}}$$

$$\vdots$$

$$A_m = C_{p_m^{\beta_{1m}}} \times C_{p_m^{\beta_{2m}}} \times \ldots \times C_{p_m^{\beta_{nm}}}$$

gde $0 \leqslant \beta_{1i} \leqslant \beta_{2i} \leqslant \ldots \leqslant \beta_{ni}$ *za* $i = 1, \ldots, m$.
Neka je $B_1, B_2, \ldots, B_n$ *niz grupa definisan sa* $B_i = \prod_{j \leqslant m} C_{p_j^{\beta_{ij}}}$. *Prema zad. 6.2.3.a) grupe* B_i *su ciklične,* $A = \prod_{i \leqslant n} B_i$, *i* $(\forall i < n)|B_i| \mid |B_{i+1}|$.

3.13.Dokazati da postoji beskonačna Abel-ova grupa A koja sadrži niz podgrupa $\ldots < A_2 < A_1 < A_0$ tako da $(\forall i \in \omega) A_i \simeq A_{i+1}$ i $\bigcap_i A_i = \mathbf{0}$.

Rešenje: Neka je $A = \sum_{i \in \omega} B_i$ *, gde* $(\forall i \in \omega) B_i \simeq Z_p$ *i neka su* $A_0 = A$, $A_1 = \sum_{1 \leqslant i} B_i$, $A_2 = \sum_{2 \leqslant i} B_i$, ...

3.14.Neka je $A = \sum_{i \in \omega} A_i$, gde $(\forall i \in \omega) A_i \simeq Z_{p^2}$ i neka je $B = A \dot{+} Z_p$. Dokazati da grupe A i B nisu medjusobno izomorfne, ali je svaka izomorfna podgrupi one druge i takodje, svaka od njih je homomorfna slika druge.

Rešenje: 1° Očigledno, grupa A se utapa u grupu $A \dot{+} Z_p$ *, tj. A se utapa u B. S druge strane* $A = A_0 + \sum_{1 \leqslant i} A_i$ *i* $A_0 \simeq Z_{p^2}$ *. Dakle postoji* $a \in A_0$ *takav da* $r(a) = p$. *Tada*

$$\langle a \rangle \dot{+} \sum_{1 \leqslant i} A_i < A \quad i \quad B = Z_p \dot{+} A \simeq \langle a \rangle \dot{+} \sum_{1 \leqslant i} A_i$$

jer $\langle a \rangle \simeq Z_p$ *i* $\sum_{1 \leqslant i} A_i \simeq \sum_{i \in \omega} A_i$ *. Dakle, grupa B utapa se u grupu A.*

2° $B/Z_p = (A \dot{+} Z_p)/Z_p = A$ *, tj. A je homomorfna slika grupe B. Dalje, neka je* $a \in A$ *odredjen u 1° . Tada*

$$A/\langle a \rangle = (A_0 + \sum_{1 \leqslant i} A_i)/\langle a \rangle \simeq A_0' + \sum_{1 \leqslant i} A_i \quad , \text{ gde } A_0' \simeq Z_p .$$

Dakle, $B \simeq A_0' \dot{+} \sum_{1 \leqslant i} A_i$ *, pa je* $B \simeq A/\langle a \rangle$.

3° Dokazujemo da grupe A i B nisu izomorfne.

Pretpostavimo suprotno, tj. $A \simeq B$. *Tada grupa A ima razlaganje*

$$A = Z_p \dot{+} D_0 \dot{+} D_1 \dot{+} \ldots \quad , \text{ gde } (\forall i \in \omega) D_i \simeq Z_{p^2} .$$

Neka je $a \in Z_p$ *generator grupe* Z_p. *Tada postoji prirodan broj n takav da* $a \in A_0 \dot{+} \ldots \dot{+} A_n$. *Neka je* $H = \sum_{n<i} A_i$. *Tada*

$$A = A_0 \dot{+} A_1 \dot{+} \ldots \dot{+} A_n \dot{+} H \ . \quad \text{Otuda nalazimo}$$

$$A/H \simeq A_0 \dot{+} A_1 \dot{+} \ldots \dot{+} A_n \simeq Z_{p^2}^n \qquad i \qquad (1)$$

$$A/H = (Z_p \dot{+} D_0 \dot{+} D_1 \dot{+} \ldots)/H \simeq Z_p \dot{+} K \qquad (2)$$

jer ako $x, y \in Z_p$ *onda* $x, y \in A_0 \dot{+} \ldots \dot{+} A_n$ *, pa* $x - y \in A_0 \dot{+} \ldots \dot{+} A_n$. *Dakle, ako su* $x, y \in Z_p$ *i* $x - y \in H$ *onda* $x - y = 0$ *jer* $(A_0 \dot{+} \ldots \dot{+} A_n) \cap H = \emptyset$ *, pa za različite* $x, y \in Z_p$ *važi* $x + H \neq y + H$.

Prema (1) grupa A/H ima tip $(p^2, p^2, \ldots, p^2)$, *dok prema (2) grupa A/H ima tip* $(p, \ldots)$, *što je u kontradikciji sa teoremom 3.6.*

7.4. GRUPE SA DELJENJEM

Aditivna grupa racionalnih brojeva Q i Prüfer-ov grup $Z(p^\infty)$ imaju sledeće zanimljivo svojstvo:

Za svaki prirodan broj $n>0$, jednačina $nx=a$ ima rešenje po x za proizvoljni element a. (*)

4.1. *Definicija: Abel-ova grupa A je grupa sa deljenjem (ili potpuna grupa) ukoliko A ima svojstvo (*) $(a\in A)$.*

Glavni primeri grupa sa deljenjem su Q i $Z(p\infty)$, kao i aditivne grupe realnih i kompleksnih brojeva, tj. R i C.
Primetimo da je A grupa sa deljenjem akko homomorfizam $\phi : x \longmapsto nx$ $(x\in A, n\in N)$ jeste na, tj. ukoliko važi $nA=A$.

Navodimo stavove o razlaganju ovih grupa.

4.2. *Teorema: Neka je A Abel-ova grupa i $B<A$ grupa sa deljenjem. Tada je B direktni sabirak grupe A, tj. postoji podgrupa $C<A$ tako da je $A = B \dot{+} C$.*

Dokaz: Neka je $\mathcal{F}=\{H \mid H<A \wedge H\cap B=\boldsymbol{0}\}$. Neposredno se proverava da $\mathcal{F}$ ispunjava uslove Zorn-ove leme, tj. svaki lanac $\mathcal{L}$ (u odnosu na $\subseteq$) iz $\mathcal{F}$ ima gornje ograničenje u $\mathcal{F}$; to je upravo $\cup\mathcal{L}$, pa prema Zorn-ovoj lemi postoji maksimalni član $C\in\mathcal{F}$. Kako je $C\cap B=\boldsymbol{0}$, to $B+C=B\dot{+}C$.

Dokazujemo da je $A=B\dot{+}C$. Pretpostavimo suprotno, tj. $B\dot{+}C<A$. Grupa $A/(B\dot{+}C)$ je sa torzijom. Zaista, neka je $a\in A$ i $C(a)=\langle a,C\rangle$. Tada $C(a)=\{na+c \mid n\in Z, c\in C\}$. Ako je $na+c\in B$ za neke $n\neq 0$ i c, tada $na\in B\dot{+}C$, pa je razred $a+(B\dot{+}C)$ element konačnog reda u grupi $A/(B\dot{+}C)$: pretpostavimo da je $a+(B\dot{+}C)$ beskonačnog reda; tada iz uslova $na\in B\dot{+}C$ sledi $n=0$, dakle i $c\in B$. Kako je $B\cap C=\boldsymbol{0}$, to $c=0$. Otuda $B\cap C(a)=\boldsymbol{0}$ ali i $C<C(a)$, što je u kontradikciji sa izborom grupe C.
Dakle, $A/(B\dot{+}C)$ je grupa sa torzijom.

Kako smo pretpostavili da je $A\neq B\dot{+}C$, to postoji $a\in A\setminus(B\dot{+}C)$ i prema prethodnom, razred $a+(B\dot{+}C)$ je konačnog reda, recimo reda m. Tada $ma\in B\dot{+}C$ pa $ma=b+c$ za neke $b\in B$, $c\in C$. B je grupa sa deljenjem, pa za neki $b_1\in B$, $mb_1=b$. Neka je $a_1=a-b_1$ i $C_1=C(a_1)=\langle a_1,C\rangle$. Tada, koristeći da je $C_1=\{ia_1+c \mid 0\leqslant i<m, c\in C\}$, nalazimo $C_1\in\mathcal{F}$, jer $C_1\cap B=\boldsymbol{0}$, ali i $C<C_1$, što je u kontradikciji sa izborom grupe C. Dakle, $A=B\dot{+}C$. ▼

Sledeći stav kazuje da se sve grupe sa deljenjem na jednostavan način izgradjuju iz aditivne grupe racionalnih brojeva Q i Prüfer-ovih grupa $Z(p^\infty)$

4.3.*Teorema:* *Svaka Abel-ova grupa A sa deljenjem je direktna suma nekih p-Prüfer-ovih grupa i izomorfnih slika grupe racionalnih brojeva, tj.*

$$A = \sum_{i\in I} B_i + \sum_{j\in J} C_j\,, \quad (\forall i\in I)(\exists p)B_i \simeq Z(p^\infty)\,, \quad (\forall j\in J)C_j \simeq Q\,.$$

Dokaz: Neka je A Abel-ova grupa sa deljenjem i $T = T(A) = \{x\in A \mid r(x) < \infty\}$, tzv. *torzijska podgrupa* grupe A. T je takodje grupa sa deljenjem jer za $x\in T$ i $n\in Z$ postoji $a\in A$ tako da $nx=a$ i $r(a) < \infty$ jer $r(x) < \infty$. Prema teoremi 4.2. postoji $C < A$ tako da $A = T \dot{+} C$. Tada $(T \dot{+} C)/T \simeq C$ i C je grupa bez torzije, jer za svaki razred $x+T \neq T$ važi takodje $nx+T \neq T$ $(n\in N)$ s obzirom da $x\notin T$, tj. $r(x)=\infty$, pa i $r(nx)=\infty$.

Ako je $C \neq \mathbf{0}$, C je grupa sa deljenjem, jer je C homomorfna slika grupe sa deljenjem (videti zadatak 4.8.).
Kako je C grupa sa deljenjem, bez torzije, tada je C vektorski prostor nad poljem racionalnih brojeva, pa prema poznatom stavu iz linearne algebre (v. teoremu 1.5.):

$$(C,+) = \sum_{j\in J} \underline{C}_j\,, \quad \text{gde}(\forall j\in J)(C_j,+) \simeq (Q,+) \qquad (1)$$

Napomena: Primetimo da je $\dim(C)=|J|$, i s obzirom da je dimenzija vektorskog prostora jedinstveno odredjena za svako razlaganje vida (1), to i za neki drugi skup indeksa J´ važi $|J'|=\dim(\underline{C})=|J|$.

Pokažimo sada da je T suma Prüfer-ovih p-grupa. Neka je za svaki prost broj p $T_p=\{x\in T \mid r(x)$ je stepen broja $p\}$. Tada $T_p < T$ i $T=\sum_p T_p$. Kako je T grupa sa deljenjem, lako se pokazuje da je takva i grupa T_p.

Dakle, bez gubljenja opštosti, može se uzeti da je T p-grupa, tj. da svaki element u T ima za red stepen broja p.
Neka je X skup elemenata iz T reda manjeg ili jednakog p. Očigledno, $X < T$. Prema zad. 2.9. X ima maksimalni nezavisni podskup $Y\subseteq X$. Neka je za svaki $y\in Y$ odredjen niz na sledeći način (što je moguće jer je T sa deljenjam): $py_1=y$, $py_2=y_1$,... Tada očigledno $\langle y_1\rangle \ll \langle y_2\rangle < \ldots$ i svaka od grupa $\langle y_i\rangle$ je ciklična reda p^i, pa prema zad. 4.7. za grupu $B_y = \langle y_1, y_2, \ldots\rangle$ važi $B_y \simeq Z(p^\infty)$; stoga i grupa $B = \langle B_y \mid y\in Y\rangle$ je sa deljenjem (jer su takve grupe $Z(p^\infty)$). Prema teoremi 4.2. B je direktan sabirak grupe T, tj. $T = B \dot{+} D$ za neku podgrupu $D < T$.
Ako je $D \neq \mathbf{0}$, onda za neki $d\in D$, $r(d)=p$, $Y \cup \{d\}$ je takodje nezavisan skup takav da $Y \subsetneq Y \cup \{d\}$, što je u kontradikciji sa izborom skupa Y.
Dakle $D = \mathbf{0}$, pa $T = B$.

Najzad, ako su $y_1,\ldots,y_n \in Y$ različiti elementi i

$$a_i \in B_{y_i}\,, \; i=1,\ldots,n \quad \text{tako da} \quad a_1 + \ldots + a_n = 0 \qquad (2)$$

onda za $p^m = \max_i r(a_i)$ važi $p^{m-1}a_i = \alpha_i y_i$, $\alpha_i\in Z$, $i=1,\ldots,n$, pa

$$0=p^{m-1}(a_1+\ldots+a_n)=\alpha_1 y_1+\ldots+\alpha_n y_n \quad \text{i} \quad \alpha_{i_0} y_{i_0} \neq 0$$

gde je $r(a_{i_0})=p^m$, što je u kontradikciji sa pretpostavkom da je skup Y nezavisan.

Dakle, uslov (2) povlači $a_1=\ldots=a_n=0$, pa

$$B=\sum_{y\in Y} B_y \,, \quad (\forall y\in Y)(\exists p)\, B_y \simeq Z(p^\infty) \,.$$

Iz (1) i (3) sledi tvrdjenje teoreme. ▼

Primeri i zadaci

4.1. Neka je $\underline{G}=(G,+)$ prebrojiva Abel-ova grupa bez torzije i sa deljenjem. Dokazati da je $\underline{G}$ izomorfna jednoj od grupa Q^n, $\sum_{i\in N} Q_i$ gde $n\in N$, $Q_i \simeq Q$.

Rešenje: Grupa $\underline{G}=(G,+)$ je prebrojiv vektorski prostor nad poljem racionalnih brojeva Q, pa je ili dimenzije $n\in N$ i tada $\underline{G}\simeq(Q^n,+)$, ili $\dim(\underline{G})=\aleph_0$ i tada $G\simeq\sum_{i\in\omega} Q_i$.

4.2. Dokazati da su svake dve Abel-ove grupe bez torzije sa deljenjem, jednake i neprebrojive kardinalnosti, medjusobno izomorfne.

Rešenje: Neka su G,H Abel-ove grupe sa deljenjem, bez torzije i jednake neprebrojive kardinalnosti. Tada su G,H vektorski prostori nad poljem racionalnih brojeva, gde napr. za $a,b\in G$, $q\in Q$, $m\in Z$, $n\in N$ i $q=m/n$ važi

$$qa=b \iff b \text{ je (jedinstveno) rešenje jednačine } ma=nx \,.$$

Tada $\dim(G)=|G|=|H|=\dim(H)$, pa kako su G i H vektorski prostori nad istim poljem, to prema teoremi 1.5. $G\simeq H$.

4.3. Dokazati da je svaka Abel-ova grupa bez torzije, sa deljenjem i kardinalnosti $2^{\aleph_0}$ izomorfna aditivnoj grupi realnih brojeva.

Rešenje: Ako je $|G|=c$, tada su G i $(R,+)$ jednake neprebrojive kardinalnosti, pa prema prethodnom zadatku $G\simeq(R,+)$.

4.4. Neka je G Abel-ova grupa i $T(G)=\{x\in G \mid r(x)<\infty\}$. Dokazati da je $T(G)<G$ i da je G/T(G) grupa bez torzije.

Rešenje: Neka je $k:G\to G/T(G)$ prirodni homomorfizam. Pretpostavimo $y\in G/T(G)$. Za neki $x\in G$, $y=k(x)$. Ako je za neki $n\in N$, $ny=0$ tada $nk(x)=0$, tj. $k(nx)=0$. Otuda $nx\in T(G)$ pa je x konačnog reda, tj. $x\in T(G)$. Otuda $y=0$.

4.5. Neka je $G=Q/Z$. Dokazati: a) G je periodična grupa ,

b) G je grupa sa deljenjem , c) $G = \sum_{p \text{ je prost broj}} Z(p^\infty)$

Rešenje: Neka je $k : G \to Q/Z$ prirodni homomorfizam.

a) Neka je $y \in Q/Z$; tada za neki $m \in Z$, $n \in N$, $y=k(m/n)$. Otuda $ny=nk(m/n)=k(nm/n)=k(m)=0$, budući da $m \in Z$ i $\ker k = Z$.

b) Neka je $a \in Q/Z$ i $n \in N$. Vršimo prenos (transfer) jednačine $nx=a$ u Q. Neka je $c \in Q$ takav da $k(c)=a$. Jednačina $nx=c$ ima rešenje u Q, $x_0=c/n$. Tada je $k(x_0)$ rešenje jednačine $nx=a$ u Q/Z, budući da iz $nx_0=c$ sledi $nk(x_0)=a$.

c) Neka je p prost broj i $(Q/Z)_p = \{x \in Q/Z \mid r(x)$ je stepen broja $p\}$, tj. $x \in (Q/Z)_p$ akko $(\exists n \in N)\ p^n x=0$ (primetimo da je 0 u Q/Z upravo Z). Otuda

$$(Q/Z)_p = \{x \in Q/Z \mid (\exists n \in N) p^n x = Z\}.$$

Kako je $x \in Q/Z$ oblika $x=k(a)=Z+a$ za neki $a \in Q$, to

$$p^n x = 0 \Leftrightarrow p^n k(a) = 0 \Leftrightarrow k(p^n a) = 0 \Leftrightarrow p^n a \in Z ,$$

jer $Z = \ker k$ akko za neki $m \in Z$, $a=m/p^n$. Otuda $(Q/Z)_p = \{Z+m/p^n \mid n \in N, m \in Z\}$. Dalje, za $m \in Z$ postoje $\alpha, m' \in Z$ tako da $m=\alpha p^n+m'$, $0 \leqslant m' < p^n$, pa

$$Z+m/p^n = k(m/p^n) = k((\alpha p^n+m')/p^n) = k(\alpha+m/p^n) = Z+\alpha+m/p^n = Z+m/p^n .$$

Stoga, $(Q/Z)_p = \{Z+m/p^n \mid n \in N,\ 0 \leqslant m < p^n\} = Z(p^\infty)$.

Ako je $x \in Q$, $x=m/n$ i $n=p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ razlaganje prirodnog broja n na proste faktore, tada za neke $\beta_i \in Z$, $x = \beta_1/p_1^{\alpha_1}+\ldots+\beta_k/p_k^{\alpha_k}$ pa $k(x) = k(\beta_1/p_1^{\alpha_1}) + \ldots + k(\beta_k/p_k^{\alpha_k})$; stoga grupe $(Q/Z)_p$ generišu Q/Z.

Ako su $p_1, \ldots, p_k$ različiti prosti brojevi onda

$$(Q/Z)_{p_k} \cap ((Q/Z)_{p_1} + \ldots + (Q/Z)_{p_{k-1}}) = \langle 0 \rangle , \quad \text{pa imamo}$$

$$Q/Z = (Q/Z)_2 \dot{+} (Q/Z)_3 \dot{+} (Q/Z)_5 \dot{+} \ldots = \sum_{p \in P} (Q/Z)_p = \sum_{p \in P} Z(p^\infty) .$$

4.6. Dokazati da je $Z(p^\infty)$ grupa sa deljenjem.

Rešenje: Neka je $a \in Z(p^\infty)$ i n prirodan broj veći ili jednak 1. Za neke $u \in N$, $0 \leqslant v < p^k$, $a=u/p^v+Z$, a jednačina $nb=a$ po b, za $b=x/p^y+Z$ ekvivalentna je sa

$$(nx/p^y - u/p^v) \in Z . \qquad (1)$$

Neka su $r, m \in N$ takvi da $(m,n)=1$ i $n=p^r m$. Tada za $y=v+r$, (1) je ekvivalentno sa $mx-u=0 \pmod{p^v}$.

Preslikavanje $f : \{0,1,\ldots,p^v-1\} \to \{0,1,\ldots,p^v-1\}$ definisano sa $f(x)=$"ostatak deljenja $mx-u$ sa p^v" je 1-1. Zaista, ako je $f(x)=f(x')$, onda $p^v \mid m(x-x')$, pa kako je $(m,p^v)=1$ sledi $p^v \mid x-x'$. Dalje, $|x-x'|<p^v$, pa $x-x'=0$. Otuda, f je <u>na</u>, dakle za neki x_0, $f(x_0)=0$; stoga za $b=x_0/p^{v+r}$ važi $nb=a$.

4.7. Neka je p prost broj i A_n ciklična grupa reda p^n ($n \in \omega$) tako da $A_0 < A_1 < \ldots$. Dokazati da je grupa $A = \bigcup_{n \in \omega} A_n$ izomorfna grupi $Z(p^\infty)$.

Rešenje: Ako je $X=\{x\in C \mid (\exists n\in N)x^{p^n}=1\}$ *i* $\cdot$ *operacija množenja kompleksnih brojeva, tada* $A\simeq(X,\cdot)$. *Preciznije, ako je* $A_n=<a_n>$, $C_n\subseteq X$, $C_n=\{x\in C\mid x^{p^n}=1\}$ *i* $\varepsilon_n=\cos(2\pi/n)+i\sin(2\pi/n)$, *tada je* $f(a_n^k)=\varepsilon_n^k$ $(n\in N,\ 0\leq k\leq n-1)$ *izomorfizam grupa* A *i* $(X,\cdot)$. *Prema zad. 6.1.19. je* $Z(p^\infty)\simeq A$.

4.8. Neka je G Abel-ova grupa sa deljenjem. Dokazati:

a) Netrivijalna homomorfna slika grupe G je takodje grupa sa deljenjem,

b) Ako je $G=A\dot{+}B$ i A je netrivijalna grupa, tada je i A grupa sa deljenjem,

c) Da li je (Z,+) homomorfna slika aditivne grupe racionalnih brojeva?

Rešenje: a) Ako je $h: G\xrightarrow{na} H$ *homomorfizam, izvršiti prenos jednačine* $nx=a$ $(a\in H)$ *u* G *(v.zad. 4.5.).*

b) A *je homomorfna slika grupe* G *preko prirodnog homomorfizma* $k: G\to G/B$

4.9. Dokazati da je direktan proizvod Abel-ovih grupa sa deljenjem takodje grupa sa deljenjem.

Rešenje: Neka su G_i, $i\in I$, *Abel-ove grupe sa deljenjem i* $G=\prod_{i\in I} G_i$. *Dalje, neka je* $f\in G$ *i* x_i *rešenja jednačina* $nx=f(i)$, $i\in I$, *u* G_i. *Tada je* $g=<x_i \mid i\in I>$ *rešenje jednačine* $nx=f$ *u* G.

4.10. Neka je G periodična Abel-ova grupa, p prost broj i $G_p=\{x\in G \mid (\exists n\in\omega)r(x)=p^n\}$

Dokazati: a) $G_p<G$, b) $G=\sum_{p\in P} G_p$, P je skup prostih brojeva ,

c) Ako je G konačna grupa, tada $\mathrm{Aut}\, G=\prod_{p\in P}\mathrm{Aut}\, G_p$.

4.11. Dokazati da je Abel-ova grupa G sa deljenjem akko svaka netrivijalna homomorfna slika grupe G nije konačna.

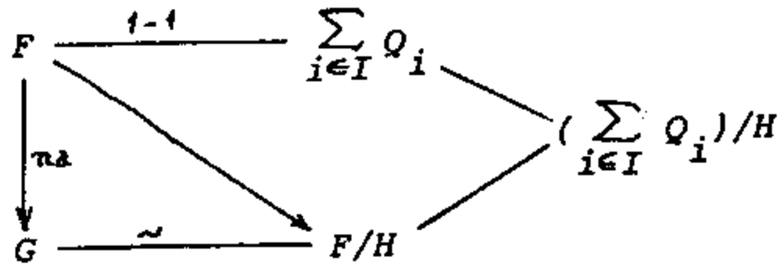
Rešenje: Ako je G *grupa sa deljenjem, onda je takva i svaka netrivijalna homomorfna slika grupe* G. *S druge strane, konačno generisane, dakle i konačne grupe nisu grupe sa deljenjem. Ukoliko pak,* G *nije grupa sa deljenjem, postoji* $n\in N$ *takav da* $nG\neq G$. *Otuda,* $H=G/nG$ *je netrivijalna Abel-ova grupa konačnog reda, pa prema stavu o dekompoziciji Abel-ovih grupa,* H *je direktna suma konačnih cikličnih grupa; otuda* G *ima netrivijalnu konačno generisanu homomorfnu sliku.*

4.12. Dokazati da za svaku Abel-ovu grupu G postoji Abel-ova grupa sa deljenjem A i utapanje $f: G\xrightarrow[1-1]{} A$.

Rešenje: I način. Dovoljno je dokazati, prema stavu kompaktnosti, da se svaka konačno generisana Abel-ova grupa utapa u Abel-ovu grupu sa deljenjem. Neka je G *konačno generisana Abel-ova grupa. Prema stavu o razlaganju konačno generisanih Abel-ovih grupa, može se uzeti da je* $G=Z^n\times\prod_{i=1}^{m} A_i$, *gde je*

Z aditivna grupa celih brojeva, A_i ciklična grupa čiji je red stepen prostog broja. Dalje, postoje utapanja $f : Z \to (Q,+)$, $g_i : A_i \to Z(p^\infty)$ gde $|A_i|=p^n$. Prema tome, G se utapa u $Q^n \times \prod_{i=1}^{m} B_i$, B_i su p-Prüfer-ove grupe; samo utapanje je odredjeno jednakošću $h(x_1,\ldots,x_n,y_1,\ldots,y_m)=(f(x_1),\ldots,f(x_n), g_1(y_1),\ldots,g_m(y_m))$.

II način. Abel-ova grupa G je homomorfna slika slobodne Abel-ove grupe F, $F = \sum_{i\in I} Z_i$, $Z_i \cong Z$, pa postoji $H < F$ tako da $G = F/H$. S druge strane, grupa F utapa se u $\sum_{i\in I} Q_i$, Q_i su izomorfne kopije aditivne grupe racionalnih brojeva, i ova grupa je grupa sa deljenjem. Može se pretpostaviti da je $F < \sum_{i\in I} Q_i$, pa i da je $H < \sum_{i\in I} Q_i$. Otuda, F/H se utapa u $(\sum_{i\in I} Q_i)/H$, a ova grupa je grupa sa deljenjem, budući da je homomorfna slika grupe sa deljenjem.



k je prirodni homomorfizam

4.13. Dokazati da je Abel-ova grupa A sa deljenjem akko A nema maksimalnih pravih podgrupa.

Rešenje: ($\Rightarrow$) Neka je A grupa sa deljenjem i $B \lhd A$. Tada je A/B netrivijalna grupa, pa je prema zad. 4.8. A/B takodje grupa sa deljenjem. Prema teoremi 4.3. A/B sadrži neku Prüfer-ovu p-grupu ili izomorfnu kopiju od Q. Kako svaka od ovih grupa sadrži pravu podgrupu, različitu od $\mathbf{0}$, to postoji $C \lhd A/B$ i $C \neq \mathbf{0}$. Ako je $k : A \to A/B$ prirodni homomorfizam, tada $B \lhd k^{-1}(C) \lhd A$. ($\Leftarrow$) Pretpostavimo da A nema maksimalnih podgrupa. Tada je svaka homomorfna slika grupe A koja je različita od $\mathbf{0}$, beskonačna. Jer, ako je $\phi : A \xrightarrow{na} B$ homomorfizam i B je konačna grupa, onda je B proizvod cikličnih grupa, recimo $B \cong Z_{n_1} \times \ldots \times Z_{n_k}$ $(k > 1)$ pa je Z_{n_1} homomorfna slika od B $(Z_{n_1} \cong B/(Z_{n_2} \times \ldots \times Z_{n_k}))$, pa i od A; to je u kontradikciji sa zadatkom 4.8. jer Z_{n_1} nije grupa sa deljenjem.

4.14. Ako je $B \lhd A$, A je Abel-ova grupa sa deljenjem, dokazati da je $|A/B| = \infty$.

4.15. Dokazati da (beskonačan) sistem jednačina S nad Abel-ovom grupom A sa deljenjem, ima rešenje akko svaki konačan podsistem od S ima rešenje u A.

Rešenje: Da postoji Abel-ova grupa B tako da $A < B$ i S ima rešenje u B, može se dokazati na razne načine. Najjednostavniji dokaz dobija se primenom stava kompaktnosti. Prema teoremi 4.2. postoji $C < B$ tako da $B = A \dot{+} C$. Tada $A = B/C$ i ako je $k : B \to A$ prirodni homomorfizam i $a_0, a_1, \ldots$ rešenje sistema

S u B, tada je $k(a_0), k(a_1), \ldots$ rešenje sistema S u A.

4.16. Dokazati da sistem

$$x_1 - px_2 = 1, \quad x_2 - p^2 x_3 = 1, \quad x_3 - p^3 x_4 = 1, \ldots$$

nema rešenja u $(Z,+)$, mada svaki njegov konačan podsistem ima rešenje.

4.17. Neka je p prost broj i neka Abel-ova grupa A sadrži podgrupu izomorfnu sa Z_{p^k} za svaki $k \in \omega$, i neka nijedna njena prava podgrupa nema to svojstvo. Dokazati da je $A \simeq Z(p^\infty)$.

Neka je za svaki $k \in \omega$, $A_k < A$, $A_k \simeq Z_{p^k}$ i neka je $B = \langle A_1, A_2, \ldots \rangle$. Tada $B < A$ i prema osobini grupe A sledi $B = A$ i A je p-grupa.

Dokazujemo da je A grupa sa deljenjem. Prema zad. 2.11. dovoljno je dokazati da je svaka netrivijalna slika grupe A beskonačna. Pretpostavimo suprotno, neka je $B < A$, A/B je konačna. Onda je i A/B p-grupa, pa prema teoremi o razlaganju konačnih grupa $A/B = Z_{p^{\alpha_1}} + \ldots + Z_{p^{\alpha_n}}$, pa kako je Z_p homomorfna slika od $Z_{p^{\alpha_1}}$ i $Z_{p^{\alpha_1}}$ homomorfna slika od $Z_{p^{\alpha_1}} + \ldots + Z_{p^{\alpha_n}}$, to možemo uzeti da je $A/B = Z_p$. Dakle, za neki $a \in A$, $B, a+B, \ldots, (p-1)a+B$ su svi razredi podgrupe B. Neka je $k \in N$ i $c \in A$ element reda p^{k+1} (takav postoji jer se $Z_{p^{k+1}}$ utapa u A). Tada $c = ia + b$, $0 < i < p$, $b \in B$, pa $pc = pia + pb$, odakle $pc \in B$ (jer $pa \in B$). Kako je $r(pc) = p^k$, to B sadrži izomorfnu kopiju od Z_{p^k} za svaki $k \in N$, što je, prema uslovu za grupu A, kontradikcija.

4.18. Ako je A Abel-ova grupa i sve prave podgrupe od A su konačne, dokazati da je $A \simeq Z(p^\infty)$ za neki prost broj p.

Rešenje: Prema teoremi 4.3. $A \simeq \sum_{i \in I} Z(p_i^\infty) + \sum_{j \in J} Q_j$, $Q_j \simeq Q$. Kako A nema beskonačnih podgrupa, to $J = \emptyset$ i $|I| = 1$.

4.19. a) Dokazati da je Q/Z izomorfna grupi svih n-tih korena iz jedinice u kompleksnoj ravni,

b) Dokazati da Abel-ova grupa A ne sadrži dve neizomorfne podgrupe akko je A izomorfna podgrupi od Q/Z.

Rešenje: b) $Q/Z = \sum_{p \in P} Z(p^\infty)$, P je skup prostih brojeva. Koristiti teoremu 4.3. o razlaganju grupa sa deljenjem.

4.20. Ako su A, A´ Abel-ove grupe sa deljenjem i A se utapa u A´ i A´ u A, dokazati da je $A \simeq A'$.

Rešenje: Prema teoremi 4.3. $A = \sum_{p \in P} \sum_{i \in I_p} A_{ip} + \sum_{j \in J} B_j$ gde je $P = \{p_0, p_1, \ldots\}$ skup prostih brojeva, $(\forall i \in I_p) A_{ip} \simeq Z(p^\infty)$ i $(\forall j \in J) B_j \simeq Q$. Neka je $\alpha_i = |I_{p_i}|$, $\beta = |J|$; tada se grupi A može pridružiti niz $(\beta, \alpha_0, \alpha_1, \ldots)$.

Dalje, za grupe A i A´ sa deljenjem važi $A \simeq A'$ *akko*

$$(\beta,\alpha_0,\alpha_1,\ldots) = (\beta',\alpha_0',\alpha_1',\ldots) .$$

Ako se A utapa u A´ onda $\beta \leqslant \beta'$, $\alpha_0 \leqslant \alpha_0'$, $\alpha_1 \leqslant \alpha_1'$,...

4.21. Ako je A Abel-ova grupa sa deljenjem i $A \dot{+} A \simeq B \dot{+} B$ onda $A \simeq B$. Dokazati.

Rešenje: Kako je A grupa sa deljenjem, takva je i grupa $A \dot{+} A$ *(videti zadatak 4.9.) pa i* $B \dot{+} B$. *Grupa B je homomorfna slika grupe* $B \dot{+} B$, *pa je prema zadatku 4.8. B takodje grupa sa deljenjem. Dalje, videti prethodni zadatak.*

8. DEJSTVO I KONAČNE GRUPE

Kao i u slučaju Abel-ovih grupa, jedan od glavnih problema u teoriji grupa uopšte predstavlja klasifikacija konačnih grupa. Pokazuje se da se sve konačne grupe mogu izgraditi od prostih, koristeći operaciju raširenja grupa. Neke od prostih grupa smo upoznali; to su grupe prostog reda i grupe A_n za $n\neq 4$ (videti teoremu 4.2.4.). U ovom poglavlju naročito važnu ulogu ima pojam *dejstva* grupe na skup. Zajedno sa teoremama Sylow-a i nekim konstrukcijama (recimo, semidirektan proizvod grupa), dejstvo ćemo koristiti da opišemo sve grupe čiji je red manji od 32.

S druge strane, postoje teoreme koje daju bližu sliku strukture konačnih grupa. U takvom smislu sigurno najvažnije mesto zauzimaju teoreme Sylow-a (dokazane 1872 god.) koje govore o egzistenciji p-podgrupa u svakoj konačnoj grupi. U čast tvorca ovih rezultata, norveškog matematičara L. Sylow-a, maksimalne p-podgrupe konačne grupe G nazivaju se Sylow-ljevim. U ovom odeljku pomenute teoreme često koristimo za opis konačnih grupa malog reda; navodimo naime potpun opis svih konačnih grupa čiji je red manji od 32.

8.1. DEJSTVO I SEMIDIREKTAN PROIZVOD

Neka je G grupa i S konačan skup.

1.1.Definicija: Homomorfizam $\theta : G \to Sym(S)$ *je dejstvo grupe G na skup S.*

Za dejstvo se takodje koristi termin *permutacijska reprezentacija* grupe G. Ukoliko je θ 1-1 preslikavanje, kaže se da je reprezentacija θ *verna*.

Ukoliko je u odredjenom kontekstu priroda dejstva θ jasna, koristi se označavanje $s^g = \theta(g)(s)$, $s \in S$, $g \in G$.

Sledećim definicijama i stavovima uvode se osnovni pojmovi pridruženi dejstvu i odredjuju njihova svojstva. Nadalje, G označava grupu a θ dejstvo grupe G na skup S.

1.2.Teorema: $(\forall g,h\in G)(\forall s\in S)\ (s^g)^h = s^{gh}$.

Dokaz: Označimo sa θ_g permutaciju $\theta(g)\in Sym(S)$, $g\in G$. Tada

$$(s^g)^h = \theta_h(\theta_g(s)) = (\theta_g\ \theta_h)(s) = \theta_{gh}(s) = s^{gh} \ . \ \blacktriangledown$$

1.3.Teorema: Neka je relacija $\sim$ skupa S definisana na sledeći način

$$x\sim y \iff (\exists g\in G)\ y = x^g \ .$$

Tada je $\sim$ relacija ekvivalencije skupa S.

Dokaz: Refleksivnost: $s^e = \theta_e(s) = I_S(s) = s$, dakle $s\sim s$ (e je jedinični element grupe G).

Simetričnost: neka je $s\sim t$. Za neki $g\in G$ je $t=s^g$, stoga

$$t^{g^{-1}} = (s^g)^{g^{-1}} = s^{gg^{-1}} = s^e = s, \text{ tj. } t\sim s.$$

Tranzitivnost: neka je $s\sim t$, $t\sim r$. Tada za neke $g,h\in G$, $t=s^g$ i $r=t^h$, odakle $r=(s^g)^h=s^{gh}$, tj. $s\sim r$. $\blacktriangledown$

1.4.Definicija: Ako je $\sim$ relacija ekvivalencije kao u prethodnoj teoremi, klasa ekvivalencije elementa $s\in S$ naziva se orbitom elementa s i označava se sa s^G.

Dakle, $s^G = \{s^g \mid g\in G\}$.

1.5.Definicija: Dejstvo θ je tranzitivno ukoliko ima tačno jednu orbitu.

1.6.Teorema: Neka je $G_s = \{g\in G \mid s^g = s\}$. Tada je G_s podgrupa grupe G i

$$|G : G_s| = |s^G| .$$

Dokaz: Zbog $s^e=s$ je $e\in G_s$.

Ako $g,h\in G_s$ tada $s^g=s$, $s^h=s$, pa $s^{gh}=(s^g)^h=s^h=s$.

Ako je $g\in G_s$, tada $s^g=s$ pa $s^{g^{-1}}=s$. Prema tome $G_s<G$.

Preslikavanje $F : s^G \to G/G_s$ definisano sa $F(s^g) = (G_s)g$ je 1-1 i na.

Primetimo da je F dobro definisano jer

$$s^g=s^h \iff s^{gh^{-1}}=s \iff gh^{-1}\in G_s \iff (G_s)g = (G_s)h \ . \ \blacktriangledown$$

Podgrupa G_s se naziva *stabilizatorom* elementa s.

1.7.Definicija: Grupa G je proširenje grupe H grupom K ukoliko $H\lhd G$, $G/H=K$.

1.8.Definicija: Grupa G je semidirektan proizvod grupa H i K ako je

$H \lhd G,\ K < G,\ H \cap K = \{1\},\ HK = G.$

Ukoliko je G semidirektan proizvod grupa H i K i ako je $H' \simeq H$, $K' \simeq K$, tada takodje kažemo da je G semidirektan proizvod grupa H' i K'.

1.9. Primer: Sledeća konstrukcija daje važan primer raširenja, odnosno semidirektnog proizvoda.

Neka su H,K grupe i $\sigma : K \to \mathrm{Aut}\, H$ homomorfizam (dakle σ je dejstvo grupe K na skup H). Dalje, neka je $\underline{G} = (G, \cdot)$ grupoid definisan na sledeći način:

$$G = \{(h,k) \mid h \in H,\ k \in K\}\ ,\quad (h,p)\cdot(g,q) \stackrel{def}{=} (h^{\sigma(q)}g,\ pq)\ ,$$

gde je $p,q \in K$; $h,g \in H$ i $h^{\sigma(p)} = \sigma(p)(h)$.

Tada je G semidirektan proizvod grupa H i K.

Zaista, neka je za $h \in H$, $p \in K$ sa h^p označen element $h^{\sigma(p)}$. Tada za h,g,k iz H, p,q,r iz K važi $(h^p)^q = h^{pq}$ (v. teoremu 1.2.). Kako je σ homomorfizam, to je takodje $(hg)^p = h^p g^p$, $h^1 = h$, $h^{p^{-1}} = g \Leftrightarrow g^p = h$. Otuda,

$$((h,p)(g,q))(k,r) = (h^q g, pq)(k,r) = ((h^q g)^r k, (pq)r) = ((h^q)^r g^r k, p(qr)) =$$
$$(h^{qr} g^r k, p(qr)) = (h,p)(g^r k, qr) = (h,p)((g,q)(k,r)),$$

što znači da je $\cdot$ asocijativna operacija. Jedinični element je $(1_H, 1_K)$. Inverzni element za (h,p) je $((h^{-1})^{p^{-1}}, p^{-1})$.

Neka je $\bar{H} = \{(h,1) \mid h \in H\}$, $\bar{K} = \{(1,k) \mid k \in K\}$. Tada važi $\bar{H} \simeq H$, $\bar{K} \simeq K$, $\bar{H} \cap \bar{K} = \{1_c\}$. Takodje $\bar{H} \lhd G$: za $x \in H$, $y \in G$, $x = (h,1)$, $y = (g,q)$ važi

$$y^{-1}xy = ((g^{-1})^{q^{-1}}, q^{-1})(h^q g, q) = (g^{-1}h^q g, 1)\ ,\ \text{tj. } y^{-1}xy \in H.$$

Kako je $\bar{H}\bar{K} = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH$ *i* $\bar{K}\bar{H} = \{(1,k)(h,1) \mid k \in K,\ h \in H\} = \{(h,k) \mid k \in K,\ h \in H\} = G$,

sledi $\bar{H}\bar{K} = G$, tj. G je semidirektan proizvod grupa H i K. ▼

Prethodno konstruisana grupa G naziva se raširenjem grupe H po K homomorfizmom σ, i koristi se oznaka $G = H \times_\sigma K$.

Primeri i zadaci

1.1. Neka je $\underline{G}$ grupa i $\theta : G \to \mathrm{Sym}(G)$ preslikavanje koje svakom $g \in G$ pridružuje unutrašnji automorfizam σ_g. Dokazati da je θ dejstvo grupe $\underline{G}$ na G. Odrediti jezgro, orbite i stabilizatore ovog dejstva.

Rešenje: Prema zadatku 3.2.25. θ je homomorfizam. Dalje,

$$g \in \ker\theta \Leftrightarrow \sigma_g = I_G \Leftrightarrow (\forall x \in G)\sigma_g(x) = x \Leftrightarrow (\forall x \in G)gx = xg \Leftrightarrow g \in Z(G)\ .$$

Otuda, $\ker\theta = Z(G)$. Za $s \in G$ je $s^G = \{s^g \mid g \in G\} = \{g^{-1}sg \mid g \in G\}$, tj. s^G je.

skup svih elemenata grupe G konjugovanih sa s. Dalje,

$$G_s = \{g \in G \mid s^g = s\} = \{g \in G \mid sg = gs\} = C(s) \ .$$

1.2. Neka je $H \prec G$ i $\theta : G \to Sym(G/H)$ preslikavanje definisano sa $\theta_g(s)=sg$, gde $g \in G$, $s \in G/H$. Dokazati da je θ dejstvo i odrediti jezgro, orbite i stabilizatore ovog dejstva.

Napomena: Ovo dejstvo naziva se *koset-reprezentacijom* grupe G (po podgrupi H).

Rešenje: $\theta_{gh}(s)=sgh=\theta_h(\theta_g(s))=(\theta_g\ \theta_h)(s)$, *tj.* $\theta_{gh}=\theta_g \circ \theta_h$, *što znači da je* θ *homomorfizam.*

$$g \in \ker\theta \Leftrightarrow \theta_g = I_{G/H} \Leftrightarrow (\forall x \in G)Hxg=Hx \Leftrightarrow (\forall x \in G)Hxgx^{-1}=H$$
$$\Leftrightarrow (\forall x \in G)g \in x^{-1}Hx \Leftrightarrow g \in \bigcap_{x \in G} \sigma_x(H)$$

(σ_x *je unutrašnji automorfizam odredjen elementom* x).

Prema tome, $\ker\theta = core(H)$.

Na primer, orbita za H je $\{\theta_g(H) \mid g \in G\} = \{Hg \mid g \in G\} = G/H$.

Otuda, postoji tačno jedna orbita, pa za svaki $s \in G/H$ $s^G = \{G/H\}$, *tj. u ovom slučaju G dejstvuje tranzitivno na G/H.*

Ako je $Hx \in G/H$ *tada stabilizator za Hx jeste* $\{g \in G \mid Hxg = Hx\}$, *tj.* $x^{-1}Hx$, *budući da je* $Hxg=Hx \Leftrightarrow g \in x^{-1}Hx$.

1.3. Koristeći prethodni zadatak dokazati Cayley-evu teoremu o reprezentaciji grupa grupama permutacija.

Rešenje: Neka je $H=\langle 1 \rangle$, *gde je 1 jedinica grupe G i* $\theta : G \to Sym(G/H)$ *dejstvo iz prethodnog zadatka. Tada* $Sym(G/H) \simeq Sym(G)$ *i* $\ker\theta = \langle 1 \rangle$, *tj.* θ *je utapanje.*

1.4. Neka je S skup svih podskupova skupa G i za $g \in G$ neka je θ_g preslikavanje odredjeno sa $\theta_g(X) = \{g^{-1}xg \mid x \in S\}$. Dokazati da je θ dejstvo grupe G na skup S i odrediti jezgro, orbite i stabilizatore ovog dejstva.

Rešenje: Za $s \in S$ *je* $\theta_{gh}(s)=(gh)^{-1}sgh=h^{-1}g^{-1}sgh=\theta_h(\theta_g(s))=(\theta_g\ \theta_h)(s)$, *tj.* $\theta_{gh}=\theta_g\ \theta_h$, *što znači da je* θ *dejstvo.*

Kako je $g \in \ker\theta$ *akko je* θ_g *identičko preslikavanje skupa* $S=\mathcal{P}(G)$, *to za jednočlane skupove* $\{x\} \in S$ *i* $g \in \ker\theta$ *važi* $g^{-1}\{x\}g = \{x\}$, *tj.* $xg=gx$.

Otuda, $\ker\theta = Z(G)$.

s^G *je familija skupova konjugovanih sa s.*

$G_s = \{g \in G \mid sg=gs\} = N(s)$, *(N(s) je normalizator skupa s).*

1.5. Neka je S skup svih funkcija $f : G \to G$. Za $g \in G$ preslikavanje θ_g je definisano sa $\theta_g(f)=h$ gde je $(\forall \alpha \in G)h(\alpha)=g^{-1}f(\alpha)g$. Dokazati da je θ dejstvo gru-

pe G na skup S i odrediti jezgro, orbite i stabilizatore ovog dejstva.

Rešenje: Za svaki α iz G je

$$\theta_{g_1g_2}(f)(\alpha)=(g_1g_2)^{-1}f(\alpha)g_1g_2=g_2^{-1}g_1^{-1}f(\alpha)g_1g_2=\theta_{g_2}(\theta_{g_1}(f))(\alpha)=((\theta_{g_1}\theta_{g_2})(f))(\alpha),$$

tj. $\theta_{g_1g_2}=\theta_{g_1}\theta_{g_2}$ *, što znači da je* θ *dejstvo.*

Kako je $g\in\ker\theta \Leftrightarrow \theta_g=I_S$ *, to za* $g\in\ker\theta$ *i konstantnu funkciju f,* $(\forall\alpha\in G)f(\alpha)=x \quad (x\in G)$*, važi* $\theta_g(f)(\alpha)=x$*, tj.* $g^{-1}xg=x$*, odnosno* $xg=gx$*.*

Otuda $\ker\theta=Z(G)$*.*

$G_f=C(s)$ *(centralizator skupa s), gde je* $s=\{f(\alpha)\mid\alpha\in G\}$*.*

1.6.Neka je $\{O_i\mid i\in I\}$ skup svih orbita dejstva σ i s_i, $i\in I$,elementi skupa S čije su orbite O_i. Dokazati:

$$|S|=\sum_{i\in I}|O_i|=\sum_{i\in I}|G:G_{s_i}|\ .$$

Napomena: Ova formula naziva se *klasovnom jednakošću* dejstva σ.

Rešenje: Orbite dejstva σ *čine jedno razbijanje, particiju skupa S pa tvrdjenje sledi prema teoremi 1.6.*

1.7.Neka je G grupa. Koristeći se odgovarajućim permutacijskim reprezentacijama dokazati:

a) Za svaki $X\subseteq G$ $N(X)<G$, N(X) je normalizator skupa X,

b) Za svaki $X\subseteq G$ $C(X)<G$, C(X) je centralizator skupa X,

c) $(\forall x\in G)(C(x)=N(x)\wedge C(x)\prec G)$, C(x) je centralizator elementa x,

d) Neka je $H\subseteq G$; broj konjugovanih skupova sa H jednak je $|G:N(H)|$,

e) Neka je $x\in G$; broj konjugovanih elemenata sa x jednak je $|G:C(x)|$,

f) (Klasovna jednakost) $|G|=|Z(G)|+\sum_{i\in I}|G:C(x_i)|$, gde $x_i\notin Z(G)$ i za $i\neq j$ x_i,x_j nisu uzajamno konjugovani.

Rešenje: Tvrdjenja slede prema već dokazanim svojstvima dejstava.

a) Videti zadatak 1.4. *b) Videti zadatak 1.5.*

d) Prema zad. 1.4. i teoremi 1.6., *e) Prema zad. 1.1. i teoremi 1.6.*

f) Neka je θ *dejstvo iz zadatka 1.1.; tada je* $G_s=C(s)$*. Primetimo da je* $C(s)=G$ *akko* $s\in Z(G)$*. Otuda, ako je* $\{x_j\mid j\in J\}$ *transverzala (izborni skup) za orbite dejstva* θ *, prema klasovnoj jednakosti iz prethodnog zadatka sledi*

$$|G|=\sum_{i\in J}|G:C(x_i)|=\sum_{x_j\in Z(G)}|G:C(x_j)|+\sum_{x_j\notin Z(G)}|G:C(x_j)|=$$

$$|Z(G)|+\sum_{i\in I}|G:C(x_i)|\ ,\quad \text{gde je } I=\{j\in J\mid x_j\notin Z(G)\}\ .$$

1.8.Dokazati da je grupa S_3 semidirektan proizvod grupa C_3 i C_2 .

Rešenje: Neka je $p=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $q=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, $A=\langle p\rangle$, $B=\langle q\rangle$. *Tada je A ciklična grupa reda 3, B ciklična grupa reda 2,* $A\lhd S_3$, $A\cap B=\langle 1\rangle$ *i* $AB=S_3$, *odakle sledi tvrdjenje.*

1.9. Dokazati da je grupa kvaterniona raširenje grupe reda 4 grupom reda 2, ali da nije semidirektan proizvod dveju grupa respektivno reda 4 i 2.

Rešenje: Grupa kvaterniona K data je tablicom u zad. 2.2.23.f). Neka je $H=\{1,-1,i,-i\}$; *tada* $K/H\simeq C_2$, *pa sledi prvi deo tvrdjenja.*
Neka su $A,B<K$ *respektivno reda 4,2, za koje važi* $A\lhd K$, $A\cap B=\langle 1\rangle$, $AB=K$. *Svaka podgrupa grupe K je normalna, odakle sledi da je K unutrašnji proizvod grupa A i B. Otuda, K je komutativna grupa kao proizvod dveju komutativnih grupa, što je kontradikcija.*

1.10. Dokazati da je S_n semidirektan proizvod grupa A_n i C_2.

Rešenje: Neka je $p\in S_n$, $p=(2\ 1)$ *i* $K=\langle p\rangle$. *Tada* $A_n\lhd S_n$, $A_n\cap K=\langle 1\rangle$, $A_nK=S_n$ *i K je ciklična grupa reda 2.*

1.11. Dokazati da je semidirektan proizvod grupa H i K poseban slučaj raširenja grupe H po K.

Rešenje: Neka je G semidirektan proizvod grupa H i K. Tada $H\lhd G$, $H\cap K=\langle 1\rangle$, $HK=G$. *Preslikavanje* $f:K\to G/H$, *gde je* $f(x)=Hx$ *odredjuje jedan izomorfizam grupa G/H i K.*
Zaista, f je homomorfizam jer $H\lhd G$; *f je 1-1 jer* $H\cap K=\langle 1\rangle$; *f je na jer* $HK=G$.

1.12. Dokazati da je dijedarska grupa reda 2n semidirektan proizvod grupa C_n i C_2 , uz odgovarajući homomorfizam σ.

Rešenje: Neka je $C_2=\{1,a\}$, $C_n=\{1,b,\ldots,b^{n-1}\}$ *i* $\theta: C_2\to Aut\,C_n$ *dejstvo odredjeno jednakošću* $\theta(a)(x)=x^{-1}$. *Dakle, koristeći oznake iz primera 1.9., imamo :* $(\forall x\in G)x^a=x^{-1}$.

Ukoliko se (1,a) identifikuje sa a i (b,1) sa b, tada u $C_n\times_\theta C_2$ *važi: a,b generišu grupu* $C_n\times_\theta C_2$ *i* $a^2=1$, $b^n=1$, $a^{-1}ba=b^{-1}$, *odakle sledi* $D\simeq C_n\times_\theta C_2$

Napomena: Primetimo da se u ovom slučaju x^a *u smislu definicije iz primera 1.9. i* $a^{-1}xa$ *poklapaju, tj.* $\theta(a)$ *i restrikcija unutrašnjeg automorfizma grupe* D_n *odredjenog elementom a poklapaju se.*

1.13. Navesti primere nekomutativnih grupa reda 36.

Rešenje: Jedan primer je dijedarska grupa D_{18} . *Dalje, kako je* $Aut\,S_3=S_3$,

to postoji izomorfizam $\theta : S_3 \to Aut\, S_3$. *Tada je* $S_3 \times_\theta S_3$ *takodje jedna nekomutativna grupa reda 36.*

1.14.Neka je G prosta grupa i $H \lessdot G$. Dokazati da je koset-reprezentacija grupe G po H verna.

Rešenje: Ako je θ *koset-reprezentacija, tada je* $\ker\theta \lhd G$. *Kako je* $\ker\theta \subseteq H$, *to* $\ker\theta \neq G$, *odakle sledi da je* $\ker\theta$ *trivijalna grupa, pa je* θ *1-1.*

1.15.Neka je $H \lessdot G$ i X transverzala particije $\{gH \mid g \in G\}$. Dokazati da je $XH = G$.

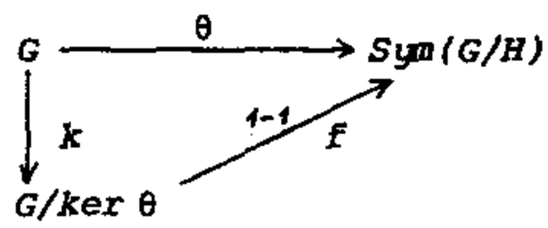
Rešenje: Neka je $g \in G$ *i* $x \in gH$. *Tada za neki* $h \in H$ $x=gh$, *odakle* $g=xh^{-1}$.
Primetimo da važi nešto jače tvrdjenje: $(\forall g \in G)(\exists_1 x \in X)(\exists_1 h \in H) g=xh$.

1.16.Ako su H,K podgrupe grupe G, dokazati: $H \subseteq N(K) \Rightarrow HK < G$.

Rešenje: Ako je $H \subseteq N(K)$ *tada* $(\forall h \in H) hK = Kh$. *Otuda* $HK = \bigcup_{h \in H} hK = \bigcup_{h \in H} Kh = KH$
Prema zadatku 2.3.10. je $HK < G$.

1.17.(n! teorema) Neka je $H < G$ i $|G : H| = n$. Dokazati da $|G : core(H)|$ deli n!.

Rešenje: Neka je $\theta : G \to Sym(G/H)$ *dejstvo iz zadatka 1.2. Prema teoremi 3.2.2. navedeni dijagram komutira, gde je k kanonski homomorfizam a f utapanje. Dalje, prema zad. 1.5.* $\ker\theta = Core(H)$ *pa je* $G/Core(H) \cong A$, *gde je* $A < Sym(G/H)$. *Kako* $|Sym(G/H)| = n!$, *prema Lagrange-ovoj teoremi* $|A|$ *deli n!* , *pa* $|G/Core(H)|$ *deli n!* .



1.18.Neka je $H < G$ konačnog indeksa. Dokazati da postoji $K \lhd G$, $K \leq H$ i K je konačnog indeksa.

Rešenje: Tvrdjenje sledi prema prethodnom zadatku.

1.19.Neka je G konačna grupa, $H < G$ i p najmanji prost broj koji deli $|G|$. Dokazati: ako je $|G : H| = p$ tada $H \lhd G$.

Rešenje: Neka je $|G : H| = p$. *Prema ni teoremi* $|G : Core(H)|$ *deli p!. S druge strane, prema Lagrange-ovoj teoremi* $|G : Core(H)|$ *deli* $|G|$. *Otuda, ako je q prost broj koji deli* $|G : Core(H)|$, *onda q deli* $|G|$ *i* $(p-1)!p$, *pa prema izboru broja p sledi* $q=p$. *Prema tome,* $|G : Core(H)| = p^n$ *za neki prirodan broj n*
Ako je $n=0$ *tada* $G = Core(H)$ *pa* $H = G$, *tj.* $H \lhd G$.
Ako je $|G : Core(H)| \geq p$, *slučaj* $n \geq 2$ *je nemoguć jer* p^2 *ne deli p!* .
Prema tome $|G : Core(H)| = p$, *pa* $|Core(H)| = |G|/|G : Core(H)| = |G|/p = |G|/|G:H|$ $= |H|$, *tj.* $|Core(H)| = |H|$. *Kako je H konačan skup i* $Core(H) \subseteq H$, *to* $H = Core(H)$ *odakle sledi* $H \lhd G$.

8.2. TEOREME SYLOW-A I KONAČNE GRUPE MALOG REDA

Kao što je u uvodu napomenuto, teoreme Sylow-a pokazuju da p-podgrupe neke konačne grupe čine izuzetno važan deo strukture te grupe.

2.1. *Definicija: Grupa H je p-grupa ako je njen red neki stepen prostog broja p.*

2.2. *Cauchy-eva lema: Ako je G konačna grupa i* $p \mid |G|$, *gde je p prost broj, tada u G postoji element a reda p.*

Dokaz: Neka je $S=\{(x_1,x_2,\ldots,x_p)\in G^p \mid x_1x_2\ldots x_p=e\}$, gde je e jedinica grupe G. Dokazujemo da je $|S|=|G|^{p-1}$. Za to je dovoljno primetiti da je preslikavanje $f(x_1,\ldots,x_{p-1})=(x_1,x_2,\ldots,x_{p-1},(x_1\ldots x_{p-1})^{-1})$, $f:G^{p-1}\xrightarrow[1-1]{na}S$. Element $f(x_1,\ldots,x_{p-1})$ pripada S budući da je $x_1x_2\ldots x_{p-1}(x_1\ldots x_{p-1})^{-1}=e$. Sada, s obzirom da p deli |G|, sledi da p deli |S|.

Neka je preslikavanje σ definisano jednakošću

$$\sigma(x_1,x_2,\ldots,x_p)=(x_p,x_1,x_2,\ldots,x_{p-1}).$$

Kako važi $xy=e \Rightarrow yx=e$, opštije $x_1x_2\ldots x_k=e \Rightarrow x_kx_1x_2\ldots x_{k-1}=e$, to je $\sigma: S\to S$. Očigledno je σ 1-1, pa $\sigma\in Sym(S)$. Dalje $\sigma^p=I_S$, tačnije $r(\sigma)=p$. Neka je C_p ciklična grupa reda p, $C_p=\langle a\rangle$ i $\theta: C_p\to\langle\sigma\rangle$, gde je $\langle\sigma\rangle$ (ciklična) podgrupa od Sym(S) generisana elementom σ, a θ *definisano sa* $\theta(a^i)=\sigma^i$. Preslikavanje $\theta: C_p\to Sym(S)$ je homomorfizam, pa C_p dejstvuje na S homomorfizmom θ. Neka su $o_1,o_2,\ldots,o_k$ orbite i $s_i\in S$ takvi da $o_i=s_i^G$. Stabilizator G_{s_i} je podgrupa grupe C_p, C_p je ciklična prostog reda, pa $G_{s_i}=\langle e\rangle$ ili $G_{s_i}=C_p$. Na osnovu jednakosti $|s^G|=|C_p:G_s|$ sledi

$$|s^G|=1 \quad \text{ili} \quad |s^G|=p \qquad (1)$$

Skup $\{o_1,\ldots,o_k\}$ čini jedno razbijanje skupa S, pa $|S|=\sum_{i=1}^{k}|o_i|$. Neka su (prema (1)) $|o_1|=1,\ldots,|o_j|=1$, $|o_{j+1}|=\ldots=|o_k|=p$. Tada, $|S|=j+p(k-j)$; kako p deli |S|, sledi da p deli j. Očigledno za $s=(e,e,\ldots,e)$, $s\in S$ i $s^G=\{s^g \mid g\in C_p\}=\{\theta^i(e,e,\ldots,e) \mid i<p\}=\{s\}$, pa je $j\geq 1$. Kako p deli j, dakle $j\geq 2$ to postoji element $u=(u_1,u_2,\ldots,u_p)$, $u\in S$, $u\neq(e,e,\ldots,e)$ takav da $u^G=\{u\}$. To znači $(\forall g\in C_p)u^g=u$, tj. $(\forall i<p)\sigma^i(u)=u$, odnosno ciklične permutacije k-torke $(u_1,u_2,\ldots,u_p)$ su jednake medjusobno. Otuda $u_1=u_2=\ldots=u_p$. Neka je $u_1=z$. Tada $u=(z,z,\ldots,z)$, $u\in S$, pa je $z^p=e$, $z\neq e$ (jer $u\neq(e,e,\ldots,e)$); dakle $r(z)=p$. ▼

Sada smo u mogućnosti da dokažemo i same teoreme Sylow-a.

Prva teorema Sylow-a predstavlja u neku ruku obrat Lagrange-ove teoreme o

podgrupama; naime kazuje za koje k (za koje naravno $k \mid |G|$) sigurno postoji podgrupa $H<G$ reda k. Podsetimo se da postoje takve konačne grupe G i prirodni brojevi k, pri čemu $k \mid |G|$, za koje ne postoji $H<G$ reda k (videti zadatak 4.2.16.).

2.3. *Prva teorema Sylow-a: Ako je G konačna grupa reda np^k, gde je p prost broj i n, p^k su uzajamno prosti, tada postoji $H<G$ reda p^k.*

Dokaz: Dokaz izvodimo indukcijom po redu grupe G. Neka je $|G|=np^k$, $k>1$ i pretpostavimo da tvrdjenje važi za sve grupe reda manjeg od $|G|$.

Postoje dve mogućnosti:

1° G ima pravu podgrupu K takvu da p ne deli $|G:K|$. Kako je $|G| = |K||G:K|$ to onda p^k deli $|K|$. Grupa K je nižeg reda nego grupa G pa, prema induktivnoj hipotezi, K sadrži grupu H i to reda p^k; stoga je H podgrupa reda p^k u grupi G.

Podgrupa H sa ovim svojstvom naziva se S_p-podgrupom (v. definiciju 2.4.).

2° Za sve $H \lhd G$ p deli $|G:H|$. Prema tome i za svaki ne-centralni $x \in G$ p deli $|G:C(x)|$. Prema klasovnoj jednakosti

$$|G| = |Z(G)| + \sum_x |G:C(x)| \quad \text{(jedan x za svaku ne-centralnu klasu)}$$

i pretpostavci $p \mid |G|$, sledi da p deli $|Z(G)|$. Prema Cauchy-evoj lemi postoji $a \in Z(G)$ reda p, pa je $N=\langle a \rangle$ ciklična grupa reda p. Kako je $N<Z(G)$, to $N \lhd G$. Neka je $\alpha : G \to G/N$ kanonski homomorfizam. Dalje, $|G/N| = |G|/|N| = np^{k-1}$, pa prema induktivnoj hipotezi G/N sadrži S_p podgrupu W reda p^{k-1}. Inverzna slika H grupe W preko homomorfizma α (tj. $H=\alpha^{-1}(W)$) je podgrupa grupe G i $N \subseteq H$. Kako je $N \lhd G$ to $N \lhd H$ i $H/N \simeq W$.
Otuda $|H/N| = p^{k-1}$, dakle $|H|/|N| = p^{k-1}$ tj. $|H| = p^k$. ▼

2.4. *Definicija: Podgrupa H grupe G je p-podgrupa Sylow-a (ili p-Sylow podgrupa), kraće S_p-podgrupa, ako je ona maksimalna p-podgrupa grupe G (p je prost broj).*

Sledeće dve teoreme Sylow-a govore o rasporedu p-podgrupa neke konačne grupe, kao i o broju S_p-podgrupa.

2.5. *(i) Druga teorema Sylow-a: Svaka p-podgrupa konačne grupe G sadržana je u nekoj S_p-podgrupi grupe G.*

(ii) Treća teorema Sylow-a: Svake dve S_p-podgrupe konačne grupe G međusobno su konjugovane. Ako je s_p broj S_p-podgrupa grupe G, tada $s_p = 1 (\mathrm{mod}\ p)$. Takodje, $s_p = |G:N(P)|$, gde je P bilo koja S_p-podgrupa grupe G, i $s_p \mid |G|$.

Dokaz: Neka je P neka S_p-podgrupa i Q p-podgrupa grupe G. Konjugacija σ_x je automorfizam grupe G i $\sigma_x(P) = P^x$, pa $P^x \leq G$. Preslikavanje σ_x je 1-1, pa $|P^x| = |P|$, odakle sledi da je i P^x S_p-podgrupa grupe G.
Neka je $S = \{P^x \mid x \in G\}$ i $\theta : G \to Sym(S)$ dejstvo konjugovanjem, tj. $(P^x)^g = P^{xg}$, $g \in G$ (v. zad. 1.1.). Primetimo da je orbita oblika $(P^x)^G = \{P^{xg} \mid g \in G\} = S$ i stabilizator $G_p x = \{g \mid P^{xg} = P^x\} = N(P^x)$.

Neka je $\theta_o = \theta|Q$ restrikcija preslikavanja θ na podgrupu Q. Tada je $\theta_o : Q \to Sym(S)$ takodje dejstvo. Prema teoremi 1.6. za orbite i stabilizatore u odnosu na Q važi:

$$|(P^x)^Q| = |Q : Q_{p^x}| = |Q|/|Q_{p^x}| = p^i/p^j = p^m \text{ , jer } Q_{p^x} < Q \text{ .}$$

Prema tome, za ma koju orbitu o (u odnosu na dejstvo θ_o) važi $p \mid |o|$ ili $|o|=1$. Primetimo da je za $o=(P^x)^Q$

$$|o|=1 \Leftrightarrow \{P^{xq} \mid q \in Q\} = \{P^x\} \Leftrightarrow (\forall q \in Q) P^{xq} = P^x \Leftrightarrow Q < N(P^x) \Leftrightarrow Q < P^x \text{ .}$$

Poslednja ekvivalencija dobijena je prema zadatku 2.6.
Kako orbite $o_1, o_2, \ldots, o_k$ čine jednu particiju skupa S i $|o_i|=1$ ili p deli $|o_i|$, prema prethodnom važi:

$$|S| = \sum_i |o_i| = \text{broj podgrupa konjugovanih sa P a koje sadrže Q} \pmod p \qquad (1)$$

Uzimajući da je Q=P prema (1) sledi

$$|S| = 1 \pmod p \qquad (2)$$

jer $P \subseteq P^x \Rightarrow P^x = P$. Iz (1) i (2) sledi za ma koju S_p-podgrupu P i p-podgrupu Q grupe G:

$$|\{P^x \mid Q \subseteq P^x\}| = 1 \pmod p \text{ .} \qquad (3)$$

(i) Neka je Q ma koja p-podgrupa grupe G. Prema (3) skup $\{P^x \mid Q \subseteq P^x\}$ je neprazan, dakle postoji S_p podgrupa P^x takva da $Q < P^x$.

(ii) Uzimajući da je Q bilo koja S_p-podgrupa, zaključujemo prema (3) da bar jedna podgrupa P^x sadrži Q, tj. $Q < P^x$. Medjutim, $|Q| = |P^x|$ (P^x je takodje S_p-grupa), pa je $Q = P^x$. Otuda $s_p = |S|$, dakle $s_p = 1 \pmod p$.
Dalje je $P^G = S$, odakle sledi $|P^G| = |G : G_p| = |G : N(P)|$, tj. $s_p = |S| = |G : N(P)|$; prema tome s_p deli $|G|$. ▼

Primeri i zadaci

2.1.Neka je $|G| = p^n$ (p je prost broj, $n \geq 1$). Dokazati da je centar Z(G) grupe G netrivijalan.

Rešenje: Prema klasovnoj jednačini (v.zad. 1.7.) važi

$$p^n = |Z(G)| + \sum_{i=1}^{k} |G : C(x_i)|,\ x_i \notin Z(G),\ za\ i \neq j\ x_i, x_j\ nisu\ konjugovani \qquad (1)$$

Kako $x_i \notin Z(G)$ to je $C(x_i)$ prava podgrupa grupe G, što znači da je broj $|G : C(x_i)| = p^n / |C(x_i)|$ deljiv sa p. Dakle i suma $\sum_{i=1}^{k} |G : C(x_i)|$ deljiva je sa p, pa prema (1) p deli $|Z(G)|$. Otuda sledi $|Z(G)| \geq p$.

2.2.Neka je G nekomutativna grupa reda 8. Dokazati da je $Z(G) \simeq C_2$ i $G/Z(G) \simeq C_2 \times C_2$.

Rešenje: Kako je $|G| = 8 = 2^3$ prema prethodnom zadatku G ima netrivijalan centar. Kako $|Z(G)| \mid 8$ to znači $|Z(G)| = 2$ ili $|Z(G)| = 4$. Ako je $|Z(G)| = 4$ tada $|G : Z(G)| = 2$ pa $G/Z(G) \simeq C_2$; prema zadatku 6.1.14. sledi da je G Abel-ova grupa, što je suprotno pretpostavci. Otuda $|Z(G)| = 2$ i G/Z(G) je grupa reda 4, pa je izomorfna jednoj od grupa $C_2 \times C_2$, C_4 .
Ako je $G/Z(G) \simeq C_4$ tada je prema zad. 6.1.14. G Abel-ova grupa, suprotno pretpostavci. Dakle, $G/Z(G) \simeq C_2 \times C_2$.

2.3.Opisati grupe reda p^2, p je prost broj.

Rešenje: Prema zadatku 2.1. G ima netrivijalan centar. Otuda, red grupe Z(G) je p ili p^2. Ako je $|Z(G)| = p^2$ tada $G = Z(G)$, dakle G je Abel-ova. Ako je $|Z(G)| = p$ tada G nije Abel-ova. Dalje, grupa G/Z(G) je prostog reda p, tj. G/Z(G) je ciklična grupa. Prema zad. 6.1.14. G je Abel-ova, što je kontradikcija.

Prema prethodnom, G je Abel-ova grupa, pa prema stavu o razlaganju konačnih Abel-ovih grupa, G je izomorfna jednoj od grupa C_{p^2} , $C_p \times C_p$.

2.4.Neka je G nekomutativna grupa reda p^3 (p je prost broj). Dokazati da je $Z(G) \simeq C_p$ i $G/Z(G) \simeq C_p \times C_p$.

Rešenje: Videti zadatke 2.2. i 2.3.

2.5.Dokazati: podgrupa p-grupe je p-grupa.

Rešenje: Tvrdjenje sledi na osnovu Lagrange-ove teoreme: red podgrupe deli red grupe.

2.6.Neka je P S_p-podgrupa konačne grupe G i Q p-podgrupa grupe G. Dokazati: $Q \trianglelefteq N(P) \Rightarrow Q \lhd P$.

Rešenje: Neka je $Q<N(P)$. Prema zad. 1.16. $PQ<G$. Dalje,

$$|PQ| = |P||Q|/|P\cap Q| = p^k \quad \text{za neki } k \geq 1 \qquad (1)$$

(v.zad. 2.3.11.b)). Dakle, $P<PQ$, P je maksimalna p-podgrupa grupe G i prema (1) PQ je p-grupa, pa $|P| = |PQ|$. Otuda $|Q| = |P\cap Q|$, pa prema $P\cap Q<Q$ sledi $Q = P\cap Q$, tj. $Q<P$.

2.7.Neka je G p-grupa reda p^n, $n\in N$. Dokazati da postoji $H\lhd G$ reda p^{n-1} .

Rešenje: Dokaz se izvodi indukcijom i sličan je dokazu Prve teoreme Sylow-a.
Za $n=1$ tvrdjenje neposredno sledi.
Pretpostavimo $n\geq 2$, $|G| = p^n$. Grupa G ima netrivijalan centar (v.zad. 2.1.), pa prema Cauchy-evoj lemi postoji $a\in Z(G)$, $r(a)=p$. Neka je $N = \langle a\rangle$. Kako je $N< Z(G)$ to $N\lhd G$, dakle postoji grupa G/N. Dalje, $|G/N| = |G|/|N| = p^{n-1}$ pa prema induktivnoj hipotezi postoji $W\lhd G/N$, $|W| = p^{n-2}$. Neka je $k : G \to G/N$ kanonski homomorfizam i $H = k^{-1}(W)$. Tada za $k_H = k|H$ važi $k_H : H \xrightarrow{na} W$ i $\ker k_H = N$, pa prema Teoremi o homomorfizmu $H/N \simeq W$, tj. $|H/N| = |W|$, odakle $|H| = |N||W| = p\cdot p^{n-2} = p^{n-1}$. Za $h\in H$ i $x\in G$ je $k(x^{-1}hx) = k(x)^{-1}k(h)k(x)$, pa kako je $W\lhd G$ sledi $x^{-1}hx\in H$, tj. $H\lhd G$.

2.8.Opisati grupe reda 6.

Rešenje: Postoje bar dve grupe reda 6: C_6 i S_3. One nisu izomorfne, jer recimo C_6 ima element reda 6, dok S_3 nema. Dokazujemo da je svaka grupa G reda 6 izomorfna jednoj od grupa C_6, S_3 .

Prema Cauchy-evoj lemi postoje $a,b\in G$ respektivno reda 3,2; neka je $P = \langle a\rangle$, $Q = \langle b\rangle$. P je indeksa 2, dakle $P\lhd G$. Dalje, ako je $x\in P\cap Q$ onda $r(x)$ deli brojeve 3 i 2, pa je $a=e$. Stoga $P\cap Q = \langle e\rangle$ i prema tome $|PQ| = |P||Q|/|P\cap Q| = 6$, odakle sledi $G = PQ$. Prema prethodnom važi

$$G = PQ, \quad P\cap Q = \langle e\rangle, \quad P\lhd G \qquad (1)$$

(tj. G je semidirektan proizvod grupa P,Q).

Razlikujemo sledeće slučajeve:

A. $Q\lhd G$. Prema (1) sledi $G \simeq P\times Q \simeq C_3\times C_2 \simeq C_6$.

B. $Q\not\lhd G$. Kako je $P\lhd G$ to element $a^b = b^{-1}ab$ pripada P, pa za neki $i\in\{0,1,2\}$ $a^b = a^i$. Ako je $i=0$ onda $a=e$, što je kontradikcija.
Ako je $a^b = a$, onda $ab=ba$, pa kako je G generisana elementima a i b, sledi da je G komutativna, što povlači $Q\lhd G$, suprotno pretpostavci.
Dakle, $a^b = a^2$, pa $G = \langle a,b\rangle$ gde a i b zadovoljavaju strukturne jednakosti: $a^3=e$, $b^2=e$, $ab=ba^2$. Otuda sledi $G\simeq S_3$. Jedan izomorfizam je $f : G \to S_3$: $f(a)=\sigma$, $f(b)=\tau$, gde $\sigma = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $\tau = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$.
Primetimo da važi $S_3 = \langle\sigma,\tau\rangle$, $\sigma^3=I$, $\tau^2=I$, $\sigma\tau=\tau\sigma^2$.

2.9.Opisati grupe reda 8.

Rešenje: Prema stavu o razlaganju konačnih Abel-ovih grupa, sve komutativne grupe reda 8 su: C_8, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$. *S druge strane postoje bar dve neizomorfne nekomutativne grupe reda 8: to su dijedarska grupa* D_4 *i grupa kvaterniona K. Dokazujemo da drugih nema.*

Neka je G nekomutativna grupa reda 8. Ukoliko je $(\forall g \in G) g^2 = e$, *tada je G komutativna. Ako postoji* $g \in G$ *reda 8 tada je G ciklična. Dakle, postoji* $a \in G$ *reda 4. Neka je* $N = \langle a \rangle$. *Kako je* $|G : N| = 2$, *sledi* $N \lhd G$. *Neka je* $b \in G \setminus N$. *Tada je element b reda 2 ili 4. Kako je* $N \lhd G$ *to* $NH < G$, *gde* $H = \langle b \rangle$. *Dalje,* $|NH| \geq 5$ *i* $|NH|$ *prema Lagrange-ovoj teoremi deli* $|G|$; *dakle* $|NH| = 8$, *tj.* $NH = G$. *Prema tome* $G = \langle a, b \rangle$. *Neka je* σ_b *unutrašnji automorfizam određen elementom b. Tada su a i* $\sigma_b(a)$ *jednakih redova, tj.* a^b *je reda 4. Kako je* $N \lhd G$ *to* $a^b = a^i$, $i \in \{1,2,3\}$.

Ako je $a^b = a$ *tada ab=ba, pa je G Abel-ova grupa.*

Kako je $r(a^2)=2$, *to* $a^b \neq a^2$.

Dakle $a^b = a^3$. *Razlikujemo sledeće slučajeve:*

A. $b^2 = e$. *Tada iz* $a^4 = e$, $b^2 = e$, $a^b = a^3$, $G = \langle a, b \rangle$ *sledi* $G \simeq D_4$.

B. $r(b)=4$. *Prema zad. 2.2.* $Z(G) \simeq C_2$, $G/Z(G) \simeq C_2 \times C_2$ *pa za svaki* $g \in G/Z(G)$ $g^2 = e$. *Otuda* $(\forall x \in G) x^2 \in Z(G)$ *pa* $a^2, b^2 \in Z(G)$. *Kako Z(G) ima dva elementa i* $a^2, b^2 \neq e$, *to* $a^2 = b^2$. *Prema prethodnom,* $G = \langle a, b \rangle$, $a^4 = b^4 = e$, $a^2 = b^2$, $a^b = a^3$, *pa je G izomorfna grupi kvaterniona K.*

2.10.Opisati grupe reda 10.

Rešenje: Postoje bar dve neizomorfne grupe reda 10; to su C_{10} *i* D_5.

Dokazujemo da drugih nema.

Neka je G grupa reda 10, a i b njeni elementi respektivno reda 5 i 2, i neka su P i Q podgrupe generisane redom elementima a i b. Kako $P \cap Q = \langle e \rangle$, *to* $G = PQ$, *tj.* $G = \langle a, b \rangle$. *Kako je* $|G : P| = 2$, *to* $P \lhd G$, *pa* $a^b = a^i$ *za neki i,* $i \in \{1,2,3,4\}$. *Iz* $b^2 = e$ *sledi* $a = a^{b^2} = a^{i^2}$, *odakle* $i^2 \equiv 1 \pmod 5$. *Otuda i=1 ili i=4. Ako je i=1 tada ab=ba i* $G \simeq C_5 \times C_2 \simeq C_{10}$.

Ako je i=4 tada $G \simeq D_5$; *strukturne jednakosti grupe G su* $a^5 = e$, $b^2 = e$, $a^b = a^4$.

2.11.Opisati grupe reda 15.

Rešenje: Neka je G grupa reda 15, $a, b \in G$ *elementi respektivno reda 5,3 i* $P = \langle a \rangle$, $Q = \langle b \rangle$. *Kako je* $|G : P| = 3$ *i 3 je najmanji prost broj koji deli 15, to prema zadatku 1.19. sledi* $P \lhd G$. *Kako je* $P \cap Q = \langle e \rangle$ *to takodje* $PQ = G$ *tj.* $G = \langle a, b \rangle$ *i G je semidirektan proizvod grupa P i Q. Kako je* $P \lhd G$, *to* $a^b \in P$, *odakle sledi* $a^b = a^i$ *za neki* $i \in \{1,2,3,4\}$.

Kako je $b^3=1$, to $a=a^{b^3}=a^{i^3}$. Otuda sledi $i^3=1 (mod\ 5)$.
Jedino rešenje ove jednačine u skupu $\{1,2,3,4\}$ je $i=1$, pa $ab=ba$. Kako a,b generišu G to sledi da je G komutativna grupa, i to $G=P\times Q\cong C_5\times C_3\cong C_{15}$.
Dakle, do na izomorfizam, postoji tačno jedna grupa reda 15; to je C_{15}.

2.12.Opisati grupe reda 12.

Rešenje: Dokazujemo da postoji tačno 5 grupa reda 12 (do na izomorfizam).
Prema stavu o dekompoziciji konačnih Abel-ovih grupa, C_{12} i $C_2\times C_2\times C_3$ su jedine Abel-ove grupe reda 12. Dalje, grupe D_6, A_4 su nekomutativne, medjusobno neizomorfne grupe reda 12. Najzad, neka je M grupa matrica (u odnosu na množenje matrica) generisana matricama

$$A=\begin{bmatrix}\varepsilon & 0\\ 0 & \varepsilon\end{bmatrix},\quad B=\begin{bmatrix}0 & i\\ i & 0\end{bmatrix}$$

ε je primitivni koren jednačine $x^3=1$, i je imaginarna jedinica.
Lako je proveriti da generatori grupe M zadovoljavaju sledeće strukturne jednakosti: $A^3=B^4=E$, $B^{-1}AB=A^{-1}$.

Grupa M je nekomutativna, reda 12, i nije izomorfna ni jednoj od grupa D_6, A_4.

Dokazujemo da je svaka grupa reda 12 izomorfna jednoj od navedenih grupa. Neka je P S_3-podgrupa i Q S_2-podgrupa grupe G. Kako je $P\cap Q=\langle e\rangle$, to $|PQ|=|P||Q|/|P\cap Q|=12$, dakle $G=PQ$.
Razlikujemo slučajeve:
A. $P\lhd G$. Ovde takodje razlikujemo dva podslučaja:
A.1. $Q\cong C_4$. Tada postoje $a,b\in G$, $r(a)=3$, $r(b)=4$, $P=\langle a\rangle$, $Q=\langle b\rangle$.
Neka je σ_b unutrašnji automorfizam generisan elementom b. Kako $r(\sigma_b)$ deli $r(b)$ (v.zad. 3.2.26.), to $r(\sigma_b)\in\{1,2,4\}$.
Ako je $r(\sigma_b)=1$ tada $a^b=a$ tj. G je Abel-ova grupa i $G\cong C_4\times C_3$.

Neka je $r(\sigma_b)=2$. Onda $\sigma_b^2=I_P$, tj. $a^{b^2}=a$. Kako je $P\lhd G$, to $a^b=a^i$ za neki $i\in\{1,2\}$, pa $a^{i^2}=a$, tj. $i^2=1 (mod\ 3)$. Otuda $i=1$ ili $i=2$.
Ako je $i=1$, onda $G\cong C_{12}$.
Ako je $i=2$ onda $a^b=a^{-1}$. U ovom slučaju generatori grupe G zadovoljavaju sledeće strukturne jednakosti: $a^3=b^4=1$, $a^b=a^{-1}$, pa je $G\cong M$.

Pretpostavimo da je $r(\sigma_b)=4$. Zbog $\sigma_b\in Aut\,P$ prema Lagrange-ovoj teoremi $r(\sigma_b)$ deli $|Aut\,P|$. Kako je $Aut\,P\cong Aut\,C_3$ i $|Aut\,C_3|=2$, to 4 deli 2; kontradikcija. Prema tome, ovaj slučaj nije moguć.
A.2. $Q\cong C_2\times C_2$. Tada postoje $b,c\in G$, $b^2=c^2=e$, $Q=\langle b,c\rangle$. Neka je $\sigma: Q\to Aut\,P$ dejstvo grupe Q na P, gde je $\sigma(x)=\sigma_x$ unutrašnji automorfizam odredjen elementom x. $Aut\,P$ ima dva elementa, pa postoje dve mogućnosti: $|Im(\sigma)|=1$ ili $|Im(\sigma)|=2$. Ako je $|Im(\sigma)|=1$ neposredno se dobija da je G komutativna, dakle $G\cong C_2\times C_2\times C_3$.

Pretpostavimo drugi slučaj i neka je $b \in \ker\sigma$ *(ako nije* $b \in \ker\sigma$ *onda je* $c \in \ker\sigma$ *ili* $bc \in \ker\sigma$ *i u takvom slučaju se izvodi slično razmatranje). Tada važi* $\sigma_b(a)=a$, *tj.* $a^b=a$. *Preslikavanje* σ *nije trivijalno, pa se može uzeti da je* $\sigma_c \neq I_P$ *(slično je ako se uzme* $\sigma_{bc} \neq I_P$*), tj.* $a^c \neq a$ *(jer a generiše P). Kako je* $P \lhd G$ *to za neki* $i \in \{1,2\}$ $a^c=a^i$, *odakle sledi* $i=2$. *Tada* $G = \langle a,b,c \rangle$, *i elementi a,b,c zadovoljavaju strukturne jednakosti:* $a^3=b^2=c^2=e$, $ab=ba$, $a^c=a^{-1}$, $bc=cb$, *pa* $G \simeq D_6$.

B. $P \not\lhd G$. *Neka je* s_3 *broj* S_3*-podgrupa grupe G. Tada* $s_3 \equiv 1 \pmod 3$, $s_3 > 1$ *(jer* $P \not\lhd G$*),* i $s_3 \mid |G|$, *tj.* $s_3 \mid 12$. *Otuda neposredno sledi* $s_3=4$.
Neka su P_1,P_2,P_3,P_4 S_3*-podgrupe grupe G i Q.* S_2*-podgrupa. Tada* $P_i \cap Q = \langle e \rangle$ *i za* $i \neq j$ $P_i \cap P_j = \langle e \rangle$, *pa* $|P_1 \cup P_2 \cup P_3 \cup P_4| = 9$, *odakle sledi da postoji tačno jedna* S_2*-podgrupa Q grupe G. Prema Drugoj i Trećoj teoremi Sylow-a, sledi* $Q \lhd G$, *pa je G semidirektan proizvod grupa P i Q.*
Razlikujemo sledeće podslučajeve:
B.1. $Q \simeq C_4$. *Neka je* $P = \langle c \rangle$, $Q = \langle a \rangle$. *Tada* $c^3=a^4=1$, *a kako je* $Q \lhd G$, *to* $a^c=a^i$ *za neki* $i \in \{1,2,3\}$. *Iz uslova* $c^3=e$ *sledi* $a=a^{c^3}=a^{i^3}$, *tj.* $i^3 \equiv 1 \pmod 4$, *odakle sledi* $i=1$. *Prema tome* $a^c=a$, *pa kako a,c generišu G, to je G komutativna, dakle i* $P \lhd G$, *suprotno pretpostavci. Prema tome, ovaj slučaj je nemoguć.*
B.2. $Q \simeq C_2 \times C_2$. *Neka su* $a,b,c \in G$ *takvi da* $Q = \langle a,b \rangle$, $P = \langle c \rangle$, $b^2=a^2=c^3=e$. *Kako G nije komutativna, dejstvo* $\sigma : P \to \mathrm{Aut}\, Q$ *konjugacije nije trivijalno pa se može uzeti* $a^c=b$. *Ako je* $b^c=a$ *onda* $a^{c^2}=(a^c)^c=b^c=a$. *Ali* $P=\langle c^2 \rangle$ *pa* $(ab)^{c^2}=a^{c^2}b^{c^2}=ab$, *odakle se neposredno izvodi da je* σ_{c^2} *trivijalan izomorfizam, tj.* $\sigma_{c^2}=I_Q$. *Medjutim,* $\sigma_c=\sigma_{c^4}=\sigma_{(c^2)^2}=\sigma_{c^2}^2=I_Q^{2^{c^2}}=I_Q$; *dakle* σ_c *je trivijalan izomorfizam suprotno pretpostavci. Slično se dokazuje da* $b^c \neq b$. *Dakle* $b^c=ab$. *Prema tome generatori grupe G zadovoljavaju sledeće strukturne jednakosti:* $a^2=b^2=c^3=e$, $b^c=ab$, $a^c=b$, *odakle sledi* $G \simeq A_4$.

2.13. Opisati grupe reda 2p, p je prost broj.

Rešenje: Neka je $|G| = 2p$, $a,b \in G$, $r(a)=p$, $r(b)=2$, $P = \langle a \rangle$, $Q = \langle b \rangle$. *Tada* $|G : P| = 2$, *dakle* $P \lhd G$. *Takodje* $P \cap Q = \langle e \rangle$ *(pretpostavljamo netrivijalan slučaj,* $p > 2$*); dakle* $G = PQ$, *tj. G je semidirektan proizvod grupa P i Q. Kako je* $P \lhd G$, *to za neki* $i \in \{1,2,\ldots,p-1\}$ $a^b=a^i$. *Kako je* $b^2=e$, *to* $a=a^{b^2}=a^{i^2}$, *dakle* $i^2 \equiv 1 \pmod p$. *Rešenja ove jednačine u skupu* $\{1,2,\ldots,p-1\}$ *su 1, p-1.*
Ako je $i=1$ *tada* $ab=ba$, *tj. G je komutativna grupa i tada* $G \simeq C_p \times C_2$.
Ako je $i=p-1$ *tada* $a^b=a^{-1}$ *i tada* $G \simeq D_p$.
Prema prethodnom, za $p > 2$ *postoje tačno dve grupe (do na izomorfizam): to su* C_{2p} *i* D_p . *Ako je* $p=2$, *jedine grupe su* C_4 *i* $C_2 \times C_2$.

2.14.Opisati grupe reda 4p, p je neparan prost broj.

Rešenje: Neka je $|G|=4p$, P S_p*-podgrupa i* Q S_2*-podgrupa grupe G. Kako je p neparan prost broj, to* $P\cap Q=<e>$, *odakle sledi* $G=PQ$.
Pretpostavimo, prvo, $P\not\lhd Q$. *Neka je* s_p *broj* S_p*-podgrupa u G. Prema teoremama Sylow-a, uz uslov* $P\not\lhd Q$, *sledi* $s_p>1$. *Kako je* $s_p\equiv 1 \pmod p$, *to* $s_p\geq p+1$. *S druge strane,* $s_p=|G:N(P)|\leq |G:P|=4$, *dakle* $p+1\leq 4$, *tj.* $p=3$, *a taj slučaj je raspravljen u zadatku 2.12. Zato pretpostavimo* $P\lhd G$.
Razlikujemo sledeće slučajeve:

<u>A.</u> $Q\simeq C_4$. *Neka je* $P=<a>$, $Q=<b>$, $a,b\in G$. *Tada* $b^4=e$, $a^p=e$.
Neka je σ_b *unutrašnji automorfizam odredjen elementom b. Tada* $r(\sigma_b)\in\{1,2,4\}$.
Ako je $r(\sigma_b)=1$ *tada* $\sigma_b=I_P$, *pa* $a^b=a$, *tj. G je Àbel-ova grupa i* $G\simeq C_4\times C_p$.
Neka je $r(\sigma_b)=2$. *Tada* $\sigma_b^2=I_P$, *tj.* $a^{b^2}=a$ *i za neki* $i\in\{1,2,\ldots,p-1\}$ $a^b=a^i$ *(jer* $P\lhd G$*). Otuda* $i^2\equiv 1 \pmod p$. *Rešenja ove jednačine su i=1, i=p-1.*
Slučaj i=1 nije moguć jer bi onda G bila komutativna grupa, a tada je $r(\sigma_b)=1$.
Dakle i=p-1. Tada je G odredjena strukturnim jednakostima $a^p=b^4=e$, $a^b=a^{p-1}$.
Egzistencija grupe G reda 4p sa ovim strukturnim jednakostima sledi iz narednog razmatranja: neka je $\sigma: C_4\to \mathrm{Aut}\, C_p$ *dejstvo odredjeno sa* $\sigma(a)(x)=x^{-1}$, *a je generator grupe* C_4; *tada je svaka grupa sa navedenim strukturnim jednakostima (reda 4p) izomorfna grupi* $C_p\times_\sigma C_4$.

Razmotrimo slučaj $r(\sigma_b)=4$. *Slično kao malopre dobija se* $a^b=a^i$ *gde* $i^4\equiv 1 \pmod p$. *Kako prema Lagrange-ovoj teoremi* $r(\sigma_b)\mid |\mathrm{Aut}\, C_p|$ *i* $|\mathrm{Aut}\, C_p|=p-1$, *to* $p\equiv 1 \pmod 4$. *Dakle, G je odredjena strukturnim jednakostima:* $a^p=b^4=e$, $ab=ba^i$, *gde* $i\neq 1$, $i^2\not\equiv 1 \pmod p$, $i^4\equiv 1 \pmod p$, *uz uslov* $p\equiv 1 \pmod 4$.

U vezi sa prethodnim dokazujemo sledeća tvrdjenja koja obezbedjuju egzistenciju i jedinost grupe sa navedenim strukturnim jednakostima:

<u>(T1)</u> *Ako je p prost broj, jednačina* $x^4\equiv 1 \pmod p$ *ima rešenje* $x\neq 1, p-1$ *u* $\{1,2,\ldots,p-1\}$ *akko* $p\equiv 1 \pmod 4$.

<u>(T2)</u> *Neka je p prost broj,* $p\equiv 1 \pmod 4$. *Tada postoji grupa* $G=<a,b>$ *reda 4p, gde* $a^p=e$, $b^4=e$, $a^b=a^i$, $i^4\equiv 1 \pmod p$, $i\not\equiv 1,-1 \pmod p$.

<u>(T3)</u> *Neka su* $i,j\in\{1,2,\ldots,p-1\}$, $i^4\equiv 1 \pmod p$, $j^4\equiv 1 \pmod p$, $i,j\not\equiv 1,-1 \pmod p$, $i\neq j$; *tada su grupe* G_1, G_2 *odredjene strukturnim jednakostima* G_1 : $a^p=b^4=e$, $a^b=a^i$, G_2 : $a^p=b^4=e$, $a^b=a^j$, *medjusobno izomorfne.*

<u>Dokaz za (T1)</u>: ($\Rightarrow$) *Neka je* $p\equiv 1 \pmod 4$ *i* $A=(Z_p\setminus\{0\},\cdot_p)$ *multiplikativna grupa polja* $\underline{Z}_p=(Z_p,+_p,\cdot_p)$. *Tada* $|A|=p-1$, *A je ciklična, pa kako 4 deli p-1, postoji podgrupa od A reda 4 (v.zad. 6.2.4.). Ova je takodje ciklična, pa za njen generator a važi* $a^4=1$ *i* $a\neq 1,-1$.
($\Leftarrow$) *Neka jednačina* $x^4-1=0$ *ima rešenja* $x\neq 1,-1$ *u* Z_p. *Skup rešenja S ove*

jednačine je podgrupa grupe A, $|S|=4$, pa prema Lagrange-ovoj teoremi $|S|$ deli $|A|$, dakle $4 \mid p-1$. ∇

Dokaz za (T2): Aut C_p je ciklična grupa reda p-1. Kako $4 \mid p-1$ to postoji podgrupa od Aut C_p reda 4 (v.zad. 6.2.4.); ova je ciklična, pa za njen generator τ važi $r(\tau)=4$. Dakle postoji dejstvo $\theta : C_4 \to \text{Aut } C_p$ odredjeno jednakošću $\theta(b)(x)=\tau(x)$, $x \in C_p$, b je generator grupe C_4. Tada $G \simeq C_p \times_\theta C_4$ zadovoljava navedene strukturne jednakosti, gde je a generator grupe C_p. ∇

Dokaz za (T3): Neka je G_1 odredjena strukturnim jednakostima $a^p=b^4=e$, $a^b=a^i$. Dokazujemo da se G_2 može dobiti "promenom notacije", tj. postoji $c \in G_1$ takav da $r(c)=4$, $a^c=a^j$. Neka je $c=ab^3$. Tada

$$c^2=ab^3ab^3=b^3a^{i^3}b^3a^{i^3}=b^6a^{i^6+i^3}=b^2a^{i^2+i^3}, \text{ otuda}$$

$$c^4=b^2a^{i^2+i^3}b^2a^{i^2+i^3}=b^4a^{(i^2+i^3)i^2}a^{i^2+i^3}=a^{1+i+i^2+i^3}=a^{(i^4-1)/(i-1)}=a^0=e .$$

Ako je $c^2=e$, tada $b^2 \in \langle a \rangle$, suprotno uslovu $\langle a \rangle \cap \langle b \rangle \simeq \langle e \rangle$, $b^2 \neq e$. Dakle, $r(c)=4$. Dalje, $a^c=a^{ab^3}=(a^a)^{b^3}=a^{b^3}=a^{i^3}=a^j$, jer $i^3=j \pmod p$ (primetimo da su i,j generatori iste ciklične grupe reda 4, upravo skupa rešenja jednačine $x^4=1$ u Z_p) . ∇

B. $Q \simeq C_2 \times C_2$. Neka je $Q=\langle b,c \rangle$, $b^2=c^2=e$, $P=\langle a \rangle$, $a^p=e$.
Dalje, neka je $\sigma : Q \to \text{Aut } P$ dejstvo konjugacijom, tj. za $x \in Q$ $\sigma(x)=\sigma_x$. Grupa Aut P je ciklična, zato ne sadrži Klein-ovu četvornu grupu, pa dejstvo σ nije verno. Otuda imamo sledeće mogućnosti: $|Im(\sigma)|=1$, $|Im(\sigma)|=2$.
Ako je $|Im(\sigma)|=1$, tada je G komutativna grupa, tj. $G \simeq C_2 \times C_2 \times C_p$.
Zato pretpostavimo $|Im(\sigma)|=2$. Dakle $\ker \sigma \neq e$, pa se može pretpostaviti $b \in \ker \sigma$. Dakle $\sigma_b(a)=ab=a$. Preslikavanje σ nije trivijalno, pa se može uzeti $\sigma_c \neq I_p$, tj. $a^c \neq a$. Otuda $a^c=a^i$ za neki $i \in \{1,2,\ldots,p-1\}$, $i \neq 1$, jer $P \lhd G$. Dalje, $\sigma_c^2=\sigma_{c^2}=\sigma_e=I_p$, odakle sledi $a^{c^2}=a$. Otuda $i^2=1 \pmod p$, pa kako σ nije trivijalno, sledi $i=p-1$. Tada je G odredjena strukturnim jednakostima: $a^p=b^2=c^2=e$, $ab=ba$, $a^c=a^{-1}$, $bc=cb$. Napomenimo da postoji grupa G reda 4p sa generatorima a,b,c koja zadovoljava navedene strukturne jednakosti:
$G \simeq C_p \times_\theta V$, gde je V Klein-ova četvorna grupa, $\theta : V \to \text{Aut } C_p$ je dejstvo, odgovarajuće prethodnom razmatranju.

Rezime: Ako je p prost broj i $p \neq 1 \pmod 4$, tada postoje (do na izomorfizam) 4 neizomorfne grupe reda 4p (od toga dve nekomutativne).
Ako je $p=1 \pmod 4$, tada postoji 5 grupa reda 4p (od toga su tri nekomutativne).

2.15. Opisati grupe reda pq, p i q su prosti brojevi.

Rešenje: Neka je G reda pq. Ukoliko je p=q tada $|G|=p^2$, pa prema zad. 2.3. $G \simeq C_{p^2}$ ili $G \simeq C_p \times C_p$. Zato pretpostavimo $p \neq q$, recimo $p < q$.

Neka je P S_p-podgrupa i Q S_q-podgrupa grupe G. Tada je $|P| = p$, $|Q| = q$, pa su P i Q ciklične grupe. Kako je $|G : Q| = p$ i p je najmanji prost broj koji deli red grupe G, prema zad. 1.19. je $Q \lhd G$. Otuda važi $PQ < G$. Lako se vidi da je $P \cap Q = \langle e \rangle$, odakle sledi

$$G = PQ, \quad P \cap Q = \langle e \rangle, \quad Q \lhd G \ . \tag{1}$$

Ako je $P \lhd G$, prema (1) sledi $G = P \times Q \simeq C_p \times C_q \simeq C_{pq}$. Primetimo da je C_{pq} jedina komutativna grupa reda pq. Zato pretpostavljamo, dalje, da je G nekomutativna, tj. $P \not\lhd G$. Kako je $Q \lhd G$ to $N(Q) = G$, odakle prema teoremama Sylow-a $s_q = |G : N(Q)| = 1$, tj. $s_q = 1$; dakle Q je jedina Sylow-ljeva q-podgrupa. S druge strane $P < N(P) \lneq G$, odakle sledi $P = N(P)$ i $|N(P)| = p$. Kako za broj S_p-podgrupa grupe G važi $s_p = |G : N(P)|$ sledi $s_p = q$. Prema teoremama Sylow-a važi $s_p = 1 (\mathrm{mod}\ p)$, tj. $q = 1 (\mathrm{mod}\ p)$. Prema prethodnom:

> Ako je $q \neq 1 (\mathrm{mod}\ p)$ i $p < q$ tada do na izomorfizam postoji tačno jedna grupa reda pq; to je C_{pq} . (2)

Pretpostavimo $q = 1 (\mathrm{mod}\ p)$. Primetimo da prema prethodnom $s_p = q$. Neka su $a, b \in G$ $P = \langle a \rangle$, $Q = \langle b \rangle$. Dakle $a^p = b^q = e$, preciznije $r(a) = p$, $r(b) = q$. Kako je $Q \lhd G$ to $b^a = b^k$ za neki $k \in \{1, 2, \ldots, q-1\}$. Zbog $a^p = e$ je $b^{k^p} = b$, tj. $k^p = 1 (\mathrm{mod}\ q)$, odnosno k je rešenje jednačine $x^p - 1 = 0$ u polju Z_q.
Ako je $k = 1$ tada je G komutativna grupa. Kako smo taj slučaj raspravili, pretpostavimo $k \neq 1$.
Dokazujemo, dalje, sledeća tvrdjenja:

(T1) Jednačina $x^p - 1 = 0$ ima rešenje $x \neq 1$ u Z_q akko $q = 1 (\mathrm{mod}\ p)$.

Dokaz: ($\Rightarrow$) Neka je $A = (Z_q \setminus \{0\}, \cdot_q)$ multiplikativna grupa polja Z_q i S skup rešenja jednačine $x^p - 1 = 0$. Lako se vidi da je $S < A$. Kako je A ciklična grupa, S je takodje ciklična; neka je w generator grupe S.
S obzirom da je $w^p = 1$ to $r(w)$ deli p, pa kako je $r(w) > 1$ to $r(w) = p$, dakle i $|S| = p$. Prema Lagrange-ovoj teoremi $|S|$ deli $|A|$, dakle $p \mid q-1$.
($\Leftarrow$) Kako $p \mid q-1$ i $|A| = q-1$, prema Cauchy-evoj lemi postoji $w \in A$, $r(w) = p$. Tada je w netrivijalno rešenje jednačine $x^p = 1$ u Z_q. ∇

(T2) Neka su p, q prosti brojevi, $p < q$, $p \mid q-1$. Tada postoji grupa $G = \langle a, b \rangle$ reda pq, gde je $a^p = b^q = e$, $b^a = b^k$, $k^p = 1 (\mathrm{mod}\ q)$, $k \neq 1 (\mathrm{mod}\ q)$.

Dokaz: Neka je $\theta : C_p \to \mathrm{Aut}\, C_q$ preslikavanje odredjeno sa $\theta(x)(y) = y^{k^i}$, $y \in C_q$, $x \in C_p$, $x = a^i$, $\cdot_q$ je množenje po modulu q, i $k^i = k \cdot_q k \cdot_q \ldots \cdot_q k$ (i puta). Tada je θ dejstvo grupe C_p na C_q, a semidirektan proizvod $G = C_q \times_\theta C_p$ zadovoljava postavljene uslove. ∇

(T3) Neka je G' grupa odredjena strukturnim jednakostima:
$c^p = d^q = e$, $d^c = d^j$, $j^p = 1 (\mathrm{mod}\ q)$, $p \mid q-1$, p, q su prosti brojevi. Ako je G grupa odredjena u (T2), tada je $G' \simeq G$.

Dokaz: Brojevi k,j su koreni jedinice u polju Z_q, $k,j\neq 1$. Kako koreni jedinice u polju obrazuju grupu, u ovom slučaju prostog reda p, to je k generator ove grupe. Dakle, za neki $i\in\{1,2,\ldots,p-1\}$ je $j=k^i$. Preslikavanje $f: G' \to G$ odredjeno sa $f(c^x d^y)=a^{xi}b^y$ jeste izomorfizam grupa G' i G. ▽

Rezime: Ako je $q\neq 1 (mod\ p)$ tada je svaka grupa reda pq izomorfna grupi C_{pq}. Ako je $q=1(mod\ p)$, tada postoje tačno dve neizomorfne grupe reda pq. Jedna je C_{pq} a druga semidirektan proizvod grupa C_p i C_q.

2.16. Opisati grupe reda p^3, p je neparan prost broj.

Rešenje: Ako je G komutativna grupa, prema stavu o dekompoziciji konačnih Abel-ovih grupa, G je izomorfna jednoj od sledećih grupa: $C_p \times C_p \times C_p$, $C_p \times C_{p^2}$, C_{p^3}.

Pretpostavljamo, dalje, da je G nekomutativna grupa. Tada prema zad. 2.4. sledi

$$G/Z(G) = C_p \times C_p \ , \quad Z(G) \simeq C_p \qquad (1)$$

Neka je $Z(G) = \langle z \rangle$. Dakle $z^p=e$. Red svakog elementa grupe G je stepen broja p, pa prema tome postoje sledeće mogućnosti:

A. $(\forall g\in G) g^p=e$. Neka je $a\in G\setminus Z(G)$; tada $a^p=e$ i $\langle a \rangle \cap Z(G) = \langle e \rangle$. Neka je $A = Z(G)\langle a \rangle$; kako je $Z(G) \lhd G$ to $A < G$. Dalje, $|A| = p^2$ pa je $|G : A| = p$. Kako je p najmanji prost broj koji deli p^3, prema zad. 1.19. je $A \lhd G$. Dalje,

$$A = \{a^i z^j \mid 0 \leq i,j < p\} \ . \qquad (2)$$

Neka je $b\in G\setminus A$. Kako je $A \lhd G$ to $a^b = z^i a^j$ za neke $i,j < p$. Neka je $k : G \to G/Z(G)$ kanonski homomorfizam; $G/Z(G)$ je komutativna grupa, pa imamo $k(a^b)=k(a)^{k(b)}=k(a)$, tj. $k(a^b)=k(a)$. S druge strane,

$$k(a^b)=k(z^i a^j)=k(z^i)k(a^j)=ek(a^j)=k(a^j) \ .$$

Otuda $k(a^j)=k(a)$ odakle sledi $a^j a^{-1} \in Z(G)$. Medjutim, $Z(G) \cap \langle a \rangle = \langle e \rangle$, pa je $a^j a^{-1}=e$, tj. $j=1$. Dakle $a^b = z^i a$. Ako je $i=0$, tada $ab=ba$ pa $a\in Z(G)$, suprotno izboru elementa a. Stoga $i\neq 0$, pa je $c=z^i$ takodje generator grupe $Z(G)$. Prema tome $a^b=ca$. Na osnovu prethodnog važi sledeće:

$$a^p=b^p=c^p=e, \quad ac=ca, \quad bc=cb, \quad a^b=ac, \quad G = \langle a,b,c \rangle \ . \qquad (3)$$

Grupa G reda p^3 sa navedenim strukturnim jednakostima postoji; G je semidirektan proizvod grupa $C_p \times C_p$ i C_p, $G = C_p^2 \times_\theta C_p$, gde je dejstvo $\theta : C_p \to Aut\, C_p \times C_p$ odredjeno sa $\theta_b(c)=c$, $\theta_b(a)=ac$; pri tom je $C_p = \langle b \rangle$, $C_p^2 = \langle a,c \rangle$, $\theta_x=\theta(x)$. Na primer $\theta_{b^2}(a)=\theta_b^2(a)=\theta_b(ac)=\theta_b(a)\theta_b(c) = ac^2$.

Ova grupa ima sledeću matričnu reprezentaciju:

$$G = \begin{bmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{bmatrix} \quad \alpha,\beta,\gamma \in \mathbb{Z}_p \ , \quad a = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \ , \quad b = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} , \quad c = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} .$$

B. Postoji $a \in G$, $r(a)=p^2$. Otuda $|G : \langle a \rangle| = p$, pa prema zad. 1.19. sledi $\langle a \rangle \lhd G$. Dalje, ako je $k : G \to G/Z(G)$ kanonski homomorfizam, važi $k(a^p)=k(a)^p=e$ $(=Z(G))$ jer prema (1) $G/Z(G) \simeq C_p \times C_p$. Otuda $a^p \in \ker k$, tj. $a^p \in Z(G)$. Kako je $r(a)=p^2$ to $Z(G)=\langle a^p \rangle$.

U daljem izvodjenju koristićemo sledeće tvrdjenje:

(T1) Postoji $y \in G \setminus \langle a \rangle$, $r(y)=p$.

Dokaz: Pretpostavimo suprotno. To znači da se svi elementi reda p nalaze u $Z(G)$, dakle postoji tačno $p-1$ element grupe G koji su reda p.

Prema klasovnoj jednakosti $p^3 = P + \sum_i |G : C(x_i)|$, $x_i \notin Z(G)$. Otuda $r(x_i)=p^2$ i $|G : C(x_i)| = p$, pa $p^3=p+pj$, gde je j manji ili jednak broju elemenata reda p^2. Stoga je $j=p^2-1$, tj. postoji p^2-1 element $a_1,\ldots,a_{p^2-1}$ reda p^2. Za $i \neq j$ je $\langle a_i \rangle \cap \langle a_j \rangle = Z(G)$; odavde je na osnovu klasovne jednačine

$$p^3 = |Z(G)| + \sum_{i=1}^{p^2-1} (|\langle a_i \rangle \setminus Z(G)|) = p + (p^2-1)(p^2-p) .$$

Iz poslednje jednakosti sledi $p=2$, suprotno pretpostavci da je p neparan prost broj. ∇

Neka je $y \in G \setminus \langle a \rangle$, $r(y)=p$. Kako je $\langle a \rangle \lhd G$ sledi $a^y=a^i$ za neki $i < p^2$. Dalje, za kanonski homomorfizam $k : G \to G/Z(G)$ važi $k(a^y)=k(a)^{k(y)}=k(a)$ jer je $G/Z(G)$ komutativna grupa. Otuda $k(a^i)=k(a)$, tj. $a^i a^{-1} \in Z(G)$, odnosno postoji $j < p$ takav da $a^i a^{-1}=a^{jp}$. Prema tome $a^y=a^{jp+1}$.

Koristeći $a^{p^2}=e$ imamo

$$a^{y^2}=(a^y)^y=(a^{jp+1})^y=(a^y)^{jp+1}=a^{(jp+1)(jp+1)}=a^{2jp+1} .$$

Slično, $a^{y^r}=a^{rjp+1}$. Z_p je polje, dakle postoji $m < p$ takav da $mj=1 \pmod p$; tada $mjp=p \pmod{p^2}$, stoga $a^{y^m}=a^{mjp+1}=a^{mjp}a=a^p a=a^{p+1}$.

Kako je $m \neq 0$ to je y^m takodje generator grupe $\langle y \rangle$; neka je $b=y^m$. Tada $a^b=a^{p+1}$. Prema tome, grupa G je u ovom slučaju odredjena strukturnim jednakostima: $a^{p^2}=b^p=e$, $a^b=a^{p+1}$.

Takva grupa G reda p^3 postoji. Recimo, G je semidirektni proizvod grupa C_{p^2} i C_p, tj. $G = C_{p^2} \times_\theta C_p$, gde je $\theta : C_p \to \mathrm{Aut}\, C_{p^2}$ a dejstvo θ je odredjeno sa $\theta_b(a)=a^{p+1}$, $\theta_b = \theta(b)$.

Prema prethodnom zaključujemo da postoji 5 grupa reda p^3. Od toga 3 su komutativne a 2 nisu.

2.17. Ako je $|G| = 2k$ i $k \in 2N+1$, dokazati da postoji $H \lhd G$, $|H| = k$.

Rešenje: Prema Cayley-evoj teoremi preslikavanje $\phi : G \to S_n$, $n=2k$, odredjeno sa $\phi(a)=p_a$, gde $p_a(x)=ax$, je utapanje.

Neka je $G' = \phi(G)$. Tada je $|G' : G' \cap A_n| \leq 2$.

Zaista, prema Prvoj teoremi o izomorfizmu je $A_n G'/A_n \simeq G'/(A_n \cap G')$.

Ako je $G' \subseteq A_n$ tada $A_n G' = A_n$, dakle $|G' : A_n \cap G'| = 1$. Ako $G' \not\subseteq A_n$ tada $A_n G' = S_n$ (jer $|G' : A_n| = 2$), pa $G'/(A_n \cap G') \simeq S_n/A_n$, odakle sledi $|G' : A_n \cap G'| = 2$.

Dakle, $G' \cap A_n \lhd G'$. Dokazujemo sada da je $|G' : G' \cap A_n| = 2$.

Prema Cauchy-evoj lemi postoji $p_a \in G'$, $r(p_a)=2$. Tada je

$p_a = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ ab_1 & ab_2 & \dots & ab_n \end{pmatrix}$, pa kako je $r(p_a)=2$, $a \neq e$. Otuda za svaki $i < n$, $ab_i \neq b_i$, dakle p_a je proizvod $k=n/2$ transpozicija. Broj k je neparan, dakle p_a je neparna permutacija; prema tome $p_a \in G' \setminus A_n$, tj. $G' \not\subseteq A_n$. Prema prethodnom sledi da je $G' \cap A_n$ normalna podgrupa od G' indeksa 2.

Dakle, i $\phi^{-1}(G' \cap A_n)$ je normalna podgrupa od G indeksa 2.

2.18. Opisati grupe reda 18.

Rešenje: Neka je $|G|=18$. Prema stavu o reprezentaciji konačnih Abel-ovih grupa, postoje sledeće komutativne grupe: $C_2 \times C_3 \times C_3$ i C_{18} .

Dalje, neka G nije komutativna. Neka je P S_3-podgrupa i Q S_2-podgrupa grupe G. Tada $|P|=9$, $|Q|=2$. Neka je $a \in G$ takav da $Q = \langle a \rangle$, $r(a)=2$.

Razlikujemo sledeće slučajeve (v.zad. 2.3.):

A. $P \simeq C_9$. Neka je $b \in G$, $P = \langle b \rangle$. Kako je $P \lhd G$ (jer $|G : P|=2$), to $b^a = b^i$ za neki $i \leq 8$. Kako je $a^2 = e$ sledi $b^{i^2} = b$, tj. $i^2 \equiv 1 \pmod 9$. Otuda $i=1$ ili $i=8$. Kako po pretpostavci G nije komutativna, sledi $i \neq 1$, tj. $i=8$.

Dakle, $a^2 = b^9 = e$, $b^a = b^{-1}$, tj. $G \simeq D_9$.

B. $P \simeq C_3 \times C_3$. Tada postoje $b, c \in G$, $P = \langle b, c \rangle$, $r(b)=r(c)=3$. Kako je $P \lhd G$ to $b^a = b^i c^j$, $c^a = b^p c^q$ za neke $i,j,p,q < 3$. Iz ovih uslova mogu se odrediti i,j,p,q.

Navodimo medjutim sledeće rešenje, koristeći elemente linearne algebre.

Element a dejstvuje na P konjugacijom, tj. postoji dejstvo $\sigma : C_2 \to \mathrm{Aut}\, C_3^2$. Kako je a element drugog reda, to odredjujemo sve elemente drugog reda u $\mathrm{Aut}\, C_3^2$. Može se uzeti da je C_3^2 vektorski prostor nad poljem Z_3 (dimenzije 2); prema tome treba odrediti sve linearne operatore $L : C_3^2 \to C_3^2$, $L^2 = I$, odnosno, u matričnoj reprezentaciji, sve matrice A nad Z_3, $A^2 = E$, $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Kako A poništava polinom $x^2 - 1$, to su sopstvene vrednosti operatora L, $x_1 = 1$, $x_2 = -1$. Prema tome, u bazi sopstvenih vektora, L ima jednu od matrica

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} , \quad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} , \quad C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} .$$

Otuda postoje dve nekomutativne grupe G za koje $P \simeq C_3 \times C_3$; to su

G_1 : $a^2 = b^3 = c^3 = e$, $b^a = b$, $c^a = c^{-1}$, $bc = cb$.

G_2 : $a^2 = b^3 = c^3 = e$, $b^a = b^{-1}$, $c^a = c^{-1}$, $bc = cb$.

Prema prethodnom, postoji 5 grupa (do na izomorfizam) reda 18: dve su komutativne i tri nekomutativne.

2.19.Opisati grupe reda 20.

Rešenje: Kako je 20=4·5, 5 je prost broj i 5=1(mod 4), prema zad. 2.14. postoji 5 neizomorfnih grupa reda 20, i to:

Komutativne : C_{20}, $C_2 \times C_2 \times C_5$.

Nekomutativne: 1° Slučaj A. u rešenju zadatka 2.14.; strukturne jednakosti su

G_1 : $a^5=b^4=e$, $a^b=a^{-1}$ $\qquad$ G_2 : $a^5=b^4=e$, $a^b=a^2$.

2° Slučaj B. u rešenju zadatka 2.14.; strukturne jednakosti su

G_3 : $a^5=b^2=c^2=e$, $ab=ba$, $bc=cb$, $a^c=a^{-1}$.

Napomena: Grupa G_2 *se može zadati i sledećim strukturnim jednakostima:* $a^5=b^4=e$, $a^b=a^3$. *Primetimo da su 2 i 3 rešenja jednačine* $i^4=1(mod\ 5)$ *po i pa prema (T3) u rešenju zadatka 2.14. ova dva skupa strukturnih jednakosti zaista odredjuju istu grupu.*

2.20.Opisati grupe reda 21.

Rešenje: Zbog 21=3·7, 3 i 7 su prosti brojevi i 3 deli 7-1, prema zadatku 2.15. postoje dve neizomorfne grupe reda 21.

Komutativna grupa je C_{21} , *a nekomutativna grupa je data strukturnim jednakostima (prema (T2) u rešenju zad. 2.15.)*

G : $a^3=b^7=e$, $b^a=b^2$.

Primetimo da prema (T3) istog zadatka, strukturne jednakosti $a^3=b^7=e$, $b^a=b^4$ *odredjuju istu grupu jer su 2 i 4 rešenja jednačine* $i^3=1(mod\ 7)$ *po i.*

2.21.Opisati grupe reda 27.

Rešenje: $27=3^3$, *3 je neparan prost broj, pa prema zadatku 2.16. postoji tačno 5 neizomorfnih grupa reda 27.*

Od toga su tri komutativne : C_{27} , $C_3 \times C_9$, $C_3 \times C_3 \times C_3$.

Postoje dve neizomorfne nekomutativne grupe reda 27. Prema rešenju zad. 2.16., date su sledećim strukturnim jednakostima:

G_1 : $a^3=b^3=c^3=e$, $ac=ca$, $bc=cb$, $a^b=ac$ *(slučaj A. u rešenju zad. 2.16.)*

G_2 : $a^9=b^3=e$, $a^b=a^4$ *(slučaj B. u rešenju zad. 2.16.)*

2.22.Opisati grupe reda 28.

Rešenje: $28=4\cdot7$, *7 je prost broj,* $7\neq1(mod\ 4)$, *pa prema zad. 2.14. postoje tačno 4 neizomorfne grupe reda 28.*

Od toga dve su komutativne : C_{28} , $C_2 \times C_2 \times C_7$.

Postoje dve neizomorfne nekomutativne grupe reda 28. Prema rešenju zadatka 2.14., te grupe date su sledećim strukturnim jednakostima:

G_1 : $a^7=b^4=e$, $a^b=a^{-1}$ (slučaj A. u rešenju zad. 2.14.)
G_2 : $a^7=b^2=c^2=e$, $ab=ba$, $bc=cb$, $a^c=a^{-1}$ (slučaj B. u rešenju z. 2.14.)

2.23.Opisati grupe reda 30.

Rešenje: Neka je $|G|=30$, $30=2\cdot3\cdot5$, pa prema zad. 2.17. postoji $H\lhd G$, $|H|=15$. Kako je $|H|=15$, prema zad. 2.11. H je ciklična grupa, pa postoji $a\in G$ takav da $H=\langle a\rangle$. Dalje, prema Cauchy-evoj lemi postoji $b\in G$, $r(b)=2$. Prema Lagrange-ovoj teoremi $b\in H$, dakle $G=H\langle b\rangle$. Kako je $H\lhd G$, to $a^b=a^i$ za neki $i<15$. Iz uslova $b^2=e$ sledi $i^2=1(\mathrm{mod}\ 15)$, odakle $i\in\{1,4,11,14\}$. Prema tome imamo sledeća 4 skupa strukturnih jednakosti, koji odredjuju sve grupe reda 30 (do na izomorfizam):
G_1 : $a^{15}=b^2=e$, $a^b=a$ (primetimo da je $G_1\cong C_{30}$) ;
G_2 : $a^{15}=b^2=e$, $a^b=a^4$;
G_3 : $a^{15}=b^2=e$, $a^b=a^{11}$;
G_4 : $a^{15}=b^2=e$, $a^b=a^{-1}$ ($G_4\cong D_{15}$) .

2.24.Opisati grupe reda 24.

Rešenje: Neka je $|G|=24$ i $P,Q\prec G$ redom S_2,S_3-podgrupe grupe G. Tada $|P|=8$, $|Q|=3$, dakle Q je ciklična i postoji $a\in G$, $r(a)=3$, $Q=\langle a\rangle$.
Razlikujemo sledeće slučajeve:
A. $Q\lhd G$. Za grupu P postoje sledeće mogućnosti:
A.1. $P\cong C_2\times C_2\times C_2$; dakle $P=\langle b,c,d\rangle$ gde

$$b^2=c^2=d^2=e\ ,\ bc=cb\ ,\ bd=db\ ,\ cd=dc \qquad (1)$$

Q je normalna podgrupa grupe G, pa P dejstvuje na Q konjugacijom. Postoje sledeće 4 mogućnosti: $a^b=a$, $a^c=a$, $a^d=a$; $a^b=a$, $a^c=a$, $a^d=a^{-1}$; $a^b=a$, $a^c=a^{-1}$, $a^d=a^{-1}$; $a^b=a^{-1}$, $a^c=a^{-1}$, $a^d=a^{-1}$.
Prvi skup strukturnih jednakosti, zajedno sa (1), odredjuje grupu $C_3\times C_2^3$. Drugi skup strukturnih jednakosti, zajedno sa (1), odredjuje semidirektan proizvod $C_3\times_\theta C_2^3$; $\theta: C_2^3\to \mathrm{Aut}\, C_3$ je dejstvo odredjeno sa $\theta(b)=I$, $\theta(c)=I$, $\theta(d)=\tau$, gde je I identičko preslikavanje skupa C_3 a τ automorfizam grupe C_3, $r(\tau)=2$.
Primetimo da treći skup strukturnih jednakosti zajedno sa (1) odredjuje grupu izomorfnu grupi $C_3\times_\theta C_2^3$, odredjenoj prethodno. Zaista, ako se u trećem skupu izabere $x=b$, $y=cd$, $z=d$ dobija se $a^x=a$, $a^y=a$, $a^z=a^{-1}$, $x^2=y^2=z^2=e$, $xy=yx$, $xz=zx$, $yz=zy$, pa tvrdjenje sledi.
Na sličan način se dokazuje da i četvrti skup strukturnih jednakosti zajedno sa (1) odredjuje grupu izomorfnu grupi definisanoj u drugom slučaju.
Dakle, u ovom slučaju postoje tačno dve neizomorfne grupe reda 24.

A.2. $P \simeq C_2 \times C_4$. Tada $P = \langle b,c \rangle$ gde

$$b^2 = c^4 = e \ , \ bc = cb \qquad (2)$$

Grupa P takodje dejstvuje na Q i postoje sledeće mogućnosti:
$a^b = a$, $a^c = a$; zajedno sa jednakostima (2) to daje $G \simeq C_2 \times C_4 \times C_3$;
$a^b = a$, $a^c = a^{-1}$; uz (2) je tada $G \simeq C_3 \times_\theta (C_2 \times C_4)$, gde je $\theta : C_2 \times C_4 \to \mathrm{Aut}\, C_3$ dejstvo odredjeno sa $\theta(b) = I$, $\theta(c) = \tau$, I je identičko preslikavanje skupa C_3 , $\tau \in \mathrm{Aut}\, C_3$, $r(\tau) = 2$, $\tau(x) = x^{-1}$;
$a^b = a^{-1}$, $a^c = a$; sa (2) je tada $G \simeq C_3 \times_\sigma (C_2 \times C_4)$, $\sigma : C_2 \times C_4 \to \mathrm{Aut}\, C_3$, $\sigma(b) =$, $\sigma(c) = I$.

Svaki drugi skup strukturnih jednakosti svodljiv je na prethodna tri, odgovarajućom promenom generatora grupe P. Dakle, u ovom slučaju postoje tačno tri neizomorfne grupe reda 24, jedna komutativna i dve nekomutativne.

A.3. $P \simeq C_8$. Tada $P = \langle b \rangle$, gde $b^8 = e$. Slično kao u slučaju A.2. dokazuje se da postoje dve neizomorfne grupe. One su date strukturnim jednakostima:
$a^3 = b^8 = e$, $a^b = a$; tada $G \simeq C_{24}$.
$a^3 = b^8 = e$, $a^b = a^{-1}$; tada je G semidirektan proizvod grupa C_8 i C_3 .

A.4. P je dijedarska grupa D_4 . Tada $P = \langle b,c \rangle$, gde

$$b^4 = c^2 = e \ , \ b^c = b^{-1} \qquad (3)$$

S obzirom da P dejstvuje na Q, slično kao u prethodnim slučajevima dolazi se do sledećih strukturnih jednakosti:
$a^b = a$, $a^c = a$, što uz (3) (i, naravno, $a^3 = e$) daje $G \simeq D_4 \times C_3$;
$a^b = a$, $a^c = a^{-1}$, što zajedno sa (3) daje $G \simeq C_3 \times_\theta D_4$, $\theta : D_4 \to \mathrm{Aut}\, C_3$, $\theta(b) = I$, $\theta(c) = \tau$, I, τ su kao u A.2.;
$a^b = a^{-1}$, $a^c = a$, što uz (3) daje $G \simeq C_3 \times_\sigma D_4$, $\sigma : D_4 \to \mathrm{Aut}\, C_3$, $\sigma(b) = \tau, \sigma(c) = I$.

Ostali slučajevi skupova strukturnih jednakosti svodljivi su na prethodna tri, odgovarajućom transformacijom skupa generatora grupe P.
Dakle, u ovom slučaju postoje tri neizomorfne (nekomutativne) grupe reda 24.

A.5. P je kvaternionska grupa K. Tada $P = \langle b,c \rangle$, gde

$$b^4 = c^4 = e \ , \ b^2 = c^2 \ , \ b^c = b^{-1} \qquad (4)$$

Grupa P dejstvuje na Q, pa imamo sledeće mogućnosti za skupove strukturnih jednakosti:
$a^b = a$, $a^c = a$; sa (4) to daje $G \simeq K \times C_3$;
$a^b = a$, $a^c = a^{-1}$; sa (4) je $G \simeq C_3 \times_\theta K$, $\theta : K \to \mathrm{Aut}\, C_3$, gde $\theta(b) = I$, $\theta(c) = \tau$, I, τ su kao u A.2.

Ostali slučajevi su svodljivi na prethodna dva, pa u ovom slučaju postoje tačno dve neizomorfne (nekomutativne) grupe reda 24.

B. $P \lhd G$, $Q \not\lhd G$. Grupa Q dejstvuje konjugacijom na P, budući da je $P \lhd G$, $P^a = P$. Dalje, $Q \not\lhd G$, pa G nije komutativna grupa, dakle unutrašnji automorfizam σ_a odredjen elementom a nije trivijalan, pa kako je $a^3 = e$, $\sigma_a^3 = \sigma_{a^3} = I$, tj. $r(\sigma_a) = 3$, otuda

$$3 \text{ deli } |\text{Aut } P| \qquad (5)$$

Razlikujemo sledeće slučajeve:

B.1. $P \simeq C_8$. Grupa $\text{Aut } C_8$ je ciklična reda 4; broj 3 ne deli broj 4, pa prema (5) ovaj slučaj nije moguć.

B.2. $P \simeq C_4 \times C_2$. Red grupe $\text{Aut } C_4 \times C_2$ je 8, a 3 ne deli 8, pa prema (5) ni ovaj slučaj nije moguć.

B.3. $P \simeq C_2 \times C_2 \times C_2$. C_2^3 je vektorski prostor nad poljem Z_2, prema tome $\text{Aut } C_2^3$ je skup regularnih linearnih operatora nad C_2^3 , pa prema stavu o reprezentaciji linearnih operatora, može se uzeti da je $\text{Aut } C_2^3$ jednak skupu regularnih matrica trećeg reda nad Z_2. S obzirom da je $r(\sigma_a) = 3$, za nas su od interesa matrice A za koje je $A^3 = E$.

Matrica $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. različita je od jedinične matrice i $A^3 = E$. Otuda za slučaj $P = \langle b,c,d \rangle$ imamo sledeće strukturne jednakosti grupe G (ostali slučajevi su svodljivi na ovaj):

$a^3 = b^2 = c^2 = d^2 = e$, $bc = cb$, $bd = db$, $cd = dc$, $b^a = c$, $c^a = bc$, $d^a = d$.

Dakle, u ovom slučaju postoji tačno jedna grupe reda 24.

B.4. $P \simeq D_4$. $|\text{Aut } D_4| = 8$, a $3 \nmid 8$, pa prema (5) ovaj slučaj nije moguć.

B.5. $P \simeq K$, K je kvaternionska grupa. Svaki $\phi \in \text{Aut } K$ odredjen je, prema zad. 2.2.3.f) sa $\phi(i) = \pm\varepsilon$, $\phi(j) = \pm\tau$, $\varepsilon \neq \tau$, $\varepsilon, \tau \in \{i,j\}$. Takodje, svako 1-1 preslikavanje $f : \{i,j\} \to \{\pm i, \pm j, \pm k\}$ produživo je do automorfizma grupe K. Dakle, $|\text{Aut } K| = 24$, broj 3 deli broj 24, pa prema Cauchy-evoj lemi K ima automorfizam reda 3. Lako je proveriti da su jedini automorfizmi reda 3 upravo produženja ϕ, ψ redom preslikavanja $f = \begin{pmatrix} i & j & k \\ j & k & i \end{pmatrix}$, $g = \begin{pmatrix} i & j & k \\ k & i & j \end{pmatrix}$ i da važi $\psi = \phi^2$. Dakle, $\sigma : C_3 \to \text{Aut } K$, $\sigma(a) = \phi$, odredjuje jedno dejstvo , i za $b = i$, $c = j$, $k = bc$ dobijaju se sledeće strukturne jednakosti:

$$a^3 = b^4 = c^4 = e \text{ , } b^2 = c^2 \text{ , } b^c = b^{-1} \text{ , } b^a = c \text{ , } c^a = b \text{ .}$$

Primetimo da strukturne jednakosti u kojima učestvuju jedino b i c predstavljaju upravo strukturne jednakosti grupe K. Ako je $\theta : C_3 \to \text{Aut } K$ dejstvo odredjeno sa $\theta(a) = \psi$, tada se pokazuje da je $K \times_\sigma C_3 \simeq K \times_\theta C_3$.

Dakle, u slučaju B.5. postoji tačno jedna (do na izomorfizam) grupa reda 24.

C. $P \not\lhd G$, $Q \not\lhd G$. Neka je $H = N(Q)$. Prema teoremama Sylow-a je $|G : N(Q)| = 1 \pmod 3$ i takodje $|G : N(Q)|$ deli $|G|$. Otuda $|G : N(Q)| \in \{1,4\}$. Kako $Q \not\lhd G$, to $N(Q) \neq G$, dakle $|H| = 6$.

Dokazujemo sledeće pomoćno tvrdjenje:

(T1) *U G ne postoji normalna podgrupa reda 6.*

Dokaz: Pretpostavimo suprotno, tj. neka je $N \triangleleft G$, $|N|=6$. *Dalje, neka je* Q_1 S_3*-podgrupa grupe N. Očigledno,* Q_1 *je takodje* S_3*-podgrupa grupe G, pa prema teoremi Sylow-a postoji* $g \in G$ *takav da* $Q = Q_1^g$. *Kako je* $N \triangleleft G$, *to* $N^g = N$, *odakle sledi* $Q_1^g < N$, *tj.* $Q < N$. *Kako je* $|N:Q|=2$, *to je* $Q \triangleleft N$; *s obzirom da su sve Sylow-ljeve 3-podgrupe konjugovane, sledi da je Q jedina* S_3*-podgrupa grupe N i grupe G. Za svaki* $g \in G$, Q^g *je* S_3*-podgrupa, pa prema jedinosti* $Q^g = Q$, *tj.* $Q \triangleleft G$, *suprotno pretpostavci, čime je dokaz završen.* ▽

Neka je θ *koset-dejstvo grupe G po H (v.zad. 1.2.). Dokazujemo da je* θ *verna reprezentacija. Kako je* $\ker\theta = core(H)$, *dovoljno je dokazati:*

(T2) $Core(H) = \langle e \rangle$.

Dokaz: Dokazujemo da je jedina normalna podgrupa grupe G sadržana u H, trivijalna. Neka je $N \triangleleft G$, $N \subseteq H$. *Prema Lagrange-ovoj teoremi* $|N| \in \{1,2,3,6\}$.
Prema (T1) je $|N| \neq 6$.
Pretpostavimo $|N|=3$. *Neka je* $k : G \to G/N$ *kanonski homomorfizam. Zbog* $|G:N|=8$ *prema zadatku 2.1. je* $Z(G/N) \neq \langle e \rangle$; *prema Cauchy-evoj lemi postoji a iz* $Z(G/N)$, $r(a)=2$. *Neka je* $X = k^{-1} \langle a \rangle$. *Kako je* $\langle a \rangle \triangleleft G/N$, *to* $X \triangleleft G$.
Dalje, $|X|=6$, *što je suprotno (T1).*
Pretpostavimo $|N|=2$. *Dakle postoji* $a \in G$, $N = \{e,a\}$. *Kako je* $r(a^x)=r(a)$, $N \triangleleft G$, *sledi* $(\forall x \in G)a^x = a$, *tj.* $N < Z(G)$. *Neka je* $k : G \to G/N$ *kanonski homomorfizam i neka su P', Q' redom* S_2, S_3*-podgrupe grupe G/N. Primetimo da je* $|G/N|=12$ *i prema zad. 2.12. je* $P' \triangleleft G/N$ *ili* $Q' \triangleleft G/N$.
Ako je $P' \triangleleft G/N$ *tada* $k^{-1}(P') \triangleleft G$ *i* $|k^{-1}(P')|=8$, *tj.* $k^{-1}(P')$ *je normalna* S_2*-podgrupa grupe G. Otuda, P je konjugovana sa* $k^{-1}(P')$, *pa zbog normalnosti podgrupe* $k^{-1}(P')$ *sledi* $P = k^{-1}(P')$. *Prema tome* $P \triangleleft G$, *suprotno pretpostavci.*
Dakle, $Q' \triangleleft G/N$. *Otuda* $k^{-1}(Q') \triangleleft G$ *i* $|k^{-1}(Q')|=6$, *suprotno (T1).*
Prema prethodnom, $|N|=1$, *N je ma koja normalna podgrupa grupe G sadržana u H, dakle* $core(H) = \langle e \rangle$. ▽

Odavde sledi da je θ *verna reprezentacija, tj.* θ *je 1-1. Kako je* $|G:H|=4$, *to* $|Sym(G/H)|=24$, *pa iz* $|G|=24$ *sledi da je* θ *izomorfizam, tj.* $G \simeq S_4$.

Rezime: Do na izomorfizam, postoji tačno 15 grupa reda 24; od toga je 12 grupa tipa A, dve grupe su tipa B i jedna tipa C. Medju njima su 3 komutativne, a ostalih 12 su nekomutativne.

2.25.Opisati grupe reda 16.

Rešenje: Razlikujemo sledeće slučajeve:

A. G ima element reda 16. Tada $G \simeq C_{16}$.

B. $(\forall x \in G)x^2=e$. Tada je G komutativna, dakle $G \simeq C_2^4$.

C. $(\exists x \in G)r(x)=8 \wedge (\exists x \in G)r(x) \leqslant 8$. Neka je $a \in G$, $r(a)=8$; tada $a^8=e$. Za $H=\langle a \rangle$ je $|G:H|=2$; sledi $H \lhd G$. Dalje, za kanonski homomorfizam $k : G \to G/H$ za sve $x \in G$ je $k(x)^2=e$, tj. $x^2 \in \ker k$, odnosno

$$(\forall x \in G)x^2 \in H \qquad (1)$$

Kako je $\langle a \rangle \lhd G$, takodje

$$(\forall x \in G)a^x \in H \qquad (2)$$

Dalje, $H \simeq C_8$, pa uzimamo $C_8=\langle a \rangle$, i tada

$\mathrm{Aut}\, H = C_2 \times C_2$, $\mathrm{Aut}\, C_8 = (\{I,\alpha,\beta,\gamma\},)$, gde $\alpha(a)=a^3$, $\beta(b)=a^5$, $\gamma(x)=x^{-1}$.

Ako je $b \in G \setminus H$ tada $G=\langle a,b \rangle$.

Razlikujemo sledeće slučajeve:

C.1. Postoji $b \in G \setminus H$ za koji je $r(b)=2$. Prema (2), za neki $i \leqslant 8$ je $a^b=a^i$. Iz uslova $b^2=e$ sledi $i^2=1 \pmod 8$, tj. $i \in \{1,3,5,7\}$.

Dakle, imamo sledeće skupove strukturnih jednakosti:

G_1 : $a^8=b^2=e$, $a^b=a$; $\qquad$ G_2 : $a^8=b^2=e$, $a^b=a^3$;

G_3 : $a^8=b^2=e$, $a^b=a^5$; $\qquad$ G_4 : $a^8=b^2=e$, $a^b=a^7$.

Očigledno, $G_1 \simeq C_8 \times C_2$, $G_4 \simeq D_8$. Neka je $C_2=\langle b \rangle$. Tada $G_2 \simeq C_8 \times_\theta C_2$, gde je $\theta : C_2 \to \mathrm{Aut}\, C_8$ dejstvo odredjeno sa $\theta(b)=\alpha$;

$G_3 \simeq C_8 \times_\sigma C_2$ gde je $\sigma : C_2 \to \mathrm{Aut}\, C_8$ dejstvo odredjeno sa $\sigma(b)=\beta$.

Dakle, postoje tačno 4 (do na izomorfizam) grupe reda 16, tipa C.1.

C.2. Postoji $b \in G \setminus H$ za koji je $r(b)=4$. Tada $b^4=e$ i zbog (1) $b^2=a^4$.

Kao u C.1. nalazimo $a^b=a$ ili $a^b=a^3$ ili $a^b=a^5$ ili $a^b=a^7$.

Ako je $a^b=a$ tada je G komutativna i $G \simeq C_8 \times C_2$, tj. $G \simeq G_1$ iz C.1.

Ako je $a^b=a^3$ tada za $c=ab$, $r(c)=2$, $a^c=a^3$, $G=\langle a,c \rangle$, tj. $G \simeq G_2$ iz C.1.

Ako je $a^b=a^5$ tada za $c=a^2b$, $r(c)=2$, $a^c=a^3$, $G=\langle a,c \rangle$, tj. $G \simeq G_3$ iz C.1.

Ako je $a^b=a^7$ imamo sledeće strukturne jednakosti:

G_5 : $a^8=b^4=e$, $b^2=a^4$, $a^b=a^7$;

tada $G \simeq \underline{A}$, gde $\underline{A}=(A,\cdot)$, $A=\{(x,i) \mid x \in \{0,1,\ldots,7\},\ i \in \{0,1\}\}$,

$(x,i)\cdot(y,j)=(x +_8 (-1)^i y +_8 4ij,\ i +_2 j)$, $+_8$ je sabiranje po modulu 8 a $+_2$ sabiranje po modulu 2. Primetimo da je u ovom slučaju $(\forall x \in G \setminus H)r(x)=4$.

Dakle, postoji tačno jedna grupa reda 16 tipa C.2. (a koja nije tipa C.1.).

C.3. Postoji $b \in G \setminus H$, $r(b)=8$. Tada $ba=a^k b$ za neki $k \in \{1,3,5,7\}$, $b^2 \in \{a^2, a^6\}$, pa $b^4=a^4$. Otuda $(ab)^4=a^{2k(1+k^2)+4}$. Kako je $2k(1+k^2)+4=0 \pmod 8$ za $k \in \{1,3,5,7\}$, to $r(ab) \leqslant 4$. Dakle, uzimajući $c=ab$, ovaj slučaj je svodljiv na prethodna dva, tj. G je izomorfna jednoj od grupa tipa C.1., C.2.

D. $(\exists x \in G)r(x)=4 \wedge (\forall x \in G)x^4=e$. Dokazujemo da važi

(T1) Postoji $a \in Z(G)$, $r(a)=2$ i $G/\langle a \rangle$ je Abel-ova grupa.

Dokaz: $Z(G) \neq \langle e \rangle$ (v.zad. 2.1.), $|Z(G)|$ je stepen broja 2, pa prema Cauchy-evoj lemi postoji $w \in Z(G)$, $r(w)=2$. Tada za $H=\langle w \rangle$, $H \subset Z(G)$, dakle $H \lhd G$ i grupa G/H ima red 8. Ako G/H nije Abel-ova, tada $G/H \simeq D_4$ ili $G/H \simeq K$, K je grupa kvaterniona (v.zad. 2.9.). Dakle, G/H je generisana sa dva elementa (v.zad. 2.9.) $\bar{x},\bar{y}$ za koje važi $r(\bar{x})=4$, $\bar{x}^{\bar{y}}=\bar{x}^{-1}$. Neka je $k : G \to G/H$ kanonski homomorfizam i $x,y \in G$ takvi da $k(x)=\bar{x}$, $k(y)=\bar{y}$. Tada $G=\langle x,y,w \rangle$; kako je $r(x) \geq r(k(x))=r(\bar{x})=4$, prema uslovu D sledi $r(x)=4$. Dalje, iz $\bar{x}^{\bar{y}}=\bar{x}^{-1}$ sledi $k(x)^{k(y)}=k(x)^{-1}$, tj. $k(x^y x)=e$, dakle $x^y=x^{-1}z$ za neki $z \in H$. Primetimo da je tada $z \in Z(G)$, $z^2=e$ i $x^2 \neq z^{-1}=z$, jer $r(\bar{x})=4$. Kako je $(x^2)^y=(x^y)^2=(x^{-1}z)^2=x^{-2}z^{-2}=x^2$, to x^2 komutira sa svim generatorima x,y,w grupe G, dakle $x^2 \in Z(G)$. Otuda $\langle x^2 z \rangle \subset Z(G)$, tj. $\langle x^2 z \rangle \lhd G$. Neka je $a=x^2 z$. Tada $a \in Z(G)$ i $a^2=x^2 z x^2 z=x^4 z^2=e$, pa je zbog $x^2 \neq z^{-1}$, $r(a)=2$.

Neka je $h : G \to G/\langle a \rangle$ kanonski homomorfizam. Elementi $h(x)$, $h(y)$, $h(w)$ generišu $G/\langle a \rangle$, pa je za komutativnost grupe $G/\langle a \rangle$ dovoljno dokazati da komutiraju njeni generatori. Element $h(w)$ komutira sa $h(x)$ i $h(y)$ jer $w \in Z(G)$, dakle i $h(w) \in Z(G/\langle a \rangle)$. Dalje

$$h(x)^{h(y)}=h(x^y)=h(x^{-1}z)=h(x^3 z)=h(xx^2 z)=h(x)h(x^2 z)=h(x)e=h(x),$$

tj. $h(x)h(y)=h(y)h(x)$. Prema tome $G/\langle a \rangle$ je komutativna grupa i tvrdjenje je dokazano. ∇

Razlikujemo sledeće slučajeve:

D.1. $G/\langle a \rangle \simeq C_4 \times C_2$. Neka je $C_4=\langle \bar{b} \rangle$, $C_2=\langle \bar{c} \rangle$. Možemo uzeti $G/\langle a \rangle = C_4 \times C_2$. Tada postoje $b,c \in G$ takvi da $k(b)=b$, $k(c)=c$ gde je k kanonski homomorfizam. Prema uslovu D i dokazu tvrdjenja (T1) važi:

$$a^2=e \wedge b^4=e \wedge (c^2=e \vee c^2=a) \wedge a^b=a \wedge a^c=a \wedge (b^c=b \vee b^c=ab) .$$

Otuda imamo sledeća 4 slučaja:

$a^2=b^4=c^2=e$, $a^b=a$, $a^c=a$, $b^c=b$; tada je G komutativna i $G \simeq C_4 \times C_2 \times C_2$;

$a^2=b^4=c^2=e$, $a^b=a$, $a^c=a$, $b^c=ab$; tada je G semidirektan proizvod grupa $(C_4 \times C_2)$, C_2, tj. $G \simeq (C_4 \times C_2) \times_\theta C_2$, gde je $\theta : C_2 \to \mathrm{Aut}\, C_4 \times C_2$ dejstvo $C_2=\langle c \rangle$, $C_4 \times C_2=\langle a,b \rangle$, $\theta(c)(b)=ab$.

$a^2=b^4=c^4=e$, $a^b=a$, $a^c=a$, $b^c=b$, $c^2=a$; tada su generatori grupe G uzajamno komutativni, pa je G komutativna grupa.

$a^2=b^4=c^4=e$, $a^b=a$, $a^c=a$, $b^c=ab$, $c^2=a$; tada je $G \simeq \underline{A}$, $\underline{A}=(A,\cdot)$, gde je

$A=\{(i,x,u) \mid i \in \{0,1\},\ x \in \{0,1,2,3\},\ u \in \{0,1\}\}$,

$(i,x,u)\cdot(j,y,v)=(i+_2 j+_2 uy+_2 uv,\ x+_4 y,\ u+_2 v)$, $+_2$ je sabiranje po modulu 2, $+_4$ sabiranje po modulu 4.

D.2. $G/\langle a \rangle \simeq C_2 \times C_2 \times C_2$. Dokazujemo da važe sledeća tvrdjenja:

(T2) $(\forall x,y \in G)(\exists z \in Z(G))\, x^y=xz$.

Dokaz: Neka je $k : G \to G/<a>$ kanonski homomorfizam. $G/<a>$ je komutativna grupa, pa $k(x^y)=k(x)^{k(y)}=k(x)$, tj. $k(x^y x^{-1})=e$, tj. $x^y x^{-1} \in Z(G)$. Otuda, za neki $z \in Z(G)$ je $x^y x^{-1}=z$, tj. $x^y=xz$. ▽

(T3) $(\forall x \in G)\,|G : C(x)| \leq 2$.

Dokaz: Ako je $x \in Z(G)$ tada $C(x)=G$, tj. $|G : C(x)|=1$. Zato neka $x \notin Z(G)$. Ako $|Z(G)| \geq 4$, tada $x \notin Z(G) \prec C(x)$ pa $|C(x)| \geq 8$, tj. $|G : C(x)| \leq 2$. Zato pretpostavimo $|Z(G)| = 2$. Tada $|Z(G)| = <a>$, i $e, ax, x, a \in C(x)$. Pretpostavimo $|C(x)|=4$. Primetimo da ako je $y \notin C(x)$, onda prema (T2) $x^y=ax$. Neka je $z \notin C(x) \cup y^{-1}C(x)$, tada $x^z=ax$. Dalje, $yz \notin C(x)$ jer ako je $yz \in C(x)$ onda $z \in y^{-1}C(x)$, suprotno izboru elementa z. Otuda $x^{yz}=ax \neq x$. S druge strane $x^{yz}=(x^y)^z=(ax)^z=a^z x^z=aax=x$; kontradikcija. Dakle, $|C(x)| \geq 8$. ▽

(T4) Neka su $x, y \in G$, $xy \neq yx$, $H = <x, y>$; tada: $|H|=8$, $|Z(H)|=2$, $|C(H)| \geq 4$.

Dokaz: Prema dokazu tvrdjenja (T2) $x^y=ax$, tj. $yx=axy$. Dalje, u $G/<a>$ svi elementi su reda 2, pa $k(x)^2=k(y)^2=e$, tj. $x^2, y^2 \in \ker k$. Otuda $x^2, y^2 \in \{a, e\}$. Prema uslovu D sledi $x^4=y^4=e$. Dakle, $H = \{e, ax, y, ax, ay, xy, axy\}$, tj. $|H| \leq 8$. Kako H nije komutativna, $|H|$ deli 16, pa H nije reda 1,2,4 (inače bi bila komutativna). Dakle. $|H|=8$.
H je nekomutativna grupa reda 8, pa prema zad. 2.2. $|Z(H)|=2$. Dalje, očigledno važi $C(H)=C(x) \cap C(y)$, pa kako za ma koje dve podgrupe H_1, H_2 grupe G važi $|G : H_1 \cap H_2| \leq |G : H_1| \cdot |G : H_2|$, prema (T3) sledi $|C(H)| \geq 4$, čime je tvrdjenje dokazano. ▽

(T5) Neka je H kao u (T4); tada : $G = HC(H)$, $|C(H)|=4$, $C(H) \prec Z(G)$.

Dokaz: Kako je $Z(H) = H \cap C(H)$, $|Z(H)|=2$ i $|C(H)| \geq 4$, sledi $C(H) \not\subseteq H$. Otuda $|HC(H)| > 8$. Kako je $H \lhd G$ (jer $|G : H|=2$) sledi $HC(H) \prec G$, pa prema Lagrange-ovoj teoremi $|HC(H)|$ deli $|G|$, tj. $|HC(H)|=16$; odnosno $G = HC(H)$. Dalje, $|HC(H)| = |H|\,|C(H)|/|H \cap C(H)|$, tj. $16 = 8|C(H)|/2$, odakle $|C(H)|=4$. Neka je $x \in C(H)$. Grupa $C(H)$ je reda 4, dakle komutativna, prema tome x komutira sa svim elementima grupe $C(H)$. Dalje, prema definiciji grupe $C(H)$, x takodje komutira sa svim elementima grupe H. Kako je $G = HC(H)$, sledi da x komutira sa svim elementima grupe G, tj. $x \in Z(G)$. Otuda $C(H) \prec Z(G)$, dakle i $C(H) \lhd G$. ▽

Razlikujemo sledeće slučajeve:

D.2.1. $C(H) \simeq C_2 \times C_2$. Tada $C(H) = <b, c>$, $b^2=c^2=e$, $bc=cb$. Dalje, $b \notin H$ ili $c \notin H$, inače bi $C(H)$ bila podgrupa od H. Pretpostavimo $b \notin H$; tada $H \cap <b> = <e>$ $H \lhd G$, $<b> \lhd G$ jer $b \in Z(G)$, $G = HC(H)$. Prema tome $G \simeq H \times <b>$, tj. G je izomorfna jednoj od grupa $D_4 \times C_2$, $K \times C_2$, K je grupa kvaterniona.

D.2.2. $C(H) \simeq C_4$. Tada za neki $c \in G$ je $C(H) = <c>$, $r(c)=4$. Pretpostavimo da je H grupa kvaterniona, tj. $H = <a, b>$, $a^4=b^4=e$, $a^2=b^2$, $a^b=a^3$.

Element c^2 je drugog reda, a^2 je jedini element drugog reda u H (jer H ima tačno jedan element drugog reda), pa kako je $c^2 \in H$ (jer $|G:H|=2$) sledi $c^2=a^2$. Tada je G odredjena strukturnim jednakostima:

$$a^4=b^4=c^4=e \ , \ a^2=b^2=c^2 \ , \ a^b=a^3 \ , \ a^c=a \ , \ b^c=b \qquad (3)$$

(koristili smo da $c \in Z(H)$).

Zaista, tada je G izomorfna grupi $\underline{A}=(A,\circ)$, gde $A=\{(x,i) \mid x \in K, \ i \in \{0,1\}\}$ K je grupa kvaterniona iz zad. 2.2.3.f), $\cdot$ množenje u toj grupi , + sabiranje po modulu 2 i $(x,u)\circ(y,v)=((-1)^{uv}x\cdot y, u+v)$.

Ako je H dijedarska grupa D_4 tada za neke $a_1,b_1 \in G$ $H=\langle a_1,b_1\rangle$, $a_1^4=b_1^2=e$, $a_1^{b_1}=a_1^3$. Tada elementi $a=a_1b_1c$, $b=b_1c$ zadovoljavaju strukturne jednakosti (3), tj. $G \approx A$.

Prema prethodnom, u slučaju D.2.2. postoji tačno jedna grupa reda 16.

Rezime: Postoji tačno 14 neizomorfnih grupa reda 16 i to: jedna grupa tipa A, jedna grupa tipa B, pet grupa tipa C i sedam grupa tipa D. Od ovih je 9 nekomutativnih (tri tipa C.1, jedna tipa C.2, dve tipa D.1 i tri tipa D.2), a 5 komutativnih.

2.26. Neka su p,q različiti prosti brojevi, $|G|=pq^n$ i neka su P,Q redom S_p, S_q-podgrupe grupe G. Dokazati: a) $P=N(P) \Rightarrow Q \lhd G$.
b) Ako je $n \in \{1,2,3\}$, tada je $P \lhd G$ ili $Q \lhd G$ ili $|G|=24$.

Rešenje: Neka je $n>1$, s_p broj S_p-podgrupa grupe G i s_q broj njenih S_q-podgrupa.

a) Neka je $P=N(P)$. Prema teoremama Sylow-a $s_p=|G:N(P)|$, tj. $s_p=|G:P|=pq^n/p=q^n$. Neka su $P_1,P_2,\ldots,P_{q^n}$ različite S_p-podgrupe od G. Tada za $i \neq j$ je $P_i \cap P_j=\langle e\rangle$, pa za $\bar{P}_i=P_i \setminus \{e\}$ i za $i \neq j$ važi $\bar{P}_i \cap \bar{P}_j=\emptyset$. Dakle, $|\bigcup_i \bar{P}_i|=q^n(p-1)$. Pretpostavimo $Q \not\lhd G$; tada postoji S_q-podgrupa Q', $Q' \neq Q$. Tada $|Q|=|Q'|=q^n$ i $|Q \cap Q'|$ deli q^n, dakle $|Q \cap Q'| \leq q^{n-1}$. Otuda $|Q \setminus Q'| > q^{n-1}$, pa kako je $Q \cap \bar{P}_i=Q' \cap \bar{P}_i=\emptyset$, sledi

$$|G| \geq |(\bigcup_i \bar{P}_i) \cup Q \cup Q'| \geq q^n(p-1)+q^n+(q^n-q^{n-1})=pq^n+q^n-q^{n-1}>|G| \ ,$$

kontradikcija. Prema tome, $Q \lhd G$.

b) Prema teoremama Sylow-a $s_p=1 \pmod p$, $s_q=1 \pmod q$. Ako je $p<q$, tada prema zad. 1.19. $Q \lhd G$. Zato pretpostavimo $p>q$ i $Q \not\lhd G$. Tada $s_q>1$, $s_q \mid pq^n$ i $s_q=|G:N(Q)| \leq |G:Q|=p$, tj. $s_q=p$. S druge strane $s_p=|G:N(P)| \leq |G:P|=q^n$ i p ne deli s_p jer $s_p=1 \pmod p$. Kako s_p deli pq^n to $s_p=q^i$, $i \in \{0,1,2,3\}$. Ako je $s_p=q^3$ tada $|G:N(P)|=q^3$, tj. $|N(P)|=p$, pa kako je $P \subseteq N(P)$ sledi $P=N(P)$. Otuda, prema a) je $Q \lhd G$, suprotno pretpostavci. Ako je $s_p=q$ tada $q=1 \pmod p$, odakle sledi $p \mid q-1$; prema tome $p<q$, suprotno pretpostavci.

Pretpostavimo $s_p=q^2$; tada $q^2=1 \pmod p$, tj. $p \mid (q-1)(q+1)$. Kako $p>q$,

to $p \mid q+1$. Dakle $q < p \leq q+1$, tj. $p=q+1$, pa je $p=3$, $q=2$. Tada važi $n \geq 2$ jer $s_p \mid pq^n$. Ako je $n=2$ onda $P = N(P)$, pa prema a) $Q \trianglelefteq G$, suprotno pretpostavci. Dakle $n \neq 3$ i $|G|=24$.

Ako je $s_p=1$, P je jedina S_p-podgrupa od G, pa prema trećoj teoremi Sylow-a, $P \trianglelefteq G$.

Napomena: Ako je $|G|=24$, $p \nmid G$, $Q \trianglelefteq G$, tada prema rešenju zad. 2.24., $G \simeq S_4$. Primetimo da i u tom slučaju G ima normalnu podgrupu; to je A_4 .

2.27. Ako je $|G| < 60$ i G je prosta grupa, tada je $|G|$ prost broj. Dokazati.

Rešenje: Neka je $|G|=n$, $n < 60$. Ako je $n < 32$ ili $n=pq^k$, $k \in \{1,2,3\}$, ili $n=p^i$, $i \geq 2$, ili $n=2m$, m je neparan broj, tvrdjenje sledi prema prethodnim zadacima. Jedini brojevi koji nisu navedenog oblika su 36 i 48.

Neka je $n=36$. Tada $n=2^2 \cdot 3^2$. Neka su P,Q redom S_2, S_3-podgrupe grupe G. Ako $Q \trianglelefteq G$ prema trećoj teoremi Sylow-a postoji S_3-podgrupa Q' grupe G, $Q' \neq Q$. Ako je $|Q \cap Q'|=1$, tada $|QQ'|=|Q||Q'|/|Q \cap Q'| = 9 \cdot 9/1 = 81$, odakle $|G| \geq 81$, suprotno pretpostavci. Dakle $|Q \cap Q'|=3$. Grupe Q,Q' su reda 9, dakle (prema zad. 2.3.) obe su komutativne, pa $Q,Q' < N(Q \cap Q')$. Otuda $QQ' \subseteq N(Q \cap Q')$. S druge strane $|QQ'|=|Q||Q'|/|Q \cap Q'| = 9 \cdot 9/3 = 27$, pa $|N(Q \cap Q')| \geq 27$. Kako je $N(Q \cap Q') < G$, to $|N(Q \cap Q')|$ deli $|G|$, tj. $|N(Q \cap Q')|=36$, pa $N(Q \cap Q')=G$. Prema tome $Q \cap Q' \trianglelefteq G$.

Neka je $n=48$. Tada $n=2^4 \cdot 3$. Neka su P,Q redom S_2, S_3-podgrupe grupe G. Pretpostavimo $P \trianglelefteq G$. Tada postoji $P' \neq P$, P' je S_2-podgrupa grupe G. $P \cap P'$ je podgrupa od P, pa $|P \cap P'| \in \{1,2,4,8\}$. Ako je $|P \cap P'| \leq 4$, onda $|PP'|=|P||P'|/|P \cap P'| \geq 16 \cdot 16/4 = 64$, tj. $|G| \geq 64$, suprotno pretpostavci. Dakle, $|P \cap P'| = 8$. Prema tome indeks podgrupe $|P \cap P'|$ u grupama P i P' je 2, pa $P \cap P' \trianglelefteq P,P'$. Otuda $P,P' < N(P \cap P')$, pa $PP' \subseteq N(P \cap P')$. S druge strane $|PP'|=|P||P'|/|P \cap P'| = 16 \cdot 16/8 = 32$, pa $|N(P \cap P')| \geq 32$. Kako je $N(P \cap P') < G$, to $|N(P \cap P')| \mid |G|$, dakle $|N(P \cap P')|=48$, tj. $N(P \cap P') = G$; prema tome $P \cap P' \trianglelefteq G$.

2.28. Dokazati da postoji beskonačno mnogo prostih brojeva p takvih da je svaka grupa reda 3p ciklična.

Rešenje: Neka je p prost broj. Prema rešenju zad. 2.15. važi:

Svaka grupa reda $3p$ je ciklična akko 3 ne deli $p-1$. (1)

Dalje, svaki prirodan broj je oblika $3k$ ili $3k+1$ ili $3k-1$ za neki $k \in N$, pa

$3 \nmid p-1 \iff (\exists m \geq 1) p=3m-1$ (2)

Dokazujemo da važi sledeće:

Postoji beskonačno mnogo prostih brojeva oblika $3m-1$. (3)

Zaista, pretpostavimo suprotno, tj. neka su $p_1,\dots,p_n$ svi prosti brojevi oblika 3m-1. Neka je $a=p_1\dots p_n$; tada za svaki $i \leqslant n$ $3a-1 > p_i$, pa 3a-1 nije prost broj oblika 3m-1. Dalje, x=1(mod 3), y=1(mod 3) povlači xy=1(mod 3), pa 3a-1 ima bar jedan prost faktor oblika p=3k-1.
Po definiciji broja a, p deli a, pa kako p deli 3a-1 sledi $p \mid -1$, tj. p=1; kontradikcija.
Tvrdjenje sledi iz (1), (2) i (3).

2.29. Odrediti najmanji neparan prirodan broj n za koji postoji nekomutativna grupa reda n.

Rešenje: Ako je $|G|=n$, $n \in 2N+1$ i $n<21$, sledi: n je prost broj ili n=9 ili n=15, pa je prema zadacima 2.3. i 2.11. G komutativna grupa. S druge strane, prema zad. 2.20. postoji nekomutativna grupa reda 21.

2.30. Opisati grupe reda 14, 22, 26, 33, 52.

Rešenje: Ako je red grupe G jednak 14, 22, 26 ili 33, videti zadatak 2.15. Ako je G =52, videti zad. 2.14.

2.31. Neka je G konačna p-grupa. Dokazati da za svaki k koji deli red grupe G postoji $H<G$, $|H|=k$.

Rešenje: Videti zadatak 2.7.

2.32. Neka je $|G|=n$ i p prost broj takav da za neki $k \in N$ važi $p^k \mid n$. Dokazati da postoji $H<G$, $|H|=p^k$.

Rešenje: Koristeći prvu teoremu Sylow-a i prethodni zadatak.

2.33. Dokazati da postoji beskonačno mnogo prostih brojeva p sa svojstvom: postoji nekomutativna grupa reda 3p.

Rešenje: Prema rešenju zadatka 2.15. dovoljno je dokazati:
(T1) Postoji beskonačno mnogo prostih brojeva p, p=1(mod 3).
Prethodno dokazujemo sledeće tvrdjenje:
(T2) Jednačina $x^2+3=0$ ima rešenje u polju Z_p akko p=1(mod 3) (p je prost broj).
Dokaz za (T2): Prema tvrdjenju (T1) u rešenju zad. 2.15. jednačina $x^3-1=0$ ima rešenje $x\neq 1$ u Z_p akko p=1(mod 3). Dalje, $x^3-1=(x-1)(x^2+x+1)$, $x^2+x+1=0 \iff ((x+1/2)/(1/2))^2+3=0$, $p\neq 2$, pa tvrdjenje sledi.
Dokaz za (T1): Pretpostavimo suprotno; neka su $p_1,\dots,p_n$ svi prosti brojevi za koje je p=1(mod 3). Neka je $a=p_1\dots p_n$ i p neki prost faktor broja a^2+3. Tada $a^2+3=0(\mathrm{mod}\ p)$, tj. jednačina $x^2+3=0$ ima rešenje u Z_p, prema

(T2) je p=1(mod 3). Prema definiciji broja a, $p \mid a$; takodje $p \mid a^2+3$, dakle $p \mid 3$, tj. p=3, što je u kontradikciji sa uslovom p=1(mod 3). ▽

Napomena: Važi sledeća teorema (Dirichlet): Neka su a,b uzajamano prosti prirodni brojevi; tada postoji beskonačno mnogo članova progresije an+b koji su prosti brojevi.

2.34. Neka je G grupa reda p^2q^2, p,q su prosti brojevi. Dokazati da G sadrži pravu normalnu podgrupu.

Rešenje: Ako je p=q, tvrdjenje sledi prema zad. 2.7.
Pretpostavimo p < q. Neka je $Q<G$ S_q-podgrupa. Ako $Q \not\lhd G$, prema trećoj teoremi Sylow-a postoji $Q' \prec G$, $Q' \neq Q$, Q' je S_q-podgrupa. Tada $|Q \cap Q'| \in \{1,q\}$. Ako je $|Q \cap Q'|=1$ tada $|QQ'|=|Q||Q'|/|Q \cap Q'|=q^2q^2/1=q^4 > |G|$, dakle $|Q \cap Q'|=q$. Dalje, $|Q|=|Q'|=q^2$, q je prost broj, pa su prema zadatku 2.3. grupe Q i Q' komutativne; dakle $Q,Q' \prec N(Q \cap Q')$. Otuda $QQ' \subseteq N(Q \cap Q')$.
Kako je $|QQ'|=|Q||Q'|/|Q \cap Q'|=q^3$, sledi $|N(Q \cap Q')| > q^3$.
$|G : N(Q \cap Q')|$ deli p^2q^2, $|G : N(Q \cap Q')| < p^2q^2/q^3=p^2/q$ i p < q, prema tome $|G : N(Q \cap Q')| \in \{1,p\}$. Ako je $|G : N(Q \cap Q')|=1$ tada $Q \cap Q' \lhd G$.
Ako je $|G : N(Q \cap Q')|=p$, tada prema zad. 1.19. $N(Q \cap Q') \lhd G$, jer je p najmanji prost broj koji deli $|G|$.

2.35. (W.Burnside): Neka je n (n > 1) prirodan broj takav da je $(n,\phi(n))=1$, gde je ϕ Euler-ova funkcija. Dokazati da je svaka grupa reda n ciklična.

Rešenje: Prema zadatku 6.2.3.c) je $\phi(n)=n(1-p_1^{-1})\ldots(1-p_k^{-1})$ gde je $n=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$ razlaganje broja n na proste faktore. S obzirom da su n i $\phi(n)$ uzajamno prosti, sledi $n=p_1p_2\ldots p_k$ i za različite $i,j \leq k$, $p_i \nmid p_j-1$.
Dokazujemo sada tvrdjenje, indukcijom po k, pretpostavljajući da n zadovoljava upravo izveden uslov.
Tvrdjenje je tačno za k=1 (prema zad. 6.1.3.) i k=2 (prema zad. 2.15.); dakle možemo uzeti da je k > 2. Dajemo sada induktivni prelaz sa k na k+1.
Neka je $|G|=n$. Ako je $K \lhd G$ i $m=|K|$, tada $m \mid n$ i neposredno se proverava da je $(m,\phi(m))=1$; dakle, po induktivnoj hipotezi, K je ciklična grupa.
Prema tome:

Svaka prava podgrupa grupe G je Abel-ova . (1)

Dokazujemo da iz uslova (1) sledi:

G ima pravu normalnu podgrupu.

Pretpostavimo suprotno, tj. neka je G prosta grupa. Kako je k > 2, G ima pravu podgrupu (recimo p-podgrupu Sylow-a), dakle G takodje sadrži neku maksimalnu podgrupu H. Kako smo pretpostavili da je G prosta , s obzirom

na maksimalnost podgrupe H i $H<N(H)$, sledi $N(H)=H$. Dakle, za $x\in G\setminus H$ je $H^x\neq H$ (ovde $H^x=x^{-1}Hx$). Kako su H, H^x prave podgrupe grupe G, iz uslova (1) sledi da su H i H^x Abel-ove grupe, pa $H\cap H^x\lhd H$ i $H\cap H^x\lhd H^x$. Otuda, $H\cap H^x\lhd <H\cup H^x>=G$, pa $H\cap H^x=\{e\}$. Dakle

$$(\forall x\in G\setminus H)H\cap H^x=\{e\}. \qquad (2)$$

Dalje, za $x,y\in G$ je

$$H^x=H^y \Leftrightarrow H^{xy^{-1}}=H \Leftrightarrow xy^{-1}\in N(H) \Leftrightarrow xy^{-1}\in H \quad (\text{jer } N(H)=H),$$

pa broj s konjugovanih grupa podgrupe H u G jednak je broju razreda podgrupe H u G, tj. $s=n/m$, gde je $|H|=m$.
S obzirom da je $(H^x\cap H^y)^{y^{-1}}=H^{xy^{-1}}\cap H$, iz uslova (2) nalazimo da različite konjugovane grupe podgrupe H sadrže jedino e kao zajednički element. Otuda, ako su H^{x_i}, $i\in I$, sve konjugovane grupe podgrupe H, sledi $|\bigcup_i H^{x_i}|=s(m-1)+1$, pa

$$|G\setminus\bigcup_i H^{x_i}|=n/m-1, \quad |\bigcup_i H^{x_i}\setminus\{e\}|=n(m-1)/m. \qquad (3)$$

Napomena: Primetimo da je (3) posledica od (2), za ma koju konačnu grupu G i $H<G$.

Kako je $H\lhd G$, to je $m\geqslant 2$, pa prema (3) postoji $a\in G\setminus\bigcup_i H^{x_i}$. Neka je $K\lhd G$ maksimalna podgrupa koja sadrži a. Tada za svaki $i\in I$, $K\nsubseteq H^{x_i}$, pa za sve $x,y\in G$ s obzirom na maksimalnost grupe H, sledi $<K^x\cup H^x>=G$. Po pretpostavci (1), K^x i H_y su Abel-ove grupe, pa $K^x\cap H^y\lhd G$ (videti pasus iznad (2)), pa kako je G prosta, to $K^x\cap H^y=\{e\}$. Dakle, ma koje dve konjugovane grupe podgrupa K i H sadrže kao zajednički element jedino e.
Ako je $|K|=m'$, prema (3) i napomeni ispod, (primetimo da K zadovoljava i uslov (2) za $H=K$, što se dokazuje isto kao za H), ako su K^{y_j}, $j\in J$, sve različite konjugovane grupe podgrupe K u G, imamo

$$|\bigcup_j K^{y_j}|=n(k-1)/m', \text{ a kako je } \bigcup_j K^{y_j}\setminus\{e\}\subseteq G\setminus\bigcup_i H^{x_i},$$

to opet prema (3) i prethodnom : $n(m'-1)/m'\leqslant n/m-1$, odakle $n+1\leqslant n/m+n/m'$ što je kontradikcija, jer $m,m'\geqslant 2$.

Ovim smo dokazali da G nije prosta; dakle postoji N, $N\lhd G$ i N je različita od G i od $\{e\}$. Red d grupe G/N deli n, pa je i $(d,\phi(d))=1$. Kako je $d<n$, po induktivnoj hipotezi G/N je ciklična, dakle i Abel-ova, pa su prema tome sve podgrupe grupe G/N komutativne. Neka je p najmanji prost broj koji deli $d=|G/N|$. Kako je G/N ciklična, to postoji podgrupa $M/N<G/N$ gde je $M<G$ i $|G/N : M/N|=p$. Kako je $|G/M|=|G/N : M/N|$ to $|G/M|=p$. Primetimo da je $M\lhd G$, jer $M/N\lhd G/N$ i $N<M$, pa se može primeniti Teorema o koresponenciji (teorema 3.2.3.(iii)). Kako $|M|\mid n$, to za $j=|M|$, $(j,\phi(j))=1$, pa

prema induktivnoj hipotezi, M je Abel-ova grupa. Ako je $p_i \neq p$ $(i<k)$ prost broj i P_i p_i-podgrupa Sylow-a od M, tada je $P_i \lhd M$ (jer je M Abel-ova), pa je prema trećoj teoremi Sylow-a P_i jedina S_{p_i}-podgrupa od M.
Dalje, za $x \in G$, $P_i^x \subseteq M^x = M$, pa kako je P_i^x u grupi M S_{p_i}-podgrupa, to $P_i^x = P_i$.
Dakle, $P_i \lhd G$ za $p \neq p_i$. Kako smo uzeli da je $k \geqslant 3$, to postcje dve različite podgrupe Sylow-a u G, recimo P_1 i P_2. Po induktivnoj hipotezi nalazimo da su G/P_1, G/P_2 Abel-ove, pa je takva i grupa $G/P_1 \times G/P_2$.
Preslikavanje $\theta: x \longmapsto (P_1x, P_2x)$ je utapanje grupe G u grupu $G/P_1 \times G/P_2$ jer $P_1 \cap P_2 = \{e\}$, pa je G izomorfna podgrupi Abel-ove grupe. Dakle i G je Abel-ova grupa ; prema teoremi o razlaganju Abel-ovih grupa je (v.zad. 6.1.12.)

$$G \simeq C_{p_1} \times C_{p_2} \times \ldots \times C_{p_k} \simeq C_n$$

2.36. Opisati grupe reda 1001.

Rešenje: $1001 = 7 \cdot 11 \cdot 13$, $\phi(1001) = 6 \cdot 10 \cdot 12 = 720$ i $(1001, \phi(1001)) = 1$, pa prema prethodnom zadatku, svaka grupa reda 1001 je ciklična.

2.37. Neka je q prost broj i G grupa reda $2^m q^n$, gde su m,n prirodni brojevi i $m \in \{1,2,3\}$. Dokazati da G sadrži normalnu podgrupu.

Napomena: Ovaj zadatak, kao i zadaci 2.7., 2.26. i 2.34. su posebni slučajevi moćne Burnside-ove teoreme: Svaka grupa reda $p^m q^n$, gde su p,q prosti brojevi, $m+n \geqslant 2$, sadrži pravu normalnu podgrupu.

Rešenje: Neka je s_q broj S_q-podgrupa grupe G. Tada $s_q = 1 (\mathrm{mod}\ q)$ i $s_q = |G : N(Q)| \leqslant 2^m$, gde je Q q-podgrupa Sylow-a. Kako $s_q \mid 2^m q^n$, to onda $s_q \in \{1,2,4,8\}$. Možemo uzeti, prema zad. 2.7., da je $q \in 2N+1$.
Ako je $s_q = 1$, onda $N(Q) = G$, dakle $Q \lhd G$.
Ako je $s_q = 2$, tada $2 = 1 (\mathrm{mod}\ q)$, što je kontradikcija.
Neka je $s_q = 4$. Tada $4 = 1 (\mathrm{mod}\ q)$, odakle $q = 3$. Kako je $|G : N(Q)| = 4$, to prema n! teoremi postoji podgrupa $K \lhd G$ takva da $K < N(Q)$ i $|G : K|$ deli 4! . Ako je G prosta grupa, onda $K = \{e\}$, pa $|G|$ deli 24, tj. $|G| \leqslant 24$; medjutim, to je kontradikcija, prema zadatku 2.27.
Neka je $s_q = 8$. Tada $8 = 1 (\mathrm{mod}\ q)$, odakle $q = 7$. Slično prethodnom slučaju, pretpostavljajući da je G prosta grupa, nalazimo da $|G|$ deli 8! . S obzirom da je $|G| = 8 \cdot 7^n$, sledi da je $|G| \leqslant 56$, što opet dovodi do kontradikcije prema zad. 2.27.

2.38. Neka je m fiksiran prirodan broj. Dokazati da prostih grupa čiji je red oblika mq^n, q je prost broj, $n \in \omega$, ima najviše konačno mnogo.

Rešenje: Neka je s_q broj S_q-podgrupa Sylow-a grupe G, gde $|G| = mq^n$. Tada

$s_q \equiv 1 \pmod q$, $s_q = |G : N(Q)| \leqslant |G : Q| = m$, gde je Q S_q-podgrupa od G. Otuda $s_q \leqslant m$, pa kako $q \mid s_q - 1$ to $q \leqslant m$, pa prostih brojeva q sa datim uslovom ima samo konačno mnogo. Dalje, prema n! teoremi, postoji $K \lhd G$ tako da $K < N(Q)$ i $|G : K| \mid s_q!$. Ako je G prosta grupa onda $|K| = 1$, pa $|G|$ deli neki broj koji je manji ili jednak broju $m!$, tj. $|G| \leqslant m!$.

2.39. Ako je G prosta grupa čiji je red manji od 120, dokazati da je G ciklična ili $G \simeq A_5$.

Rešenje: Koristiti zadatke 2.7., 2.27., 2.34. i 2.37.

9. REŠIVE I NILPOTENTNE GRUPE

U ovom delu biće reči o izvesnim razlaganjima grupa na podgrupe. Ispituju se nizovi tih podgrupa, koji nose odredjene informacije o strukturi grupe o kojoj je reč. Na primer, grupe koje imaju kompozicioni **niz** dužine 1 su proste. Zatim, grupa sa kompozicionim **nizom** dužine n+1 je raširenje grupe sa kompozicionim **nizom** dužine n pomoću proste grupe, itd.

9.1. NORMALNI **NIZ** GRUPE I REŠIVE GRUPE

1.1. Definicija: Opadajući normalni lanac grupe G je niz podgrupa

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n \rhd \ldots$$

gde je G_i prava normalna podgrupa u G_{i-1} $(i=1,2,\ldots)$.

Ako je za neki $n \in N$

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{e\} \qquad (1)$$

onda ovaj niz nazivamo *normalnim* **nizom** grupe G. Grupe G_i/G_{i+1} $(i=0,1,\ldots,n-1)$ su *faktori* normalnog **niza**, a n je *dužina* **niza**.
Svaka grupa ima normalni **niz** (zadatak 1.1.)

1.2. Definicija: Rastući normalni lanac grupe G je niz podgrupa

$$\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n \lhd \ldots$$

gde je G_i prava normalna podgrupa u G_{i+1} $(i=0,1,\ldots)$ i svaka podgrupa G_i se sadrži u nekom normalnom **nizu** *te grupe.*

Konačnost svih opadajućih normalnih lanaca grupe G, odnosno konačnost svih njenih rastućih normalnih lanaca, su važne odrednice grupe G (v.zad. 1.5.). Kaže se, kraće, da grupa *zadovoljava oba uslova lanaca* , ako su joj konačni svi normalni lanci.

Normalni **niz**

$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_m = \{e\} \qquad (2)$$

je *upotpunjenje* **niza** (1) ako je $(\forall i \leq n)(\exists j \leq m) G_i = H_j$.
Odnosno, (2) je dobijen od (1) umetanjem novih članova.

Dva normalna **niza** grupe G

$$G = A_0 \rhd A_1 \rhd \ldots \rhd A_n = \{e\}, \quad G = B_0 \rhd B_1 \rhd \ldots \rhd B_m = \{e\}$$

su *ekvivalentna* ako je n=m i ako postoji $f \in S_n$ tako da je

$$A_i/A_{i+1} \simeq B_{f(i)}/B_{f(i)+1} \ .$$

Ova relacija je relacija ekvivalencije na skupu svih normalnih **nizova** grupe G.

(U zadatku 1.7. dat je primer ekvivalentnih normalnih **nizova** za grupu C_6).

1.3. *Teorema (Schreier): Svaka dva normalna* **niza** *grupe G imaju ekvivalentna upotpunjenja.*

Dokaz: Neka su $G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{e\}$ (1)

$G = H_0 \rhd H_1 \rhd \ldots \rhd H_k = \{e\}$ (2)

dva normalna **niza** grupe G. Upotpunimo ih tako da budu jednake dužine, nk, i da su im faktori izomorfni. Neka su

$$G_{ij} = G_i(G_{i-1} \cap H_j), \ i=1,\ldots,n; \ j=0,1,\ldots,k \qquad (3)$$

Za fiksirano i, za niz podgrupa $G_{i0}, G_{i1}, \ldots, G_{ik}$ važi

$G_{i0} = G_i(G_{i-1} \cap G) = G_{i-1}$ (jer $G_i \prec G_{i-1}$),

$G_{i,j-1} > G_{ij}$ (jer $H_{j-1} > H_j$),

$G_{ik} = G_i(G_{i-1} \cap \{e\}) = G_i$.

Dakle, izmedju G_{i-1} i G_i možemo postaviti k-1 podgrupu G_{ij}, gde je i=1,..,n ; j=1,...,k-1 (isključili smo slučajeve j=0, j=k da se ne bi ponavljale podgrupe G_i). Tako je dobijen **niz**

$$G = G_0 > \ldots > \underbrace{G_i(G_{i-1} \cap H_{j-1})}_{G_{i,j-1}} > \underbrace{G_i(G_{i-1} \cap H_j)}_{G_{ij}} > \ldots > G_n = \{e\} \qquad (4)$$

u kome ima nk znakova > .Uz to, medju podgrupama **niza** može biti i jednakih.

Popunimo sada i **niz** (2): izmedju svake dve podgrupe H_{i-1} i H_i ubacujemo po sledećih n-1 podgrupa

$$H_{ij} = H_j(H_{j-1} \cap G_i), \ \ j=1,\ldots,k; \ i=1,\ldots,n-1 \ , \qquad (5)$$

(jer je, kao i gore, $H_{0j}=H_{j-1}$, $H_{nj}=H_j$).

Tako je dobijen **niz**

$$G = H_0 > \ldots > \underbrace{H_j(H_{j-1} \cap G_{i-1})}_{H_{i-1,j}} > \underbrace{H_j(H_{j-1} \cap G_i)}_{H_{ij}} > \ldots > H_k = \{e\} \qquad (6)$$

koji takodje ima nk znakova > .

Dokažimo još da su **nizovi** (4) i (6) ekvivalentni i da je svaki od njih normalan. Uočimo podgrupe $G_{i,j-1}$, G_{ij}, $H_{i-1,j}$, H_{ij}. Za njih važi sledeće: kako su G_i, G_{i-1}, H_j, H_{j-1} podgrupe u G za koje je $G_i \lhd G_{i-1}$, $H_j \lhd H_{j-1}$, prema lemi Zassenhaus-a je

$$G_i(G_{i-1} \cap H_j) \lhd G_i(G_{i-1} \cap H_{j-1}) \quad \text{i} \quad H_j(H_{j-1} \cap G_i) \lhd H_j(H_{j-1} \cap G_{i-1})$$

i

$$\frac{G_i(G_{i-1} \cap H_{j-1})}{G_i(G_{i-1} \cap H_j)} \simeq \frac{H_j(H_{j-1} \cap G_{i-1})}{H_j(H_{j-1} \cap G_i)}$$

Odnosno, koristeći (3) i (5) je $G_{ij} \lhd G_{i,j-1}$, $H_{ij} \lhd H_{i-1,j}$ i

$$G_{i,j-1}/G_{ij} \simeq H_{i-1,j}/H_{ij} \qquad (7)$$

Dakle, nizovi(4) i (6) su normalni (jer, ako u (4) ima susednih podgrupa koje su jednake, one se mogu izbaciti; pri tom su, zbog (7), jednake i odgovarajuće podgrupe u (6), odakle ih takodje treba izbaciti). Koristeći (7), oni su i ekvivalentni. ▼

1.4.*Definicija: Normalni niz (1) grupe G je kompozicioni ako je G_{i+1} maksimalna normalna podgrupa u G_i (i=0,1,...,n-1).*

Drugim rečima, normalni niz je kompozicioni, ako nema upotpunjenja različitih od samog sebe.
Prema zadatku 1.2., svi faktori kompozicionog niza su proste grupe. I obratno, svaki normalni niz čiji su svi faktori prosti, je kompozicioni.
Očigledno, proste grupe imaju kompozicioni niz dužine 1.
Nemaju sve grupe kompozicione nizove Jedan potreban i dovoljan uslov dat je u zadatku 1.5.

1.5.*Teorema (Jordan-Hölder): Svaka dva kompoziciona niza grupe G su ekvivalentna.*

Dokaz: Prema Schreier-ovoj teoremi, svaka dva kompoziciona niza grupe G imaju ekvivalentna upotpunjenja. Kako je svako upotpunjenje kompozicionog niza sam taj niz (tj. nema pravih upotpunjenja), to su svaka dva kompoziciona niza ekvivalentna. ▼

Obrat ove teoreme ne važi (videti zad. 1.4.).

1.6.*Definicija: Grupa G je rešiva ako ima normalni niz čiji su faktori Abel-ove grupe.*

Takav normalni niz naziva se *rešivim* nizom za grupu G.
Prilikom dokazivanja da je neka grupa rešiva, od koristi mogu biti zadaci 1.13. i 1.14.

Naziv "rešiva grupa" potiče od veze izmedju ovih grupa i rešivosti polinomnih jednačina $a_0+a_1x+...+a_nx^n=0$ nad poljem kompleksnih brojeva. Naime, korene polinoma $a_0+a_1x+...+a_nx^n$ je moguće izraziti pomoću koeficijenata a_i (i=0,1,...,n) i konačnog broja operacija +,-,·,:, $\sqrt[m]{}$ (tj. polinomna jednačina $a_0+a_1x+...+a_nx^n=0$ je rešiva) akko je njemu pridružena grupa Galois-a rešiva u smislu definicije 1.6..
Tako se egzistencija, u ovom smislu nerešive polinomne jednačine 5-og stepena dokazuje na sledeći način: postoji polinom f(x) 5-og stepena čija je

grupa Galois-a simetrična grupa S_5 (Abel); prema zadatku 1.9., S_5 nije rešiva grupa, pa je f(x)=0 nerešiva polinomna jednačina.

Rešivost je jedno uopštenje komutativnosti.
Rešive grupe dobijaju se iz Abel-ovih, raširenjem.

Primeri i zadaci:

1.1. Dokazati da svaka grupa G ima normalni **niz**, koji prolazi kroz datu (pravu) normalnu podgrupu H te grupe.

*Rešenje: Jedan normalni **niz** je* $G \rhd H \rhd \{e\}$.

1.2. Normalni **niz** grupe G je kompozicioni akko su mu svi faktori prosti. Dokazati.

Rešenje: Koristeći tvrdjenje: H je maksimalna normalna podgrupa u G akko je G/H prosta grupa (v.zad. 3.2.31.).

1.3. Dokazati da svaka konačna grupa ima kompozicioni **niz**.

Rešenje: Indukcijom po kardinalnom broju n grupe G.
*Za n=1, kompozicioni **niz** je* $G = \{e\}$.
*Pretpostavka: svaka grupa sa najviše k elemenata ima kompozicioni **niz**.*
Neka je $|G| = k+1$. *Ako je G prosta grupa, njen kompozicioni **niz** je* $\{e\} \lhd G$.
Ako G nije prosta, izaberimo medju njenim normalnim podgrupama, maksimalnu, N. Tada je

$$G \rhd \underbrace{N \rhd N_j \rhd \ldots \rhd N_1 \rhd \{e\}}_{\text{kompozicioni } \textbf{niz} \text{ za } N}$$

*kompozicioni **niz** grupe G (jer je, prema zad. 3.2.31., G/N prosta grupa).*

1.4. Ako dve grupe G_1 i G_2 imaju jednake kompozicione faktore, ispitati da li je $G_1 \simeq G_2$.

Rešenje: Prema zad. 8.2.8., postoje dve neizomorfne grupe reda 6: $C_6 = \langle c; c^6 = 1 \rangle$ *i* $G = \langle a,b; a^3 = 1,\ b^2 = 1, (ab)^2 = 1 \rangle$. *Podgrupa* $G_1 = \{1, a, a^2\}$ *je reda 3 i indeksa 2 u grupi G, tj.* $G_1 \lhd G$. *Pri tome je* $G/G_1 \simeq C_2$ *i* $G_1 \simeq C_3$, *pa je **niz*** $G \rhd G_1 \rhd \{e\}$ *kompozicioni.*
Za grupu C_6 *jedan od ekvivalentnih kompozicionih **niz**ova je* $C_6 \rhd G_2 \rhd \{e\}$, *gde je* $G_2 = \langle 1, c^2, c^4 \rangle$ *i* $C_6/G_2 \simeq C_2$, $G_2 \simeq C_3$.
Dakle, G i C_6 *imaju jednake kompozicione faktore* C_2 *i* C_3, *a* $G \neq C_6$.

1.5. Grupa G ima kompozicioni **niz** akko zadovoljava oba uslova lanaca (tj.akko

su joj svi rastući i opadajući normalni lanci konačni). Dokazati.

Rešenje: ($\Rightarrow$) Neka G ima kompozicioni ***niz***

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{e\} \qquad (1)$$

Ako G ima beskonačan opadajući ili rastući normalni lanac, tada od nekog njegovog segmenta možemo konstruisati normalni ***niz*** *dužine veće od n. Prema teoremi 1.3., taj* ***niz*** *ima upotpunjenje koje je ekvivalentno sa (1), dakle i iste dužine kao (1), što nije tačno.*

($\Leftarrow$) Neka je H proizvoljna podgrupa u G. Dokažimo da medju normalnim podgrupama grupe H postoji maksimalna. Zaista, ako {e} nije maksimalna normalna podgrupa u H, tada postoji H_1 tako da je $\{e\} \lhd H_1 \lhd H$. Dalje, ako H_1 nije maksimalna, postoji H_2 tako da je $\{e\} \lhd H_1 \lhd H_2 \lhd H$, itd. Lanac $\{e\} \lhd H_1 \lhd H_2 \lhd \ldots$ je konačan (prema uslovu konačnosti svih rastućih normalnih lanaca), čime je egzistencija maksimalne normalne podgrupe H dokazana. Neka je, stoga, G_1 maksimalna normalna podgrupa u G, G_2 maksimalna u G_1, G_3 u G_2, itd. Prema uslovu konačnosti svih opadajućih lanaca, konačan je i $G_1 \rhd G_2 \rhd G_3 \rhd \ldots$, pa je ovaj ***niz*** *kompozicioni.*

1.6. Ispitati imaju li kompozicione **nizove** sledeće grupe:

a) Beskonačna ciklična grupa, b) Simetrična grupa S_6 .

Rešenje: a) $C_\infty = \langle a \rangle$ nema kompozicioni ***niz****, jer svaki normalni* ***niz*** *ima netrivijalno upotpunjenje. Naime, sve podgrupe C_∞ su takodje beskonačne ciklične grupe, pa su normalni sledeći* ***nizovi***

$$\langle a \rangle \rhd \langle a^2 \rangle \rhd \{e\}$$
$$\langle a \rangle \rhd \langle a^2 \rangle \rhd \langle a^4 \rangle \rhd \{e\}$$
$$\vdots$$
$$\langle a \rangle \rhd \langle a^2 \rangle \rhd \langle a^4 \rangle \rhd \ldots \rhd \langle a^{2^n} \rangle \rhd \ldots$$

b) Kompozicioni ***niz*** *je $S_6 \rhd A_6 \rhd \{e\}$ (A_6 je, prema 4.2.15. prosta grupa).*

1.7. Za sledeće grupe odrediti sve kompozicione **nizove**:

a) C_6 , b) K (K je grupa kvaterniona) , c) S_4 .

Rešenje: Prema Jordan-Hölder-ovoj teoremi, dovoljno je odrediti jedan kompozicioni ***niz*** *za grupu G; njim su, do na izomorfizam, odredjeni svi ostali.*

a) Neka je $C_6 = \langle a \rangle$; tada $C_6 \rhd \langle a^2 \rangle \rhd \{e\}$.

Postoji i drugi kompozicioni ***niz****, ekvivalentan gornjem: $C_6 \rhd \langle a^3 \rangle \rhd \{e\}$.*

b) $K = \langle a, b; a^4 = 1, a^2 = b^2, ba = a^3 b \rangle$ (v.zad. 8.2.9.); $K \rhd \langle a \rangle \rhd \langle a^2 \rangle \rhd \{e\}$.

c) $S_4 \rhd A_4 \rhd V \rhd G_1 \rhd \{e\}$, gde je V Klein-ova grupa, a $G_1 = \langle (1\ 2)(3\ 4) \rangle$.

1.8. Dokazati da je svako upotpunjenje rešivog **niza**, rešiv **niz** .

1.9.Dokazati: a) Simetrična grupa S_n je rešiva akko je $n \leqslant 4$

b) Alternirajuća grupa A_n je rešiva akko je $n \leqslant 4$.

Rešenje: a) $\underline{S}_1$: $S_1 = \{1\}$ *pa je* $\underline{S}_1 \rhd \{1\}$

$\underline{S}_2$: $S_2 = \{(1), (1\ 2)\}$, *pa je* $\underline{S}_2 \rhd \{1\}$

$\underline{S}_3$: $S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$,

$\underline{S}_3 \rhd \underline{G}_2 \rhd \{1\}$, *gde je* $G_2 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$

$\underline{S}_4$: $\underline{S}_4 \rhd A_4 \rhd V \rhd G_1 \rhd \{1\}$ *(v.zad. 1.7.)*

Prema tome, S_1, S_2, S_3 *i* S_4 *su rešive grupe.*

Neka je $n \geqslant 5$. *Kako je* A_n *jedina prava normalna podgrupa u* S_n *(v.zad.4.2.17.) a* A_n *je prosta grupa (videti teoremu 4.2.4.), to je*

$$S_n \rhd A_n \rhd \{1\}$$

jedini normalni niz za S_n. *Kako su faktori ovog niza grupe* C_2 *i* A_n, *a* A_n *nije Abel-ova grupa, to* S_n *nije rešiva grupa.*

b) Za n=1,2,3,4 grupa A_n *je rešiva, kao podgrupa rešive grupe* S_n *(v.zad. 1.13.).*

Neka je $n \geqslant 5$. *Ako je* A_n *rešiva grupa, tada je, s obzirom na to da je* S_n/A_n *takodje rešiva (jer je* $S_n/A_n \simeq C_2$*), prema zad. 1.14. rešiva i grupa* S_n. *To je, medjutim, u suprotnosti sa dokazanim pod a).*

1.10.Grupa T(n) regularnih trougaonih matrica reda n nad poljem F je rešiva. Dokazati.

Rešenje: Označimo sa UT(n) podgrupu trougaonih matrica sa jedinicama na glavnoj dijagonali. Neposredno se proverava da je $UT(n) \lhd T(n)$ *i da je grupa T(n)/UT(n) izomorfna grupi D(n) dijagonalnih matrica. Grupa D(n) je Abel-ova, pa stoga i rešiva, a grupa UT(n) je nilpotentna (v.zad. 2.16.), dakle opet rešiva (v.zad. 2.13.). Koristeći zad. 1.14., odavde sledi rešivost i grupe T(n).*

1.11.Dokazati da su dijedarske grupe D_n rešive.

Rešenje: U dijedarskoj grupi $D_n = \langle a, b; a^n = b^2 = (ab)^2 = 1 \rangle$ *je podgrupa* $A = \langle a \rangle$ *ciklična i indeksa 2. Znači da je niz* $\{1\} \lhd A \lhd G$ *rešiv.*

1.12.Dokazati da je konačna grupa rešiva akko ima kompozicioni niz čiji su faktori ciklične grupe prostog reda.

Rešenje: U literaturi se najčešće rešivost konačnih grupa definiše na ovaj način. Zatim se dokazuje da je uslov iz definicije 1.6. potreban i dovoljan. ($\Leftarrow$) *Neka grupa G ima kompozicioni niz čiji su faktori (ciklične) grupe prostog reda. Tada su ti faktori i Abel-ovi, tj. G je rešiva grupa.*

($\Rightarrow$) Neka je G konačna rešiva grupa. Tvrdjenje:

Kompozicioni faktori grupe G su ciklične grupe prostog reda,

dokazujemo indukcijom po $|G|$.

Za $|G|=1$ i $|G|=p$ (p je prost broj), tvrdjenje sledi neposredno.

Dokažimo prvo da svaka (konačna) rešiva grupa G za koju je $|G|\neq 1$ i $|G|\neq p$ (p je prost broj), ima pravu normalnu podgrupu H.

Ako G nije Abel-ova, a ima Abel-ove faktore u normalnom nizu, to znači da je dužina tog niza veća od 1, tj. postoji H, $H \lhd G$.

Ako je G Abel-ova, ona ima pravu (normalnu) podgrupu H (osim u slučajevima da je $|G|=1$ ili $|G|=p$).

Indukcijska pretpostavka: neka sve rešive grupe čiji je red manji od n imaju kompozicione faktore koji su prostog reda.

Neka je $|G|=n$. Prema gornjoj pretpostavci, za H ($H \lhd G$) i G/H postoje ovakvi kompozicioni nizovi

$$\{1\} = H_0 \lhd H_1 \lhd \ldots \lhd H_k = H$$

$$\{1\} = F_0 \lhd F_1 \lhd \ldots \lhd F_j = G/H$$

(faktori su prostog reda). Neka je $f : G \to G/H$ prirodni homomorfizam. Tada za svaku podgrupu F_i ($i=0,1,\ldots,j$) iz G/H postoje podgrupe A_i iz G takve da je: $(\forall i \leq j)(H \prec A_i \wedge A_i/H \simeq F_i)$.

Označimo $f^{-1}(F_i) = A_i$. *Pri tom je* $f^{-1}(F_0) = f^{-1}(\{1\}) = H$.

Sada možemo konstruisati kompozicioni niz za G, sa traženim svojstvom:

$$\{1\} = H_0 \lhd H_1 \lhd \ldots \lhd H_k \lhd A_1 \lhd \ldots \lhd A_j = G$$

($H_k = H = A_0$).

1.13. Ako je G rešiva grupa, dokazati da su rešive:

a) Sve podgrupe grupe G , b) Sve faktor-grupe grupe G .

Rešenje: a) Neka je

$$\{1\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G \qquad (1)$$

gde su G_{j+1}/G_j Abel-ove grupe ($j=0,1,\ldots,n-1$), rešivi niz za grupu G, i neka je $H \prec G$.

Označimo sa $H_i = H \cap G_i$ ($i=0,1,\ldots,n$); za ove podgrupe grupe H je ispunjeno sledeće: zbog $H_{i+1} \prec G_{i+1}$, $G_i \lhd G_{i+1}$ ($i=0,1,\ldots,n-1$), prema Prvoj teoremi o izomofizmu je

$$H_{i+1} \cap G_i \lhd H_{i+1} \quad i \quad G_i H_{i+1}/G_i \simeq H_{i+1}/(G_i \cap H_{i+1}) .$$

Kako je $H_{i+1} \cap G_i = H \cap G_{i+1} \cap G_i = H_i \cap G_{i+1} = H_i$, *to je*

$$H_i \lhd H_{i+1} \quad i \quad H_{i+1}/H_i \simeq G_i H_{i+1}/G_i$$

Dakle,

$$\{1\} = H_0 \lhd H_1 \lhd \ldots \lhd H_n = H \qquad (2)$$

je normalni niz za grupu H.

Zbog $G_iH_{i+1} = G_i(H \cap G_{i+1}) \prec G_{i+1}$ *je* $G_iH_{i+1}/G_i \prec G_{i+1}/G_i$.
Po pretpostavci, grupe G_{i+1}/G_i *su Abel-ove, pa su Abel-ove i podgrupe* G_iH_{i+1}/G_i, *odnosno (njima izomorfne) podgrupe* H_{i+1}/H_i .
Dakle, niz (2) je rešivi niz grupe H.

b) Neka je G rešiva grupa čiji je rešivi niz (1). Neka je, dalje, $N \lhd G$; *jedan normalni niz grupe G koji "prolazi" kroz podgrupu N je*

$$\{1\} = N_0 \lhd N \lhd G \qquad (3)$$

Prema Schreier-ovoj teoremi, nizovi (1) i (3) imaju ekvivalentna upotpunjenja; prema zad. 1.8., upotpunjenje niza (1) je rešivi niz. Postoji, dakle rešivi red koji je upotpunjenje niza (3) i koji je ekvivalentan upotpunjenju niza (1):

$$\{1\} \lhd \ldots \lhd N \lhd H_1 \lhd H_2 \lhd \ldots \lhd H_k = G \ .$$

Uvedimo oznaku $N = H_0$. *Tada, za* $i=0,1,\ldots,k-1$ *imamo:*

$$N \lhd H_i \ , \quad N \lhd H_{i+1} \ , \quad H_i \lhd H_{i+1} \ .$$

Odavde, prema Drugoj teoremi o izomorfizmu sledi

$$H_i/N \lhd H_{i+1}/N \quad i \quad (H_{i+1}/N)/(H_i/N) \simeq H_{i+1}/H_i \ .$$

Prema tome, niz

$$\{1\} = N/N \lhd H_1/N \lhd \ldots \lhd H_k/N = G/N \qquad (4)$$

je normalan za grupu G/N. Kako su H_{i+1}/H_i *Abel-ove grupe, Abel-ove su i* $(H_{i+1}/N)/(H_i/N)$, *tj. niz (4) je rešiv.*

1.14. Neka je $N \lhd G$, i neka su N i G/N rešive grupe. Dokazati da je tada i G rešiva grupa.

Rešenje: Kao u zadatku 1.12., ako je

$$\{1\} = N_0 \lhd N_1 \lhd \ldots \lhd N_k = N \ , \quad \{1\} = K_0 \lhd K_1 \lhd \ldots \lhd K_j = G/N \ ,$$

tada je rešivi niz za G:

$$\{1\} \lhd N_1 \lhd \ldots \lhd \underbrace{N_k}_{f^{-1}(K_0)} \lhd f^{-1}(K_1) \lhd \ldots \lhd f^{-1}(K_j) = G$$

gde je $f : G \to G/N$ *prirodni homomorifzam.*

1.15. Ako je $G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{1\}$ normalni (rešivi) niz rešive grupe G, dokazati da je :

$G_i \rhd G^{(i)}$ $(i=0,1,\ldots,n)$, gde je $G^{(i)}$ i-ta izvedena grupa za G.

Uputstvo: Indukcijom po i.

1.16. Dokazati da je grupa G rešiva akko postoji $n \in N$ tako da je za n-tu izvedenu grupu $G^{(n)}$ grupe G ispunjeno $G^{(n)} \simeq \{1\}$.

Rešenje: ($\Rightarrow$) Ako je G rešiva grupa, sa rešivim nizom:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{1\},$$

prema zad. 1.15. je $G_i \rhd G^{(i)}$. *Dakle,* $G^{(n)} = \{1\}$.

(⇐) Ako je $G^{(n)} = \{1\}$, *tada normalni* ***niz*** $G \rhd G' \rhd \ldots \rhd G^{(n)} = \{1\}$ *ispunjava uslove definicije rešivih grupa.*

1.17.Dokazati da su rešive sledeće grupe:

a) Abel-ove, b) Grupa kvaterniona, c) Konačne p-grupe,

d) Grupe reda pq (p,q su prosti brojevi),

e) Grupe reda p^2 (p je prost broj).

Rešenje: a) Za svaku Abel-ovu grupu G postoji rešivi red: $\{1\} \lhd G$.

b) Videti zad. 1.7.b) , c) Indukcijom po $|G|$

d) Dokazati prvo da, ako je $p < q$, *G ima tačno jednu normalnu podgrupu reda q.*

e) Sve grupe reda p^2 *su Abel-ove, tj. prema a) rešive.*

1.18.Ako su A i B normalne rešive podgrupe grupe G, takva je i podgrupa AB. Dokazati.

Rešenje: Prema Prvoj teoremi o izomorfizmu je $A \cap B \lhd G$ *(odakle i* $A \cap B \lhd B$*) i* $AB/A \simeq B/(A \cap B)$. *Prema zad. 1.13. je* $B/(A \cap B)$ *rešiva grupa, pa je rešiva i grupa AB/A. Odavde, zbog zad. 1.14., je AB rešiva grupa.*

1.19.Ako su H i K normalne podgrupe grupe G, takve da su G/H i G/K rešive grupe, dokazati da je rešiva i grupa $G/(H \cap K)$.

1.20.Dokazati da je rešiva grupa koja ima kompozicioni niz, konačna.

Rešenje: Neka je G rešiva grupa, čiji je rešivi ***niz***

$$\{1\} = H_0 \lhd H_1 \lhd \ldots \lhd H_m = G .$$

Ovaj ***niz*** *i kompozicioni* ***niz*** *grupe G, koji po pretpostavci postoji, imaju zajedničko upotpunjenje - do na ekvivalentnost:*

$$\{1\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G \qquad (1)$$

Niz (1) je, dakle, kompozicioni i, prema zad. 1.8. rešivi ***niz*** *za G. Stoga su grupe* G_{i+1}/G_i *Abel-ove i proste (i=0,1,...,n-1); odnosno,* ***niz****ovi grupa* G_{i+1}/G_i *su prosti brojevi. Neka je* $|G_{i+1}/G_i| = q_i$ *(*q_i *su prosti brojevi, i=0,1,...,n-1). Tada,* $|G_1/G_0| = |G_1/\{1\}| = |G_1| = q_o$. *Dalje,* $|G_2/G_1| = q_1$, *tj.* $|G_2| = |G_1| \cdot |G_2 : G_1| = q_0 q_1$, *itd.* $|G| = |G_n| = q_0 q_1 \ldots q_{n-1}$.

1.21.Dokazati da je direktan proizvod konačnog broja rešivih grupa, rešiva grupa.

Rešenje: Neka je $G = G_1 \times G_2$; *tada* $G_1 \simeq G/G_2$. *Ako su rešive grupe* G_1 *i* G_2, tj. grupe G/G_2 i G_2, tada je, prema zad. 1.14. rešiva i grupa G.

9.2. CENTRALNI NIZ GRUPE I NILPOTENTNE GRUPE

Medju normalnim nizovima, pored kompozicionih i rešivih, važnu ulogu imaju i tzv. centralni nizovi grupe G.

2.1. *Definicija:* *Komutant podgrupa* A *i* B, *u oznaci* $[A,B]$ *je sledeća podgrupa u* G

$$[A,B] = \langle\, |\, a,b\, |\, \mid a\in A,\ b\in B \,\rangle .$$

2.2. *Definicija:* *Niz* $\{e\} = A_0 \lhd A_1 \lhd \ldots \lhd A_n = G$ *je centralni za grupu* G *ako je*

$$A_{i+1}/A_i < Z(G/A_i) \quad (i=0,1,\ldots,n-1) \qquad (1)$$

Da je ovako definisan niz zaista normalan, videti zadatak 2.6. Štaviše, svaka od podgrupa A_i je normalna u G.
Umesto uslova (1) često koristimo njemu ekvivalentan uslov

$$[A_{i+1},G] < A_i$$

(videti zadatak 2.5.).

Medju centralnim nizovima definišu se i tzv. *gornji* i *donji* centralni nizovi.

2.3. *Definicija:* *Grupa* G *ima donji centralni niz dužine* k

$$G = L_0 \rhd L_1 \rhd \ldots \rhd L_k \rhd L_{k+1} = \{e\}$$

ako je $L_{i+1} = [L_i,G]$, $(i=0,1,\ldots,k)$.

Da je donji centralni niz dobro definisan, tj. da je zaista centralni, dokazuje se u zad. 2.7.

2.4. *Definicija:* *Grupa* G *ima gornji centralni niz dužine* k

$$\{e\} = U_0 \lhd U_1 \lhd \ldots \lhd U_k = G$$

ako je $U_{i+1}/U_i = Z(G/U_i)$, $(i=0,1,\ldots,k-1)$.

U prethodnim definicijama "postoji donji (gornji) centralni niz grupe G" znači da postoji *konačan* takav niz, tj. da se u konačno mnogo koraka dolazi do grupe {e} (odnosno G). Generalniji pojmovi rastućih i opadajućih centralnih lanaca, u ovoj knjizi nisu korišćeni.
U zadatku 2.8. pokazuje se da je niz iz definicije 2.4. zbilja "gornji" medju svim centralnim redovima. Slično, zadatkom 2.9. ilustrovano je da je niz iz definicije 2.3. "donji".

2.5. *Definicija:* *Grupa* G *je nilpotentna ako je ispunjen jedan od sledeća tri ekvivalentna uslova:*

(i) postoji centralni niz grupe G
(ii) " donji centralni niz grupe G
(iii) " gornji " " " "

Minimalna dužina tih nizova je klasa nilpotencije.

Jedinična grupa {e} je klasa nilpotencije 0.
Da su gornja tri uslova zaista ekvivalentna, dokazuje se zadacima 2.8.i 2.9.
Nilpotentnost je takodje jedno uopštenje komutativnosti.
Ako **klase** svih Abel-ovih, rešivih i nilpotentnih grupa označimo redom sa $\mathcal{A}$, $\mathcal{R}$ i $\mathcal{N}$, tada je $\mathcal{A} \subseteq \mathcal{R} \subseteq \mathcal{N}$.

Primeri i zadaci

2.1. Dokazati da je za komutant $[A,B]$ podgrupa A i B grupe G ispunjeno sledeće:
a) $[A,B]=[B,A]$, b) Ako je $A \prec B$, tada $[G,A] \prec [G,B]$,
c) $[A,B]=\{e\}$ akko $A \prec C_G(B)$, d) $[A,G] \prec A$ akko $A \lhd G$,
e) $[A,B] \lhd \langle A,B \rangle$, f) Ako su $A,B \lhd G$, tada $[A,B] \lhd G$,
g) Ako su A i B karakteristične (potpuno invarijantne) podgrupe grupe G, tada je i podgrupa $[A,B]$ karakteristična (potpuno invarijantna) u G.

Rešenje: a) Neka je $a \in A$, $b \in B$. Tada $[a,b]^{-1}=(a^{-1}b^{-1}ab)^{-1}=b^{-1}a^{-1}ba=[b,a]$. Kako elementi $[a,b]^{-1}$ takodje generišu grupu $[A,B]$, tvrdjenje je dokazano.
d) Neka je $a \in A$, $g \in G$. Ako $[a,g] \in A$, tj. postoji $a' \in A$ tako da $a^{-1}g^{-1}ag=a'$, onda je $g^{-1}ag=aa' \in A$, tj. $A \lhd G$.
Obratno, iz $g^{-1}ag \in A$ sledi $a^{-1}g^{-1}ag \in A$, za svako $a \in A$, $g \in G$.
f) Neka su $a \in A$, $b \in B$, $g \in G$.
$g^{-1}[a,b]g = g^{-1}a^{-1}b^{-1}abg = g^{-1}a^{-1}gg^{-1}b^{-1}gg^{-1}agg^{-1}bg = [g^{-1}ag, g^{-1}bg] \in [A,B]$
(jer $g^{-1}ag \in A$, $g^{-1}bg \in B$).
g) Neka je $f : G \to G$ homomorfizam, i neka je $f(A) \prec A$, $f(B) \prec B$. Tada, za $a \in A$ $b \in B$: $f[a,b] = f(a)^{-1}f(b)^{-1}f(a)f(b) = [f(a),f(b)] \in [A,B]$.

2.2. Ako je $[A,G']=\{e\}$, dokazati da je $[A',G]=\{e\}$ (A', G' su tim redom komutanti grupa A i G).

2.3. Dokazati da je $[AB,C]=[A,C][B,C]$, **gde** su $A,B,C \lhd G$.

Rešenje: Kako je $[A,C] \prec [AB,C]$ i $[B,C] \prec [AB,C]$, to je i $[A,C]\,[B,C] \prec [AB,C]$.
Neka je, dalje, $a \in A$, $b \in B$, $c \in C$. Tada
$[ab,c] = b^{-1}a^{-1}c^{-1}acbb^{-1}c^{-1}bc = b^{-1}[a,c]b[b,c]$.

Odnosno, $[ab,c] \in b^{-1}[A,C]\,b\,[B,C]$. *Kako je* $[A,C] \lhd G$ *(v.zad. 2.1.f)), to je* $b^{-1}[A,C]\,b\,[B,C] = [A,C][B,C]$, *tj.* $[ab,c] \in [A,C][B,C]$, *ili*

$$[AB,C] < [A,C][B,C].$$

2.4. Neka je $G = H \times K$; dokazati:

a) Ako je $h_1, h_2 \in H$ i $k_1, k_2 \in K$, tada $[(h_1,k_1),(h_2,k_2)] = ([h_1,h_2],[k_1,k_2])$

b) Ako su $H_1, H_2 < H$ i $K_1, K_2 < K$, tada $[H_1 \times K_1, H_2 \times K_2] = [H_1,H_2] \times [K_1,K_2]$

2.5. Ako je $N \lhd G$ i $N < H < G$, dokazati da je $[H,G] < N$ akko $H/N < Z(G/N)$

Rešenje: Neka je $\phi : G \to G/N$ *prirodni homomorfizam.*

$(\Rightarrow)$ $[H,G] < N \Rightarrow (\forall h \in H)(\forall g \in G)\,\phi[h,g] = 1$

$\Rightarrow (\forall h \in H)(\forall g \in G)\,\phi(h)^{-1}\phi(g)^{-1}\phi(h)\phi(g) = 1$

$\Rightarrow (\forall h \in H)(\forall g \in G)\,\phi(h)\phi(g) = \phi(g)\phi(h)$

$\Rightarrow (\forall h \in H)\,\phi(h) \in Z(\phi(G))$

$\Rightarrow H/N < Z(G/N))$

$(\Leftarrow)$ *Neka je* $\phi(H) < Z(\phi(G))$. *Tada, za sve* $h \in H$, $g \in G$

$$\phi[h,g] = \phi(h)^{-1}\phi(g)^{-1}\phi(h)\phi(g) = \phi(h)^{-1}\phi(h)\phi(g)^{-1}\phi(g) = 1,$$

odnosno $[H,G] < N$.

2.6. Dokazati da je za članove A_i centralnog niza $\{e\} = A_0 < A_1 < \ldots < A_n = G$ ispunjeno: $A_i \lhd G$ $(i=0,1,\ldots,n)$.

Rešenje: Kako je $A_i < A_{i+1}$, *to je* $[A_i,G] \underset{①}{\leq} [A_{i+1},G] \underset{②}{\leq} A_i$.

① *prema 2.1.b)*

② *prema zad. 2.5. je* $A_{i+1}/A_i < Z(G/A_i)$ *akko* $[A_{i+1},G] < A_i$

Dalje, $[A_i,G] < A_i \underset{③}{\Longleftrightarrow} A_i \lhd G$.

③ *koristeći 2.1.d).*

2.7. Dokazati da je za članove L_i donjeg centralnog niza $G = L_0 > L_1 > \ldots > L_k = \{e\}$ ispunjeno:

a) L_i $(i=1,2,\ldots,k-1)$ je potpuno invarijantna podgrupa u G,

b) $L_i/L_{i+1} < Z(G/L_{i+1})$, $i=0,1,\ldots,k-1$.

Rešenje: a) Indukcijom po dužini k donjeg centralnog ***niza.***

Kako je $L_i = [L_{i-1},G]$ $(i=1,2,\ldots,k)$, *to je za* $i=1$ $L_1 = [G,G] = G'$; *prema zad. 3.3.4.,* G' *je potpuno invarijantna.*

Neka je L_j *potpuno invarijantna, tj. neka je za proizvoljni homomorfizam* $\phi : G \to G$ *ispunjeno* $\phi(L_j) < L_j$. *Tada*

$$\phi(L_{j+1}) = \phi[L_j,G] \underset{①}{=} [\phi(L_j),\phi(G)] \underset{②\,③}{<} [L_j,G] = L_{j+1}$$

① ϕ *je homomorfizam, tj.* $\phi[a,b] = \phi(a^{-1}b^{-1}ab) = \phi(a)^{-1}\phi(b)^{-1}\phi(a)\phi(b)$
$= [\phi(a),\phi(b)]$

② $\phi(G) \prec G$ *i* $\phi(L_j) \prec L_j$ *(indukcijska pretpostavka)*

③ *prema zad. 2.1.b)*

b) Koristeći zadatak 2.5.

2.8. Ako je $\{e\}=A_0 \lhd A_1 \lhd \ldots \lhd A_n=G$ centralni niz minimalne dužine n za grupu G, tada G ima gornji centralni red takodje dužine n

$$\{e\}=U_0 \lhd U_1 \lhd \ldots \lhd U_n=G ,$$

pri čemu je $A_i \prec U_i$ za sve i=1,2,...,n . Dokazati.

Rešenje: Prema definicijama 2.3. i 2.4., za podgrupe A_i, U_i *važi:*

$$[A_{i+1},G] \prec A_i \qquad (*)$$
$$U_{i+1}/U_i = Z(G/U_i) \qquad i=0,1,\ldots,n-1 \qquad (**)$$

Dokaz izvodimo indukcijom po dužini k centralnog niza.

k=1 : $[A_1,G] \prec A_0$ *, tj.* $[A_1,G]=\{e\}$ *(jer je* $A_0=\{e\}$*). Odavde, prema 2.1.c) je* $A_1 \prec C_G(G)$*, tj.* $A_1 \prec Z(G)$*. Kako je* $U_1=Z(G)$*, to je* $A_1 \prec U_1$*.*

Neka je $A_k \prec U_k$ *, i neka je* $f : G \to G/U_k$

$$[A_{k+1},G] \underset{①}{\prec} A_k \underset{②}{\prec} U_k$$

① *prema (*)*

② *indukcijska pretpostavka*

Koristeći zad. 2.5., odavde sledi da je $A_{k+1}/U_k \prec Z(G/U_k)$ *; prema (**) je* $Z(G/U_k) = U_{k+1}/U_k$ *, odakle* $A_{k+1} \prec U_{k+1}$ *.*

Dakle, za svako k (k=1,...,n) je $A_k \prec U_k$*. Otud,* $A_n \prec U_n$*. Kako je* $A_n=G$*, iz* $G \prec U_n$ *sledi* $U_n=G$*. Dakle, G ima gornji centralni niz dužine m,* $m \leq n$*. Kako je po pretpostavci n najmanja dužina centralnog niza, m=n.*

2.9. Ako je $G=B_0 \rhd B_1 \rhd \ldots \rhd B_m=\{e\}$ centralni niz minimalne dužine m za grupu G, tada G ima donji centralni niz takodje dužine m

$$G=L_0 \rhd L_1 \rhd \ldots \rhd L_m=\{e\} ,$$

pri čemu je $L_i \prec B_i$ za sve i=1,2,...,n . Dokazati.

Rešenje: Za podgrupe B_i, L_i *važi:*

$$[B_i,G] \prec B_{i+1} \qquad (*)$$
$$L_{i+1} = [L_i,G] \qquad i=0,1,\ldots,m-1 \qquad (**)$$

Indukcijom po dužini k centralnog niza:

$$L_1 = [L_0,G] = [G,G] = G'$$
$$[B_0,G] \prec B_1 \text{ , tj. } G' \prec B_1 \text{ , odnosno } L_1 \prec B_1 .$$

Neka je $L_k \lhd B_k$. *Tada:* $L_{k+1} \underset{①}{=} [L_k, G] \underset{②}{\lhd} [B_k, G] \underset{③}{\lhd} B_{k+1}$

① *prema (**)*

② *prema indukcijskoj pretpostavci i primenom 2.1.b)*

③ *prema (*)*

Dakle, $L_m \lhd B_m$, *tj.* $L_m = \{e\}$ *(jer je* $B_m = \{e\}$*). Odnosno, grupa G ima donji centralni niz dužine m.*

2.10. Dokazati da su Abel-ove grupe nilpotentne.

Rešenje: Neka je G Abel-ova grupa. Ako je $|G|=1$, *G je nilpotentna klase 0. Ako je* $|G| \neq 1$, *tada je* $\{e\} = U_0 \lhd U_1 = G$ *gornji centralni niz za G (jer je* $U_1 = Z(G)$, *a* $Z(G) = G$ *ako je G Abel-ova grupa). Prema tome, netrivijalne Abel-ove grupe su nilpotentne, klase 1.*

2.11. Ako je G nilpotentna grupa, dokazati:

a) Svaka podgrupa H grupe G je nilpotentna

b) Svaka količnička grupa G/N, (N⊲G), je nilpotentna.

Rešenje: Neka je

$$G = L_0 \rhd L_1 \rhd \ldots \rhd L_k = \{e\} \qquad (*)$$

donji centralni niz nilpotentne grupe G.

a) Ako je $H \lhd G$, *ispitujemo postoji li donji centralni niz za H, tj. postoji li* $n \in N$, *tako da je* $H_n = \{e\}$ *i* $H_{i+1} = [H_i, H]$ $(i = 0, 1, \ldots, n-1 \; ; \; H_0 = H)$.

Dokažimo indukcijom da je za svako i, $H_i \lhd L_i$.

$i=0$: $H_0 \lhd L_0$ *(tj.* $H \lhd G$*)* ;

$i=1$: $H_1 \lhd L_1$ *(tj.* $H' \lhd G'$*)* ,

Neka je $H_i \lhd L_i$. *Tada :* $H_{i+1} = [H_i, H] \underset{① ②}{\lhd} [L_i, H] \underset{①}{\lhd} [L_i, G] = L_{i+1}$

① *prema 2.1.b)*

② *indukcijska pretpostavka .*

Prema tome je $H_k \lhd L_k$, *tj.* $H_k \lhd \{e\}$, *odakle* $H_k = \{e\}$. *Dakle, H ima donji centralni niz dužine manje ili jednake k, odnosno H je nilpotentna grupa.*

b) Uočimo grupe $f(L_0)$, $f(L_1)$, ..., $f(L_k)$, *gde je* $f : G \to G/N$ *prirodni homomorfizam . Ako isključimo eventualna ponavljanja medju njima, dobićemo niz dužine manje ili jednake k, koji je donji centralni za grupu f(G).*

2.12. Ispitati nilpotentnost sledećih grupa:

a) Grupe kvaterniona, b) Grupe $G = \langle (1\ 2\ 3), (4\ 5), (1\ 2) \rangle$

c) Grupe bez centra

Rešenje: a) K je nilpotentna klase 2

b) G nije nilpotentna, jer je $S_3 = \langle (1\ 2\ 3), (1\ 2) \rangle \lhd G$

c) G nije nilpotentna, jer ako je Z(G)={e}, tada su članovi gornjeg centralnog niza $U_1=\{e\}=U_2=\ldots$, tj. ne dostižu grupu G.

2.13. Dokazati da je svaka nilpotentna grupa rešiva.

Rešenje: Neka je G nilpotentna grupa klase n čiji je gornji centralni niz $\{e\}=U_0 \triangleleft U_1 \triangleleft \ldots \triangleleft U_k=G$. Kako je $U_{i+1}/U_i=Z(G/U_i)$, to su U_{i+1}/U_i Abel-ove grupe, pa je grupa G rešiva.

2.14. Dokazati dá nije svaka rešiva grupa nilpotentna.

Rešenje: Primer: grupa S_3 .
Prema zad. 1.9., S_3 je rešiva, ali nije rilpotentna, jer je grupa bez centra (v.zad. 2.12.c)).

2.15. Ispitati nilpotentnost grupa: a) S_n , b) A_n .

Rešenje: a) S_1 je nilpotentna klase 0 . S_2 je nilpotentna klase 1.
S_n, $n \geqslant 3$ nije nilpotentna (videti zadatke 4.2.18. i 2.13.)
b) A_1 i A_2 su nilpotentne klase 0. A_3 je nilpotentna klase 1 (jer je $A_3 \simeq C_3$).
A_n, $n \geqslant 4$ nije nilpotentna.

2.16. Dokazati da je grupa trougaonih matrica reda n nad poljem F, kod kojih su svi elementi na glavnoj dijagonali jednaki 1, nilpotentna.

Rešenje: Kao u zadatku 1.10., označimo grupu trougaonih matrica reda n (nad poljem F), kod kojih su svi elementi na glavnoj dijagonali jednaki 1 sa UT(n). Dalje, sa $UT^k(n)$ (k=1,2,...,n) označimo podgrupu ove grupe, koju čine matrice sa nulama na k-1 dijagonali iznad glavne (na glavnoj dijagonali su jedinice).
Očigledno je $UT^1(n)=UT(n)$, $UT^n(n)=\{e\}$, i za $A=\|a_{ij}\| \in UT^k(n)$ je $a_{ij} \neq 0$ samo ako je $i=j$ ili $i \leqslant j-k$. Dokažimo da je niz

$$UT(n)=UT^1(n) > UT^2(n) > \ldots > UT^n(n)=\{e\}$$

centralni.
Koristeći zad. 2.5. dovoljno je dokazati da je za sve $k \in \{1,\ldots,n-1\}$

$$\left[UT^k(n), UT(n)\right] < UT^{k+1}(n) \ .$$

Neka je $A=\|a_{ij}\| \in UT(n)$, $B=\|b_{ij}\| \in UT^k(n)$; dokažimo da $ABA^{-1}B^{-1} \in UT^{k+1}(n)$.
Označimo sa $C=\|c_{ij}\|=A^{-1}$, $D=\|d_{ij}\|=B^{-1}$, $U=\|u_{ij}\|=ABA^{-1}$. Tada je

$$u_{ij} \underset{①}{=} \sum_{i<p<q<j} a_{ip}b_{pq}c_{qj} \underset{②}{=} \sum_{i<p<j} a_{ip}c_{pj} + \sum_{i<p<q<j} a_{ip}b_{pq}c_{qj}$$

① *jer su A,B,C trougaone matrice*

② *suma je razdvojena na dva sabirka: za $p=q$ i $p<q$.*

Za ove dve sume važi: $\sum_{i\leqslant p\leqslant j} a_{ip}c_{pj} = \begin{cases} 1, & \text{za } i=j \\ 0, & \text{za } i\neq j \end{cases}$

$\sum_{i\leqslant p<q\leqslant j} a_{ip}b_{pq}c_{qj} \neq 0$ za $i<j-k$ (jer je $b_{pq}\neq 0$ samo za $p\leqslant q-k$).

Dakle, $u_{ij}\neq 0$ za $i=j$ ili $i\leqslant j-k$, odnosno $ABA^{-1}\in UT^k(n)$.

Dalje, $\sum_p b_{ip}d_{p,i+k} \overset{③}{=} b_{i,i+k} + d_{i,i+k} \overset{④}{=} 0$, tj.

$$d_{i,i+k} = -b_{i,i+k} \qquad (*)$$

③ $B,D\in UT^k(n)$

④ za $i\neq j$ je $\sum_p b_{ip}d_{pj}=0$

Zatim,

$$u_{i,i+k} = a_{ii}b_{i,i+k}c_{i+k,i+k} = b_{i,i+k} \qquad (**)$$

Slično se izvodi da je element na $(i,i+k)$-om mestu matrice UB^{-1} jednak

$$u_{i,i+k} + d_{i,i+k} \overset{⑤}{=} b_{i,i+k} - b_{i,i+k} = 0, \text{ za sve } i\in\{1,\ldots,n\}$$

⑤ primenom (*) i (**)

Dakle, $UB^{-1} = ABA^{-1}B^{-1}\in UT^{k+1}(n)$. Kako je grupa $[UT(n),UT^k(n)]$ generisana elementima oblika $ABA^{-1}B^{-1}$ ($A\in UT(n)$, $B\in UT^k(n)$), time je dokazano da ova grupa pripada $UT^{k+1}(n)$.

2.17. Dokazati da je grupa G nilpotentna klase 2 akko $G'\prec Z(G)$.

Rešenje: G je nilpotentna klase 2 $\overset{①}{\Leftrightarrow} L_2=\{e\} \overset{②}{\Leftrightarrow} [G',G]=\{e\} \overset{③}{\Leftrightarrow} G'\prec Z(G)$

① prema zad. 2.9.

② jer je $L_2=[L_1,G]=[G',G]$

③ prema zad. 2.5., gde je $H=G'$, $N=\{e\}$.

2.18. Ako su grupe H i G/H ($H\lhd G$), nilpotentne, da li je nilpotentna i grupa G?

Rešenje: Iz nilpotentnosti grupa H, ($H\lhd G$) i G/H ne sledi uvek nilpotentnost grupe G. Neka je, na primer, $G=S_3$ i $H=\{I,(1\ 2\ 3),(1\ 3\ 2)\}$. H je indeksa 2 u S_3, dakle je $H\lhd G$. Osim toga je $H\simeq C_3$, tj. H je nilpotentna. Dalje, $S_3/H\simeq C_2$, tj. S_3/H je nilpotentna. Medjutim, S_3 nije nilpotentna (videti rešenje zadatka 2.14.).

2.19. Dokazati da su nilpotentne sve konačne p-grupe.

Rešenje: Neka je G konačna p-grupa. Konstruišimo za nju gornji centralni **niz**. $U_0=\{e\}$. Kako je prema zad. 8.2.1. $Z(G)\neq\{e\}$, to je $U_1=Z(G)$. Dalje, $U_2/U_1=Z(G/U_1)$. S obzirom da je $G/Z(G)$ ponovo p-grupa, to je (opet koristeći zad. 8.2.1.) $Z(G/U_1)\neq\{e\}$. Prema tome je $U_2/U_1\neq\{e\}$, odnosno $U_1\prec U_2$. Slično i dalje, ako je $U_i\neq G$, $U_{i+1}/U_i=Z(G/U_i)$ ($\neq\{e\}$), sledi $U_i\prec U_{i+1}$. Kako je G konačna grupa, za neko n biće $U_n=G$, pa je

$$\{e\}=U_0 \lhd U_1 \lhd \ldots \lhd U_n=G$$

gornji centralni niz za G, tj. G je nilpotentna.

2.20. Ako je G nilpotentna grupa i $H \lneq G$, tada je $H \lneq N_G(H)$. Dokazati.

Rešenje: Kako je $x^{-1}Hx=H$ *ako* $x \in H$, *to je* $H < N_G(H)$. *Dokažimo stoga da nije* $H=N_G(H)$, *ako je H prava podgrupa nilpotentne grupe G.*

Neka je, naprotiv, $H=N_G(H)$. *Tada su svi članovi gornjeg centralnog niza grupe G*

$$\{e\}=U_0 \lhd U_1 \lhd \ldots \lhd U_k=G ,$$

podgrupe u H. Zaista, $U_0 < H$. *Ako* $U_i < H$, *tada iz* $[U_{i+1}, G] < U_i$ *sledi* $[U_{i+1}, H] < H$. *Dalje,*

$$(\forall x \in U_{i+1})(\forall h \in H)\, xhx^{-1}h^{-1} \in H \Leftrightarrow (\forall x \in U_{i+1})(\forall h \in H)\, xhx^{-1} \in H$$
$$\Leftrightarrow (\forall x \in U_{i+1})\, xHx^{-1} < H ,$$

odnosno, $U_{i+1} < N_G(H)=H$. *Odavde,* $U_k < N_G(H)$, *tj.* $G < H$, *odnosno G=H. Kako je to u kontradikciji sa pretpostavkom* $H \lneq G$, *to je zaista* $H \lneq N_G(H)$.

2.21. Dokazati da su dijedarske grupe D_n nilpotentne ako je n stepen broja 2.

Rešenje: Grupe D_{2^k} *su konačne 2-grupe, pa njihova nilpotentnost sledi prema zadatku 2.19.*

2.22. Ako je $F \lneq Z(G)$ i ako je G/F nilpotentna grupa, dokazati da je tada i grupa G nilpotentna.

Rešenje: Neka je G/F nilpotentna grupa klase n, čiji je donji centralni niz $G/F=L_0 \rhd L_1 \rhd \ldots \rhd L_n=\{e\}$, *i neka je* $f : G \to G/F$ *prirodni homomorfizam. Tada je*

$$L_0=G/F=f(G)$$
$$L_1=[f(G), f(G)]=f[G,G]$$
$$L_2=[L_1, f(G)]=f[[G,G],G]$$
$$\vdots$$

Posmatrajmo niz. $G=f^{-1}(L_0) \rhd f^{-1}(L_1) \rhd \ldots \rhd f^{-1}(L_n) \rhd \{e\}$

Kako je $f^{-1}(L_n)=F$ *i* $F \lneq Z(G)$, *to je ovaj niz donji centralni, dužine n+1, za grupu G.*

2.23. Dokazati da je u nilpotentnoj grupi G presek svake prave normalne podgrupe N sa centrom Z(G) netrivijalan.

2.24. Dokazati da je direktan proizvod konačnog broja nilpotentnih grupa, nilpotentna grupa.

Rešenje: Neka su A i B nilpotentne grupe, čiji su centralni nizovi

$$\{e\}=A_0 \lhd A_1 \lhd \dots \lhd A_n=A \qquad (1)$$

$$\{e\}=B_0 \lhd B_1 \lhd \dots \lhd B_m=B \qquad (2)$$

Popunimo niz za A (ako je n<m), ubacivanjem nepravih članova $A_i \lhd A_i \lhd \dots \lhd A_i$ $(1 \leqslant i \leqslant n)$, *tako da bude n=m. Konstruišimo zatim sledeći niz grupa*

$$A_0 \times B_0,\ A_1 \times B_1, \dots, A_n \times B_n .$$

Prema zad. 5.3.8. je $(A_i \times B_i) \lhd (A_{i+1} \times B_{i+1})$ $(i=0,1,\dots,n-1)$.

Dalje je $[A_i \times B_i, A \times B] = [A_i, A] \times [B_i, B]$ *(v.zad. 2.4.b))*

Kako je prema zad. 2.5. za članove nizova (1) i (2) ispunjeno

$$[A_i, A] \prec A_{i-1}, \quad [B_i, B] \prec B_{i-1},$$

to je $[A_i \times B_i, A \times B] \prec A_{i-1} \times B_{i-1}$.

Dakle, niz $\{e\}=A_0 \times B_0 \lhd A_1 \times B_1 \lhd \dots \lhd A_n \times B_n = A \times B$

je centralni za grupu $A \times B$, *tj.* $A \times B$ *je nilpotentna grupa.*

2.25. Konačna grupa G je nilpotentna akko je G direktan proizvod svojih p-podgrupa Sylow-a. Dokazati.

Rešenje: ($\Rightarrow$*) Neka je S proizvoljna p-podgrupa Sylow-a u grupi G. Neka je, dalje,* $N=N_G(S)$. *S obzirom da je G konačna grupa, može se dokazati da je za grupu N ispunjeno:* $N=N_G(N)$.

Primenom zadatka 2.20. dobijamo da N nije prava podgrupa u G, dakle N=G.

Iz $N_G(S)=G$ *sledi medjutim* $S \lhd G$.

Dakle, svaka p-podgrupa Sylow-a grupe G je normalna, pa s obzirom na Tre-ću teoremu Sylow-a, za svaki prost broj p za koji je ispunjeno $p \mid |G|$, *G ima tačno jednu* S_p*-podgrupu. Ako su* $H_1, \dots, H_k$ *sve podgrupe Sylow-a u G, onda su ispunjeni uslovi definicije 5.1.2., pa je* $G \cong H_1 \times \dots \times H_k$.

($\Leftarrow$*) Kako je G konačna grupa, sve njene p-podgrupe Sylow-a su konačne. Prema zad. 2.19., te podgrupe su nilpotentne, a prema zad. 2.24. nilpotentan je i njihov direktan proizvod.*

10. SLOBODNE ALGEBRE

U izučavanju opštih algebarskih struktura naročito važnu ulogu ima pojam *slobodne algebre*. To naravno važi i za grupe, tako da postoje u savremenoj teoriji grupa čitave oblasti u kojima se kao glavno sredstvo koriste osobine i konstrukcije slobodnih grupa. Naime, reč je o predstavljanju grupa, slobodnom proizvodu grupa, problemu reči, odredjivanju varijete grupa, kao i o nekim drugim pojmovima i konstrukcijama. To je glavni razlog uključivanja ovakvog poglavlja u ovu knjigu, tim pre što se mnoge konstrukcije koje se odnose na grupe, bez velikih izmena prenose i na druge algebarske strukture.

10.1. UNIVERZALNE ALGEBRE I NJIHOV DIREKTAN PROIZVOD

Neka je n prirodan broj, $n>1$, i A neki skup. Pod n-arnom operacijom skupa A podrazumevamo svako preslikavanje $F : A^n \to A$. Broj n je *dužina* (arnost, broj argumentnih mesta) operacije F, i koristi se oznaka ar(F)=n. Ako je ar(F)=1 kažemo da je F unarna operacija, za ar(F)=2 binarna i za ar(F)=3 ternarna.

1.1.Definicija: Algebra ili algebarska struktura je svaka trojka $\underline{A}=(A,\Omega,C)$ *gde je* Ω *skup nekih operacija skupa A, a C je skup nekih konstanti iz A.*

Ukoliko je $\Omega=\{F_1,\ldots,F_m\}$, $C=\{a_1,\ldots,a_n\}$ piše se i $\underline{A}=(A,F_1,\ldots,F_m,a_1,\ldots,a_n)$. Slično, za $\Omega=\{F_i \mid i\in I\}$, $C=\{c_j \mid j\in J\}$, $\underline{A}=(A,F_i,a_j)_{i\in I,j\in J}$.

Algebra $\underline{A}$ čiji je domen A jednočlan skup je *trivijalna*, a ukoliko je $A=\emptyset$, *prazna* algebra.

Algebarski jezik je svaki skup $L=\mathcal{F}\cup\mathcal{C}$ sintaksnih objekata takvih da $\mathcal{F}\cap\mathcal{C}=\emptyset$. Elementi skupa $\mathcal{F}$ nazivaju se funkcijskim ili operacijskim znacima, a elementi skupa C simbolima konstanti. Na skupu $\mathcal{F}$ definisana je funkcija arnosti $Ar : \mathcal{F} \to \mathbb{N}\setminus\{0\}$.

Algebra jezika L je svaka algebra $\underline{A}=(A,\Omega,C)$ takva da je svakom $f\in\mathcal{F}$ dodeljena jedinstvena operacija $F=f^A$ skupa A za koju je ar(F)=Ar(f) ; svakom $c\in C$ pridružena je jedinstvena konstanta $c^A\in A$. Za $s\in L$, s^A se naziva *interpretacijom* simbola s.

Skup konstanti C jezika L označavaćemo i sa $Const_L$.

Algebre $\underline{A}$ i $\underline{B}$ su *istotipne* ukoliko su algebre istog jezika.

Podalgebra algebre $\underline{A}=(A,F_i,a_j)_{i\in I,j\in J}$ je svaki podskup $B\subseteq A$ takav da je $\underline{B}=(B,G_i,a_j)_{i\in I,j\in J}$ takodje algebra, gde je $G_i=F_i\restriction B^{ar(F_i)}$. Dakle, $a_j\in B$ i $G_i : B^n \to B$ za $i\in I$, $j\in J$, $n=ar(F_i)$.

Ubuduće dajemo definicije i teoreme uglavnom za algebre sa konačnim brojem operacija i konstanti, sa napomenom da se one po pravilu neposredno prenose na opšti slučaj.

1.2. *Definicija: Neka su* $\underline{A}=(A,F_1,\ldots,F_m,a_1,\ldots,a_n)$, $\underline{B}=(B,G_1,\ldots,G_m,b_1,\ldots,b_n)$ *istotipne algebre. Preslikavanje* $h : A \to B$ *je homomorfizam algebre* $\underline{A}$ *u algebru* $\underline{B}$ *akko za svaki* i, $1\leqslant i\leqslant m$, *važi*

$$(\forall x_1,\ldots,x_k\in A)h(F_i(x_1,\ldots,x_k))=G_i(h(x_1),\ldots,h(x_k)) ,$$

gde je $k=ar(F_i)$ *i za sve* j, $1\leqslant j\leqslant n$, $h(a_j)=b_j$.

Ako je h homomorfizam algebre $\underline{A}$ u algebru $\underline{B}$, tada koristimo oznaku $h : \underline{A} \to \underline{B}$. Ako je h preslikavanje redom na, 1-1, 1-1 i na, ili B=A, kažemo respektivno da je h *epimorfizam, monomorfizam (utapanje), izomorfizam, endomorfizam*. Ako je h endomorfizam i izomorfizam, tada se h naziva *automorfizmom*. Skupovi endomorfizama i automorfizama algebre $\underline{A}$ označavaju se redom sa End A , Aut A .

Direktan proizvod istotipnih algebri $\underline{A}$ i $\underline{B}$ je algebra $\underline{C}=\underline{A}\times\underline{B}$ definisana na sledeći način: $C=A\times B$, a za funkcijski znak f arnosti n

$$f^C((x_1,y_1),\ldots,(x_n,y_n))=(f^A(x_1,\ldots,x_n),f^B(y_1,\ldots,y_n))$$

gde $x_1,\ldots,x_n\in A$, $y_1,\ldots,y_n\in B$. Simbol konstante d interpretira se na sledeći *način:* $d^C=(d^A,d^B)$.

Na sličan način definiše se proizvod od n ($n\in N$, $n\geqslant 3$) algebarskih istotopnih struktura. Dajemo definiciju proizvoda proizvoljnog broja algebri.

1.3. *Definicija: Neka je* $\{\underline{A}_i \mid i\in I\}$ *familija istotipnih algebarskih struktura. Direktan proizvod* $\underline{A}=\prod_{i\in I}\underline{A}_i$ *je algebra odredjena na sledeći način:* $A=\prod_i A_i$; *ako je f operacijski znak dužine n i* $g_1,\ldots,g_n$ *iz* $\prod_i A_i$, *onda*

$$f^A(g_1,\ldots,g_n)=\langle f^{A_i}(g_1(i),\ldots,g_n(i)) \mid i\in I\rangle ;$$

ako je c simbol konstante tada $c^A=\langle c^{A_i} \mid i\in I\rangle$.

Preslikavanje $\pi_i : \prod_i A_i \to A_i$ odredjeno sa $\pi_i(g)=g(i)$ za $g\in\prod_i A_i$, naziva se *projekcijom*; napomenimo da je π_i homomorfizam algebre $\prod_i \underline{A}_i$ na $\underline{A}_i$.

Primeri i zadaci

1.1.Odrediti broj n-arnih operacija skupa A ukoliko je :

a) A konačan skup , b) A beskonačan skup .

Rešenje: $|\{f \mid f : A^n \to A\}| = |A|^{|A|^n}$. *Otuda, ako je* $|A|=k$ *imamo:*

a) $|A|^{|A|^n} = k^{k^n}$ *, ako je k konačan broj ,*

b) Ako je k beskonačan, $k^n = k$ *i* $k^k = 2^k$*, pa je* $|A|^{|A|^n} = 2^k$.

1.2.Dokazati da za svaki jezik L i svaki neprazan skup X postoji algebarska struktura jezika L čiji je domen X .

Rešenje: Neka je $a \in X$*. Jedna algebra* $\underline{A}$ *jezika L sa domenom X odredjena je sledećom interpretacijom: za* $c \in Const_L$ $c^A = a$ *; za funkcijski znak* $f \in L$ *dužine n neka je* $(\forall a_1,\ldots,a_n \in A) f^A(a_1,\ldots,a_n) = a$.

1.3.Neka su $\underline{A},\underline{B},\underline{C}$ istotipne algebre i $h : \underline{A} \to \underline{B}$, $g : \underline{B} \to \underline{C}$ homomorfizmi. Dokazati :

a) $g \circ h$ je homomorfizam algebre $\underline{A}$ u algebru $\underline{C}$;

b) Ako su g,h epimorfizmi, tada je i $g \circ h$ epimorfizam ;

c) Ako su g,h monomorfizmi, tada je i $g \circ h$ monomorfizam .

Rešenje: Ako je $c \in L$ *simbol konstante, tada* $(g \circ h)(c^A) = g(h(c^A)) = g(c^B) = c^C$.

Ako je $F \in L$ *n-arni funkcijski znak, tada za sve* $a_1,\ldots,a_n \in A$

$$(g \circ h)(F^A(a_1,\ldots,a_n)) = g(h(F^A(a_1,\ldots,a_n))) = g(F^B(h(a_1),\ldots,h(a_n))) =$$
$$F^C(g(h(a_1)),\ldots,g(h(a_n))) = F^C((g \circ h)(a_1),\ldots,(g \circ h)(a_n)) .$$

1.4.Ako je $\circ$ operacija slaganja funkcija, dokazati:

a) $(\mathrm{End}\,\underline{A}, \circ, I_A)$ je monoid ;

b) $(\mathrm{Aut}\,\underline{A}, \circ, I_A)$ je grupa .

Napomena: Ove algebarske strukture ubuduće kraće obeležavamo sa $\mathrm{End}\,\underline{A}$, $\mathrm{Aut}\,\underline{A}$.

Rešenje: Prema prethodnom zadatku: $g,h \in \mathrm{End}\,\underline{A} \Rightarrow g \circ h \in \mathrm{End}\,\underline{A}$.

Ako je $g \in \mathrm{Aut}\,\underline{A}$*, tada je* $g^{-1} \in \mathrm{Aut}\,\underline{A}$ *: Ako je* $c \in L$ *simbol konstante, onda* $g(c^A) = c^A$*, odakle* $c^A = g^{-1}(c^A)$*. Ako je F n-arni operacijski znak i* $a_1,\ldots,a_n \in A$*, tada, s obzirom da je g na, postoje* $b_1,\ldots,b_n \in A$ *takvi da* $g(b_i) = a_i$ *, dakle i* $g^{-1}(a_i) = b_i$ *. Otuda*

$$g^{-1}(F^A(a_1,\ldots,a_n)) = g^{-1}(F^A(g(b_1),\ldots,g(b_n))) = g^{-1}(g(F^A(b_1,\ldots,b_n))) =$$
$$F^A(b_1,\ldots,b_n) = F^A(g^{-1}(a_1),\ldots,g^{-1}(a_n)) ,$$

dakle, g^{-1} *je homomorfizam.*

1.5.Dokazati da je svaki monoid izomorfan monoidu $\mathrm{End}\,\underline{A}$ za neku algebru $\underline{A}$.

Rešenje: Neka je $\underline{S}=(S,\cdot,1)$ *monoid i* $\underline{A}=(A,f_a)_{a\in A}$ *algebra definisana na sledeći način:* $S=A$ *i za svaki* $a\in A$ *neka je* $(\forall x\in A)f_a(x)=xa$. *Dalje, neka je za svaki* $a\in A$ $h_a:A\to A$, *gde* $(\forall x\in A)h_a(x)=ax$. *Tada*

1° $h_a=h_b$ *akko* $a=b$, *jer iz* $h_a=h_b$ *sledi* $a=h_a(1)=h_b(1)=b$.

2° $h_a\in End\,\underline{A}$; *zaista,* $h_a(f_b(x))=a(xb)=(ax)b=f_b(h_a(x))$.

3° *Ako je* $g\in End\,\underline{A}$ *i* $a=g(1)$, *onda* $g=h_a$: $g(x)=g(f_x(1))=f_x(f(1))=f_x(a)=ax=h_a(x)$; *dakle* $End\,\underline{A}=\{h_a \mid a\in A\}$.

4° *Preslikavanje* $F:S\to End\,A$ *gde je* $(\forall a\in S)F(a)=h_a$ *je izomorfizam:* $F(ab)(x)=h_{ab}(x)=(ab)x=a(bx)=(h_a\circ h_b)(x)=(F(a)\circ F(b))(x)$, *tj.* $F(ab)=F(a)\circ F(b)$, *što znači da je F homomorfizam.*

Očigledno, F je <u>na</u>. *Dalje, ako je* $F(a)=F(b)$, *onda* $h_a=h_b$, *odakle prema* *1°* , $a=b$.

1.6.Dokazati da je svaka grupa izomorfna grupi Aut $\underline{A}$ za neku algebru $\underline{A}$.

Rešenje: Videti prethodna dva zadatka.

1.7.Ako je $\underline{A}$ najviše prebrojiva algebra, tada:

$$|\mathrm{Aut}\,\underline{A}|>\aleph_0 \Rightarrow |\mathrm{Aut}\,A|=2^{\aleph_0}.$$

Rešenje: Uvedimo najpre nekoliko pojmova koje koristimo u dokazu.

Konačna permutacija skupa A je svaka permutacija nekog konačnog podskupa od A. Dalje, neka je G grupa nekih permutacija skupa A, tj. $G<Sym(A)$.

Konačna permutacija p skupa A je produživa (u odnosu na G) ukoliko postoji $g\in G$ *tako da* $p\subseteq g$. *Najzad, grupa G je kompletna ukoliko zadovoljava uslov:*

Ako je $p_0\subseteq p_1\subseteq p_2\subseteq\ldots$ *lanac produživih konačnih permutacija i* $f=\bigcup_n p_n$ *je permutacija skupa A, onda* $f\in G$.

Prelazimo sada na dokaz samog tvrdjenja.

<u>*(T1)*</u>: *Ako je* $G=\mathrm{Aut}\,\underline{A}$, *tada je G kompletna grupa.*

Dokaz: Neka je $f=\bigcup_n p_n$ *gde je* $p_0\subseteq p_1\subseteq\ldots$ *lanac produživih konačnih permutacija i neka je* $f\in Sym(A)$. *Dalje, ako je F n-arna operacija algebre* $\underline{A}$ *i ako su* $a_1,\ldots,a_n\in A$, *onda s obzirom da je* $A=Dom(f)=\bigcup_n Dom(p_n)$, *postoji* $m\in\omega$ *tako da* $a_1,\ldots,a_n,F(a_1,\ldots,a_n)\in Dom(p_m)$. *Dalje,* p_m *je produživa, dakle postoji* $g\in\mathrm{Aut}\,\underline{A}$ *tako da* $p_m\subseteq g$. *Otuda*

$f(F(a_1,\ldots,a_n))=p_m(F(a_1,\ldots,a_n))=g(F(a_1,\ldots,a_n))=F(g(a_1),\ldots,g(a_n))=F(p_m(a_1),\ldots,p_m(a_n))=F(f(a_1),\ldots,f(a_n))$, *tj.* $f\in\mathrm{Aut}\,\underline{A}$.

<u>*(T2)*</u>: *Ako je G neprebrojiva i kompletna grupa permutacija prebrojivog skupa A, onda* $|G|=2^{\aleph_0}$.

Dokaz: Pokažimo najpre

Za svaki konačan niz $a_1,\dots,a_n$ elemenata skupa A,

postoji $g\in G$ tako da $g(a_i)=a_i$, $i=1,\dots,n$, $g\neq I_A$. (1)

Zaista, skup $\{(f(a_1),\dots,f(a_n))\mid f\in G\}$ je prebrojiv (jer je A^n prebrojiv), pa s obzirom da je G neprebrojiv, postoje $f_1,f_2\in G$ tako da $f_1\neq f_2$ i

$(f_1(a_1),\dots,f_1(a_n))=(f_2(a_1),\dots,f_2(a_n))$.

Tada $g=f_1^{-1}f_2$ ispunjava gornji uslov.

Dalje, tačno je sledeće:

Ako je p konačna produživa permutacija, tada postoje

različite konačne produžive permutacije q,r takve da (2)

$p\subsetneq q,r$.

Neka je $p=\begin{pmatrix}a_1 & \dots & a_n\\ b_1 & \dots & b_n\end{pmatrix}$. *Prema (1) postoji $g\in G$ tako da $g(a_i)=a_i$, $i=1,\dots,n$ i za neki $a\in A$ $g(a)\neq a$. Kako je p produživa permutacija, postoji $h\in G$ tako da $p\subseteq h$. Neka su*

$$q=\begin{pmatrix}a_1 & \dots & a_n & a\\ b_1 & \dots & b_n & h(a)\end{pmatrix}\qquad r=\begin{pmatrix}a_1 & \dots & a_n & a\\ b_1 & \dots & b_n & h(g(a))\end{pmatrix}.$$

Tada su q i r očigledno konačne permutacije skupa A, $p\subseteq q,r$ i q,r su produžive jer $q\subseteq h$, $r\subseteq h\circ g$. Ovim je (2) dokazano.

Najzad dokazujemo

Ako je p konačna produživa permutacija i $a\in A$, tada

postoji konačna produživa permutacija q tako da $p\subseteq q$ (3)

i $a\in Dom(q)\cap Im(q)$.

Zaista, ako je $p=\begin{pmatrix}a_1 & \dots & a_n\\ b_1 & \dots & b_n\end{pmatrix}$ *produživa, onda postoji $g\in G$ tako da $p\subseteq g$.*

Tada $q=p\cup\{(a,\ g(a)),\ (q^{-1}(a),\ a)\}$ **zadovoljava postavljene uslove.**

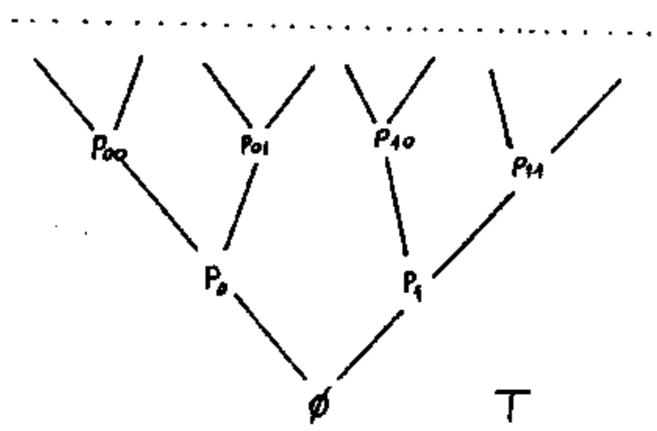
Neka je $A=\{a_1,a_2,\dots\}$. S obzirom da je $\emptyset$ permutacija praznog skupa a isto tako $\emptyset$ je produživa (svaki $g\in G$ produžuje $\emptyset$), koristeći (2) i (3) konstruiše se drvo T tako da je:

1° Uredjenje drveta T je inkluzija ;

2° Svaki član drveta T je konačna produživa permutacija ;

3° Ako je p_α član drveta T, onda $p_{\alpha 0}\neq p_{\alpha 1}$;

4° Ako je α niz (članova 0,1) dužine n, onda $a_n\in Dom(p_\alpha)\cap Im(p_\alpha)$.



Otuda, ako je γ grana drveta T i $f_\gamma=\bigcup_{p\in\gamma} p$, onda je f_γ permutacija skupa A, pa s obzirom da je G kompletna grupa sledi $f_\gamma\in G$. S druge strane, drvo T

ima $2^{\aleph_0}$ grana (koliko i funkcija iz skupa $A \to \{0,1\}$), pa sledi da je $\{f_\gamma \mid \gamma$ je grana drveta $T\}$ moći $2^{\aleph_0}$, dakle $|G| = 2^{\aleph_0}$. ∇

Prema (T1) i (T2) sledi tvrdjenje zadatka.

1.8. Ako su $\underline{B}_i$, $i \in I$, podalgebre algebre $\underline{A}$, dokazati da je i $\bigcap_i B_i$ podalgebra algebre $\underline{A}$.

Rešenje: Neka je $F \in L$ n-arni funkcijski znak i $a_1,\ldots,a_n \in \bigcap_i B_i$. Tada $(\forall i \in I)(a_1,\ldots,a_n \in B_i)$, pa kako su B_i podalgebre od $\underline{A}$, sledi

$$(\forall i \in I)(F^A(a_1,\ldots,a_n) \in B_i) \text{ , tj. } F^A(a_1,\ldots,a_n) \in \bigcap_i B_i .$$

Dakle, $\bigcap_i B_i$ je zatvoren za sve operacije algebre $\underline{A}$. Slično, za svaki simbol konstante $c \in L$, $c^A \in \bigcap_i B_i$.

1.9. Ako je $h : \underline{A} \to \underline{B}$ homomorfizam istotipnih algebri $\underline{A}$ i $\underline{B}$, dokazati da je $h(A)$ podalgebra algebre $\underline{B}$.

Rešenje: Neka je $h : \underline{A} \to \underline{B}$ homomorfizam i $D = h(A)$. Ako je $c \in L$ simbol konstante, onda $c^B = h(c^A)$, dakle $c^B \in D$.

Ako je f n-arni operacijski znak i $d_1,\ldots,d_n \in D$, tada za neke $a_1,\ldots,a_n \in A$ $d_i = h(a_i)$ i $f^B(d_1,\ldots,d_n) = f^B(h(a_1),\ldots,h(a_n)) = h(f^A(a_1,\ldots,a_n))$, tj. $f^B(d_1,\ldots,d_n) \in D$. Dakle, D je zatvoren za operacije algebre $\underline{B}$.

1.10. Neka je $h : \underline{A} \to \underline{B}$ utapanje algebre $\underline{A}$ u algebru $\underline{B}$. Dokazati:

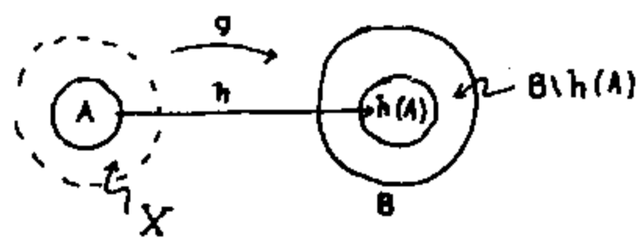
a) Postoji algebra $\underline{C}$, $\underline{C}$ je podalgebra algebre $\underline{B}$ i izomorfizam $f : \underline{A} \to \underline{C}$ tako da $f \subseteq h$.

b) Postoji algebra $\underline{D}$, $\underline{A}$ je podalgebra algebre $\underline{D}$ i izomorfizam $g : \underline{D} \xrightarrow{\sim} \underline{B}$ takav da $h \subseteq g$.

Rešenje: a) $\underline{C} = h(\underline{A})$ (videti prethodni zadatak).

b) Neka je X neki skup za koji je $X \cap A = \emptyset$, $|X| = |B \setminus h(A)|$.

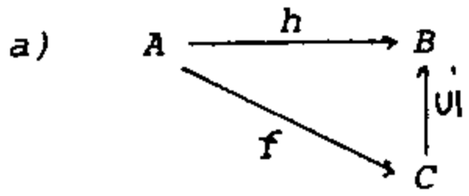
Dakle, postoji $g : A \cup X \xrightarrow[1-1]{na} B$ tako da $g \restriction A = h$ i $g \restriction X : X \xrightarrow[1-1]{na} B \setminus h(A)$.

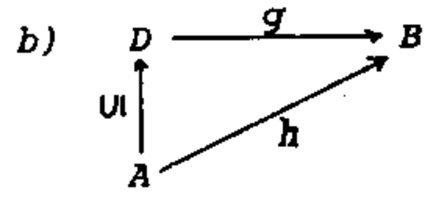


Neka je $D = A \cup X$, f n-arni funkcijski znak i $d_1,\ldots,d_n \in D$. Tada

$$f^D(d_1,\ldots,d_n) \overset{def}{=} g^{-1}(f^B(g(d_1),\ldots,g(d_n))), \quad c^D = c^A \text{ za } c \in Const_L .$$

Lako se pokazuje da je za ovako definisanu algebru $\underline{D}$, $g : \underline{D} \xrightarrow{\sim} \underline{B}$, $\underline{A} \subseteq \underline{D}$ i $h \subseteq g$. Dakle, sledeći dijagrami komutiraju:

a)


b)


1.11.Ako algebarski zakon u=v važi u svim algebrama $\underline{A}_i$ ($i\in I$) nekog jezika L, onda taj isti zakon važi i u proizvodu $\underline{A} = \prod_{i\in I} \underline{A}_i$. Dokazati.

Rešenje: Neka su $u(x_1,\ldots,x_n)$, $v(x_1,\ldots,x_n)$ *termi jezika L i pretpostavimo da zakon u=v važi u svim algebrama* $\underline{A}_i$, $i\in I$. *Tada za* $\underline{A} = \prod_i \underline{A}_i$ *i* $f_1,\ldots,f_n\in A$, *prema prethodnom zadatku, za svaki* $i\in I$ *važi*

$$\pi_i(u^A(f_1,\ldots,f_n))=u^{A_i}(\pi_i(f_1),\ldots,\pi_i(f_n))=u^{A_i}(f_1(i),\ldots,f_n(i))=$$
$$v^{A_i}(f_1(i),\ldots,f_n(i))=v^{A_i}(\pi_i(f_1),\ldots,\pi_i(f_n))=\pi_i(v^A(f_1,\ldots,f_n)) ,$$

odakle $u^A(f_1,\ldots,f_n) = v^A(f_1,\ldots,f_n)$.

1.12.Dokazati: projekcija $\pi_i : \prod_i \underline{A}_i \to \underline{A}_i$ je epimorfizam .

Rešenje: Preslikavanje π_i *je očigledno* <u>*na*</u>. *Dokazujemo da je* π_i *homomorfizam . Neka je* $\underline{A} = \prod_i \underline{A}_i$, $F\in L$ *n-arni operacijski znak i* $f_1,\ldots,f_n\in A$. *Tada*

$$\pi_i(F^A(f_1,\ldots,f_n))=\pi_i(\,<F^{A_i}(f_1(i),\ldots,f_n(i)) \mid i\in I>\,)\ ^{1)}=$$
$$F^{A_i}(f_1(i),\ldots,f_n(i))=F^{A_i}(\pi_i(f_1),\ldots,\pi_i(f_n)) .$$

1.13.Neka su $h_i : \underline{A}_i \to \underline{B}_i$, $i\in I$, homomorfizmi istotipnih algebri $\underline{A}_i, \underline{B}_i$. Dokazati da je preslikavanje $h : \prod_i A_i \to \prod_i B_i$ definisano sa

$$h(f) = <h_i(f(i)) \mid i\in I> \ , \quad f\in \prod_i A_i$$

homomorfizam proizvoda $\underline{A} = \prod_i \underline{A}_i$ u proizvod $\underline{B} = \prod_i \underline{B}_i$.

Rešenje: Neka je F n-arni operacijski znak i $f_1,\ldots,f_n\in A$. *Tada*

$$h(F^A(f_1,\ldots,f_n)) = h(\,<F^{A_i}(f_1(i),\ldots,f_n(i)) \mid i\in I>\,)$$
$$= \ <h_i(F^{A_i}(f_1(i),\ldots,f_n(i))) \mid i\in I> \quad ①$$
$$= \ <F^{B_i}(h_i(f_1(i)),\ldots,h_i(f_n(i))) \mid i\in I> \quad ②$$
$$= \ F^B(h(f_1),\ldots,h(f_n))$$

① *prema definiciji preslikavanja h*

② *jer su* h_i *homomorfizmi* .

1.14.Stepen algebre $\underline{A}$ je svaki proizvod $\prod_{i\in I} \underline{A}_i$, gde $(\forall i\in I)\underline{A}_i = \underline{A}$. Ovaj stepen označava se sa $\underline{A}^I$. Dokazati:

a) Ako je p permutacija skupa A tada je preslikavanje $g : \underline{A}^I \to \underline{A}^I$ definisano sa

---

1) $<f(i) \mid i\in I>$ je još jedna oznaka za funkciju $f : I \to X$. Dakle, $f = <f(i) \mid i\in I>$.

sano sa $g(f)=<f(p(i)) \mid i\in I>$ automorfizam algebre $\underline{A}^I$;

b) Ako je $|I|\geqslant 2$ tada $\underline{A}^I$ ima netrivijalan automorfizam.

Rešenje: a) Neka je $\underline{B}=\underline{A}^I$, *F n-arni operacijski znak i* $f_1,\ldots,f_n\in B$.

Tada $g(F^B(f_1,\ldots,f_n))=g(<F^A(f_1(i),\ldots,f_n(i) \mid i\in I>)$

$$=<F^A(f_1(p(i)),\ldots,f_n(p(i)) \mid i\in I>$$

$$=F^B(g(f_1),\ldots,g(f_n)) ,$$

tj. g je homomorfizam.

Primetimo da je $g(f)=f\circ p$, *pa kako je p permutacija, iz* $g(f_1)=g(f_2)$ *sledi* $f_1=f_2$, *tj. g je 1-1.*

Ako je $h\in B$, *onda* $g(h\circ p^{-1})=h$, *tj. g je* na .

b) Jedan netrivijalan automorfizam možemo dobiti prema a) ukoliko se izabere $p\neq I_B$ *i preslikavanje g kao u a)* .

1.15. Ako je I beskonačan skup i za svaki $i\in I$ je $|A_i|\geqslant 2$, dokazati da je $|\prod_i A_i|\geqslant 2^{\aleph_0}$.

Rešenje: Neka je $2=\{0,1\}$. *Kako je za svaki* $i\in I$ $|A_i|\geqslant 2$, *to postoje funkcije* $h_i : 2 \xrightarrow[1-1]{} A_i$. *Tada* $h : 2^I \xrightarrow[1-1]{} \prod_i A_i$ *gde za* $f\in 2^I$

$h(f)=<h_i(f(i)) \mid i\in I>$. *Otuda*

$|\prod_i A_i|\geqslant |2^I|=2^{|I|}\geqslant 2^{\aleph_0}$.

10.2. JEDNAKOSNE KLASE

Neka je $L=\mathcal{F}\cup\mathcal{C}$ algebarski jezik, gde je $\mathcal{F}$ skup funkcijskih znakova i $\mathcal{C}$ skup simbola konstanti. Niz $Term_n$ $(n\in N)$ definiše se induktivno na sledeći način:

$Term_0=Pr\cup\mathcal{C}$, gde je $Pr=\{x_0,x_1,\ldots\}$ skup promenljivih ;

$Term_{n+1}=Term_n\cup\{f(t_1,\ldots,t_k) \mid f\in\mathcal{F},\ ar(f)=k,\ t_1,\ldots,t_k\in Term_n\}$.

Skup *terma* (*izraza*) jezika L je $Term(L)=\bigcup_n Term_n$.

Ako je $t\in Term(L)$, *složenost terma t*, u oznaci $sl(t)$, je prirodan broj k+1 takav da $t\in Term_{k+1}\setminus Term_k$. Ako je $t\in Pr\cup\mathcal{C}$ onda $sl(t)=0$. Napomenimo da se većina dokaza o svojstvima terma t izvodi indukcijom po složenosti tog terma. Ukoliko su sve promenljive koje se javljaju u termu u neke od promenljivih $x_1,\ldots,x_k$ onda koristimo oznaku $u(x_1,\ldots,x_k)$.

Pod *algebarskim zakonom* jezika L podrazumevamo svaku formulu oblika

u=v gde su u,v termi jezika L.

Neka je $\underline{A}$ algebra jezika $L=\mathcal{F}\cup\mathcal{C}$, u term jezika L i $x_1,\ldots,x_k$ promenljive koje se pojavljuju u termu u. Tada u odredjuje jedinstveno, tzv. *term-preslikavanje* $u^A : A^k \to A$. Vrednost preslikavanja u^A definiše se induktivno po složenosti terma u:

Neka su vrednosti promenljivih $x_1,\ldots,x_k$ redom $d_1,\ldots,d_k$; ako je sl(u)=0 i u je promenljiva x_i, tada $u^A=d_i$, a ukoliko je u simbol konstante c, tada $u^A=c^A$.

Neka je sl(u)=n+1; tada za neki $f\in\mathcal{F}$, $u_1,\ldots,u_k\in Term_n$, k=ar(f), $u^A=f^A(u_1^A,\ldots,u_k^A)$ [1]. U ovom slučaju vrednost terma u označavamo takodje sa $u^A(d_1,\ldots,d_k)$.

Algebra $\underline{A}$ *zadovoljava zakon* u=v akko
$(\forall x_1,\ldots,x_k\in A)u^A(x_1,\ldots,x_k)=v^A(x_1,\ldots,x_k)$.

2.1. *Definicija: Neka je Z neki skup algebarskih zakona algebarskog jezika L. Klasa $\mathcal{M}$ svih algebri jezika L je varijete ili jednakosna klasa (primitivna klasa, algebarska mnogostrukost) klase zakona Z akko svaka algebra $\underline{A}\in\mathcal{M}$ zadovoljava svaki zakon iz Z.*
Klasa algebri $\mathcal{M}$ je varijete jezika L ukoliko je $\mathcal{M}$ varijete za neku klasu zakona Z jezika L.

Varijete $\mathcal{M}$ je *trivijalan* akko $\mathcal{M}$ sadrži jedino trivijalnu algebru jezika L.

Bilo koji skup algebarskih znakova nazivaćemo ponekad i *algebarskom teorijom*, ili jednostavno *teorijom* (mada ovaj pojam može imati i neka druga značenja). Takodje, članove teorije nazivamo aksiomama te teorije.

---

[1] Ovde se koristi sledeća teorema o jedinstvenosti čitanja terma:
Za svaki term u, sl(u)=n+1, postoji jedinstven $f\in\mathcal{F}$, jedinstveni termi $u_1,\ldots,u_r$ složenosti n takvi da $u=f(u_1,\ldots,u_r)$.

Primeri i zadaci

2.1. Neka su $\underline{A}$, $\underline{B}$ algebre jezika L i $h : \underline{A} \to \underline{B}$ homomorfizam. Ako je $F(x_1,\ldots,x_n)$ term jezika L i F^A, F^B odgovarajuće term-operacije redom u algebrama $\underline{A}$, $\underline{B}$, tada je h homomorfizam algebre $(\underline{A},F^A)$ u algebru $(\underline{B},F^B)$.

Rešenje: Očigledno, dovoljno je dokazati

$$(\forall a_1,\ldots,a_n \in A)h(F^A(a_1,\ldots,a_n))=F^B(h(a_1),\ldots,h(a_n)) \qquad (1)$$

Tvrdjenje (1) dokazujemo indukcijom po složenosti terma F ; uz pretpostavku da su promenljivima $x_1,x_2,\ldots$ dodeljene vrednosti redom $a_1,a_2,\ldots$ razlikujemo sledeće slučajeve:

1° sl(F)=0 ; postoje tada dva podslučaja:

F je promenljiva x_i ; tada $h(F^A(a_1,\ldots,a_n))=h(a_i)=F^B(h(a_1),\ldots,h(a_n))$.

F je simbol konstante c ; tada $h(F^A(a_1,\ldots,a_n))=h(c^A)=c^B=F^B(h(a_1),\ldots)$

Primetimo da vrednosti funkcija F^A, F^B ne zavise od vrednosti svojih argumenata.

2° sl(F)=k+1 ; tada postoji m-arni ($m \leqslant n$) funkcijski znak f i termi $t_1,\ldots,t_m$ složenosti manje ili jednake k , pa je

$$\begin{aligned} h(F^A(a_1,\ldots,a_n)) &\overset{①}{=} h(f^A(t_1^A(a_1,\ldots,a_n),\ldots,t_m^A(a_1,\ldots,a_n))) \\ &\overset{②}{=} f^B(h(t_1^A(a_1,\ldots,a_n)),\ldots,h(t_m^A(a_1,\ldots,a_n))) \\ &\overset{③}{=} f^B(t_1^B(h(a_1),\ldots,h(a_n)),\ldots,t_m^B(h(a_1),\ldots,h(a_n))) \\ &\overset{①}{=} F^B(h(a_1),\ldots,h(a_n)) \end{aligned}$$

① *prema induktivnoj definiciji vrednosti terma*

② *jer je h homomorfizam*

③ *prema induktivnoj hipotezi*

2.2. Neka je Z skup celih brojeva, F unarni operacijski simbol i jezik L={+,F}.

a) Dokazati da postoji formula predikatskog računa prvog reda jezika L koja definiše operaciju množenja u algebri $(Z,+,F^Z)$ ako je $F^Z(x)=x^2$.

b) Ne postoji term t jezika L tako da je $x\cdot y=t^Z(x,y)$, $x,y\in Z$, ukoliko je $F^Z(x)=x^2$.

c) Ne postoji formula predikatskog računa prvog reda jezika L koja definiše operaciju množenja u Z ako je $F^Z(x)=x^3$.

Rešenje: a) U strukturi celih brojeva važi ekvivalencija

$$z=x\cdot y \Leftrightarrow (x+y)^2=x^2+2z+y^2 .$$

Dakle, formula $\phi(x,y,z)$: $F(x+y)=F(x)+F(y)+z+z$

definiše operaciju množenja u $(Z,+,F^Z)$.

b) Ukoliko je $t(x_1,\ldots,x_n)$ *term jezika L, tada je*

$\frac{\partial t}{\partial x \partial y}(0,\ldots,0)$ *deljiv sa 2 , dok* $\frac{\partial xy}{\partial x \partial y}=1$.

c) Preslikavanje $f: x \to -x$ *je automorfizam algebre* $(Z,+,F^Z)$ *, ali nije automorfizam algebre* $(Z,+,F^Z,\cdot)$ *(videti prethodni zadatak) .*

2.3.Dokazati da je svaki varijete neprazan.

Rešenje: Svaki varijete sadrži trivijalnu algebru.

2.4.Neka je $\mathcal{M}$ varijete. Dokazati:

a) Ako $\underline{A}\in\mathcal{M}$ i $\underline{B}$ je podalgebra algebre $\underline{A}$, tada $\underline{B}\in\mathcal{M}$;

b) Ako $\underline{A}\in\mathcal{M}$ i $\underline{B}$ je homomorfna slika algebre $\underline{A}$, tada $\underline{B}\in\mathcal{M}$;

c) Ako za svaki $i\in I$ $\underline{A}_i\in\mathcal{M}$, tada $\prod_i \underline{A}_i\in\mathcal{M}$.

Rešenje: Neka je $u(x_1,\ldots,x_n)=v(x_1,\ldots,x_n)$ *zakon jezika L.*

a) Ako je $\underline{B}\subseteq\underline{A}$ *i* $b_1,\ldots,b_n\in B$ *, onda za svaki term* $t(x_1,\ldots,x_n)$ *jezika L važi* $t^B(b_1,\ldots,b_n)=t^A(b_1,\ldots,b_n)$.

b) Videti zadatak 2.1.

c) Videti zadatak 1.11.

2.5.Dokazati da svaki netrivijalni varijete sadrži beskonačnu algebru.

Rešenje: Ako je $\underline{A}\in\mathcal{M}$ *i* $|A|\geq 2$*, onda prema prethodnom zadatku* $\underline{A}^N\in\mathcal{M}$ *(N je skup prirodnih brojeva).*

2.6.Neka je $\mathcal{M}$ varijete, $\underline{A}\in\mathcal{M}$ konačna algebra, $|A|>1$. Dokazati da $\mathcal{M}$ sadrži beskonačno mnogo konačnih neizomorfnih algebri.

Rešenje: Ako je $\underline{A}\in\mathcal{M}$ *konačna netrivijalna algebra, tada* $\underline{A}^2$, $\underline{A}^3,\ldots\in\mathcal{M}$ *i za* $i\neq j$ *je* $\underline{A}^i\not\cong\underline{A}^j$.

2.7.Neka je $\mathcal{M}$ netrivijalan varijete nekog najviše prebrojivog jezika. Dokazati da za svaku algebru $\underline{A}$ i svaki $X\subseteq A$, postoji algebra $\underline{B}\subseteq\underline{A}$ takva da $X\subseteq B$ i $|B|\leq\max(\aleph_0,|X|)$.

Rešenje: Neka je $X\subseteq A$ *i* $\underline{B}$ *podalgebra od* $\underline{A}$ *generisana skupom X. Neposredno se proverava da je*

$$B=\{t^A(a_1,\ldots,a_n)\mid t(x_1,\ldots,x_n)\in Term(L),\ n\in N,\ a_1,\ldots,a_n\in X\} \qquad (1)$$

Naime, dovoljno je proveriti sledeće:

1° Svaka podalgebra algebre $\underline{A}$ *koja sadrži skup X, sadrži skup sa desne strane jednakosti (1) ; označimo taj skup sa Y .*

2° Y je podalgebra algebre $\underline{A}$.

Neka je $S_\omega(X)$ skup svih nizova $\langle a_n \mid n\in N\rangle$ čiji elementi pripadaju skupu X, s tim da je počev od nekog n, $a_n=a_{n+1}=\ldots$

Prema (1), preslikavanje $h : Term(L) \times S_\omega(X) \to B$

definisano sa $h(t,\bar{x})=t(x_{i1},\ldots,x_{in})$ *, gde su* $x_{i1},\ldots,x_{in}$ *promenljive koje imaju pojavljivanja u termu t, jeste* <u>na</u>.

Dakle, $|B| \leqslant |Term(L) \times S_\omega(X)|$.

Kako je $|Term(L)|=\aleph_0$, $|S_\omega(X)|=max(\aleph_0,|X|)$ *, tvrdjenje sledi.*

<u>Napomena</u>: *Iz ovog zadatka lako je izvesti sledeću interesantnu posledicu: Ako je* $\mathcal{M}$ *netrivijalni varijete i* $|L| \leqslant \aleph_0$ *, onda za svaki beskonačni kardinal k,* $\mathcal{M}$ *sadrži algebru kardinalnosti k.*

2.8. Sledeće klase algebri predstaviti kao jednakosne klase. Odrediti pripadne jezike: a) Grupe , b) Prsteni ,
c) Vektorski prostori nad poljem realnih brojeva ,
d) Mreže ,

Rešenje: c) Jedna mogućnost : $L=\{+,-,0\} \cup \{\bar{r} \mid r\in R\}$ *, gde je* $\bar{r}$ *unarni operacijski znak . Aksiome su :*

1° Aksiome Abel-ovih grupa za +,−,0 ;

2° Za svaku trojku realnih brojeva (r,s,u) :

$\bar{r}(x)+\bar{s}(x)=\bar{u}(x)$ *, ako je* $r+s=u$,

$\bar{r}(\bar{s}(x))=\bar{u}(x)$ *, ako je* $r\cdot s=u$,

$\bar{1}(x)=x$

$\bar{r}(x+y)=\bar{r}(x)+\bar{r}(y)$.

d) $L=\{\wedge,\vee\}$. *Aksiome:*

$x\wedge y=y\wedge x$, $x\vee y=y\vee x$,

$x\wedge(x\vee y)=x$, $x\vee(x\wedge y)=x$,

$x\wedge x=x$, $x\vee x=x$,

$(x\wedge y)\wedge z=x\wedge(y\wedge z)$, $(x\vee y)\vee z=x\vee(y\vee z)$.

Ako se ovim aksiomama doda aksioma $x\wedge(y\vee z)=(x\wedge y)\vee(x\wedge z)$, *dobijaju se aksiome distributivnih mreža.*

2.9. Koje su od navedenih klasa algebri, jednakosne klase:
a) Ciklične grupe , b) Abel-ove grupe , c) Abel-ove grupe sa torzijom ,
d) Abel-ove grupe bez torzije , e) Polja .

Rešenje: a) Nije jednakosna klasa , *b) Jeste ,*

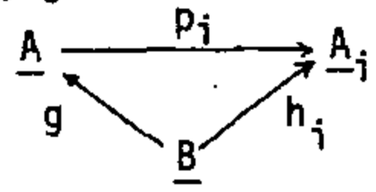
c) Nije jednakosna klasa, s obzirom da ova klasa algebri nije zatvorena za proizvode.

d) Nije varijete, jer ova klasa algebri nije zatvorena za homomorfizme ,

e) Nije varijete, jer polja nisu zatvorena za proizvode .

2.10. Neka je $\underline{A} = \prod_i \underline{A}_i$ proizvod familije algebri neke jednakosne klase $\mathcal{M}$. Dokazati da $\underline{A}$ ima sledeće svojstvo:

(*) Ako je $\underline{B} \in \mathcal{M}$ i $h_i : \underline{B} \to \underline{A}_i$ su homomorfizmi ($i \in I$), tada postoji jedinstveno preslikavanje $g : \underline{B} \to \underline{A}$ tako da za svaki $i \in I$ navedeni dijagram komutira, tj. $h_i = p_i \circ g$, ($p_i = \pi_i$).



Rešenje: Preslikavanje $g : B \to A$ definisano sa $g(b) = \langle h_i(b) \mid i \in I \rangle$, $b \in B$ ima navedeno svojstvo dijagrama.

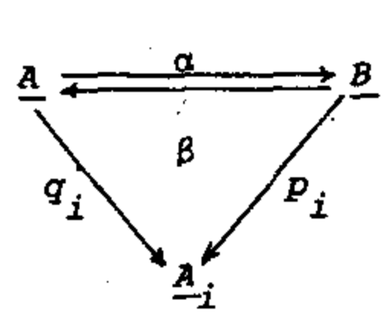
Ako je $g' : B \to A$ takodje preslikavanje sa ovim svojstvom, onda $(\forall b \in B)(p_i \circ g')(b) = h_i(b)$, $i \in I$, odakle $g'(b) = \langle h_i(b) \mid i \in I \rangle$.

2.11. Neka su $\underline{A}_i$ algebre jednakosne klase $\mathcal{M}$, $\underline{A} \in \mathcal{M}$ i $q_i : \underline{A} \to \underline{A}_i$ homomorfizmi sa svojstvom (*) iz prethodnog zadatka (uzimajući $q_i = p_i$). Dokazati da je $\underline{A} \simeq \prod_i \underline{A}_i$.

Rešenje: Neka je $\underline{B} = \prod_i \underline{A}_i$ i neka su $p_i : \underline{B} \to \underline{A}_I$, $i \in I$, projekcije.

Tada postoje homomorfizmi $\alpha : \underline{A} \to \underline{B}$,

$\beta : \underline{B} \to \underline{A}$ takvi da je: $p_i \circ \alpha = q_i$, $q_i \circ \beta = p_i$ ($i \in I$). Otuda, za $f \in B$ za svaki $i \in I$ važi



$p_i((\alpha \circ \beta)(f)) = (p_i \circ \alpha \circ \beta)(f) = (q_i \circ \beta)(f) = p_i(f)$;

dakle $(\alpha\beta)(f) = f$. Stoga

$$\alpha \circ \beta = I_B \qquad (1)$$

Dalje, $q_i \circ \beta \circ \alpha = q_i$, $q_i \circ I_A = q_i$, pa prema uslovu jedinstvenosti sledi

$$\beta \circ \alpha = I_A \qquad (2)$$

Iz (1) i (2) je sada $\alpha : \underline{A} \xrightarrow{\sim} \underline{B}$.

2.12. Neka je $\mathcal{M}$ klasa periodičnih Abel-ovih grupa. Dokazati da $\mathcal{M}$ nije zatvorena za proizvode algebri, ali za ma koju familiju $\underline{A}_i \in \mathcal{M}$ postoji algebra $\underline{A} \in \mathcal{M}$ sa svojstvom (*) iz zadatka 2.10.

Rešenje: Neka su $\underline{A}_i \in \mathcal{M}$, $i \in I$. Dalje, neka je $\underline{A} \subset \prod_i \underline{A}_i$,

$A = \{f \in \prod_i A_i \mid f$ je konačnog reda u $\prod_i A_i\}$.

Tada $\underline{A} \in \mathcal{M}$ i $\underline{A}$ zajedno sa projekcijama $\pi_i : \underline{A} \to \underline{A}_i$ ($i \in I$) zadovoljava uslov (*).

S druge strane, ciklične grupe C_n ($n \in N$) pripadaju $\mathcal{M}$, dok $\prod_n C_n \notin \mathcal{M}$.

10.3. SLOBODAN PROIZVOD ALGEBRI

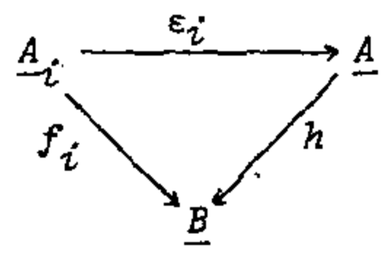
U prethodnom poglavlju uverili smo se da proizvod algebri u nekoj jednakosnoj klasi ima strukturno svojstvo (*) (videti zadatak 2.10.). Ukoliko se ovo svojstvo dualizuje, tj. okrenu strelice u dijagramu (*), onda dobijamo nov koncept, *slobodan proizvod algebri*[1].

3.1. Definicija: Neka je $\mathcal{M}$ klasa nekih istotipnih algebri i neka su $\underline{A}_i \in \mathcal{M}$, $i \in I$. Algebra $\underline{A} \in \mathcal{M}$ je slobodan proizvod u $\mathcal{M}$ algebri $\underline{A}_i$ ukoliko važi:

Postoje monomorfizmi $\varepsilon_i : \underline{A}_i \to \underline{A}$ takvi da

(i) Algebra $\underline{A}$ je generisana skupom $\bigcup_i \varepsilon_i(A_i)$

(ii) Ako je $\underline{B}$ algebra u $\mathcal{M}$ i $f_i : \underline{A}_i \to \underline{B}$ su homomorfizmi za $i \in I$, tada postoji homomorfizam $h : \underline{A} \to \underline{B}$ takav da za svaki $i \in I$, $h \circ \varepsilon_i = f_i$.



U takvom slučaju kažemo, takodje, da $(\underline{A}, \varepsilon_i)_{i \in I}$ odredjuje slobodan proizvod.

Klasa algebri $\mathcal{M}$ je *zatvorena* za slobodne proizvode ukoliko za svaku familiju $\langle \underline{A}_i \mid i \in I \rangle$ algebri iz $\mathcal{M}$ postoji njihov slobodan proizvod $\underline{A} \in \mathcal{M}$. Sledeća teorema kazuje u kojem slučaju neka familija algebri $\underline{A}_i$, $i \in I$, ima slobodan proizvod u jednakosnoj klasi.

3.2. Teorema: Neka je $\mathcal{M}$ jednakosna klasa i $\underline{A}_i$, $i \in I$ neke njene algebre.

Familija algebri $\underline{A}_i$, $i \in I$, ima slobodan proizvod u $\mathcal{M}$ ako i samo ako postoji algebra $\underline{B} \in \mathcal{M}$ tako da se svaka algebra $\underline{A}_i$ utapa u $\underline{B}$.

Ukoliko je $\underline{A}$ slobodan proizvod algebri $\underline{A}_i$ ($i \in I$) u $\mathcal{M}$, tada se, očigledno, za algebru $\underline{B}$ iz teoreme može uzeti upravo algebra $\underline{A}$. Drugi, manje trivijalan deo dokaza navodimo u odeljku o slobodnim algebrama (videti zadatak 5.19.).

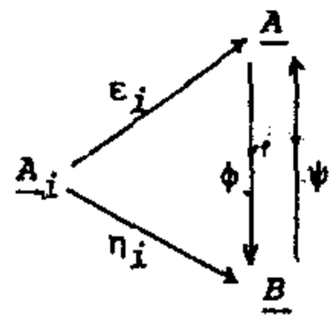
---

[1] Ovaj pojam uveo je R.Sikorski 1952. godine.

Primeri i zadaci

3.1. Ako je $\underline{A} \in \mathcal{M}$ slobodan proizvod algebri $\underline{A}_i$ $(i \in I)$ iz jednakosne klase $\mathcal{M}$, tada je on jedinstven do na izomorfizam. Dokazati.

Rešenje: Neka su $(\underline{A}, \varepsilon_i)_{i \in I}$ *i* $(\underline{B}, \eta_i)_{i \in I}$ *slobodni proizvodi algebri* $\underline{A}_i$ $(i \in I)$ *u jednakosnoj klasi* $\mathcal{M}$. *Tada postoje homomorfizmi* $\phi : \underline{A} \to \underline{B}$, $\psi : \underline{B} \to \underline{A}$ *takvi da* $\phi \circ \varepsilon_i = \eta_i$, $\psi \circ \eta_i = \varepsilon_i$. *Neka je* $b \in B$. *Algebra* $\underline{B}$ *generisana je sa* $\bigcup_i \eta_i(A_i)$, *pa za neki izraz* t *i* $a_1 \in A_1, \ldots, a_n \in A_n$ $(\underline{A}_1, \ldots, \underline{A}_n$ *su neke od algebri* $\underline{A}_i)$,



$$b = t^B(\eta_1(a_1), \ldots, \eta_n(a_n)) .$$

Otuda,
$$\psi(b) = \psi(t^B(\eta_1(a_1), \ldots, \eta_n(a_n)))$$
$$= t^A((\psi \circ \eta_1)(a_1), \ldots, (\psi \circ \eta_n)(a_n)) = t^A(\varepsilon_1(a_1), \ldots, \varepsilon_n(a_n)) .$$

Dalje,
$$(\phi \circ \psi)(b) = \phi(t^A(\varepsilon_1(a_1), \ldots, \varepsilon_n(a_n)) = t^B((\phi \circ \varepsilon_1)(a_1), \ldots, (\phi \circ \varepsilon_n)(a_n))$$
$$= t^B(\eta_1(a_1), \ldots, \eta_n(a_n)) = b .$$

Dakle, $\phi \circ \psi = I_B$. *Slično,* $\psi \circ \phi = I_A$, *pa su* ϕ, ψ *izomorfizmi.*

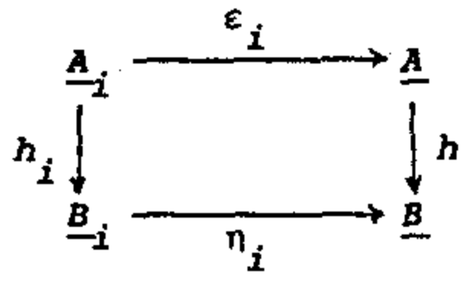
3.2. Neka su $\underline{A}_i, \underline{B}_i \in \mathcal{M}$ $(i \in I)$ i $\underline{A}, \underline{B} \in \mathcal{M}$ redom slobodni proizvodi algebri $\underline{A}_i$, $\underline{B}_i$ $(i \in I)$. Dalje, neka su $h_i : \underline{A}_i \to \underline{B}_i$ homomorfizmi. Dokazati da postoji homomorfizam $h : \underline{A} \to \underline{B}$ tako da važi

a) Ako je za svaki $i \in I$ h_i na, onda je h na.

b) Ako je za svaki $i \in I$ h_i 1-1, onda je h 1-1.

c) Ako je za svaki $i \in I$ h_i izomorfizam, onda je h izomorfizam.

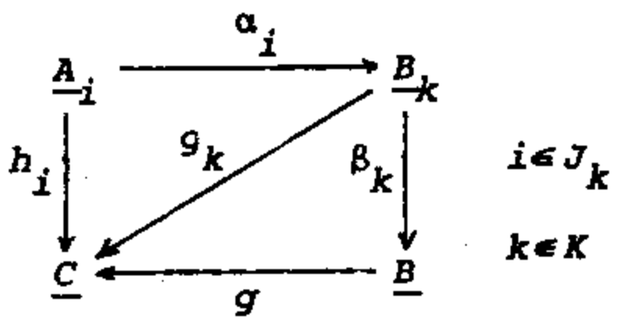
Rešenje: Ako su $(\underline{A}_i, \varepsilon_i)_{i \in I}$, $(\underline{B}, \eta_i)_{i \in I}$ *slobodni proizvodi i* $h_i : \underline{A}_i \to \underline{B}_i$ *homomorfizmi, tada postoji homomorfizam* $h : \underline{A} \to \underline{B}$ *tako da navedeni dijagram komutira, tj.* $h \circ \varepsilon_i = \eta_i \circ h_i$.
Dalje, slično kao u prethodnom zadatku.



3.3. Dokazati da je slobodan proizvod asocijativan: ukoliko je $\{J_k \mid k \in K\}$ particija skupa L, $\underline{A}_i \in \mathcal{M}$ za $i \in I$, $\underline{B}_k$ su slobodni proizvodi algebri $\underline{A}_j$, $j \in J_k$, $\underline{A}$ je slobodan proizvod algebri $\underline{A}_i$ i $\underline{B}$ je slobodan proizvod $\underline{B}_k$, $k \in K$, onda $\underline{A} \cong \underline{B}$.

Rešenje: Neka je $(\underline{B}_k, \alpha_i)_{i \in J_k}$ *slobodan proizvod algebri* $\underline{A}_i$, $i \in J_k$ *i neka je*

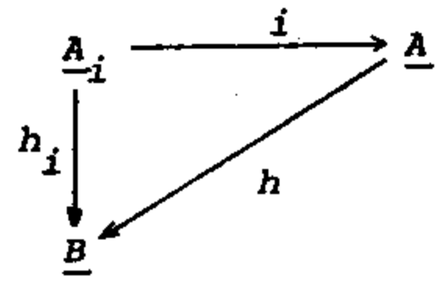
$(\underline{B}, \beta_k)_{k\in K}$ *slobodan proizvod algebri* $\underline{B}_k$, $k \in K$, *u varijeteu* $\mathcal{M}$. *Neka je* $\mathcal{C} \in \mathcal{M}$ *i neka su* $h_i : \underline{A}_i \to \underline{C}$ *homomorfizmi* $(i \in I)$. $(\underline{B}_k, \alpha_i)_{i\in J_k}$ *je slobodan proizvod, pa postoji homomorfizam* $g_k : \underline{B}_k \to \underline{C}$, *tako da* $g_k \circ \alpha_i = h_i$. *Slično, postoji homomorfizam* $g : B \to \underline{C}$ *tako da* $g \circ \beta_k = g_k$, $k \in K$, *tj.* $g \circ \beta_k \circ \alpha_i = h_i$.



Dakle, za $\varepsilon_{ik} = \beta_k \circ \alpha_i$, $i \in J_k$, $k \in K$, $(\underline{B}, \varepsilon_{ik})_{i\in J_k, k\in K}$ *je slobodan proizvod algebri* $\underline{A}_i$, $i \in I$, *pa* $\underline{B} \cong \underline{A}$.

3.4. Dokazati da je klasa konačnih Abel-ovih grupa zatvorena za konačne slobodne proizvode, ali ne i za beskonačne.

Rešenje: Slobodan proizvod Abel-ovih grupa $\underline{A}_i = (A_i, +, 0)$, $1 \leq i \leq n$, *je* $(\underline{A}, \varepsilon_i)_{i\leq n}$ *gde* $\underline{A} = \prod_i \underline{A}_i$, $\varepsilon_1(x) = (x, 0, \ldots, 0)$, $\varepsilon_2(x) = (0, x, 0, \ldots, 0)$, $\ldots$, $\varepsilon_n(x) = (0, \ldots, 0, x)$. *Ako su* $h_i : \underline{A}_i \to \underline{B}$ *homomorfizmi u Abel-ovu grupu* $\underline{B}$, *tada navedeni dijagram komutira za* $h : \underline{A} \to \underline{B}$ *gde* $h(x_1, \ldots, x_n) = h_1(x_1) + \ldots + h_n(x_n)$. *Primetimo da je* $h : \underline{A} \to \underline{B}$ *homomorfizam.*



Ukoliko je ova klasa algebri zatvorena za proizvoljne proizvode, onda postoji i proizvod $\underline{A}$ *cikličnih grupa* C_n, $n \in N$. *Tada* $|A| > |C_n| = n$ *za svaki prirodan broj n, tj.* $\underline{A}$ *nije konačna algebra.*

3.5. Dokazati da je varijete Abel-ovih grupa zatvoren za slobodne proizvode.

Rešenje: Ako su $\underline{A}_i$, $i \in I$, *Abel-ove grupe tada je* $(\underline{A}, \varepsilon_i)_{i\in I}$ *slobodan proizvod ovih grupa, gde* $\underline{A} = \sum_{i\in I} \underline{A}_i$, *tj.* $\underline{A} \subseteq \prod_i \underline{A}_i$,

$$A = \{f \in \prod_i A_i \mid f(i) \neq 0 \text{ za sve } i \in I \text{ osim konačno mnogo}\},$$

$$\varepsilon_i : A_i \to A, \quad \varepsilon_i(a)(j) = \begin{cases} 0, & \text{za } j \neq i \\ a, & \text{za } j = i \end{cases}$$

Dakle, slobodan proizvod grupa $\underline{A}_i$ *je* $\sum_i \underline{A}_i$.

3.6. Dokazati da su jednakosne klase grupa, monoida i prstena sa jedinicom, zatvorene za slobodne proizvode.

Rešenje: Prema teoremi 3.2. dovoljno je dokazati da u svakom od slučajeva za algebre $\underline{A}_i \in \mathcal{M}$ $(i \in I)$, *postoji algebra* $\underline{B}$ *koja sadrži izomorfne kopije svake od algebri* $\underline{A}_i$. *To svojstvo ima algebra* $\underline{B} = \prod_i \underline{A}_i$. *Utapanje* $h_i : \underline{A}_i \to \underline{B}$ *dato je sa*

$$h_i(a)(j) = \begin{cases} 1_j, & \text{za } j \neq i \\ a, & \text{za } j = i \end{cases}, \quad a \in A_i,$$

1_i *je jedinica algebre* $\underline{A}_i$.

3.7. Neka je $\underline{A}_i$, $i \in I$, familija Abel-ovih grupa, $|I| \geqslant 2$, tako da nijedna od grupa $\underline{A}_i$ nije trivijalna. Ako su $\underline{A}, \underline{B}$ slobodni proizvodi ovih algebri redom u jednakosnoj klasi grupa i jednakosnoj klasi Abel-ovih grupa, onda $\underline{A} \neq \underline{B}$.

Rešenje: Primetimo da je grupa $\underline{B}$ komutativna. Dokazaćemo da $\underline{A}$ nije komutativna grupa. Neka su $\underline{A}_i = (A_i, \cdot, 1)$ $(i=1,2)$ dve grupe iz familije $\underline{A}_i$ $(i \in I)$.

Odredimo grupu $\underline{C}=(C, \cdot, 1)$ na sledeći način:

- *C je skup svih reči oblika $a_1 b_1 \ldots a_n b_n$, $a_1, \ldots, a_n \in A_1$, $b_1, \ldots, b_n \in A_2$, gde $a_1, \ldots, a_n \neq 1$, $b_1, \ldots, b_n \neq 1$.*
- *Operacija $\cdot$ definisana je za $u, v \in C$ sa:*

ako $u = a_1 b_1 \ldots a_m b_m x_1 y_1 \ldots x_k y_k$, $v = y_k^{-1} x_k^{-1} \ldots y_1^{-1} x_1^{-1} c_1 d_1 \ldots c_n d_n$, $k \geqslant 1$, gde $a_i, x_i, d_i \in A_1$, $b_i, y_i, c_i \in A_2$ i $b_m c_1 \neq 1$, onda

$$u \cdot v = a_1 b_1 \ldots a_m b' d_1 c_2 \ldots d_{n-1} c_n d_n \text{ . gde } b' = b_m c_1 \text{ ,}$$

u svakom drugom slučaju $u \cdot v$ je nadovezivanje reči u, v .

Za grupu C očigledno važi:

1° Za $a \in A_1$, $b \in A_2$, ako $a, b \neq 1$ onda $a \cdot b \neq b \cdot a$.

2° Inkluzivna preslikavanja $h_i : A_i \to C$ $(i=1,2)$ su utapanja grupa $\underline{A}_i$ u $\underline{C}$.

3° Prema definiciji slobodnog proizvoda $(\underline{A}, \varepsilon_i)_{i \in I}$ postoji $h : \underline{A} \to \underline{C}$ tako da $h \circ \varepsilon_i = h_i$.

Dakle, $h(\varepsilon_1(a)\varepsilon_2(b)) = h(\varepsilon_1(a))h(\varepsilon_2(b)) = a \cdot b \neq b \cdot a = h(\varepsilon_2(b)\varepsilon_1(a))$, tj. $\varepsilon_1(a)\varepsilon_2(b) \neq \varepsilon_2(b)\varepsilon_1(a)$. Stoga $\underline{A}$ nije Abel-ova grupa, pa $A \neq B$.

10.4. KONGRUENCIJE

Relacija ekvivalencije $\sim$ skupa A je *kongruencija* algebre $\underline{A} = (A, F_1, \ldots, F_m, a_1, \ldots, a_n)$ akko za svaki i, $1 \leqslant i \leqslant m$, i $k = ar(F_i)$ važi

$$(\forall x_1, \ldots, x_k, y_1, \ldots, y_k \in A)(x_1 \sim y_1 \wedge \ldots \wedge x_k \sim y_k \Rightarrow F(x_1, \ldots, x_k) \sim F(y_1, \ldots, y_k))$$

4.1. Teorema: Neka su $\underline{A}$, $\underline{B}$ istotipne algebre i $H : \underline{A} \to \underline{B}$ homomorfizam. Tada je $\ker H = \{(x,y) \in A^2 \mid H(x) = H(y)\}$ kongruencija algebre $\underline{A}$.

Dokaz je dat u okviru zadatka 4.6.

Relacija $\ker H$ naziva se *jezgrom* preslikavanja H.

4.2. Teorema: Neka je $\underline{A} = (A, F_1, \ldots, F_m, a_1, \ldots, a_n)$ algebra i $\sim$ njena kongruencija. Tada je $\underline{B}$ $(B, G_1, \ldots, G_m, b_1, \ldots, b_n)$ istotipna algebra, ako je $B = A/\sim$, $b_j = a_j/\sim$ za $1 \leqslant j \leqslant n$, i za svaki i, $1 \leqslant i \leqslant n$, ako je $ar(F_i) = k$ onda $G_i(x_1/\sim, \ldots, x_k/\sim) = F_i(x_1, \ldots, x_k)/\sim$, $(x_1, \ldots, x_k \in A)$. Preslikavanje $h : A \to B$, $h(x) = x/\sim$ je homomorfizam algebre $\underline{A}$ na algebru $\underline{B}$.

Dokaz: Najpre pokažimo da su operacije $G_1,\dots,G_m$ algebre $\underline{B}$ dobro definisane. Neka su $x_1,\dots,x_n,y_1,\dots,y_n \in A$ tako da $x_i/\sim = y_i/\sim$ $(i=1,\dots,n)$. Tada $x_i \sim y_i$, pa $F(x_1,\dots,x_n) \sim F(y_1,\dots,y_n)$. Otuda $F(x_1,\dots,x_n)/\sim = F(y_1,\dots,y_n)/\sim$. Preslikavanje h je homomorfizam, jer

$$h(F_i(x_1,\dots,x_n)) = F_i(x_1,\dots,x_n)/\sim = G_i(x_1/\sim,\dots,x_n/\sim)$$
$$= G_i(h(x_1),\dots,h(x_n)) . \blacktriangledown$$

Algebra $\underline{B}$ iz prethodne teoreme označava se sa $\underline{A}/\sim$ i naziva se *količničkom algebrom*. Preslikavanje h naziva se *kanonskim* ili *prirodnim homomorfizmom*.

Primeri i zadaci

4.1. Ako su q_i, $i \in I$, kongruencije algebre $\underline{A}$, tada je $\bigcap_i q_i$ takodje kongruencija algebre $\underline{A}$. Dokazati.

Rešenje: Neka je $q = \bigcap_i q_i$.

Relacija q je refleksivna: ako je $a \in A$, *onda* aqa *jer* $(\forall i \in I)\, a\, q_i\, a$.

Relacija q je simetrična: ako $a,b \in A$ *i* $a\,q\,b$ *onda* $(\forall i \in I)\, a\, q_i\, b$, *odakle s obzirom na simetričnost relacija* q_i, *sledi* $(\forall i \in I)\, b\, q_i\, a$, *tj.* $b\,q\,a$

Relacija q je tranzitivna: Ako su $a,b,c \in A$ *i* $a\,q\,b$, $b\,q\,c$, *tada* $(\forall i \in I)(a\, q_i\, b \wedge b\, q_i\, c)$ *odakle sledi* $(\forall i \in I)\, a\, q_i\, c$, *tj.* $a\,q\,c$.

Najzad, dokažimo da je q saglasna sa operacijama algebre $\underline{A}$. *Neka je F n-arna operacija algebre* $\underline{A}$ *i* $a_1,\dots,a_n \in A$, $b_1,\dots,b_n \in A$ *tako da* $a_1\,q\,b_1$, $a_2\,q\,b_2$, …, $a_n\,q\,b_n$. *Tada za svaki* $i \in I$, $a_1\,q_i\,b_1,\dots,a_n\,q_i\,b_n$, *pa kako su relacije* q_i *saglasne sa operacijama algebre* $\underline{A}$, *sledi da je za svaki* $i \in I$ $F(a_1,\dots,a_n)\, q_i\, F(b_1,\dots,b_n)$, *tj.* $F(a_1,\dots,a_n)\, q\, F(b_1,\dots,b_n)$.

4.2. Neka su q,r kongruencije algebre $\underline{A}$. Dokazati da je $q \circ r$ kongruencija algebre $\underline{A}$ akko $q \circ r = r \circ q$.

Rešenje: Označimo sa Δ_A *tzv. dijagonalu skupa* A^2, *tj.* $\Delta_A = \{(x,x) \mid x \in A\}$.
Dalje, ako je $q \subseteq A^2$ *onda* $q^{-1} = \{(x,y) \mid (y,x) \in q\}$.
Neposredno se proverava da važi sledeće:

1° *q je refleksivna akko* $\Delta_A \subseteq q$;

2° *q je simetrična akko* $q^{-1} = q$;

3° *q je tranzitivna akko* $q \circ q \subseteq q$;

4° $(q \circ r)^{-1} = r^{-1} \circ q^{-1}$, $r \subseteq A^2$;

5° $q \subseteq r \Rightarrow q \circ t \subseteq r \circ t \wedge t \circ q \subseteq t \circ r$, $t \subseteq A^2$.

Dakle, $q\subseteq A^2$ je relacija ekvivalencije skupa A akko $\Delta_A\subseteq q$, $q^{-1}=q$ i $q\circ q=q$ (ako je $\Delta_A\subseteq q$ onda $q\subseteq q\circ q$).

Dokažimo najpre sledeće tvrdjenje:

(T1): Ako su q,r relacije ekvivalencije skupa A, onda je $q\circ r$ relacija ekvivalencije akko $q\circ r=r\circ q$.

Dokaz: ($\Rightarrow$) Neka je $q\circ r$ relacija ekvivalencije. Tada prema 2^0 i 4°

$$q\circ r=(q\circ r)^{-1}=r^{-1}\circ q^{-1}=r\circ q \text{ , dakle } q\circ r=r\circ q.$$

($\Leftarrow$) Pretpostavimo $q\circ r=r\circ q$. Kako je $\Delta_A\subseteq q,r$ to $\Delta_A\subseteq q\circ r$, tj. relacija $q\circ r$ je refleksivna. Dalje, $(q\circ r)^{-1}=r^{-1}\circ q^{-1}=r\circ q=q\circ r$, tj. $q\circ r$ je simetrična.

Najzad, s obzirom da je $\circ$ asocijativna operacija, koristeći uslov $q\circ r=r\circ q$ i $q^2=q$, $r^2=r$, sledi

$$(q\circ r)\circ(q\circ r)=(q\circ q)\circ(r\circ r)=q\circ r \text{ , tj. } q\circ r \text{ je tranzirivna.} \quad \nabla$$

Dokazujemo sada i samo tvrdjenje zadatka. Ako je $q\circ r$ kongruencija onda je $q\circ r$ relacija ekvivalencije, pa prema T1, $q\circ r=r\circ q$.

Pretpostavimo da je $q\circ r=r\circ q$. Prema T1 je $t=q\circ r$ relacija ekvivalencije. Neka je F n-arna operacija algebre $\underline{A}$ i $a_1,\ldots,a_n,b_1,\ldots,b_n\in A$ takvi da $a_1\,t\,b_1$, $\ldots$, $a_n\,t\,b_n$. Tada je za neke $c_1,\ldots,c_n\in A$ $a_1\,q\,c_1$, $\ldots$, $a_n\,q\,c_n$, $c_1\,r\,b_1$, $\ldots$, $c_n\,r\,b_n$, odakle sledi

$F(a_1,\ldots,a_n)\,q\,F(c_1,\ldots,c_n)$, $F(c_1,\ldots,c_n)\,r\,F(b_1,\ldots,b_n)$, tj.

$F(a_1,\ldots,a_n)\,t\,F(b_1,\ldots,b_n)$.

4.3. Neka su q,r kongruencije grupe G. Dokazati da su $q\circ r$ i $q\cap r$ kongruencije grupe G. Prema zad. 3.2.13. ovim kongruencijama odgovaraju normalne podgrupe grupe G. Odrediti te podgrupe.

Rešenje: Neka su H_q, H_r normalne podgrupe koje odgovaraju redom kongruencijama q,r. Podsetimo se da $x\,q\,y$ akko $xy^{-1}\in H_q$, $H_q=\{x\in G \mid x\,q\,1_G\}$.

Otuda za $x,y\in G$ važi:

$$x(q\cap r)y \Leftrightarrow (x\,q\,y)\wedge(x\,r\,y) \Leftrightarrow xy^{-1}\in H_q \wedge xy^{-1}\in H_r \Leftrightarrow xy^{-1}\in H_q\cap H_r,$$

tj.

$$H_{q\cap r}=H_q\cap H_r .$$

Prema zadatku 4.1. sledi takodje da je $q\cap r$ kongruencija grupe G. Dalje,

$$x(q\circ r)y \Leftrightarrow (\exists z)(x\,q\,z\wedge z\,r\,y) \Leftrightarrow (\exists z)(xz^{-1}\in H_q\wedge zy^{-1}\in H_r)$$
$$(\exists z)(\exists h_1\in H_q)(\exists h_2\in H_r)(x=h_1z\wedge z=h_2y)$$
$$(\exists h_1\in H_q)(\exists h_2\in H_2)(x=h_1h_2y) \Leftrightarrow xy^{-1}\in H_qH_r .$$

Dakle, $x(q\circ r)y \Leftrightarrow xy^{-1}\in H_qH_r$. Kako su $H_q,H_r\lhd G$ to je i $H_qH_r\lhd G$, pa je $q\circ r$ kongruencija i

$$H_{q\circ r}=H_qH_r .$$

4.4. Neka je $\underline{A}$ algebra sa svojstvom: za ma koje dve kongruencije q,r algebre $\underline{A}$ je $q \circ r = r \circ q$. Ako je Q_A skup svih kongruencija algebre $\underline{A}$, dokazati da je $(Q_A, \cap, \circ)$ modularna mreža.

Rešenje: Proveravamo jedino uslov modularnosti:

$$q \subseteq r \Rightarrow r \cap (q \circ t) \subseteq q \circ (r \cap t) \ , \ q,r,t \in Q_A \ .$$

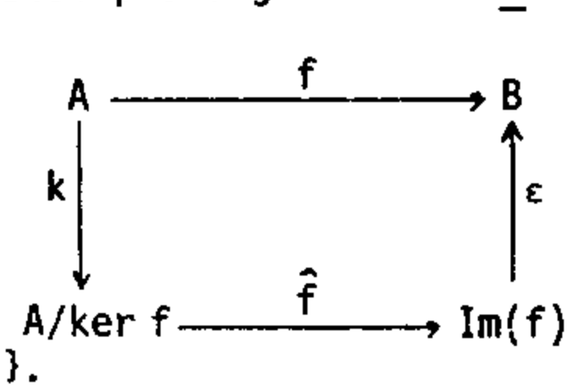
Neka je $q \subseteq r$ i pretpostavimo $(a,b) \in r \cap (q \circ t)$. Tada $(a,b) \in r$ i $(a,b) \in q \circ t$. Kako je $q \circ t = t \circ q$, to postoji $c \in A$ takav da $(a,c) \in t$ i $(c,b) \in q$. Zbog $q \subseteq r$ je $(c,b) \in r$, pa i $(b,c) \in r$ (jer $r^{-1} = r$). Odavde i iz $(a,b) \in r$ sledi $(a,c) \in r$, pa $(a,c) \in t \cap r$. Kako $(c,b) \in q$ to $(a,b) \in (t \cap r) \circ q$. S obzirom da je slaganje kongruencija u Q_A komutativno, sledi $(a,b) \in q \circ (t \cap r)$.

Primetimo da su prema zadacima 4.1. i 4.2. relacije $r \cap (q \circ t)$, $q \circ (r \cap t)$ kongruencije algebre A (ukoliko su t,q i r kongruencije te algebre).

4.5. Neka je G grup, Q_G skup svih kongruencija grupe G i $\mathcal{N}(G)$ skup svih normalnih podgrupa od G. Dokazati: a) $(Q_G, \cap, \circ)$ je modularna mreža,
b) $(Q_G, \cap, \circ) \simeq (\mathcal{N}(G), \cap, \vee)$ gde je $H_1 \vee H_2 \overset{def}{=} H_1 H_2$.

Rešenje: Prema zadacima 4.2. i 4.3. slaganje kongruencija u grupi je komutativno. Videti prethodni zadatak.

4.6. Dokazati teoremu o homomorfizmu: Ako su $\underline{A}$, $\underline{B}$ istotipne algebre i $f : \underline{A} \to \underline{B}$ je homomorfizam, tada $f = \varepsilon \circ \hat{f} \circ k$, gde je k prirodni homomorfizam (dakle epimorfizam), $\hat{f}$ je izomorfizam i ε utapanje.



Rešenje: Neka je $q = \ker f = \{(x,y) \in A^2 \mid f(x) = f(y)\}$.
Dokazujemo da je q kongruencija. Neka je F n-arni operacijski simbol jezika algebri $\underline{A}$, $\underline{B}$ i pretpostavimo $x_1 \, q \, y_1, \ldots, x_n \, q \, y_n$. Tada $f(x_1) = f(y_1), \ldots, f(x_n) = f(y_n)$, pa

$$f(F^A(x_1,\ldots,x_n)) = F^B(f(x_1),\ldots,f(x_n)) = F^B(f(y_1),\ldots,f(y_n))$$
$$= f(F^A(y_1,\ldots,y_n) \ , \ \text{tj.} \ \ F^A(x_1,\ldots,x_n) \, q \, F^B(y_1,\ldots,y_n) \ .$$

Dalje, $x/q = y/q \Rightarrow f(x) = f(y)$, pa preslikavanje $\hat{f} : A/q \to B$ definisano sa $\hat{f}(x/q) = f(x)$ jeste dobro definisano. Ono je takodje i homomorfizam: za $a_1, \ldots, a_n \in A$ i $\underline{A}' = \underline{A}/q$ je

$$\hat{f}(F^A(a_1/q,\ldots,a_n/q)) = \hat{f}(F^A(a_1,\ldots,a_n)/q) = f(F^A(a_1,\ldots,a_n)) = F^B(f(a_1),\ldots,f(a_n)).$$

4.7. Dokazati Prvu teoremu o izomorfizmu: Ako je $\underline{B}$ podalgebra algebre $\underline{A}$ i q je kongruencija u $\underline{A}$, tada je $B^q = \bigcup_{x \in B} x/q$ podalgebra algebre $\underline{A}$, $q' = q \cap \underline{B}^2$ je kongruencija algebre $\underline{B}$ i

$$\underline{B}/q' \simeq \underline{B}^q/q \ .$$

Rešenje: Dokažimo najpre da je B^q podalgebra algebre $\underline{A}$. Neka je F n-arna operacija algebre $\underline{A}$ i $a_1,\ldots,a_n \in B^q$. Tada za neke $b_1,\ldots,b_n \in B$, $a_1 \, q \, b_1, \ldots, a_n \, q \, b_n$; q je kongruencija pa $F(a_1,\ldots,a_n) \, q \, F(b_1,\ldots,b_n)$. Medjutim, $F(b_1,\ldots,b_n) \in B$ pa $F(a_1,\ldots,a_n) \in B^q$. Dakle, B^q je zatvoren za operacije algebre $\underline{A}$, pa je B^q podalgebra od $\underline{A}$.

Neposredno se proverava da je q' kongruencija algebre $\underline{B}$.

Ako su $a,b \in B$ i $a/q' = b/q'$ onda $(a,b) \in q'$, pa $(a,b) \in q$, odakle sledi $a/q = b/q$. Dakle, preslikavanje $f : B/q' \to B^q/q$, odredjeno sa $f(a/q') = a/q$, $a \in B$, je dobro definisano. f je na jer za $b \in B^q$ postoji $a \in B$ tako da $b \, q \, a$, tj. $b/q = a/q$, pa $f(a/q) = b/q$. Slično se pokazuje da je f 1-1 i homomorfizam, tj. f je izomorfizam algebri B/q' i B^q/q.

4.8. Dokazati Lemu Zassenhaus-a: Neka su $\underline{B}$, $\underline{C}$ podalgebre algebre $\underline{A}$ i q,r kongruencije redom u $\underline{B}$, $\underline{C}$. Neka su sve kongruencije u $\underline{B} \cap \underline{C}$ komutativne (tj. za svake dve kongruencije s,t algebre $\underline{B} \cap \underline{C}$ je $s \circ t = t \circ s$). Tada je $q \circ r \circ q$ kongruencija algebre $(B \cap C)^q$, $r \circ q \circ r$ je kongruencija algebre $(B \cap C)^r$ i pri tom važi:

$$(B \cap C)^q / q \circ r \circ q \simeq (B \cap C)^r / r \circ q \circ r \ .$$

Rešenje: Neka je $D = B \cap C$, $q' = q \cap C^2$, $r' = r \cap B^2$. Tada $q \circ r \circ q = q \circ r' \circ q$ i $(q \circ r \circ q) \circ (q \circ r \circ q) = q \circ r' \circ q' \circ r' \circ q = q \circ r' \circ q$, tj. $q \circ r \circ q$ je tranzitivna relacija. Dalje, neposredno se proverava da je $q \circ r \circ q$ refleksivna i simetrična relacija, i da je ona saglasna sa operacijama algebre $\underline{A}$; dakle $q \circ r \circ q$ je kongruencija u D^q. Slično se dokazuje da je $r \circ q \circ r$ kongruencija u D^r, a $q' \circ r'$ u D. Kako je $(q \circ r \circ q) \cap D^2 = q' \circ r'$, prema Prvoj teoremi o izomorfizmu sledi da je $D^q / q \circ r \circ q \simeq D/q' \circ r'$. Simetričnim postupkom nalazimo $D^r / r \circ q \circ r \simeq D/q' \circ r'$, odakle sledi $D^q / q \circ r \circ q \simeq D^r / r \circ q \circ r$.

4.9. Neka je I beskonačan skup, $\underline{A}_i$ $(i \in I)$ familija istotipnih algebri i $\underline{A} = \prod_i \underline{A}_i$. Dokazati da je relacija $\sim$ kongruencija algebre $\underline{A}$ ako je $\sim$ definisana na sledeći način: $f \sim g \Leftrightarrow \{i \in I \mid f(i) = g(i)\}^C$ je konačan .

Rešenje: Dokažimo, recimo, da je $\sim$ tranzitivna relacija. Neka su $f \sim g$, $g \sim h$, $f,g,h \in A$ i $X = \{i \in I \mid f(i) = g(i)\}$, $Y = \{i \in I \mid g(i) = h(i)\}$, $Z = \{i \in I \mid f(i) = h(i)\}$. Tada $X \cap Y \subseteq Z$, odakle $Z^C \subseteq X^C \cup Y^C$. Po pretpostavci X^C, Y^C su konačni skupovi, dakle Z^C je konačan skup, tj. $f \sim h$.

Dokazujemo sada da je $\sim$ *saglasna sa operacijama algebre* $\underline{A}$. *Neka su* $f_1 \sim g_1$, $\ldots$, $f_n \sim g_n$, $f_1,\ldots,f_n,g_1,\ldots,g_n \in A$ *i neka je* F *n-arna operacija algebre* $\underline{A}$. *Tada je za neke n-arne operacije* F_i $(i \in I)$ *algebri* $\underline{A}_i$,

$$F(f_1,\ldots,f_n) = \langle F_i(f_1(i),\ldots,f_n(i)) \mid i \in I \rangle .$$

Dalje, neka je $X_k=\{i \in I \mid f_k(i)=g_k(i)\}$, $k=1,\ldots,n$ *i*

$$X=\{i \in I \mid F(f_1,\ldots,f_n)(i)=F(g_1,\ldots,g_n)(i)\} .$$

Tada $X \supseteq X_1 \cap \ldots \cap X_n$, *odakle* $X^c \subseteq X_1^c \cup \ldots \cup X_n^c$. *Prema uslovu o funkcijama* f_k,g_k *skupovi* X_k^c *su konačni, dakle i skup* X^c *je konačan ; stoga*

$$F(f_1,\ldots,f_n) \sim F(g_1,\ldots,g_n) .$$

10.5. SLOBODNE ALGEBRE

Jednakosna logika je u bliskoj vezi sa slobodnim algebrama; naime, kao što će se videti, mnoge konstrukcije u vezi sa slobodnim algebrama proističu iz svojstava jednakosne logike.

Neka je L algebarski jezik. Jedina (shema) aksioma jednakosne logike J je formula u=u , u $\in$Term(L).

Pravila izvodjenja u J su

$$(P_1)\ \frac{u=v}{v=u}\ , \qquad (P_2)\ \frac{u=v\ ,\ v=w}{u=w}\ , \qquad (P_3)\ \frac{u_1=v_1,\ldots,u_n=v_n}{f(u_1,\ldots,u_n)=f(v_1,\ldots,v_n)}$$

gde su u,v,w,u_i,v_i termi jezika L a f funkcijski znak iz L dužine n.

5.1. *Definicija: Neka je Z skup zakona jezika L. Jednakost u=v je posledica zakona Z u J , u oznaci* $Z \underset{J}{\vdash} u=v$, *ukoliko važi:*

Postoji niz $\alpha_1,\ldots,\alpha_n$ *takav da*

(i) α_n *je u=v ,*

(ii) α_i *je jednakost iz jezika L ,*

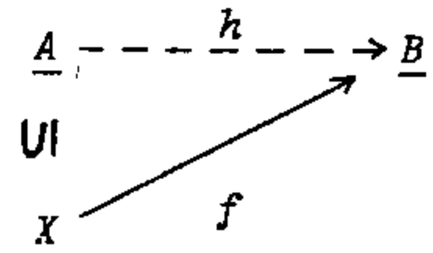
(iii) svaki α_i *je aksioma logike J ili* $\alpha_i \in Z$ *ili se* α_i *dobija primenom nekog od pravila izvodjenja* $(P_1),(P_2),(P_3)$ *iz prethodnih članova niza* $\alpha_1,\ldots,\alpha_{i-1}$.

S obzirom na napomenu iz odeljka 10.2., skup algebarskih zakona Z čini jednu teoriju ; posledice skupa Z nazivamo takodje i *teoremama* teorije Z.

Navodimo sada definiciju slobodne algebre, pojma koji je fundamentalan u teoriji univerzalnih algebri.

5.2. *Definicija: Neka je* $\mathfrak{M}$ *klasa algebri jezika L i X neki skup. Algebra*

$\underline{A} \in \mathcal{M}$ je <u>slobodna algebra</u> za $\mathcal{M}$, nad skupom slobodnih generatora X akko $X \subseteq A$ i za svaku algebru $\underline{B} \in \mathcal{M}$, svako preslikavanje $f : X \to B$, postoji jedinstven homomorfizam $h : \underline{A} \to \underline{B}$ takav da $f \subseteq h$.



Dakle, navedeni dijagram komutira.

5.3. <u>Teorema</u>: *Za svaki algebarski jezik L, svaku klasu zakona Z jezika L, netrivijalan varijete $\mathcal{M}$ klase zakona Z i skup X, postoji jedinstvena (do na izomorfizam) slobodna algebra $\underline{A}$ sa skupom slobodnih generatora X.*

Dokaz[1]: Neka je $L = \mathcal{F} \cup \mathcal{C}$ neki (moguće beskonačan) algebarski jezik. Bez gubljenja opštosti možemo pretpostaviti da je $X \subseteq Pr$[2] (dakle Pr može biti proizvoljno veliki skup). Najpre se dokazuje da za varijete $\mathcal{M}$ klase zakona $Z = \emptyset$ postoji slobodna algebra sa skupom slobodnih generatora X. To će biti tzv. *apsolutno slobodna* ili *termovska algebra* $\underline{A}$ jezika L definisana na sledeći način:

domen algebre $\underline{A}$ je

$A = \{t \in Term(L) \mid$ svaka promenljiva koja se javlja u t pripada skupu $X\}$;

ako je c simbol konstante onda $c^A = c$; ako je f funkcijski znak tada je

$$f^A(u_1,\ldots,u_k) = f(u_1,\ldots,u_k)\ ,\ k = ar(f)\ ,\ u_1,\ldots,u_k \in A\ .$$

Koristeći induktivnu definiciju terma i teoremu o jedinstvenosti čitanja (porekla) terma dokazuje se da za svaku algebru $\underline{B} \in \mathcal{M}$, svako preslikavanje $f : X \to B$ proširuje se do jedinstvenog homomorfizma $h : \underline{A} \to \underline{B}$. Primetimo da algebra $\underline{A}$ ne zadovoljava druge algebarske zakone osim trivijalnih.

Drugi korak prema konstrukciji slobodne algebre za $\mathcal{M}$ je odredjivanje jedne kongruencije u upravo definisanoj termovskoj algebri $\underline{A}$.

Neka je $R = \{(u,v) \mid (u=v) \in Z\}$. Primetimo da je $R \subseteq A^2$.

Dalje, neka je $\sim = \cap\{S \mid R \subseteq S\ ,\ S$ je kongruencija algebre $\underline{A}\}$. Tada važi:

1° $\sim$ je kongruencija algebre $\underline{A}$ (tačnije, $\sim$ je najmanja kongruencija algebre $\underline{A}$ koja sadrži relaciju R).

2° Količnička algebra $\underline{A}/\sim$ je slobodna algebra za varijete $\mathcal{M}$ sa skupom slobodnih generatora $X/\sim = \{x/\sim \mid x \in X\}$. Koristeći uslov da $\mathcal{M}$ sadrži netrivijalnu algebru, sledi da za različite x,y važi $x/\sim \neq y/\sim$, tj. $|X| = |X/\sim|$. ▼

---

[1] Neki detalji dokaza dati su takodje u zadatku 5.6.

[2] Pr je skup promenljivih.

5.4. Napomena: Relacija $\sim$ u 1° može se odrediti korišćenjem jednakosne logike ; naime, $\sim = \{(u,v) \mid Z \vdash_J u=v\}$.

5.5. Napomena: Ukoliko je $X \cap Term(L)=\emptyset$, sa neznatnom promenom može se izvršiti direktna konstrukcija slobodne algebre (za neku klasu algebri) sa skupom slobodnih generatora X. Naime, jedino se menja domen apsolutno slobodne algebre $\underline{A}$ iz prethodnog dokaza, tj.

$$A=\{v \in Term(L \cup X) \mid v \text{ je zatvoren term}\},$$

(term v je zatvoren ukoliko ne sadrži promenljive).
Dakle, s obzirom na Napomenu 5.4. i teoreme 4.2. i 5.3., za skup X važi:

5.6. *Teorema: Neka je $\underline{B}$ algebra jezika $L=\mathcal{F} \cup \mathcal{C}$ definisana na sledeći način:*
domen algebre $\underline{B}$ je $B=\{v/\sim \mid v \in Term(L \cup X)$, v je zatvoren term$\}$,
gde $u \sim v$ akko $Z_X \vdash_J u=v$, i

$$Z_X=\{u(d_1,\ldots,d_n)=v(d_1,\ldots,d_n) \mid u(x_1,\ldots,x_n), v(x_1,\ldots,x_n) \in Term(L \cup X),$$
$$d_1,\ldots,d_n \in X, (u=v) \in Z\} .$$

Operacije f^B algebre $\underline{B}$ su sledeće: za funkcijski znak $f \in \mathcal{F}$ i $v_1/\sim$, .. , $v_n/\sim \in B$ je $f^B(v_1/\sim,\ldots,v_n/\sim)=f(v_1,\ldots,v_n)/\sim$;
za simbol konstante $c \in C$ je $c^B=c/\sim$.
Tada je $\underline{B}$ slobodna algebra za varijete $\mathcal{M}$ klase zakona Z sa skupom slobodnih generatora X .

Primeri i zadaci

5.1. Dokazati da je varijete $\mathcal{M}$ klase zakona Z trivijalan akko $Z \vdash_J x=y$, gde su x,y različite promenljive.

Rešenje: ($\Rightarrow$) Pretpostavimo da je $\mathcal{M}$ trivijalan varijete; dakle sve algebre iz $\mathcal{M}$ su jednočlane. Stoga zakon x=y važi na svim algebrama varijetea pa prema stavu potpunosti za jednakosnu logiku $Z \vdash_J x=y$.
($\Leftarrow$) Sledi neposredno .

5.2. Neka je $L=\{\cdot\} \cup \{a,b,1\}$. Dokazati : Z, $a^3=a$, $b^3=b$, $ab=1 \vdash_J a=b$, $a^2=1$ gde je Z skup zakona za klasu monoida.

Rešenje: Koristeći zakone iz Z i jednakosti $a^3=a$, $b^3=b$, $ab=1$ postoji sledeće izvodjenje u jednakosnoj logici:
$a=a \cdot 1=a \cdot ab=a^2b=a^2 \cdot 1 \cdot b=a^2 \cdot ab \cdot b=a^3b^2=a \cdot b^2=ab \cdot b=1 \cdot b=b$.
Dakle a=b . Iz jednakosti ab=1 sledi $a^2=1$.

5.3. Neka je G skup aksioma grupe u jeziku $L=\{\cdot, ^{-1}, 1\}$. Dokazati:

a) G, $a^7=1$, $b^3=1$, $ba=a^3b \vdash_J a=1$,

b) G, $bab=a$, $aba=b \vdash_J a^4=1$, $b^2=a^2$.

Rešenje: a) Neka je $a^7=1$, $b^3=1$, $ba=a^3b$. Iz treće jednakosti sledi $b^3a=b^2a^3b$, pa kako je $b^3=1$, to je $a=b^2a^3b$. Koristeći više puta treću jednakost sledi $b^2a^3b=bbaa^2b=ba^3ba^2b=...=ba^9b^2$, tj. $a=ba^2b^2$, jer $a^7=1$. Dalje, $ba^2b^2=baab^2=a^3bab^2=a^6b^3=a^6$; dakle $a=a^6$, pa $a^2=a^7=1$, odnosno $a^2=1$, $a^5=1$. Otuda $a=a\cdot1\cdot1=a\cdot a^7\cdot a^7=a^{15}=(a^5)^3=1^3=1$.

b) Pretpostavimo $bab=a$, $aba=b$. Tada

$$a^2=(bab)(bab)=babbab=bab(aba)ab=bababa^2b=bababa(bab)b=bababababab^2.$$ *Dakle*

$$a^2=bababababab^2 . \qquad (1)$$

Odavde nalazimo $a^2=b(aba)b(aba)b^2=bbbbb^2=b^6$, tj.

$$a^2=b^6 . \qquad (2)$$

Simetričnim postupkom nalazimo

$$b^2=a^6 \qquad (3)$$

Iz (1), dalje, imamo : $a^2=bababababab(aba)=(bab)a(bab)a(bab)a=aaaaaa$, dakle

$$a^2=a^6 \qquad (4)$$

Iz (3) i (4) sledi $a^2=b^2$. Iz (4) sledi $a^{-2}a^2=a^{-2}a^6$, tj. $a^4=1$.

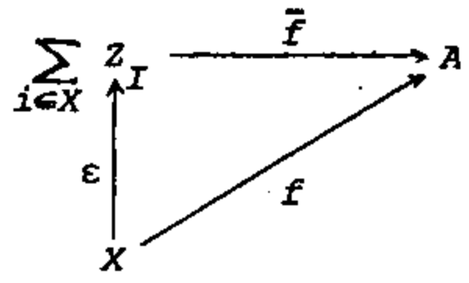
Primetimo da je jednakost $a^2=b^2$ izvedena koristeći jedino polazne jednakosti i zakon asocijativnosti.

5.4.Dokazati da klasa cikličnih grupa ima slobodnu algebru.

Rešenje: Aditivna grupa celih brojeva $\underline{Z}=(Z,+,0)$ je slobodna algebra sa jednim slobodnim generatorom $a=1$, u klasi cikličnih grupa.

Primetimo da za svaku (cikličnu) grupu G i $m\in G$ postoji homomorfizam $f:\underline{Z}\to G$ tako da $f(1)=m$.

5.5.Dokazati da varijete Abel-ovih grupa ima slobodnu algebru nad svakim skupom X slobodnih generatora.



Rešenje: Neka je za svaki $i\in X$, Z_i aditivna grupa celih brojeva. Tada je suma grupa Z_i (videti poglavlje o Abel-ovim grupama), $\sum_{i\in X} Z_i$, slobodna grupa nad X ukoliko je ε odredjeno sa $\varepsilon_i(j)=\begin{cases}1_i, & \text{za } j=i\\ 0, & \text{za } j\neq i\end{cases}$.

Za svaki $x\in\sum_{i\in X} Z_i$ postoje jedinstveni celi brojevi $x_1,...,x_n$ takvi da $x=x_1\varepsilon_1+...+x_n\varepsilon_n$. Ako je $f:X\to A$, $\underline{A}$ je Abel-ova grupa , tada je preslikavanje $\bar{f}:\sum_{i\in X} Z_i \to A$

definisano sa $\bar{f}(\sum_{i\leq n} x_i\varepsilon_i) = \sum_{i\leq n} x_i f(i)$ *homomorfizam grupe* $\sum_{i\in X} Z_i$ *u grupu* $\underline{A}$, *i* $\bar{f}$ *proširuje* f .

5.6.Obrazložiti detalje dokaza teoreme 5.3.; odnosno, ako je $\underline{A}$ apsolutno slobodna algebra jezika L i Z skup nekih zakona jezika L, dokazati da za $\tau=\{(u,v) \mid u,v\in Term(L), Z \vdash_J u=v\}$ važi:

a) τ je kongruencija algebre $\underline{A}$,

b) $\tau = \cap\{\sigma \mid \tau\subseteq\sigma$ i σ je kongruencija u $\underline{A}\}$, c) $\underline{A}/\tau$ je slobodna algebra.

Rešenje: a) Dokažimo najpre da je τ *relacija ekvivalencije. Neka su* u,v,w *iz* $Term(L)$. *Zbog* $Z\vdash u=u$ *je* $(u,u)\in\tau$.

Ako je $(u,v)\in\tau$ *onda* $(v,u)\in\tau$ *jer* $Z\vdash u=v$ *povlači* $Z\vdash v=u$.

Pretpostavimo $(u,v),(v,w)\in\tau$. *Tada* $Z\vdash u=v$, $Z\vdash v=w$, *pa* $Z\vdash u=w$, *tj.* $(u,w)\in\tau$.

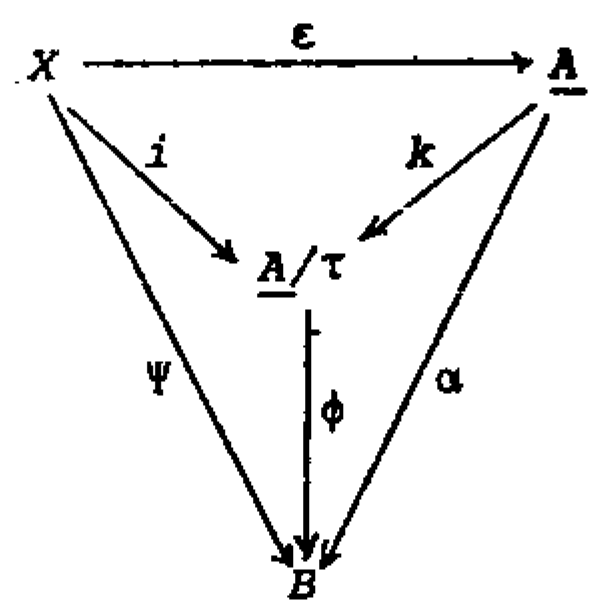
Dokazujemo sada saglasnost τ *sa operacijama algebre* $\underline{A}$. *Neka je* F *n-arni operacijski znak i* F^A *njegova interpretacija u algebri* $\underline{A}$. *Pretpostavimo* $(u_1,v_1),\dots,(u_n,v_n)\in\tau$. *Tada* $Z\vdash u_1=v_1,\dots, Z\vdash u_n=v_n$. *Prema pravilu* (P_3) *supstitucije za jednakosnu logiku sledi* $Z\vdash F(u_1,\dots,u_n)=F(v_1,\dots,v_n)$. *Kako je* $F^A(u_1,\dots,u_n)=F(u_1,\dots,u_n)$, *sledi* $(F^A(u_1,\dots,u_n),F^A(v_1,\dots,v_n))\in\tau$.

b) Neka je $\rho=\cap\chi$, *gde* $\chi=\{\sigma \mid \tau\subseteq\sigma$ *i* σ *je kongruencija algebre* $\underline{A}\}$.

Za svaki $\sigma\in\chi$ *je* $\tau\subseteq\sigma$, *dakle* $\tau\in\bigcap_{\sigma\in\chi}\sigma$, *tj.* $\tau\subseteq\rho$.

Prema a) τ *je kongruencija algebre* $\underline{A}$ *i* $\tau\subseteq\tau$, *pa* $\tau\in\chi$. *Otuda* $\rho\subseteq\tau$.

c) Neka je $(u=v)\in Z$. *Dokazujemo da* $\underline{A}/\tau$ *zadovoljava zakon* $u(x_1,\dots,x_n)=v(x_1,\dots,x_n)$. *Neka je* $k:\underline{A}\to\underline{A}/\tau$ *kanonsko preslikavanje i* $w_1,\dots,w_n$ *su iz A. Tada za* $\underline{A}'=\underline{A}/\tau$,



$u^{A}(w_1/\tau,\dots,w_n/\tau)=u^{A'}(k(w_1),\dots,k(w_n))=$

$k(u^A(w_1,\dots,w_n))$.

U apsolutno slobodnoj algebri $\underline{A}$ *važi* $u^A(w_1,\dots,w_n)=u(w_1,\dots,w_n)$. *Kako* $(u=v)\in Z$, *primenom supstitucije sledi* $Z\vdash u(w_1,\dots,w_n)=v(w_1,\dots,w_n)$, *tj.* $(u(w_1,\dots,w_n),v(w_1,\dots,w_n))\in\tau$. *Dakle* $k(u(w_1,\dots,w_n))=k(v(w_1,\dots,w_n))$. *Kako je* k *homomorfizam i* $v(w_1,\dots,w_n))=v^A(w_1,\dots,w_n)$, *sledi* $k(v(w_1,\dots,w_n))=v^{A'}(w_1/\tau,\dots,w_n/\tau)$. *Stoga* $u^{A'}(w_1/\tau,\dots,w_n/\tau)=v^{A'}(w_1/\tau,\dots,w_n/\tau)$, *tj. zakon* $u=v$ *važi u* $\underline{A}/\tau$, *što znači da* $\underline{A}/\tau\in\mathfrak{M}$.

Dokazujemo sada da je $\underline{A}/\tau$ *slobodna algebra nad X varijeteta* $\mathfrak{M}$.

Neka je preslikavanje $i:X\to A/\tau$ *definisano sa* $i(x)=x/\tau$.

Neka je $\underline{B}\in\mathfrak{M}$ *proizvoljna algebra i neka su preslikavanja na dijagramu (po-*

red već uvedenih) odredjena na sledeći način:

$\Psi : X \to B$ *je proizvoljna funkcija ,*

$\varepsilon : X \to A$, *je inkluzivno preslikavanje,* $\varepsilon(x)=x$, $x \subset X$,

$\alpha : A \to B$ *je homomorfizam takav da je* $\varepsilon\alpha = \Psi$ *; preslikavanje* α *sa ovim svojstvom postoji s obzirom da je* $\underline{A}$ *apsolutno slobodna algebra.*

Dalje, neka su u,v termi takvi da $u/\tau=v/\tau$. *Tada* $(u,v)\in\tau$, *tj.* $Z \vdash u=v$. *Kako* $\underline{B}$ *zadovoljava zakone iz Z, to zakon u=v važi u* $\underline{B}$. *Dakle,* $u^B(\alpha(x_1),\ldots,\alpha(x_n))=v^B(\alpha(x_1),\ldots,\alpha(x_n))$; α *je homomorfizam, pa* $\alpha(u^A(x_1,\ldots,x_n))=\alpha(v^A(x_1,\ldots,x_n))$. *Dalje* $u^A=u$, $v^B=v$, *pa* $\alpha(u)=\alpha(v)$.

Dakle, za ma koje terme u,v važi: $u/\tau = v/\tau \Rightarrow \alpha(u)=\alpha(v)$, *pa je preslikavanje* $\phi : A/\tau \to B$, *odredjeno sa* $\phi(u/\tau)=\alpha(u)$ *dobro definisano. Za ovako odredjeno* ϕ *lako se proverava da je homomorfizam i da navedeni dijagram komutira; izmedju ostalog je* $\phi\bullet\kappa=\alpha$.

Prema prethodnom, $\underline{A}/\tau$ *je slobodna algebra varijetea* $\mathfrak{M}$ *nad X.*

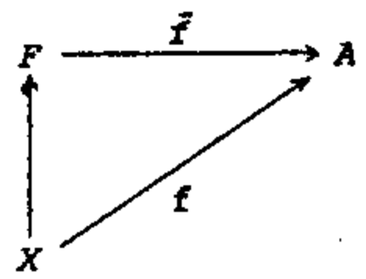
Primetimo da ako nije $Z \vdash x=y$, *x,y su promenljive iz X, onda* $(x,y)\notin\tau$, *pa* $x/\tau \neq y/\tau$. *Otuda možemo uzeti da je* $X \subseteq A/\tau$, *odnosno da je i inkluzivno preslikavanje.*

5.7. Neka je $L=\{\cdot,^{-1},1\}$ jezik teorije grupa, Z_G aksiome te teorije i $Z=Z_G\cup\{x^2=1\}$ Dokazati: ako je $\underline{G}$ slobodna algebra sa konačnim skupom slobodnih generatora varijetea $\mathfrak{M}$ klase zakona Z, onda je $\underline{G}$ konačna.

Rešenje: Ako je $\underline{G} \in \mathfrak{M}$ *generisana sa n elemenata onda* $|G| \leqslant 2^n$. *Primetimo, najpre, da ukoliko G zadovoljava zakone Z, onda je G komutativna algebra. Dokaz dalje teče indukcijom. Neka je* $a \in G$, $a \neq 1$. *Tada za* $N=\{1,a\}$, *važi* $N \lhd G$, *i zakon* $x^2=1$ *važi u* G/N , *pa* $|G/N| \leqslant 2^{n-1}$ *(po indukcijskoj hipotezi). S druge strane,* $|G/N|=|G| : |N|=|G| : 2$, *odakle sledi* $|G| \leqslant 2^{n-1}\cdot 2$.

5.8. Opisati slobodne semigrupe.

Rešenje: Neka je F skup svih reči (konačnih nizova) nad skupom X. Ako je $\underline{A}$ *semigrupa i* $f : X \to A$, *tada se f proširuje do preslikavanja* $\bar{f} : F \to A$, *gde je* $\bar{f}(a_1,\ldots,a_n) = f(a_1)\ldots f(a_n)$, $a_1,\ldots,a_n \in X$. *Prema zadatku 1.4.3. (poglavlja o grupoidima)* $(F,*)$ *je semigrupa (* je nadovezivanje), i* $\bar{f}$ *je homomorfizam*



5.9. Opisati slobodnu komutativnu semigrupu sa prebrojivo mnogo generatora.

Rešenje: Ova algebra izomorfna je strukturi $\underline{A}=(\{2,3,4,\ldots\},\cdot)$, *gde je* $\cdot$

množenje prirodnih brojeva. Slobodni generatori ove algebre su prosti brojevi. Videti takodje zadatak 1.4.13. (poglavlja o grupoidima).

5.10. Opisati slobodne grupe.

Rešenje: Neka je $X=\{x_i \mid i\in I\}$ *i neka je W skup reči oblika* $x_1^{\alpha_1}\dots x_n^{\alpha_n}$, $x_i\in X$, $\alpha_i\in\{1,-1\}$, $i=1,\dots,n$, $n\in N$. *Reč*

$$a_1 a_2 \dots a_k \qquad (*)$$

gde je $a_i=x$ *ili* $a_i=x^{-1}$ *za neki* $x\in X$, *je u svedenom obliku akko za sve i,* $1\leqslant i\leqslant k$, *važi: ako je* $a_i=x^{\alpha}$, $x\in X$, *tada* $a_{i-1}\neq x^{-\alpha}$ $(\alpha\in\{1,-1\})$. *Dakle,* $x_1x_2x_3^{-1}$ *je svedena reč (ukoliko su* x_1,x_2,x_3 *različiti elementi skupa X), dok* $x_1x_2x_2^{-1}x_1^{-1}x_3$ *to nije.*

Neka je W_0 *skup svih svedenih reči iz W.*

Reč w' je dobijena od reči w elementarnom transformacijom ukoliko je w' nastala od w brisanjem ili dodavanjem podreči oblika aa^{-1}, *tj.* $w'=u_1aa^{-1}u_2$ *gde je* $w=u_1u_2$ *ili* $w=v_1aa^{-1}v_2$ *i* $w'=v_1v_2$.

Reči u,v su elementarno ekvivalentne, u oznaci $u\sim v$, *ukoliko je v dobijena od u primenom elementarnih transformacija; odnosno, postoji niz* $w_1,\dots,w_n$ *tako da* $u=w_1$ *i* $v=w_n$ *i za svaki* $i<n$ w_{i+1} *je dobijena iz* w_i *primenom jedne elementarne transformacije. Neposredno se proverava da važi:*

Relacija $\sim$ *je relacija ekvivalencije skupa* W_0. *(1)*

Lema 1: $(\forall u,v\in W)(u\sim v \Rightarrow u=v)$.

Dokaz: Neka su $u,v\in W_0$, $u\neq v$. *Pretpostavimo* $u\sim v$; *tada možemo izabrati niz* $w_1,\dots,w_n$, $u=w_1$, $v=w_n$ *koji obezbedjuje* $u\sim v$ *i pri tom broj m slova u ovom nizu je manji ili jednak broju slova u svakom drugom izvodjenju za* $u\sim v$. *Reči u,v su svedene, dakle* $|w_2|>|w_1|$, $|w_{n-1}|>|w|$, *gde* $|w|$ *označava broj slova reči w. Otuda postoji i,* $1<i<n$, *tako da* $|w_i|>|w_{i-1}|$, $|w_{i+1}|$. *Tada je* w_{i-1} *nastala brisanjem* aa^{-1} *iz* w_i, *a* w_{i+1} *brisanjem podreči* bb^{-1} *iz* w_i. *Razlikujemo sledeće slučajeve:*

1^0 aa^{-1}, bb^{-1} *su iste reči, dakle* $w_{i-1}=w_{i+1}$ *pa postoji izvodjenje za* $u\sim v$ *sa manjim brojem slova od m, suprotno izboru broja m.*

2^0 *Podreči* aa^{-1}, bb^{-1} *se delimično poklapaju. Tada* w_i *sadrži podreč* $aa^{-1}a$ *i* w_{i-1}, w_{i+1} *nastaju iz* w_i *zamenom te reči sa a, dakle opet* $w_{i-1}=w_{i+1}$, *suprotno izboru broja m.*

3^0 *Podreči* aa^{-1}, bb^{-1} *se ne preklapaju u* w_i. *Tada* $w_i=paa^{-1}qbb^{-1}r$, $w_{i-1}=pqbb^{-1}r$, $w_{i+1}=paa^{-1}qr$; *dakle* $w_1,\dots,w_{i-1},\dots,w_{i-1},pqr,w_{i+1},\dots,w_n$ *je izvodjenje za* $u\sim v$ *koje ima m-4 slova, suprotno izboru broja m.* ▼

Lema 2 : Za sve $u,v \in W$ važi : $u \sim v$ akko $G_P \underset{J}{|\!-} u=v$,

gde su G_p aksiome grupa u jeziku $L=\{\cdot, ^{-1}, 1\}$.

Dokaz: Ako je $u \sim v$ onda postoji izvodjenje $w_1, w_2, \ldots, w_n$ za $u \sim v$. Tada je $w_1=w_2$, $w_2=w_3, \ldots, w_{n-1}=w_n$ dokaz za $u=w$ u J.
S druge strane, $\sim$ je kongruencija apsolutno slobodne algebre $\underline{G}$ jezika L.To važi, jer prema (1) $\sim$ je relacija ekvivalencije, i takodje je: ako je $u \sim v$ i $w_1, \ldots, w_n$ je izvodjenje za $u \sim v$, onda je $w_1 w, \ldots, w_n w$ izvodjenje za $uw \sim vw$ tj. važi $u \sim v \Rightarrow uw \sim vw$.
Slično se dokazuje : $u \sim v \Rightarrow wu \sim wv$.
Prema zadatku 5.6. sledi $G_P |\!- u=v \Rightarrow u \sim v$, jer
$\{(u,v) \mid (u=v) \in G_P\} \subseteq \sim$, *i* $\{(u,v) \mid G_P |\!- u=v\}$ *je najmanja kongruencija koja sadrži $\{(u,v) \mid (u=v) \in G_P\}$. Ovim je dokaz leme završen.* ▼

Najzad, primetimo da za ma koje $u,v \in W$ postoji tačno jedna reč $w \in W$ takva da $uv \sim w$. Reč w se dobija iz uv primenom elementarnih transformacija.

Prema prethodno rečenom, ako je F_X slobodna grupa nad X i ako je $\underline{A}$ apsolutno slobodna algebra, onda $\underline{F}_X = \underline{A}/\sim$ i $F_X=\{w/\sim \mid w \in W_0\}$. Takodje, $(W_0, \cdot, ^{-1}, 1)$ je grupa, gde je: za $u,v,w \in W_0$ $u \cdot v=w$ akko $G_P |\!- uv=w$, $u^{-1}=v$ akko $G_P |\!- u^{-1}=v$. Preslikavanje $\phi : W_0 \to F_X$, $\phi(w)=w/\sim$ je izomorfizam grupa $(W_0, \cdot, ^{-1}, 1)$ i $\underline{F}_X$: ϕ je <u>na</u> jer $F_X=\{w/\sim \mid w \in W_0\}$; ϕ je 1-1 prema lemi 1; najzad, ako je $w=u \cdot v$, onda $G_P |\!- uv=w$ odakle sledi $u/\sim \cdot v/\sim = w/\sim$, tj. $\phi(uv)=\phi(u)\phi(v)$.
Dakle, $(W_0, \cdot, ^{-1}, 1)$ je slobodna algebra nad X.
Primetimo da su članovi ovako konstruisane slobodne grupe, predstavnici klasa kongruencije (to su upravo svedene reči) a ne same klase kongruencije.

5.11. Odrediti broj reči dužine k u :
a) Slobodnoj semigrupi sa n slobodnih generatora,
b) Slobodnoj grupi sa n slobodnih generatora.

Rešenje: a) Prema zadatku 5.8. postoji slobodna semigrupa nad X čiji su elementi upravo svi konačni nizovi elemenata iz X. Dakle, ako $|X|=n$ tada ovakvih nizova dužine k ima n^k.
b) Ako je $X=\{a_1, a_2, \ldots, a_n\}$, onda, prema zadatku 5.10. možemo uzeti da su to svi nizovi dužine k skupa $\{a_1, a_1^{-1}, \ldots, a_n, a_n^{-1}\}$ tako da uzastopni članovi niza nisu vida a, a^{-1} ili $a^{-1}a$. Ako sa σ_k označimo broj ovih nizova i ako je $w_1 \ldots w_{k-1} w_k$ jedan takav niz, vidimo da za w_k postoji 2n-1 mogućih vrednosti; dakle $\sigma_k = \sigma_{k-1} \cdot (2n-1)$. Kako je $\sigma_1 = 2n$, to $\sigma_k = 2n(2n-1)^{k-1}$.

5.12. Neka je A slobodna algebra za varijete $\mathfrak{m}$ sa slobodnim generatorima $a_1, \ldots, a_n$.
Ako je $u^A(a_1, \ldots, a_n) = v^A(a_1, \ldots, a_n)$, tada u=v važi na svim algebrama varijetea $\mathfrak{m}$.

Rešenje: Neka je $\underline{B}\in\mathfrak{M}$. *Dokazujemo da zakon* $u(x_1,\ldots,x_n)=v(x_1,\ldots,x_n)$ *važi u algebri* $\underline{B}$. *Kako su* $a_1,\ldots,a_n$ *slobodni generatori slobodne algebre* $\underline{A}$, *to za ma koje elemente* $b_1,\ldots,b_n\in B$ *postoji homomorfizam* $h:\underline{A}\to\underline{B}$ *tako da* $h(a_i)=b_i$ $i=1,\ldots,n$. *Kako važi* $u^A(a_1,\ldots,a_n)=v^A(u_1,\ldots,a_n)$, *to* $h(u^A(a_1,\ldots,a_n))=h(v^A(a_1,\ldots,a_n))$, *tj.* $u^B(h(a_1),\ldots,h(a_n))=v^B(h(a_1),\ldots,h(a_n))$ *odakle sledi*

$$u^B(b_1,\ldots,b_n)=v^B(b_1,\ldots,b_n) \qquad (1)$$

Jednakost (1) važi, dakle, za bilo koje elemente $b_1,\ldots,b_n\in B$; *stoga zakon* $u=v$ *važi u algebri* $\underline{B}$.

5.13. Neka varijete $\mathfrak{M}$ sadrži konačnu netrivijalnu algebru. Dokazati da su slobodne algebre $\underline{A}$, $\underline{B}$ čiji su skupovi slobodnih generatora redom X,Y izomorfne akko $|X|=|Y|$ [1].

Rešenje: Neka je X skup slobodnih generatora slobodne algebre $\underline{A}\in\mathfrak{M}$. *Dokazujemo da je X minimalan skup koji generiše* $\underline{A}$, *tj. ako je* $Y\subseteq X$ *i* $|Y|<|X|$ *onda podalgebra* $\underline{B}$ *generisana skupom Y nije jednaka* $\underline{A}$. *Zaista, neka je* $f:Y\xrightarrow[1-1]{}X$. *Tada* $X\setminus f(Y)\neq\emptyset$, *pa postoji* $y\in X\setminus f(Y)$. *Algebra* $\underline{B}$ *je takodje slobodna algebra varijetea* $\mathfrak{M}$ *sa skupom Y slobodnih generatora, pa postoji homomorfizam* $\hat{f}:\underline{B}\to\underline{A}$ *takav da* $f\subseteq\hat{f}$. *Dokažimo da* $y\notin\hat{f}(B)$. *Pretpostavimo suprotno; tada* $y=\hat{f}(b)$ *za neki b, tj.* $y=\hat{f}(v^B(y_1,\ldots,y_n))$ *gde* $v\in Term(L)$, $y_1,\ldots,y_n\in Y$. *Kako* $\underline{B}\subseteq\underline{A}$ *i* $\hat{f}\restriction Y=f$, *to* $y=v^A(f(y_1),\ldots,f(y_n))$, *tj. za neke* $x_i(=f(y_i))$ *iz X važi:* $y=v^A(x_1,\ldots,x_n)$. *Prema prethodnom zadatku sledi da zakon*

$$y=v(x_1,\ldots,x_n) \qquad (1)$$

važi u svim algebrama varijetea $\mathfrak{M}$. *Kako promenljiva y nije ni jedna od* $x_1,\ldots,x_n$, *onda se u ovom zakonu, y može zameniti nekom drugom promenljivom z ; dakle*

$$z=v(x_1,\ldots,x_n)\ . \qquad (2)$$

Iz (1) i (2) nalazimo y=z, tj. $\mathfrak{M}$ *je trivijalan varijete, suprotno pretpostavci da sadrži netrivijalnu algebru. Dakle,* $y\notin\hat{f}(\underline{B})$, *pa* $\underline{B}\subsetneq\underline{A}$.

Primetimo da smo prema prethodnom dokazali nešto jače tvrdjenje:

(T1): Ako su Y,X skupovi slobodnih generatora slobodne algebre $\underline{A}$ *generisane skupom X, i ako je* $f:Y\xrightarrow[1-1]{}X$ *preslikavanje koje nije na onda postoji jedinstveno utapanje* $\hat{f}:\underline{B}\xrightarrow[1-1]{}\underline{A}$ *koje nije na, gde je* $\underline{B}$ *podalgebra generisana sa Y.*

---

[1] Ovaj zadatak omogućava uvodjenje pojma *ranga* algebre $\underline{A}$, u oznaci rang $\underline{A}$; naime, rang $\underline{A}$ je najmanji kardinalni broj $|X|$ takav da je X skup slobodnih generatora za $\underline{A}$.

Neka je sada $\underline{A}\in\mathcal{M}$ slobodna algebra sa beskonačnim skupom slobodnih generatora X. Dokazujemo

(T2): Ako skup Y generiše $\underline{A}$, onda $|Y| \geqslant |X|$.

Dokaz: Pretpostavimo da Y generiše $\underline{A}$ i da je $k=|X|$, $\lambda=|Y|$. Za svaki element $y\in Y$ postoji term t i elementi $x_1,\ldots,x_n\in X$ tako da $y=t^{\underline{A}}(x_1,\ldots,x_n)$. Dakle, $y\in \underline{B}_y$ gde je $\underline{B}_y\subseteq\underline{A}$ generisana skupom $X_y=\{x_1,\ldots,x_n\}$. Kako Y generiše $\underline{A}$, to skup $\bigcup_{y\in Y} X_y$ takodje generiše $\underline{A}$, pa s obzirom da je $\bigcup_{y\in Y} X_y\subseteq X$, prema (T1) sledi

$$X=\bigcup_{y\in Y} X_y \qquad (3)$$

Skup X je beskonačan i za svaki $y\in Y$, X_y je konačan; dakle i skup Y je beskonačan. Iz (3) sledi

$$k=|X| \leqslant |Y|\cdot \sup_{y\in Y}|X_y| \leqslant \lambda\cdot\aleph_0$$

Kako je λ beskonačan kardinal, to $\lambda\cdot\aleph_0=\lambda$, dakle $k\leqslant\lambda$. ▽

Prema (T2) neposredno sledi

(T3): Ako je $\underline{A}\in\mathcal{M}$ slobodna algebra generisana redom skupovima slobodnih generatora X,Y, od kojih je bar jedan beskonačan, onda $|X|=|Y|$.

Razmotrimo najzad slučaj slobodne algebre $\underline{A}\in\mathcal{M}$ generisane konačnim skupom slobodnih generatora X. Po pretpostavci, u $\mathcal{M}$ postoji konačna netrivijalna algebra $\underline{B}$. Svako preslikavanje $f: X\to B$ proširuje se do jedinstvenog homomorfizma $f:\underline{A}\to\underline{B}$ pa je broj svih homomorfizama iz $\underline{A}$ u $\underline{B}$ jednak $|B^X|=|B|^{|X|}$. Dakle, ako je Y neki drugi skup slobodnih generatora koji generiše algebru $\underline{A}$, onda $|B^Y|=|B^X|$, pa kako su skupovi X,Y konačni, sledi $|X|=|Y|$.

5.14. Ako je $\mathcal{M}$ klasa istotipnih algebri zatvorena za izomorfizme, podalgebre i direktne proizvode, dokazati da $\mathcal{M}$ sadrži slobodnu algebru nad svakim skupom X slobodnih generatora.

Rešenje: Bez gubljenja opštosti možemo uzeti da je $X=\{x_j \mid j\in J\}$ neki skup promenljivih. Dalje, neka je $\{q_i \mid i\in I\}$ skup svih kongruencija apsolutno slobodne algebre $\underline{A}$ nad X (jezika L klase algebri $\mathcal{M}$), takvih da $\underline{A}/q_i\in\mathcal{M}$.

Primetimo da za svaku algebru $\underline{B}\in\mathcal{M}$ koja je generisana nekim skupom Y, $|Y|\leqslant|X|$, postoji kongruencija q algebre $\underline{A}$ tako da $\underline{B}\cong\underline{A}/q$. Zaista, neka je $f: X\xrightarrow{na} Y$. Tada postoji homomorfizam $\hat{f}:\underline{A}\xrightarrow{na}\underline{B}$ takav da $f\subseteq\hat{f}$ i tada $\underline{B}\cong\underline{A}/\ker\hat{f}$. Lako je proveriti da

$$\ker\hat{f}=\{(u(x_1,\ldots,x_n),v(x_1,\ldots,x_n)) \mid n\in N,\ u,v\in Term(L),\ x_1,\ldots,x_n\in X,\ u^B(f(x_1),\ldots,f(x_n))=v^B(f(x_1),\ldots,f(x_n))\} \qquad (1)$$

Dakle, za dovoljno veliki skup X postoji kongruencija q algebre $\underline{A}$ *tako da* $\underline{A}/q \in \mathcal{M}$.

Neka su $\underline{A}_i = \underline{A}/q_i$, $i \in I$, *i neka je* $\underline{B}$ *podalgebra proizvoda* $\prod_{i\in I} \underline{A}_i$ *generisana skupom* $Y=\{a_j \mid j\in J\}$, *gde* $a_j(i)=x_j/q_i$, $i\in I$, $j\in J$. *Prema izboru kongruencija* q_i , $i\in I$, *i pretpostavkama o klasi* $\mathcal{M}$, *sledi* $\prod_i \underline{A}_i \in \mathcal{M}$, *i* $\underline{B}\in\mathcal{M}$.

Dokazujemo da je $\underline{B}$ *slobodna algebra u* $\mathcal{M}$ *sa skupom slobodnih generatora X. Zato, neka je* $\underline{D}\in\mathcal{M}$ *bilo koja algebra i* $f : Y \to D$ *neka funkcija. Preslikavanje f produžićemo do homomorfizma* $h : \underline{B} \to \underline{D}$.

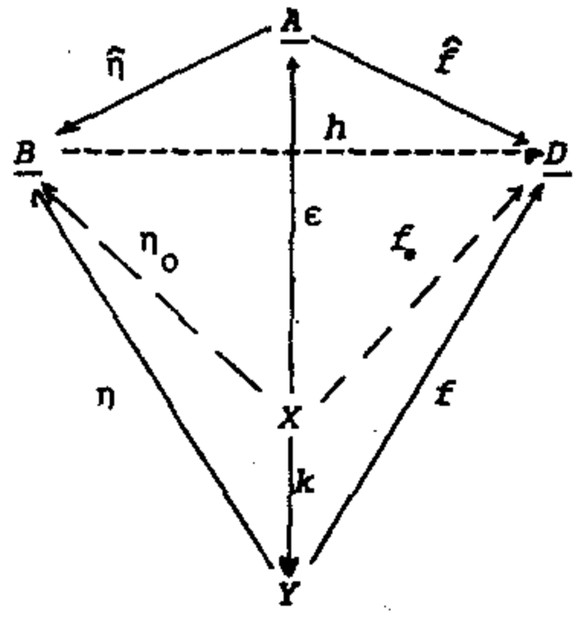
Uvedimo najpre sledeća preslikavanja:

$k : X \to Y$, $k(x_j)=a_j$, $j\in J$;

$f_o : X \to D$, $f_o = f\circ k$;

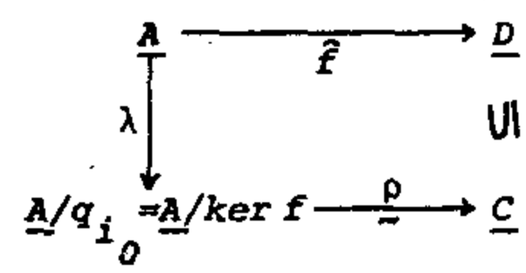
$\eta : Y \to B$, η *je inkluzivno preslikavanje;*

$\eta_o : X \to B$, $\eta_o = \eta\circ k$;



$\underline{A}$ *je apsolutno slobodna algebra, dakle postoji homomorfizam* $\hat{f} : \underline{A} \to \underline{D}$ *takav da* $\hat{f}\circ\varepsilon = f_0$, *gde je* $\varepsilon : X \to A$ *inkluzivno preslikavanje. Iz istog razloga postoji homomorfizam* $\hat{\eta} : \underline{A} \to \underline{B}$ *tako da* $\hat{\eta}\circ\varepsilon = \eta_o$.

Prema tome navedeni dijagram komutira. Dalje, postoji razlaganje homomorfizma $\hat{f}$, *kao što je prikazano na drugom dijagramu ; dakle,* $\lambda : \underline{A} \to \underline{A}/\ker f$ *je kanonski homomorfizam ,* $\rho : \underline{A}/\ker f \to \underline{C}$ *je izomorfizam i* $\underline{C}$ *je podalgebra algebre* $\underline{D}$. *Kako je* $\underline{D}$ *iz* $\mathcal{M}$ *i* $\mathcal{M}$ *je zatvorena za izomorfne slike i podalgebre, sledi* $\underline{A}/\ker f \in \mathcal{M}$, *pa za neki* $i_0\in I$, $q_{i_0} = \ker f$.



Homomorfizam $h : \underline{B} \to \underline{D}$ *odredićemo tako da bude* $h\circ\hat{\eta} = \hat{f}$, *tj. za u iz Term(L),* $h(\hat{\eta}(u)) = \hat{f}(u)$. *Stoga dokazujemo:*

(T1): Neka su $u,v \in Term(L)$; *tada:* $\eta(u) = \eta(v) \Rightarrow f(u) = f(v)$.

Dokaz: Neka su $u=u(x_1,\dots,x_n)$, $v=v(x_1,\dots,x_n)$, $x_1,\dots,x_n$ *termi jezika L. Tada*

$$\hat{\eta}(u)=\eta(u^A(x_1,\dots,x_n))=u^B(\hat{\eta}(x_1),\dots,\hat{\eta}(x_n))=u^B(\eta_o(x_1),\dots,\eta_o(x_n))=$$
$$u^B((\eta\circ k)(x_1),\dots,(\eta\circ k)(x_n))=u^B(\eta(a_1),\dots,\eta(a_n))=u^B(a_1,\dots,a_n).$$

Slično, $\hat{\eta}(v)=v^B(a_1,\dots,a_n)$.

Ako je $\underline{E}=\underline{A}/q_{i_0}$, *tada*

$$u^B(a_1,\dots,a_n)(i_0)=u^E(a_1(i_0),\dots,a_n(i_0))=u^E(x_1/q_{i_0},\dots,x_n/q_{i_0}) .$$

Slično

$$v^B(a_1,\dots,a_n)(i_0)=v^E(x_1/q_{i_0},\dots,x_n/q_{i_0}) .$$

Odavde nalazimo, pretpostavljajući $\hat{\eta}(u)=\hat{\eta}(v)$,

$$\rho(u^E(x_1/q_{i_0},\ldots,x_n/q_{i_0}))=\rho(v^E(x_1/q_{i_0},\ldots,x_n/q_{i_0}))\ .$$

Kako je $x_i/q_{i_0}=\lambda(x_i)$, *sledi*

$$u^C((\rho\circ\lambda)(x_1),\ldots,(\rho\circ\lambda)(x_n))=v^C((\rho\circ\lambda)(x_1),\ldots,(\rho\circ\lambda)(x_n))\ ,$$

tj.

$$u^D(f(a_1),\ldots,f(a_n))=v^D(f(a_1),\ldots,f(a_n))\ ,$$

jer $\underline{C}\subseteq\underline{D}$, $\hat{f}\restriction X=f_0$, $\hat{f}=\rho\circ\lambda$, $f_0=f\circ k$ *i* $f_0(x_i)=f(a_i)$, $i\in I$. *Ovim je tvrdjenje dokazano.* ∇

Preslikavanje $h:\underline{B}\to\underline{D}$ *definisano sa* $h(\eta(u))=f(u)$ *je dobro definisano, homomorfizam je algebre* $\underline{B}$ *u* $\underline{D}$ *i zadovoljava jednakost*

$$h\circ\eta=f \qquad (2)$$

Zaista, kako je $h\circ\hat{\eta}=\hat{f}$, *onda* $h\circ\hat{\eta}\circ\varepsilon=\hat{f}\circ\varepsilon$, *dakle* $h\circ\eta_0=f_0$. *Otuda* $h\circ\eta\circ k=f\circ k$, *tj. za sve* $x\in X$ $(h\circ\eta)(k(x))=f(k(x))$, *pa kako je k* $\underline{na}$ *preslikavanje, to* $(\forall y\in Y)(h\circ\eta)(y)=f(y)$, *tj. važi (2).*

Ovim je tvrdjenje zadatka u potpunosti dokazano.

5.15. Dokazati teoremu Birkhoff-a: Ako je $\mathcal{M}$ klasa algebri zatvorena za direktne proizvode, podalgebre i homomorfne slike, tada je $\mathcal{M}$ jednakosna klasa (varijete).

Rešenje: Neka je Z klasa svih zakona jezika L koji su zadovoljeni u svim algebrama klase $\mathcal{M}$ *i neka je* $\mathcal{N}$ *varijete klase zakona Z. Prema definiciji varijetea, neposredno sledi* $\mathcal{M}\subseteq\mathcal{N}$. *Dokazujemo da važi i*

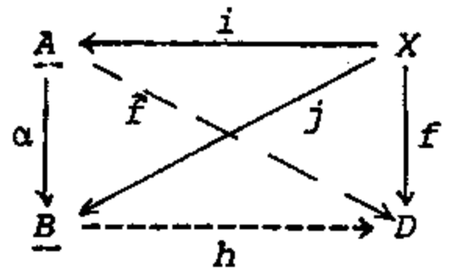
$$\mathcal{N}\subseteq\mathcal{M} \qquad (1)$$

Prema prethodnom zadatku klasa $\mathcal{M}$ *ima slobodnu algebru nad svakim skupom X slobodnih generatora. Prema zadatku 5.12. sledi da ukoliko je* $\underline{B}\in\mathcal{M}$ *slobodna algebra sa beskonačnim skupom slobodnih generatora, onda zakon u=v važi u* $\underline{B}$ *akko* $(u=v)\in Z$.

Neka je $\underline{D}\in\mathcal{N}$, $|X|\geqslant\max(|D|,\aleph_0)$ *i* $\underline{B}\in\mathcal{M}$ *slobodna algebra sa skupom X slobodnih generatora. Možemo uzeti da je X skup nekih promenljivih. Prema poslednjoj primedbi važi*

Ako $u^{\underline{B}}(x_1,\ldots,x_n)=v^{\underline{B}}(x_1,\ldots,x_n)$ *tada zakon u=v važi u* $\underline{B}$. (2)

Neka je $\underline{A}$ *apsolutno slobodna algebra nad X i* $f:X\xrightarrow{na}D$ *proizvoljno preslikavanje. Tada postoji homomorfizam* $\hat{f}:\underline{A}\to\underline{D}$. *Takodje, postoji homomorfizam* $\alpha:\underline{A}\to\underline{B}$. *Dakle, sledeći dijagram komutira*



i : X → A je inkluzivno preslikavanje

j : X → B je inkluzivno preslikavanje

Kako je f $\underline{na}$ *to je i* $\hat{f}$ $\underline{na}$.

Ako je $u=u(x_1,\ldots,x_n)$ *term jezika* L, $x_1,\ldots,x_n\in X$, *tada*
$\alpha(u)=\alpha(u^A(x_1,\ldots,x_n))=u^B(\alpha(x_1),\ldots,\alpha(x_n))=u^B(j(x_1),\ldots,j(x_n))=u^B(x_1,\ldots,x_n)$.
S druge strane
$\hat{f}(u)=\hat{f}(u^A(x_1,\ldots,x_n))=u^D(\hat{f}(x_1),\ldots,\hat{f}(x_n))=u^D(f(x_1),\ldots,f(x_n))$.
Dakle, ako su $u,v\in Term(L)$ *takvi da* $\alpha(u)=\alpha(v)$, *onda*
$u^B(x_1,\ldots,x_n)=v^B(x_1,\ldots,x_n)$, *pa prema (2) važi*
$u^D(f(x_1),\ldots,f(x_n))=v^D(f(x_1),\ldots,f(x_n))$. *Stoga važi implikacija:*

$$\alpha(u)=\alpha(v) \Rightarrow \hat{f}(u)=\hat{f}(v) \qquad (3)$$

Prema tome, preslikavanje $h : B \to D$ *definisano jednakošću* $h(\alpha(u))=f(u)$ *je dobro definisano i za njega je ispunjeno*

$$h\circ j=f \quad i \quad h \text{ je epimorfizam} . \qquad (4)$$

Dakle, $\underline{D}=h(\underline{B})$, *pa kako je klasa* $\mathcal{M}$ *zatvorena za homomorfizme , sledi* $\underline{D}\in\mathcal{M}$, *tj. važi (1). Prema tome,* $\mathcal{M}$ *je varijete klase zakona Z.*

5.16. Neka je Φ disjunkcija jednakosti jezika L. Ako Φ važi u svim algebrama varijetea $\mathcal{M}$, tada postoji jedan član disjunkcije, u=v, formule Φ takav da u=v važi u svim algebrama iz $\mathcal{M}$. Dokazati.

Rešenje: Neka je Φ *oblika* $u_1=v_1 \vee \ldots \vee u_n=v_n$ *i neka je* $\underline{A}\in\mathcal{M}$ *slobodna algebra sa beskonačnim skupom slobodnih generatora* $X=\{a_i \mid i\in I\}$. *Dalje, neka su vrednosti promenljivih slobodni generatori, tako da različitim promenljivima u* Φ *odgovaraju različite vrednosti. Tada u* $\underline{A}$ *važi*
$u_1^A(a_1,\ldots,a_k)=v_1^A(a_1,\ldots,a_k) \vee \ldots \vee u_n^A(a_1,\ldots,a_k)=v_n^A(a_1,\ldots,a_k)$,
pa za neki $i\leq n$ *u* $\underline{A}$ *važi* $u_i^A(a_1,\ldots,a_k)=v_i^A(a_1,\ldots,a_n)$.
S obzirom da su $a_1,\ldots,a_n$ *slobodni generatori algebre* $\underline{A}$, *to prema zadatku 5.12. zakon* $u_i=v_i$ *važi u svim algebrama varijetea* $\mathcal{M}$.

5.17. Neka je σ formula $(\forall x,y)(x^2=y^2 \vee xy=yx)$. Dokazati:
a) Postoji nekomutativna grupa koja zadovoljava σ.
b) Ako je $\mathcal{M}$ neki varijete grupa i σ je tačna u svim grupama $G\in\mathcal{M}$, tada je svaka grupa iz $\mathcal{M}$ komutativna.

Rešenje: a) Grupa kavaterniona zadovoljava rečenicu σ.
b) Ukoliko je σ *tačna u svim grupama jednakosne klase* $\mathcal{M}$, *onda prema prethodnom zadatku u svim grupama jednakosne klase* $\mathcal{M}$ *važi jedan od zakona* $xy=yx$, $x^2=y^2$. *Ukoliko* $x^2=y^2$ *važi u* $\mathcal{M}$, *tada* $x^2=1$ *takodje važi u* $\mathcal{M}$. *Ali, svaka grupa koja zadovoljava zakon* $x^2=1$ *je komutativna.*

5.18. Dokazati stav potpunosti za jednakosnu logiku: Ako je $\mathcal{M}$ varijete klase zakona Z (jezika L), onda za svaku formulu u=v jezika L važi

$$Z \underset{J}{\vdash} u=v \quad \text{akko } u=v \text{ važi u svim algebrama varijetea } \mathcal{M}.$$

Rešenje: Neka je $\mathcal{M}$ varijete klase zakona Z. Indukcijom po dužini dokaza u jednakosnoj logici dokazuje se:

Ako $Z \vdash u=v$ tada sve algebre iz $\mathcal{M}$ zadovoljavaju zakon $u=v$. Pretpostavimo sada da nije $Z \vdash u=v$, i neka je $\underline{B} \in \mathcal{M}$ slobodna algebra sa prebrojivo mnogo slobodnih generatora. Ako je $\underline{A}$ apsolutno slobodna algebra nad X možemo uzeti $\underline{B}=\underline{A}/\sim$ gde je

$\sim = \{(u,v) \mid u,v \in Term(L)$ *sa promenljivima u skupu X,* $Z \vdash u=v\}$,

(videti zadatak 5.6.). Tada $u/\sim \neq v/\sim$ jer nije $u \sim v$.

Neka je $u=u(x_1,\ldots,x_n)$, $v=v(x_1,\ldots,x_n)$. Tada $u^B(x_1/\sim,\ldots,x_n/\sim)=u/\sim$ i $v^B(x_1/\sim,\ldots,x_n/\sim)=v/\sim$, dakle

$$u^B(x_1/\sim,\ldots,x_n/\sim) \neq v^B(x_1/\sim,\ldots,x_n/\sim) ,$$

pa zakon $u=v$ ne važi u algebri $\underline{B}$.

5.19. Neka je $\mathcal{M}$ varijete i $\underline{A}_i \in \mathcal{M}$ za $i \in I$. Tada slobodan proizvod algebri $\underline{A}_i$ $(i \in I)$ postoji u $\mathcal{M}$ akko postoji algebra $\underline{B} \in \mathcal{M}$ takva da se svaka algebra $\underline{A}_i$ utapa u $\underline{B}$. Dokazati.

Rešenje: Neka je L algebarski jezik varijetea $\mathcal{M}$ i pretpostavimo da je $\mathcal{M}$ klase zakona Z. Jezik L obogaćujemo na sledeći način. Neka je za svaki $i \in I$ $S_i = \{\underline{a} \mid a \in A_i\}$. Ovde $\underline{a}$ označava nov simbol konstante, dakle $\underline{a} \notin L$. Možemo uzeti da su $\underline{a}$, $\underline{b}$ različiti simboli ukoliko $a,b \in A$ i $a \neq b$, ili, ako a,b pripadaju različitim algebrama familije $\underline{A}_i$, $i \in I$. Neka je

$$L^* = L \cup \Big(\bigcup_{i \in I} S_i \Big) .$$

Dalje, neka je za svaki $i \in I$

$$\Sigma_i = \{ u(\underline{a}_1,\ldots,\underline{a}_n)=v(\underline{a}_1,\ldots,\underline{a}_n) \mid u,v \in Term(L),\ a_1,\ldots,a_n \in A_i,\ n \in \omega,$$
$$u^{A_i}(a_1,\ldots,a_n)=v^{A_i}(a_1,\ldots,a_n)\}.$$

Tada je

$$Z^* = Z \cup \Big(\bigcup_{i \in I} \Sigma_i \Big)$$

klasa zakona jezika L i neka je $\mathcal{M}^*$ varijete odredjen sa Z^* .

Po pretpostavci, za svaki $i \in I$ postoji utapanje $h_i : \underline{A}_i \to \underline{B}$. Tada $\underline{B}^* \in \mathcal{M}^*$ gde $\underline{B}^* = (\underline{B}, h_i(a))_{i \in I, a \in A_i}$.

Neka je $\underline{A}^*$ slobodna algebra varijetea $\mathcal{M}^*$ sa skupom slobodnih generatora $X=\emptyset$. Očigledno, $\underline{A}^*$ je oblika $\underline{A}^* = (\underline{A}, a')_{i \in I, a' \in A_i}$ gde je $\underline{A}$ neka algebra varijetea $\mathcal{M}$, ovde je a' interpretacija simbola $\underline{a}$ u $\underline{A}^*$, tj. $a' = \underline{a}^{A^*}$, $\underline{a} \in \bigcup_i S_i$.

Neka je $\varepsilon_i : A_i \to A$ definisano sa $\varepsilon_i(a)=a'$, $a \in A_i$.

Dokažimo da je ε_i utapanje algebre $\underline{A}_i$ u algebru $\underline{A}$.

- *ε_i je homomorfizam: neka je F n-arni operacijski znak jezika L i $a_1,\ldots,a_n,a$ iz A_i takvi da $a=F^{A_i}(a_1,\ldots,a_n)$. Tada*

$(\underline{a} = F(\underline{a}_1,\ldots,\underline{a}_n)) \in \sum^*$, odakle sledi $a' = F^{A^*}(a'_1,\ldots,a'_n)$.
Otuda $$\varepsilon_i(F^{A_i}(a_1,\ldots,a_n)) = F^{A}(\varepsilon_i(a_1),\ldots,\varepsilon_i(a_n)).$$

• ε_i je 1-1: kako je $\underline{A}^*$ slobodna algebra varijetea $\mathcal{M}^*$, to postoji homomorfizam $\Psi : \underline{A}^* \to \underline{B}^*$; dakle $\Psi(a') = h_i(a)$ za $a \in A_i$, $i \in I$. Kako za različite $a,b \in A_i$ $h_i(a) \neq h_i(b)$, sledi $(\Psi \circ \varepsilon_i)(a) \neq (\Psi \circ \varepsilon_i)(b)$, tj. $\varepsilon_i(a) \neq \varepsilon_i(b)$.

Najzad, neka je $\underline{C} \in \mathcal{M}$ i za svaki $i \in I$ neka je $\alpha_i : \underline{A}_i \to \underline{C}$ homomorfizam. Neposredno se proverava da je $\underline{C}^* \in \mathcal{M}^*$, gde $\underline{C}^* = (\underline{C}, \alpha_i(a))_{i \in I, a \in A_i}$.
A^* je slobodna algebra varijetea $\mathcal{M}^*$, **dakle postoji homomorfizam** $\alpha : A^* \to C^*$. Stoga, $\alpha(a') = \alpha_i(a)$ za $i \in I$, $a \in A_i$, tj. $\alpha\varepsilon_i = \alpha_i$. Očigledno, α je takodje homomorfizam algebre $\underline{A}$ u algebru $\underline{C}$.

Dakle, $(A, \varepsilon_i)_{i \in I}$ je slobodan proizvod algebri A_i .

10.6. STRUKTURNE JEDNAKOSTI - PREDSTAVLJANJE ALGEBRI

U dokazu teoreme 5.3., domen slobodne algebre $\underline{A}/_{\sim}$ za varijete $\mathfrak{M}$ sastoji se od klasa kongruencije $v/_{\sim}$, $v \in Term(L)$. Prirodno se postavlja pitanje mogu li se iz ovih klasa izabrati predstavnici, i nad njima konstruisati odgovarajuća slobodna algebra. Otuda se uvode sledeći pojmovi ($L, \mathfrak{M}, Z, X, A, \sim$ su kao u teoremi 5.3. i napomeni 5.5.):

6.1. Definicija: Neki skup zatvorenih terma M jezika $L \cup X$ je skup markera[1] *(svedenih) ukoliko su ispunjeni sledeći uslovi:*

(i) Za svaki zatvoren term u jezika $L \cup X$ postoji $m \in M$ tako da $u \sim m$.

(ii) Ako je $m \in M$ i c simbol konastante iz $L \cup X$ koji se javlja u m , tada $c \in M$ ili postoji $d \in C \cup X$ takav da $c \sim d$.

Neki skup S formula oblika u=m, gde je u zatvoren term jezika $L \cup X$, $m \in M$, je *skoro tablica* akko za svaki funkcijski znak $f \in L$, $ar(f)=k$, važi:

$(\forall m_1, \ldots, m_k \in M)(\exists_1 m \in M)(f(m_1, \ldots, m_k)=m) \in S$;

ako $(u=m) \in S$ tada $u \sim m$;

ako $(f(t_1, \ldots, t_k)=m) \in S$ tada $t_1, \ldots, t_k, m \in M$.

Skoro tablica je *slegnuta* ukoliko za sve $m, m' \in M$, $m \sim m' \Rightarrow m=m'$.

Rešavajuća struktura je algebra $\underline{M}$ jezika $L \cup X$ definisana na sledeći način: domen algebre $\underline{M}$ je skup markera M. Za funkcijski znak $f \in L$, $ar(f)=k$, $m_1, \ldots, m_k, m \in M$, $f^M(m_1, \ldots, m_k)=m$ akko $(f(m_1, \ldots, m_k)=m) \in S$. Za simbol konstante $c \in L \cup X$, $c^M=m$ akko $(c=m) \in S$.

6.2. Teorema (S.Preš[2]*:*

A. Sledeći usl... su ekvivalentni:

(i) S je sl... za skoro tablica

(ii) Rešavaj... struktura $\underline{M}$ zadovoljava sve zakone skupa S.

(iii) Postoji ...gebra $\underline{B}$ jezika $L \cup X$ tako da za sve $m_1, m_2 \in M$ $m_1 \neq m_2 \rightarrow m_1^B \neq m_2^B$

(iv) Ako je $t \in M$, vrednost terma t u rešavajućoj strukturi $\underline{M}$ je t, tj. $t^M=t$.[3]

---

1) Tačnije $(\mathfrak{M}, Z, X)$-markera, ali ovaj prefiks ubuduće izostavljamo.

2) Videti [12].

3) Primetimo da je svaki element t domena M term, dakle može se govoriti o vrednosti terma t u algebri $\underline{M}$.

B. Rešavajuća struktura $\underline{M}$ je slobodna algebra za varijete $\mathcal{M}$ sa skupom slobodnih generatora X akko zadovoljava ove uslove:

(i) S je slegnuta skoro tablica ,

(ii) $\underline{M}$ zadovoljava sve zakone iz Z .

Neka je Z skup nekih zakona algebraskog jezika L , K neki skup simbola konstanti i R skup jednakosti u=v, gde su u,v zatvoreni termi jezika $L \cup K$.

6.3. *Definicija: Uredjeni par (K;R) naziva se postavkom (prezentacijom, predstavljanjem), a elementi skupa R strukturnim jednakostima.*

Za postavku Π koristimo sledeću oznaku: $\Pi = \langle K;R \rangle$.
Za slobodnu algebru $\underline{A}$ jezika $L \cup K$ klase zakona $Z \cup R$ sa skupom slobodnih generatora $X = \emptyset$, kažemo da je odredjena prezentacijom Π, u oznaci $\underline{A} = \underline{A}_{\Pi}$.

6.4. Napomena: Neka je $\underline{A}_n = (\underline{A}, a_i)_{i \in I}$, a_i je interpretacija simbola $c_i \in K$ u $\underline{A}_{\Pi}$, $K = \{c_i \mid i \in I\}$, algebra odredjena prezentacijom $\Pi = \langle K;R \rangle$. Tada:

1° $\underline{A}_{\Pi}$ je generisana elementima skupa $\{a_i \mid i \in I\}$,

2° Kako je $\underline{A}_{\Pi}$ slobodna algebra za $Z \cup R$, to svaka algebra $\underline{B}$ koja zadovoljava zakone iz Z i generisana je elementima $b_i \in B$ tako da $(\underline{B}, b_i)_{i \in I}$ zadovoljava zakone iz $Z \cup R$, jeste homomorfna slika algebre $\underline{A}$. Uslov da $(\underline{B}, b_i)_{i \in I}$ zadovoljava zakone iz $Z \cup R$ može se zameniti ovim:
Ako za sve $a_{i_1}, \ldots, a_{i_n}, b_{i_1}, \ldots, b_{i_n}$ i svaki zakon
$u(c_1, \ldots, c_n) = v(c_1, \ldots, c_n)$ iz R važi implikacija
$u^A(a_{i_1}, \ldots, a_{i_n}) = v^A(a_{i_1}, \ldots, a_{i_n}) \Rightarrow u^B(b_{i_1}, \ldots, b_{i_n}) = v^B(b_{i_1}, \ldots, b_{i_n})$,
onda postoji homomorfizam $h : \underline{A} \to \underline{B}$ tako da $(\forall i \in I) h(a_i) = b_i$.

3° Neka je $\underline{C}$ slobodna algebra za jezik $L \cup K$ za praznu klasu zakona , i $\sim$ najmanja kongruencija algebre $\underline{C}$ tako da $(u=v) \in R$ povlači $u^C = v^C$, tj.
$\sim = \{\rho \mid \rho$ je kongruencija algebre $\underline{C}$ i $\{(u^C, v^C) \mid (u=v) \in R\} \in \rho\}$.
Tada je $A_{\Pi} = \underline{C}/\sim$, gde je $\Pi = \langle K;R \rangle$.

Napomenimo da je $u^C \sim v^C$ akko $Z \cup R \underset{J}{\vdash} u=v$, gde su u,v,zatvoreni termi jezika $L \cup K$.

Primeri i zadaci

U sledećim slučajevima odrediti slobodnu algebru $\underline{A}$ jezika L nad skupom K slobodnih generatora, klase zakona Z .

6.1. $L=\{1,\cdot,a,b\}$, $Z=\{(x\cdot y)\cdot z=x\cdot(y\cdot z),\ x\cdot y=y\cdot x,\ 1\cdot x=x,\ a^3=a,\ b^3=b,\ ab=1\}, K=\emptyset$

Rešenje: Za skup markera može se uzeti $M=\{1,a,b,a^2,b^2\}$. *Tablica algebre* $\underline{A}$ *je*

	1	a	a^2	b	b^2
1	1	a	a^2	b	b^2
a	a	a^2	a	1	b
a^2	a^2	a	a^2	a	1
b	b	1	a	b^2	b
b^2	b^2	b	1	b	b^2

6.2. $L=\{1,\cdot\}$, $Z=\{(x\cdot y)\cdot z=x\cdot(y\cdot z),\ x\cdot y=y\cdot x,\ x^2=1,\ 1\cdot x=x\}$, $K=\{a,b\}$

Rešenje: Jedan skup markera je $M=\{1,a,b,ab\}$; *tablica algebre* $\underline{A}$ *je*

	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

6.3. $L=\{\cdot\}$, $Z=\{(x\cdot y)\cdot z=x\cdot(y\cdot z),\ x\cdot y=y\cdot x,\ x^4=x^2\}$, $K=\{a,b,c\}$

Rešenje: Jedan skup (neekvivalentnih) markera je

$$M=\{a^\alpha b^\beta c^\gamma \mid \alpha,\beta,\gamma\in\{0,1,2,3\}\}$$

Ovde $a^0=b^0=c^0=1$. *Algebra* $\underline{A}$ *je konačna i* $|A|=4^3=64$.

Na primer, u algebri $\underline{A}$ *za* $x=a^3b^2c$, $y=a^2b^2c$ *je* $x\cdot y=a^3b^2c^2$.

6.4. $L=\{1,\cdot\}$, $Z=\{(x\cdot y)\cdot z=x\cdot(y\cdot z),\ x\cdot y=y\cdot x,\ 1\cdot x=x\}$, $K=\{a_1,a_2,\ldots\}$

Rešenje: $\underline{A}=(N,\cdot,1)$, $N=\{1,2,3,\ldots\}$ $a\cdot$ *je množenje prirodnih brojeva.*

Jedan izomorfizam $f:\underline{N}\to\underline{A}$ *dat je sa*

$$f(p_{i_1}^{\alpha_1}\ldots p_{i_n}^{\alpha_n})=a_{i_1}^{\alpha_1}\ldots a_{i_n}^{\alpha_n}\ ,\quad \alpha_1,\ldots,\alpha_n\in\{1,2,\ldots\},\ p_1,p_2,\ldots \text{ je}$$

niz prostih brojeva $2,3,5,7,11,\ldots$.

6.5. $L=\{\cdot\}$, $Z=\{(x\cdot y)\cdot z=x\cdot(y\cdot z)\ ,\ x^2=x\}$, $K=\{a,b\}$.

Rešenje: Skup markera je $M=\{a,b,ab,ba,aba,bab\}$. *Npr.* $(aba)(bab)=ab,\ldots$

6.6. $L=\{\cdot\}$, $Z=\{xy=x\}$, $K=\{a,b,c\}$.

Da li je algebra $\underline{A}$ izomorfna slobodnoj algebri $\underline{A}'$ odredjenoj istim skupom K i zakonom $xy=y$?

Rešenje: Jedan skup markera je $M=\{a,b,c\}$ *, a tablica algebre* $\underline{A}$ *je*

	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

Tablica druge algebre $\underline{A}'$ *je*

	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

$\underline{A} \not\cong \underline{A}'$ *jer algebra* $\underline{A}$ *ima desnu jedinicu a algebra* $\underline{A}'$ *nema.*

6.7. $L=\{\cdot\}$, $Z=\{xy=yx,\ x^2=x,\ ((xy)z)u=(x(yz))u,\ (xy)(zu)=((xy)z)u\}$, $K=\{a,b\}$.

Rešenje: Dokazujemo da je svaki zatvoren term jezika U *ekvivalentan u jednakosnoj logici jednom od terama iz skupa* $M=\{a,b,ab,a(ab),b(ab)\}$.

Dokaz izvodimo indukcijom po dužini $|t|$ *terma* t.

Neka je $|t|=4$ *, tada* t *ima jedan od oblika*

$$((xy)z)u\ ,\quad (xy)(zu)\ ,\quad (x(yz))u\ ,\quad x((yz)u)\ ,\quad x(y(zu))\ .$$

Prema datim zakonima važi:

$$(xy)(zu)=((xy)z)u=(x(yz))u \qquad (1)$$

Kako je $x((yz)u)=((yz)u)x=(y(zu))x=x(y(zu))$ *, to*

$$x((yz)u)=x(y(zu)) \qquad (2)$$

Skup K *je dvočlan, pa za* $x,y,z\in K$ *važi* $x=y$ *ili* $x=z$ *ili* $y=z$. *Ako je* t *oblika (1), onda:*

ako je $x=y$ *tada* $t=((xy)z)u=(xz)u$ *jer* $x^2=x$ *,*

ako je $x=z$ *tada* $t=((xy)z)u=(z(xy))u=((zx)y)u=(xy)u$ *,*

ako je $y=z$ *tada* $t=(x(yz))u=(xy)u$.

Odavde se lako dobija $Z\vdash_J t=u$ *za neki* $u\in M$.

Slično važi ukoliko je t *oblika (2).*

Neka je $\alpha=ab$, $\beta=a(ab)$, $\gamma=b(ab)$. *Tada skoro-tablica* S *, odnosno pripadna rešavajuća struktura* $\underline{M}$ *izgleda ovako*

	a	b	α	β	γ
a	a	α	β	β	β
b	α	b	γ	γ	γ
α	β	γ	α	α	α
β	β	γ	α	β	γ
γ	β	γ	α	α	γ

Neposredno se proverava da je S *slegnuta skoro tablica i da* $\underline{M}$ *zadovoljava sve zakone iz* Z. *Dakle,* $\underline{M}$ *je slobodna algebra nad* $\{a,b\}$ *za dati skup zakona* Z .

6.8. $L=\{0,\cdot,+,-\}$, Z : aksiome prstena sa jedinicom, $2x=x$, $x^2=x$; $K=\{a,b,c\}$

Rešenje: Kako je $(x+y)^2=x+y$ *i* $(x+y)^2=x^2+xy+yx+y^2=x+y+xy+yx$ *to* $x+y+xy+yx=x+y$, *tj.* $xy+yx=0$. *Otuda* $xy=-yx=yx$ *jer* $x=-x$. *Dakle,* $Z\vdash_J xy=yx$.

Odavde se neposredno izvodi da se za skup markera može uzeti

$$M=\{\alpha\cdot 1+\beta_1 a+\beta_2 b+\beta_3 c+\gamma_1 ab+\gamma_2 ac+\gamma_3 bc+\lambda abc \mid \alpha,\beta_i,\gamma_i,\lambda\in\{0,1\}\}\ .$$

Dakle, $|M|=2^8$.

Slobodna algebra za Z nad $\{a,b,c\}$ *izomorfna je prstenu* $(\mathcal{P}(X),\cap,\Delta,\emptyset,X)$ *gde je X skup od 8 elemenata a* Δ *je simetrična razlika.*

6.9. $L=\{0,\cdot,+,-\}$, Z : aksiome prstena, $xy=yx$, $x^2=x$; $K=\{a,b,c\}$

Rešenje: Za skup markera može se uzeti

$$M=\{\alpha_1 a+\alpha_2 b+\alpha_3 c+\beta_1 ab+\beta_2 ac+\beta_3 bc+\gamma abc \mid \alpha_1,\alpha_2,\alpha_3,\beta_1,\beta_2,\beta_3,\gamma \in Z\}$$

$Z=\{\ldots,-2,-1,0,1,2,\ldots\}$.

6.10. $L=\{0,1,\wedge,\vee,'\}$, Z : aksiome Boole-ove algebre ; $K=\{a,b\}$

Rešenje: Slobodna algebra ima 16 članova ; to su disjunkti elemenata ab, ab', a'b, a'b' i konstanti 0,1 .

6.11. $L=\{0,1,a,b,\wedge,\vee,'\}$, Z : aksiome Boole-ove algebre, $a\wedge b=0$; $K=\emptyset$

Rešenje: Ova algebra ima 8 članova.

6.12. $L=\{1,\cdot,^{-1}\}$, Z : aksiome grupe, $xy=yx$, $x^3=1$; $K=\{a,b\}$.

Rešenje: $\underline{A}\cong C_3\times C_3$

6.13. $L=\{1,\cdot,^{-1}\}$, Z : aksiome grupa, $x^2=1$; $K=\{a_1,a_2,\ldots,a_n\}$.

Rešenje: $\underline{A}\cong C_2^n$

6.14. $L=\{1,\cdot,^{-1},a,b\}$, Z : aksiome grupe , $a^5=1$, $b^2=1$, $ba=ab^4$; $K=\emptyset$

Rešenje: $\underline{A}\cong D_5$.

U sledećim zadacima odrediti algebru $\underline{A}_\Pi$ odredjenu prezentacijom $\Pi=<K;R>$ za klasu zakona Z jezika L:

6.15. $\Pi=<a,b;\ a^3=a,b^3=b,ab=1>$, Z : aksiome komutativnih monoida, $L=\{1,\cdot\}$.

Rešenje: Za skup markera može se uzeti $\{1,a,b,a^2,b^2\}$.

6.16. $\Pi=<a,b,c;\ \emptyset>$, $Z=\{xy=yx\}$, $L=\{\cdot\}$

Rešenje: Jedan skup markera je $\{a,b,c\}$

6.17. $\Pi=<a,b;\ 10a=0,5b=0,4a=3b,a^2=3a,b^2=2a,ab=4a>$, Z : aksiome komutativnog prstena , $L=\{+,\cdot,0\}$.

Rešenje: $\underline{A}_\Pi=(Z_{10},+_{10},\cdot_{10},0)$. *Razmotriti preslikavanje* $\phi: A \to Z_{10}$, *gde* $\phi(a)=3$, $\phi(b)=4$.

6.18. $\Pi = \langle a,b;\ a^5=1, b^2=1, ba=ab^4 \rangle$, Z : aksiome grupa , $L=\{1,\cdot,^{-1}\}$.

Rešenje: $\underline{A}_\Pi \cong D_5$.

6.19. $\Pi = \langle a,b;\ a \wedge b=0 \rangle$, Z : aksiome Boole-ovih algebri , $L=\{\wedge, \vee, ', 0, 1\}$.

Rešenje: $\underline{A}_\Pi \cong \underline{2}^3$ ($\underline{2}^3$ *je Boole-ova algebra od 8 elemenata).*

6.20. $\Pi = \langle a_1, a_2, \ldots;\ \{a_i a_j = a_j a_i \mid i,j \in N\} \rangle$, Z : aksiome monoida, $L=\{1,\cdot\}$.

Rešenje: $\underline{A}_\pi \cong (N,\cdot,1)$ *, gde je* $N=\{1,2,3,\ldots\}$ *i* $\cdot$ *množenje prirodnih brojeva. Razmotriti preslikavanje* $\phi : \underline{A}_\Pi \to N$ *, gde je* $\phi(a_i)=p_i$ *,* p_i *je i-ti prost broj .*

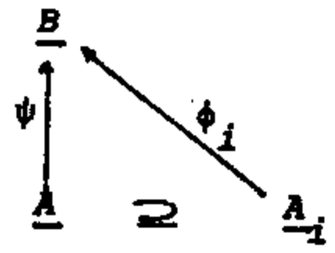
6.21. Dokazati tvrdjenja iz napomene 6.4.

6.22. Neka je $\mathcal{M}$ varijete klase zakona Z. Algebra $\underline{A} \in \mathcal{M}$ je slobodan proizvod u $\mathcal{M}$ nekih svojih podalgebri $\underline{A}_i$, $i \in I$, ukoliko je za svaki $i \in I$ algebra $\underline{A}_i$ odredjena nekom prezentacijom $\Pi_i = \langle K_i; R_i \rangle$ za klasu zakona Z tako da je

$$\Pi = \langle K; R \rangle$$

prezentacija algebre $\underline{A}$ za klasu zakona Z , gde je K disjunktna unija skupova K_i , a R disjunktna unija skupova R_i , i za svaki par $i \neq j$, $A_i \cap A_j$ je minimalna podalgebra algebre $\underline{A}$.

Rešenje: Neka je $\mathcal{M}'$ *varijete klase zakona* $Z' = Z \cup R$ *. Ako je L jezik klase zakona Z , tada je jezik L' klase zakona Z' dobijen dodavanjem novih simbola konstanti, upravo onih koji se javljaju u R. Dakle,* $L' = L \cup \{c_i \mid i \in I\}$ *za neki skup I. Tada je algebra* $\underline{A}' = (\underline{A}, a_i)_{i \in I}$ *odredjena prezentacijom* Π*, slobodna algebra nad praznim skupom generatora.*
Neka je $\underline{B} \in \mathcal{M}$ *proizvoljna algebra i neka su* $\phi_i : \underline{A}_i \to \underline{B}$ *neki homomorfizmi. Tada algebra* $\underline{B}$ *ima raširenje do algebre* $\underline{B}' = (\underline{B}, b_i)_{i \in I}$ *varijetea* $\mathcal{M}'$*. Neka je* ϕ *preslikavanje odredjeno sa* $\phi = \bigcup_I \phi_i$ *. S obzirom da je* $\underline{A}'$ *slobodna algebra varijetea* $\mathcal{M}'$*, to postoji homomorfizam* $\psi : \underline{A}' \to \underline{B}$ *tako da* $\phi \leq \psi$ *. Dakle dijagram komutira za svaki* $i \in I$*. Otuda,* $\underline{A}$ *je slobodan proizvod algebri* $\underline{A}_i$ *.*



6.23. Odrediti slobodan proizvod monoida $\langle a_i; \emptyset \rangle$, $i \in N$, u varijeteu komutativnih monoida.

11. SLOBODNE GRUPE, SLOBODAN PROIZVOD

11.1. SLOBODNE GRUPE

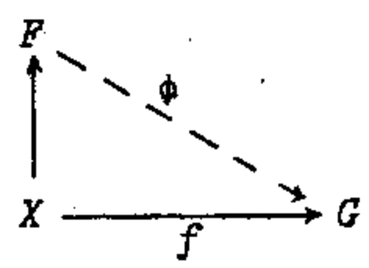
U poglavlju 10. bilo je reči o slobodnim algebrama uopšte. Konkretizujući definicije i teoreme za jedan poseban jezik L i posebnu klasu zakona Z, u slučaju grupa, kao osnovno izdvajamo sledeće.

Neka je $L=\{\cdot, ^{-1}, e\}$, gde su $\cdot$ i $^{-1}$ redom operacijski znaci dužine dva i jedan, a e je simbol konstante. Dalje, neka je Z sledeća klasa algebarskih zakona

$$Z: \quad \begin{array}{l} (x\cdot y)\cdot z = x\cdot(y\cdot z) \\ x\cdot x^{-1} = e, \quad x^{-1}\cdot x = e \\ x\cdot e = x, \quad e\cdot x = x \end{array}$$

Algebra jezika L koja zadovoljava zakone Z je *grupa*. Dakle, klasa $\mathcal{M}$ svih grupa je jedan varijete (za Z) - *varijete grupa*.

1.1. *Definicija: Grupa F je slobodna (za klasu svih grupa $\mathcal{M}$) sa skupom slobodnih generatora X ako je $X \subseteq F$ i za svaku grupu G iz $\mathcal{M}$ i svako preslikavanje $f: X \to G$, postoji jedinstveni homomorfizam $\phi: F \to G$ koji je proširenje preslikavanja f.*



Prema teoremi 5.3. iz poglavlja 10., važi:

1.2. *Teorema: Za varijete grupa $\mathcal{M}$ i za svaki skup X, postoji jedinstvena (do na izomorfizam) slobodna grupa F sa skupom slobodnih generatora X.*

Konstrukcija slobodne grupe nad proizvoljnim skupom slobodnih generatora, data je u zadatku 10.5.10.

Neka je Ab sledeća klasa algebarskih zakona

$$Ab = Z \cup \{xy=yx\}$$

(tj. teorija Abel-ovih grupa).

1.3. *Definicija: Grupa G je slobodna Abel-ova grupa ako je G slobodna algebra jezika L klase zakona Ab, sa skupom slobodnih generatora X.*

Iz istih razloga kao i teorema 1.2., važi sledeća

1.4. *Teorema: Za svaki skup X postoji slobodna Abel-ova grupa sa skupom slobodnih generatora x.*

Konstrukcija slobodne Abel-ove grupe data je u zadatku 10.5.5.

1.5. *Definicija: Rang slobodne grupe F, u oznaci rang F, je* $|X|$.

Da je rang dobro definisan, dokazano je u zadatku 1.2.
Slobodnu grupu konačnog ranga n, obeležavamo i sa F_n.

Slobodna grupa F je generisana skupom svojih slobodnih generatora (v. zad. 1.1.). Nije, medjutim, svaki skup generatora za F, ujedno i skup *slobodnih* generatora za F (v.zad. 1.8.). Koristićemo stoga dve oznake - $F = \langle X \rangle$ i $F = \langle X \rangle_s$ koje, redom, znače: "F je generisana sa X", i "F je slobodno generisana sa X".
Skup X slobodnih generatora za F naziva se i *bazom* grupe F.

Prema teoremi 5.6. iz poglavlja 10., važi

1.6. *Teorema: Neka je G grupa odredjena na sledeći način:*

$G = \{C_t \mid t \in Term(L),\ t \text{ je zatvoren term}\}$,

gde su C_t *klase ekvivalencije u odnosu na relaciju*

$$t_1 \sim t_2 \overset{def}{\Longleftrightarrow} Z_X \underset{J}{\vdash} t_1 = t_2$$

$$Z_X = \{t_1(x_1,\ldots,x_n) = t_2(y_1,\ldots,y_m) \mid (t_1=t_2) \in Z;\ x_1,\ldots,x_n,y_1,\ldots,y_m \in Term(L \cup X)\}$$

Operacije $\circ$ *i* $\tilde{}$ *(koje odgovaraju operacijskim slovima* $\cdot$ *i* $^{-1}$ *iz L)*
su

$$C_{t_1} \circ C_{t_2} = C_{t_1 \cdot t_2}, \quad \tilde{C_{t_1}} = C_{t_1^{-1}}$$

Konstanti e iz L odgovara konstanta C_e *(u oznaci* 1_G*).*

Tada je G slobodna grupa generisana skupom X.

Dalje, direktno prema 10.6. uvode se pojmovi *naznačenih* terma *(markera)*, *skoro-tablice*, *slegnute* skoro-tablice i *rešavajuće strukture*.
Za grupe važi specijalni slučaj teoreme 10.6.1.

Svaki element g ($\neq 1$) slobodne grupe F, $F = \langle X \rangle_s$, se jedinstveno prikazuje izrazom u tzv. *svedenom* obliku

$$g = x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k} \qquad (k > 0) \qquad (*)$$

($x_i \in X$, $\varepsilon_i = \pm 1$, $x_i = x_{i+1} \Rightarrow \varepsilon_i \neq -\varepsilon_{i+1}$) (videti zadatak 10.5.10.)
Broj k je *dužina* izraza g. Dužina jediničnog elementa je 0.
Dakle, dužina izraza g_1 predstavljenog u obliku

$$g_1 = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \ldots x_k^{\alpha_k} \qquad (*')$$

gde je $x_i \neq x_{i+1}$ $(i=1,\ldots,k-1)$, $\alpha_j \in Z \setminus \{0\}$ $(j=1,\ldots,k)$, je $|\alpha_1|+\ldots+|\alpha_k|$.
Tvrdjenje da se svaki nejedinični element iz F jedinstveno predstavlja pomoću (*), naziva se često *teoremom o normalnoj formi*. Zahvaljujući ovoj

teoremi se i može govoriti o *dužini izraza*, odnosno *dužini elementa* grupe predstavljenog odgovarajućim izrazom.

Odgovor na pitanje kakve su podgrupe slobodne grupe, daje naredna teorema 1.8., za čiji se dokaz koriste sledeći pojmovi.
Neka je G grupa, H njena podgrupa i $Hx_1, Hx_2, \ldots$ razlaganje G po desnim razredima od H. Izaberimo iz svakog razreda Hg po jednog predstavnika $\bar{g}$, birajući iz razreda H jedinični element. Skup T svih takvih predstavnika naziva se – *(desna) transverzala za H u G*. Funkcija $\psi : G \to T$ za koju je

$$\psi(g) = t \quad \text{za onaj } t \in T \text{ za koji je } gt^{-1} \in H \quad (g \in G,\ t \in T)$$

je *izborna funkcija* za transverzalu T.

1.7. Definicija: *Neka je F slobodna grupa sa skupom X slobodnih generatora i neka je $H < F$. Transverzala T za H u F je Schreier-ova transverzala ako je za svaki izraz $t = x_1^{\varepsilon_1} \ldots x_k^{\varepsilon_k}$ u svedenom obliku (*) ispunjeno: ako $t \in T$, tada svaki početni podizraz $x_1^{\varepsilon_1} \ldots x_i^{\varepsilon_i}$ $(i < n)$ takodje pripada T.*

1.8. Teorema: *(Nielsen-Schreier): Svaka podgrupa slobodne grupe je slobodna.*

Dokaz je dat u zadatku 1.15.

O predstavljanju (prezentaciji) slobodne grupe (pored zadatka 1.1.) biće detaljnije reči u narednom poglavlju.

Slobodne grupe su u izvesnom smislu univerzalne za sve grupe (videti zadatak 1.6.).

Primeri i zadaci

1.1. Neka je $F=(F,\cdot)$ grupa i $X \subseteq F$. Dokazati da je F slobodna grupa sa bazom X akko je: (i) $F = \langle X \rangle$,
(ii) Ne postoji netrivijalna strukturna jednakost nad elementima iz X[1].

Rešenje: Neposredno prema zadatku 10.5.10. Naime, svaki element iz F se jedinstveno predstavlja sa

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_m^{\varepsilon_m} \quad (\varepsilon_i = \pm 1,\ x_i \in X,\ x_i = x_{i+1} \Rightarrow \varepsilon_i \neq -\varepsilon_{i+1}) .$$

---

[1] Odnosno, elementi iz X ne zadovoljavaju ni jednu jednakost koja ne bi bila posledica zakona grupe.

Napomena: Grupa F_n ne može imati manje od n generatora (može ih imati više). Slobodnih generatora može imati samo n. Može se dokazati da je svaki skup od n generatora grupe F_n istovremeno i skup slobodnih generatora za F_n .

1.2. Neka su F i G slobodne grupe čiji su skupovi slobodnih generatora redom neprazni skupovi A i B. Dokazati:

$$F \simeq G \Leftrightarrow |A| = |B|.$$

Rešenje: Na osnovu zadatka 10.5.13.

1.3. Dokazati da slobodna grupa F nije Abel-ova ako je rang $F > 1$.

Rešenje: Neka je $F = \langle X \rangle_s$, gde je $|X| \geqslant 2$. Tada postoje $a,b \in X$ za koje je $a \neq b$. Izrazi ab i ba su u svedenom obliku i različiti medjusobno (v.zad. 10.5.10.), pa predstavljaju dva različita elementa slobodne grupe.

1.4. Dokazati da su svi elementi slobodne grupe F (koji su različiti od 1), beskonačnog reda.

Rešenje: Neka je $F = \langle X \rangle_s$ i $a \in F$, $a \neq 1$, a se jedinstveno predstavlja izrazom u svedenom obliku

$$a = x_1^{n_1} x_2^{n_2} \ldots x_k^{n_k} , \quad x_i \in X,\ n_i \in Z \setminus \{0\},\ x_i \neq x_{i+1} .$$

Ako je $x_1 \neq x_k$ ili $n_1 \neq -n_k$, tada je

$$a^m = \underbrace{(x_1^{n_1} \ldots x_k^{n_k}) \ldots (x_1^{n_1} \ldots x_k^{n_k})}_{m \text{ puta}}$$

takodje u svedenom obliku; dakle $(\forall m \in N) a^m \neq 1$, pa je a beskonačnog reda. Ako je $x_1 = x_k$ i $n_1 = -n_k$, tada može biti i $x_2 = x_{k-1}$ i $n_2 = -n_{k-1}$, itd. Kako je $a \neq 1$, postoji j $(1 < j \leqslant \left|\frac{k+1}{2}\right|)$ tako da je $x_j \neq x_{k+1-j}$ ili $n_j \neq -n_{k+1-j}$. Odnosno, a je oblika

$$a = x_1^{n_1} \ldots x_j^{n_j} x_{j+1}^{n_{j+1}} \ldots x_{k-j}^{n_{k-j}} x_{k+1-j}^{n_{k+1-j}} \ldots x_{k-1}^{n_{k-1}} x_k^{n_k} = x_1^{n_1} \ldots a' \ldots x_k^{n_k}$$

Izraz za a' zadovoljava uslove prvog slučaja, pa je a' beskonačnog reda. Stoga je i a beskonačnog reda, jer je konjugovan sa a'.

1.5. Ispitati da li su slobodne sledeće grupe:

a) Konačne , b) Abel-ove , c) $C_\infty \times C_\infty$

d) $G = \langle a,b;\ a = b^2 \rangle$, e) $G = \langle a,b;\ a^2 = b^2 \rangle$.

Rešenje: a) Prema zad. 1.4. svi elementi ($\neq 1$) slobodne grupe su beskonačnog reda. Dakle, (netrivijalne) konačne grupe nisu slobodne.

b) Prema zad. 1.3., Abel-ova je samo slobodna grupa F_1 $(F_1 \simeq C_\infty)$.

c) Grupa $G = C_\infty \times C_\infty$ je Abel-ova. Ako je slobodna, prema b) je $G \simeq C_\infty$ što je, prema zad. 5.3.5. nemoguće.

d) Kako je $\langle a,b;\ a=b^2 \rangle \simeq \langle b \rangle$ *(videti odeljak 12.2. i zadatak 12.2.1.), to je G slobodna grupa* $(\simeq F_1)$.

e) U G postoji netrivijalna strukturna jednakost $a^2b^{-2}=1$, *pa G nije slobodna sa bazom* $\{a,b\}$. *Takodje,* $G \neq F_1$ *jer*

$$F_1 \simeq \langle a \rangle \simeq \langle a,b;\ a=b \rangle \simeq \langle a,b;\ a=b, a^2=b^2 \rangle$$

(v.zad. 12.2.1.), tj. u slobodnoj grupi važi: $a^2=b^2 \Rightarrow a=b$.

1.6.Dokazati: a) Svaka grupa je homomorfna slika neke slobodne grupe ,

b) Svaka grupa sa n generatora je homomorfna slika slobodne grupe F_n .

Rešenje: a) Neka je $\underline{G}=(G,\cdot)$ *proizvoljna grupa i* $F=\langle G \rangle_s$. *Identičko preslikavanje* $I : G \xrightarrow[1-1]{na} G$ *se jedinstveno produžuje do homomorfizma* $\phi : F \xrightarrow{na} G$.

b) Slično, neka je $G=\langle X \rangle$, *gde je* $|X|=n$, *i neka je* $F=\langle X \rangle_s$. *Postoji preslikavanje* $f : X \xrightarrow{1-1} G$, $f(x)=x$ *za* $x \in X$, *i jedinstveni homomorfizam* $\phi : F \to G$ *koji je* <u>*na*</u> .

1.7.U sledećim primerima slobodnih grupa F i njihovih podgrupa H, ispitati da li je $H \lhd F$ i naći indeks $|F:H|$.

a) $F_2=\langle a,b \rangle$, H_1 je skup svih elemenata iz F_2 predstavljenih izrazima parne dužine,

b) $F_2=\langle a,b \rangle$, $H_2=\langle a^2,b^2,ab \rangle$,

c) $F_2=\langle a,b \rangle$, $H_3=\langle a^2,b^2,(ab)^2 \rangle$,

d) $F_2=\langle a,b \rangle$, $H_4=\langle a \rangle$,

d) $F_n=\langle a_1,\ldots,a_n \rangle$, $H_5=\langle x^2 \mid x \in F_n \rangle$.

Rešenje: a) Razredi po H_1 *u* F_2 *su* H_1 *i* aH_1 . *Dakle,* $|F_2:H_1|=2$, *pa je* $H_1 \lhd F_2$.

Primetimo da je H_1 *normalno zatvorenje u* F_2 *nad skupom* $\{a^2,ab\}$. *Označimo sa* $H'=[\{a^2,ab\}]^{F_2}$, *Zaista,*

$$F_2/H' = \langle a,b;\ a^2=1, ab=1 \rangle = \langle a,b;\ a^2=1, a=b \rangle = \langle a;\ a^2=1 \rangle = C_2$$

(koristili smo zad. 12.1.11. i Tietze-ove transformacije; videti odeljak 12.2.). Odnosno, $|F_2:H'|=2$. *Kako je* $H' < H_1$ *i* $|F_2:H_1|=|F_2:H'|\,|H':H_1|$ *sledi* $H'=H_1$.

b) Kako su izrazi a^2,b^2,ab *parne dužine, to je* $H_2 < H_1$. *Lako se pokazuje da se svaki izraz parne dužine može predstaviti proizvodom elemenata* a^2,b^2, *ab i njima inverznih; dakle* $H_1=H_2$.

Napomena: H_2 *je slobodno generisana elementima* a^2,b^2,ab.

c) $H_3 \lhd F_2$, $|F_2:H_3|=2$

d) Podgrupa H_4 *nije normalna u* F_2, *jer* $a^k \in H_4$ *ali* $ba^kb^{-1} \notin H_4$, $|F_2:H_4|=\infty$

e) $H_5 \lhd F_n$, $|F_n:H_5|=2^n$.

1.8.Neka je F slobodna grupa i H njena podgrupa generisana elementima u,v,...

iz F. a) Dokazati da H ne mora biti slobodno generisana sa u,v,...
b) Ako je X minimalan [1] skup generatora podgrupe H, dokazati da H ne mora biti slobodno generisana sa X.

Rešenje: Neka je $F_2 = \langle a,b \rangle_s$, $H = \langle a,a^2 \rangle$. *H je slobodna grupa sa bazom* $X = \{a,a^2\}$ *akko je* $H = \langle X \rangle$ *i ne postoji (netrivijalna) strukturna jednakost nad elementima iz X (zad. 1.1.). Medjutim,* $a^2 = a \cdot a$.
Slično je i za podgrupu $\bar{H} = \langle a^2, b^2, ab, ba \rangle$, *gde je* $(ba)(a^2)^{-1}(ab) = b^2$.
(Prema zad. 1.7.b), $\bar{H}$ *je slobodno generisana elementima* a^2, b^2, ab.)
b) Primer: $F_2 = \langle a,b \rangle_s$, $H = \langle a, b^2, ab^3 \rangle$.
Skup $X = \{a, b^2, ab^3\}$ *je minimalan ali ne i slobodan skup generatora za H.*

1.9. Dokazati da je u slobodnoj grupi $F_2 = \langle a,b \rangle$ podgrupa H, generisana skupom X, slobodno generisana sa X, ako je
a) $X = \{ab, a^2b^2, a^3b^3, \ldots\}$, b) $X = \{aba^3, a^2b\}$,
c) $X = \{b^{-1}ab,\ b^{-2}ab^2,\ b^{-3}ab^3, \ldots\}$.

Rešenje: Koristeći zadatak 1.1. dokazujemo da ne postoji netrivijalna strukturna jednakost nad elementima iz X, tj. da je svaki izraz t koji je u svedenom obliku (formiran od elemenata iz X i njihovih inverznih elemenata), različit od 1. U narednim slučajevima dokaz da je $t \neq 1$ *izvodi se indukcijom.*
a) Svakom elementu w iz F_2 *koji je predstavljen izrazom* $w = c_{i_1}^{\alpha_1} \ldots c_{i_k}^{\alpha_k}$ *u svedenom obliku (*$c_i \in \{a,b\}$, $c_{i_j} \neq c_{i_{j+1}}$, $\alpha_j \in Z \setminus \{0\}$*), pridružimo broj* $l(w) = k$ *(tzv. "slogovnu" dužinu).*
Jednostavnom indukcijom se dokazuje da je $l(x_{i_1}^{\alpha_1} \ldots x_{i_n}^{\alpha_n}) \geq n+1$ *ako su* $x_i \in X$, $\alpha_i \in \{1,-1\}$ *i* $x_{i_j} = x_{i_{j+1}} \Rightarrow \alpha_{i_j} \neq -\alpha_{i_{j+1}}$.
b) Svaki izraz t, u svedenom obliku, nad aba^3 *i* a^2b *završava se sa* a^3 *ili* $b^{-1}a^{-1}$ *ili b ili* $b^{-1}a^{-2}$.
c) Proizvodi elemenata $x_k = b^{-k}ab^k$ $(k=1,2,\ldots)$ *i inverznih* x_k^{-1} , *posle dovodjenja na svedeni oblik*

$$x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \ldots x_{i_k}^{\alpha_k}$$

$(i_j \in \{1,2,\ldots\},\ i_j = i_{j+1} \Rightarrow \alpha_j \neq -\alpha_{j+1})$ *završavaju se sa* $a^{\alpha_k} b^{i_k}$

1.10. Dokazati da slobodna grupa ranga većeg od 1 ima trivijalan centar.

Rešenje: Neka je $F = \langle X \rangle_s$ *i neka je Z(F) netrivijalan, tj. neka je* $z \in Z(F)$ *i* $z \neq 1$. *Kako je z iz F, to je on oblika*

---

[1] Skup X je *minimalan skup generatora* grupe G, ako nijedan pravi podskup od X ne generiše G.

$z=x_1^{\alpha_1}x_2^{\alpha_2}\dots x_k^{\alpha_k}$ $(x_i\in X,\ x_i\neq x_{i+1},\ \alpha_i\in Z\setminus\{0\},\ i\in\{1,\dots,k\})$.

Neka je, dalje, $y\in X$.

Ako je $k=1$ i $y\neq x_1$, tada je $x_1^{\alpha_1}y\neq yx_1^{\alpha_1}$.

Ako je $k>1$, *tada je*

$$x_1z=x_1^{\alpha_1+1}x_2^{\alpha_2}\dots x_k^{\alpha_k}\neq x_1^{\alpha_1}x_2^{\alpha_2}\dots x_k^{\alpha_k}x_1=zx_1$$

(jer je $x_1\neq x_2$*); dakle,* $z\notin Z(F)$, *suprotno pretpostavci.*

1.11. Odrediti transverzalu T podgrupe H u grupi G ako je

a) $G=C_4$, $H=\{1,a^2\}$, b) $G=K$ (grupa kvaterniona), $H=Z(K)$.

Rešenje: a) $T=\{1,a\}$

b) $G=\{1,a,a^2,a^3,b,ab,a^2b,a^3b\}$, $H=\{1,a^2\}=Z(G)$, $T=\{1,a,b,ab\}$.

1.12. Neka je F slobodna grupa sa bazom X, $H<F$, T transverzala za H i $\phi: F\to T$ izborna funkcija za T. Dokazati da je:

a) Funkcija ϕ ima sledeća svojstva

1° $\phi(g)=1\Leftrightarrow g\in H$, 2° $\phi(\phi(g))=\phi(g)$,

3° $\phi(\phi(g_1)g_2)=\phi(g_1g_2)$, $(g,g_1,g_2\in F)$

b) Skup $\{tx^{\pm1}\phi(tx^{\pm1})^{-1}\mid t\in T,\ x\in X\}$ generiše H,

c) Skup $\{tx\phi(tx)^{-1}\mid t\in T,\ x\in X\}$ *generiše H.*

Rešenje: a) Treća navedena jednakost je tačna akko su $\phi(u)v$ *i* uv *u istom razredu po H. A oni to jesu jer* $\phi(u)$ *i u jesu u istom razredu po H.*

b) Neka je $h=x_1^{\varepsilon_1}\dots x_k^{\varepsilon_k}$ $(x_i\in X,\ \varepsilon_i=\pm1)$ *proizvoljan element iz H. Označimo sa* $t_0,t_1,\dots,t_k$ iz T koset-predstavnike za početne podizraze od h:

$$t_0=1,\quad t_i=\phi(x_1^{\varepsilon_1}\dots x_i^{\varepsilon_i}),\ i=1,\dots,k.$$

Zbog $h\in H$, *prema a)*1°, biće $t_k=\phi(x_1^{\varepsilon_1}\dots x_k^{\varepsilon_k})=\phi(h)=1$. *Tako imamo*

$$h=t_0x_1^{\varepsilon_1}t_1^{-1}\cdot t_1x_2^{\varepsilon_2}t_2^{-1}\cdot\dots\cdot t_{k-2}x_{k-1}^{\varepsilon_{k-1}}t_{k-1}^{-1}\cdot t_{k-1}x_k^{\varepsilon_k}t_k^{-1}.$$

Ostaje da pokažemo da je svaki element $t_{i-1}x_i^{\varepsilon_i}t_i^{-1}$ $(i=1,\dots,k)$ *oblika* $tx^{\pm1}\phi(tx^{\pm1})^{-1}$, *odnosno da je* $t_i=\phi(t_{i-1}x_i^{\varepsilon_i})$. *Ovo je tačno, jer prema a)*3°

$$t_i=\phi(x_1^{\varepsilon_1}\dots x_{i-1}^{\varepsilon_{i-1}}x_i^{\varepsilon_i})=\phi(\phi(x_1^{\varepsilon_1}\dots x_{i-1}^{\varepsilon_{i-1}})x_i^{\varepsilon_i})=\phi(t_{i-1}x_i^{\varepsilon_i}).$$

c) Prema b) dovoljno je da dokažemo da se svaki element $tx^{-1}\phi(tx^{-1})^{-1}$ *može napisati kao proizvod elemenata oblika* $tx\phi(tx)^{-1}$ *i njima inverznih. U stvari,* $tx^{-1}\phi(tx^{-1})^{-1}$ *je inverzan elementu* $t_1x\phi(t_1x)^{-1}$, *gde je* $t_1=\phi(tx^{-1})$. *Zaista,* $\phi(t_1x)=\phi(\phi(tx^{-1})x)=\phi(t)=t$ *(prema a)*3°*), pa imamo*

$$(t_1x\phi(t_1x)^{-1})^{-1}=\phi(t_1x)\quad x^{-1}t_1^{-1}=tx^{-1}\phi(tx^{-1})^{-1}.$$

1.13. *Dokazati da za svaku podgrupu H slobodne grupe F postoji Schreier-ova* transverzala.

Rešenje: Neka je $H \leq F$, $F = \langle X \rangle$. Parcijalnom Schreier-ovom transverzalom za H u F nazovimo svaki podskup $T \subseteq F$ takav da su koseti Ht, $t \in T$ svi različiti i da za svako $t = x_1^{\varepsilon_1} \ldots x_k^{\varepsilon_k}$ iz T ($x_i \in X$, $\varepsilon_i = \pm 1$) svi početni podizrazi $x_1^{\varepsilon_1} \ldots x_i^{\varepsilon_i}$ takodje pripadaju T. Skup parcijalnih Schreier-ovih transverzala za H u F je neprazan (jer sadrži $\{1\}$) i zatvoren za unije lanaca. Zaključujemo prema Zorn-ovoj lemi da postoji maksimalna parcijalna Schreier-ova transverzala za H; označimo je sa T_0. Još treba pokazati da je $HT_0 = F$.

Pretpostavimo da je $HT_0 \neq F$; neka je $u = x_1^{\varepsilon_1} \ldots x_k^{\varepsilon_k}$ element minimalne dužine $k \geq 1$ iz $F \setminus HT_0$. Onda je $x_1^{\varepsilon_1} \ldots x_{k-1}^{\varepsilon_{k-1}} \in HT_0$ i $Hx_1^{\varepsilon_1} \ldots x_{k-1}^{\varepsilon_{k-1}} = Ht$ za neko $t \in T_0$. Tako dobijamo $Hu = Htx_k^{\varepsilon_k}$ i $Htx_k^{\varepsilon_k} \cap HT_0 = \emptyset$. Sada je $T_0 \cup \{tx_k^{\varepsilon_k}\}$ parcijalna Schreier-ova transverzala koja strogo sadrži T_0, što je u kontradikciji sa maksimalnošću T_0. Dakle, $HT_0 = F$, tj. T_0 je Schreier-ova transverzala za H.

1.14. Neka je F slobodna grupa sa bazom X, $H \prec F$, T Schreier-ova transverzala za H i $\phi : F \to T$ izborna funkcija za T. Ako je

$$t_1 x^{\varepsilon} \neq \phi(t_1 x^{\varepsilon}) , \quad t_2 y^{\delta} \neq \phi(t_2 y^{\delta})$$

($x, y \in X$; $t_1, t_2 \in T$; $\varepsilon, \delta \in \{1, -1\}$), dokazati

a) Izrazi $t_1 x^{\varepsilon} \phi(t_1 x^{\varepsilon})^{-1}$ i $t_2 y^{\delta} \phi(t_2 y^{\delta})^{-1}$ su u svedenom obliku,

b) Ako je $\phi(t_1 x^{\varepsilon}) \neq t_2$, tada posle skraćivanja izraza

$$t_1 x^{\varepsilon} \phi(t_1 x^{\varepsilon})^{-1} t_2 y^{\delta} \phi(t_2 y^{\delta})^{-1}$$

podizrazi x^{ε} i y^{δ} ostaju neskraćeni.

Rešenje: a) Pretpostavimo da je izraz $t_1 x^{\varepsilon} \phi(t_1 x^{\varepsilon})^{-1}$ skrativ. Tada se t_1 završava sa $x^{-\varepsilon}$ ili se $\phi(t_1 x^{\varepsilon})$ završava sa x^{ε}. U prvom slučaju je $t_1 = t' x^{-\varepsilon}$, odnosno $t_1 x^{\varepsilon} = t'$, za neko $t' \in T$. Onda, $\phi(t_1 x^{\varepsilon}) = \phi(t') = t' = t_1 x^{\varepsilon}$, što po pretpostavci nije tačno. U drugom slučaju imamo $\phi(t_1 x^{\varepsilon}) = t'' x^{\varepsilon}$, za neko $t'' \in T$. Znači, $t_1 x^{\varepsilon}$ i $t'' x^{\varepsilon}$ su u istom razredu po H, pa su t_1 i t'' takodje u istom razredu po H, što povlači $t_1 = t''$, opet suprotno sa pretpostavkom $\phi(t_1 x^{\varepsilon}) \neq t_1 x^{\varepsilon}$.

b) Prema a), skraćivanje u navedenom izrazu, ako ga uopšte ima, mora početi na delu izmedju x^{ε} i y^{δ}. Označimo $\phi(t_1 x^{\varepsilon})$ sa t'. Po pretpostavci je $t' \neq t_2$, pa ako se x^{ε} ili y^{δ} mogu skratiti, onda je $t' x^{-\varepsilon}$ početni podizraz od t_2 (i, kao takav, element od T) ili je $t_2 y^{\delta}$ početni podizraz od t', pa stoga element od T. Recimo da je $t' x^{-\varepsilon} \in T$; tada imamo

$$t' x^{-\varepsilon} = \phi(t' x^{-\varepsilon}) = \phi(\phi(t_1 x^{\varepsilon}) x^{-\varepsilon}) = \phi(t_1) = t_1 ,$$

pa $t'=t_1x^{\varepsilon}$ *, odnosno* $\phi(t_1x^{\varepsilon})=t_1x^{\varepsilon}$ *, suprotno pretpostavci. Slično se obara i druga mogućnost :* $t_2y^{\delta}\in T$.

1.15. Dokazati teoremu Nielsen-Schreier-a: Svaka podgrupa slobodne grupe je slobodna.

Rešenje: Neka je $F=<X>$, $H<F$ *i T Schreier-ova transverzala za H, čija je egzistencija dokazana zadatkom 1.13. Neka je* $\phi : F \to T$ *odgovarajuća izborna funkcija.*

Označimo sa Y skup svih netrivijalnih elemenata oblika $tx\phi(tx)^{-1}$ *, dokazaćemo da je Y skup slobodnih generatora za H. Iz zadatka 1.12.c) sledi da Y generiše H. Ostaje da pokažemo da medju elementima iz Y nema netrivijalnih zavisnosti. Neka je onda*

$$u=(t_1x_1\phi(t_1x_1)^{-1})^{\varepsilon_1}\cdot(t_2x_2\phi(t_2x_2)^{-1})^{\varepsilon_2}\cdot\ldots\cdot(t_kx_k\phi(t_kx_k)^{-1})^{\varepsilon_k}$$

neskrativi izraz po generatorima $t_ix_i\phi(t_ix_i)^{-1}\in Y$ *;* $\varepsilon_i=\pm 1$.
Uslov neskrativosti znači da ni za jedno $i\in\{2,\ldots,k\}$ *nije* $t_{i-1}=t_i$, $x_{i-1}=x_i$ *i* $\varepsilon_{i-1}=-\varepsilon_i$. *Treba da dokažemo da je* $u\neq 1$ *u F. Prema zadatku 1.12., svako* $(t_ix_i\phi(t_ix_i)^{-1})^{-1}$ *možemo napisati u obliku* $t_i'x_i^{-1}\phi(t_i'x_i^{-1})^{-1}$ *, gde je* $t_i'=\phi(t_ix_i)$. *Tako možemo pretpostaviti da je izraz u oblika*

$$u=t_1x_1^{\varepsilon_1}\phi(t_1x_1^{\varepsilon_1})^{-1}\cdot t_2x_2^{\varepsilon_2}\phi(t_2x_2^{\varepsilon_2})^{-1}\cdot\ldots\cdot t_kx_k^{\varepsilon_k}\phi(t_kx_k^{\varepsilon_k})^{-1} ,$$

gde uslov neskrativosti glasi: ni za jedno $i\in\{2,\ldots,k\}$ *nije* $\phi(t_{i-1}x_{i-1}^{\varepsilon_{i-1}})=t_i$, $x_{i-1}=x_i$ *i* $\varepsilon_{i-1}=-\varepsilon_i$.
Pošto je svaki od izraza $t_ix_i^{\varepsilon_i}\phi(t_ix_i^{\varepsilon_i})^{-1}$ *neskrativ (zadatak 1.14.a)), sledi da skraćivanja u izrazu u moraju početi na delovima* $\phi(t_{i-1}x_{i-1}^{\varepsilon_{i-1}})^{-1}t_i$. *Prema zadatku 1.14.b), ako je* $\phi(t_{i-1}x_{i-1}^{\varepsilon_{i-1}})\neq t_i$ *, onda skraćivanje ne dolazi do* $x_{i-1}^{\varepsilon_{i-1}}$, *niti do* $x_i^{\varepsilon_i}$. *Dakle, ako bi bilo* $u=1$ *moralo bi za neko* $i\in\{2,\ldots,k\}$ *biti* $\phi(t_{i-1}x_{i-1}^{\varepsilon_{i-1}})=t_i$. *Posle ovog skraćivanja, izraz u je oblika*

$$u=\ldots\ t_{i-1}x_{i-1}^{\varepsilon_{i-1}}x_i^{\varepsilon_i}\phi(t_ix_i^{\varepsilon_i})^{-1}\ldots$$

Vidi se da simboli $x_{i-1}^{\varepsilon_{i-1}}$ *i* $x_i^{\varepsilon_i}$ *mogu biti skraćeni jedino ako je* $x_{i-1}=x_i$ *i* $\varepsilon_{i-1}=-\varepsilon_i$. *A to je upravo ono što ne može biti, prema pretpostavci o neskrativosti izraza u po generatorima iz Y.*

Zaključak je da je svaki neskrativi izraz po generatorima iz Y, različit od 1, odnosno da su elementi iz Y slobodni generatori slobodne grupe H koju generišu.

1.16. Neka je F slobodna grupa konačnog ranga n, i neka je H podgrupa konačnog indeksa $|F:H|=j$ u F. Dokazati da je H konačnog ranga m i da je za brojeve m,n,j ispunjeno: $j=\frac{m-1}{n-1}$.

Rešenje: Schreier-ova transverzala T (videti prethodni zadatak) u ovom slučaju ima j elemenata. Svakom paru (x,t), gde je $x \in X$, $X=\{x_1,\ldots,x_n\}$, $t \in T$, *odgovara izraz* $tx\phi(tx)^{-1}$. *Ako sa d označimo broj parova (x,t) za koje je* $\phi(tx)=tx$, *onda je, prema dokazu prethodnog zadatka,* $m=nj-d$. *Jednakost* $\phi(tx)=tx$ *važi ako i samo ako je tx izraz u svedenom obliku i* $tx \in T$. *S obzirom da svako* $t' \in T \setminus \{1\}$ *odredjuje tačno jedno* $t \in T$ *i jedno* $x \in X$ *tako da je tx u svedenom obliku i* $tx=t'$, *to je* $d=|T|-1=j-1$. *Tako se dobija* $m=nj-j+1$, *odakle neposredno sledi tražena jednakost.*

1.17. Svaka podgrupa konačnog indeksa u slobodnoj grupi beskonačnog ranga, ima beskonačan rang. Dokazati.

Rešenje: Na osnovu prethodnih zadataka.

1.18. Neka je F_n slobodna grupa ranga n ($n \geqslant 1$). Dokazati:

a) Za proizvoljni prirodni broj i, postoji podgrupa H indeksa i ,

b) Ako su H i K podgrupe jednakih indeksa, j, tada je $H \simeq K$.

Rešenje: a) Neka je $X=\{x_1,\ldots,x_n\}$ *i* $F=\langle X\rangle_s$, *i neka je* $C_i=\langle a \mid a^i\rangle$ *ciklična grupa reda i. Preslikavanje* $f: X \to C_i$ *odredjeno recimo sa* $f(x_j)=a$ $(j=1,\ldots,n)$ *ima jedinstveno homomorfno proširenje* $\phi: F \to C_i$. *Odavde,* $F/\ker\phi \simeq C_i$, *pa je* $H=\ker\phi$ *podgrupa indeksa i .*

b) Neka je $|F_n : H|=|F_n : K|=j$. *Prema zad. 1.17. je* $\operatorname{rang} H=\operatorname{rang} K$, *odakle sledi* $H \simeq K$ *(v.zad. 1.2.).*

1.19. Da li je svaka lokalno slobodna[1)] grupa slobodna, i obratno?

Rešenje: Sve slobodne grupe su i lokalno slobodne (teorema Nielsen-Schreiera, videti zadatak 1.1.5).

Obratno nije tačno. Kontraprimer:

Grupa $\underline{Q}=(Q,+)$ *(Q - skup racionalnih brojeva) je lokalno slobodna, ali nije slobodna.*

Zaista, $\underline{Q}$ *je Abel-ova grupa, a od slobodnih, Abel-ova je samo grupa* F_1 *(videti zadatak 1.3.). Medjutim,* $\underline{Q}$ *nije generisana jednim svojim elementom. Ako je* $p/q \in Q$, *tada je podgrupa* $H=\langle p/q\rangle=\{pk/q \mid k \in Z\}$ *očigledno različita od grupe* $\underline{Q}$. *Stoga,* $\underline{Q}$ *nije slobodna grupa.*

---

1) Grupa G je *lokalno slobodna* ako svaki konačan podskup S iz G generiše slobodnu grupu.

11.2. SLOBODAN PROIZVOD GRUPA

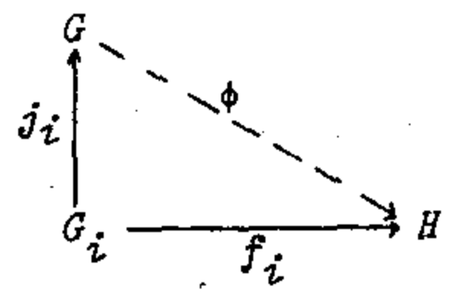
Slobodan proizvod je u izvesnom slmislu generalizacija pojma slobodne grupe (slobodne grupe su slobodni proizvodi svojih podgrupa, itd.; videti Napomenu 2.7.).

Kao kod direktnog proizvoda, i ovde se može govoriti o *razlaganju* date grupe (na slobodan proizvod svojih podgrupa), kao i o *konstrukciji* nove grupe (slobodnim proizvodom) od date familije grupa.

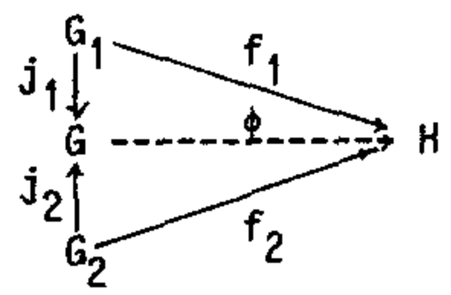
2.1. *Definicija:* *Neka je* $\{G_i \mid i \in I\}$ *proizvoljna familija grupa. (Spoljašnji)* *slobodan proizvod* *grupa* G_i, *u oznaci* $G = \prod_{i\in I}^{*} G_i$, *je grupa* G *sa svojstvom :*

(i) Za svaki $i \in I$, *postoji homomorfno 1-1 preslikavanje* $j_i : G_i \to G$,

(ii) Za proizvoljnu grupu H *i proizvoljnu familiju* $\{f_i \mid i \in I\}$ *homomorfizama* $f_i : G_i \to H$, *postoji jedinstveni homomorfizam* $\phi : G \to H$ *koji proširuje, preko* j_i, *svaki od homomorfizama* f_i $(i \in I)$.



Za slobodni proizvod dve grupe, dijagram iz definicije je dat na slici.



Koristeći zadatke 10.3.1. i 10.3.6. sledi

2.2. *Teorema:* *Za proizvoljnu familiju grupa* G_i $(i \in I)$, *postoji jedinstven (do na izomorfizam) slobodan proizvod tih grupa.*

Jedan opis grupe $\prod^{*} G_i$ dat je u zadatku 2.1. Da je $\prod^{*} G_i$ zaista grupa, sledi i iz zadatka 2.2.

2.3. *Definicija:* *Grupa* G *je (unutrašnji)* *slobodan proizvod svojih podgrupa* H_i $(i \in I)$, *ako se svaki element* $g \in G$ $(g \neq 1)$ *jedinstveno predstavlja sa*

$$g = h_1 h_2 \dots h_n \qquad (**)$$

gde su $h_i \neq 1$, $h_i \in H_{j_i}$, $H_{j_i} \neq H_{j_{i+1}}$ $(j_i \in I,\ i \in \{1,\dots,n\})$, *(tj.* h_i *i* h_{i+1} *nisu iz iste podgrupe* H_k*).*

Za izraz $h_1 h_2 \dots h_n$ iz (**) kažemo takodje da je u *svedenom*, neskrativom obliku. *Dužina* mu je n [1] (videti fusnotu na narednoj strani).

U zadatku 2.2. dokazuje se da je grupa iz definicije 2.3. izomorfna slobodnom proizvodu grupa H_i $(i \in I)$ iz definicije 2.1. (grupe H_i se utapaju

u G, pa se H_i mogu tretirati kao stvarne, aktuelne podgrupe u G). Stoga se i koristi ista oznaka, $G = \prod_{i\in I}^{*} H_i$.
Ako je I konačan skup, pišemo i $G = H_1 * H_2 * \ldots * H_n$.

2.4. *Definicija:* *Grupa G je* <u>*nerazloživa*</u> *u slobodan proizvod (pravih) podgrupa akko iz* $G = A * B$ *sledi* $A \simeq \{1\}$ *ili* $B \simeq \{1\}$.

Važnu ulogu u ovoj oblasti teorije grupa imaju sledeće teoreme.

2.5. *Teorema (Kuroš): Neka je H podgrupa slobodnog proizvoda* $G = \prod_{i\in I}^{*} G_i$.
Tada je $H \simeq F * \prod_{j}^{*} H_j$, *gde je F slobodna grupa, a svaka grupa* H_j *je izomorfna izvesnoj podgrupi neke od grupa* G_i .

2.6. *Teorema (Gruško-Neumann): Neka je F slobodna grupa i neka je preslikavanje* $f : F \to \prod_{i\in I}^{*} H_i$ *homomorfizam. Tada postoje slobodne grupe* F_i *takve da je* $f(F_i) = H_i$ $(i \in I)$ *i* $F = \prod_{i\in I}^{*} F_i$.

2.7. Napomena: Za slobodne grupe i njihovu generalizaciju, slobodan proizvod grupa, dokazuju se mnogi srodni rezultati. Na primer:

- Svaki element se jedinstveno predstavlja u svedenom obliku (tj. važe tzv. teoreme o normalnoj formi: oblici (*) iz 11.1. i (**) iz 11.2.)
- Centar je {1} (zadaci 1.10. i 2.13.).
- Svojstva "biti slobodna grupa" i "biti slobodan proizvod grupa" su, u izvesnom smislu, nasledna. Preciznije, svaka podgrupa slobodne grupe je slobodna (teorema 1.8.), a svaka podgrupa slobodnog proizvoda $\prod_{i\in I}^{*} G_i$ je slobodan proizvod (nekih grupa izomorfnih podgrupama iz G_i) ili je slobodna grupa ili izomorfna podgrupi neke od grupa G_i (teorema 2.5.).

---

1) Kada se govori o *dužini elementa* grupe G, misli se uvek na dužinu *izraza* koji predstavlja taj element, a koji je u svedenom obliku ((*) iz 11.1., (**). iz ovog odeljka ili (***) iz 11.3.).

Primeri i zadaci

2.1. Za datu familiju grupa G_i $(i \in I)$, opisati konstrukciju grupe $\prod_{i \in I}^{*} G_i$.

Rešenje: Opis grupe $\prod_{i \in I}^{*} G_i$ *je u potpunosti sličan opisu slobodne grupe F iz zadatka 10.5.10.*

Neka su grupe G_i $(i \in I)$ *takve da je* $G_i \cap G_j = \emptyset$ *za sve* $i,j \in I$, $i \neq j$ *(što se, preimenovanjem, uvek može postići). Neka je* $X = \bigcup_{i \in I} G_i$. *Označimo sa M skup svih izraza t nad X (jezika L), koji su u svedenom obliku u sledećem smislu: t=e ili*

$$t = g_1 g_2 \cdots g_k \qquad (1)$$

gde je $g_i \in G_{j_i} \setminus \{1_{j_i}\}$, $j_i \in I$, *a* g_i *i* g_{i+1} *pripadaju različitim grupama* G_{j_i} *i* $G_{j_{i+1}}$, *za sve* $i \in \{1,\ldots,k-1\}$. *Dalje, kao u zadatku 10.5.10.*

2.2. Ako je G unutrašnji slobodan proizvod svojih podgrupa H_i $(i \in I)$ (u smislu definicije 2.3.), tada je G izomorfna slobodnom proizvodu grupa H_i $(i \in I)$ (u smislu definicije 2.1.). Dokazati.

Rešenje: Neka je M skup svih izraza $g = g_1 \ldots g_k$ *u svedenom obliku (1) iz zadatka 2.1. Dalje, neka su* $\odot$ *i* $\overset{-1}{\odot}$ *operacije u M, kao u zadatku 10.5.10. Odnosno, ako su* $m_1, m_2 \in M$, *tada se* $m_1 \odot m_2$ *dobija iz* $m_1 \cdot m_2$ $(\cdot \in L)$ *svodjenjem na oblik (1) (tj. ako postoje* g_i *i* g_{i+1} *koji su oba u* G_j, *zameniti* $g_i g_{i+1}$ *sa g iz* G_j *za koji je* $g = g_i g_{i+1}$ *i izostaviti pojavljivanja konstante e - ako nisu oba* m_1 *i* m_2 *upravo e; inače,* $m_1 \odot m_2 = e$*). Slično,*

$$g^{\overset{-1}{\odot}} = (g_1 g_2 \cdots g_k)^{\overset{-1}{\odot}} \underset{=}{\overset{def}{=}} g_k^{-1} \cdots g_2^{-1} g_1^{-1}$$

gde je g_i^{-1} *rezultat operacije* $^{-1}$ *u grupi* G_{j_i} *).*

Prema prethodnom zadatku, $G = (M, \odot, \overset{-1}{\odot})$ *je slobodan proizvod grupa* G_i $(i \in I)$. *Dokažimo da je* $G \simeq \bar{G}$, *gde je* $\bar{G}$ *slobodan proizvod svojih podgrupa* $\bar{G}_i$, $G_i \simeq \bar{G}_i$ *za sve* $i \in I$.

Konstruišimo prvo grupe $\bar{G}_i$ *izomorfne redom grupama* G_i $(i \in I)$. *Svakom elementu* $x \in G_i$ $(x \neq 1)$ *pridružimo preslikavanje* $f_x : M \to M$:

$$f_x(g) = \begin{cases} g_1 \ldots g_k x\,, & \text{ako je } g_k \notin G_i \\ g_1 \ldots g_{k-1} g'\,, & \text{ako je } g_k \in G_i \text{ i } g_k x \neq 1\,,\ g_k x = g' \\ g_1 \ldots g_{k-1}\,, & \text{ako } g_k \in G_i \text{ i } g_k x = 1 \end{cases}$$

f_1 *je identičko preslikavanje I.*

Lako se pokazuje da je ovako uvedeno preslikavanje f_x, *1-1 i na (jer* $f_{xy} = f_x \circ f_y$, $f_x \circ f_{x^{-1}} = I$*).*

Skup $\{f_x \mid x \in G_i\}$ *čini grupu u odnosu na množenje preslikavanja, izomorfnu grupi* G_i . *Dakle, definisali smo izomorfizme* $\psi_i : G_i \xrightarrow{u} S_M$, *gde je* S_M *simetrična grupa skupa M* ($\psi_i(x)=f_x$).
Označimo $\psi_i(G_i)=\bar{G}_i$ $(i \in I)$. *Neka je* $\bar{G}$ *sledeća grupa :* $\bar{G} = \langle \bar{G}_i \mid i \in I \rangle$, $(\bar{G} < S_M)$.

Dokažimo sada da je $\bar{G}$ *slobodan proizvod svojih podgrupa* $\bar{G}_i$ $(i \in I)$. *Definišimo preslikavanje* $h : G \to \bar{G}$ *na sledeći način: neka je* $g=g_1 \ldots g_k$ *iz M* ($g_i \in G_{j_i}$)

$$h(g)=\psi_{j_i}(g_1)\circ\ldots\circ\psi_{j_k}(g_k)=f_{g_1}\circ\cdots\circ f_{g_k} \qquad (2)$$

Svako preslikavanje f_g *iz* $\bar{G}$ *se na jedinstven način predstavlja pomoću (2), proizvodom funkcija* f_{g_j} *(koristeći svedenost za g). Dakle,* $\bar{G}$ *je slobodan proizvod podgrupa* $\bar{G}_i$ $(i \in I)$.
Lako se pokazuje (takodje koristeći svedenost za g) da je h izomorfizam.

Dokazali smo time i da je $G = (M, \odot, {}^{-1})$ ($= \prod_{i \in I}^{*} G_i$) *zaista grupa. Pri tom se grupe* G_i *utapaju u G. S obzirom na dokazani izomorfizam, opravdano je korišćenje iste oznake,* $\prod^{*}$, *za slobodne proizvode iz definicija 2.1. i 2.3.*

2.3. Dokazati da je $\langle A,B \rangle = G$ i $A \cap B = \{1\}$, ako je $G = A * B$.

Rešenje: Preciznije, grupa $G = A * B$ *je generisana izomorfnim slikama* $\bar{A}$ *i* $\bar{B}$ *grupa A i B, i* $\bar{A} \cap \bar{B} = \{1\}$. *Nadalje, medjutim, ovu razliku ne naglašavamo.*
Da je $G = \langle A,B \rangle$ *sledi iz prethodnog zadatka.*

Neka je $g \in A \cap B$, $g \neq 1$. *Kako je* $g \notin A * B$, *g ima jedinstveni svedeni zapis pomoću elemenata iz A i B: napr.* $g=a_1 b_1$. *Takodje, jer* $g \in A \cap B$, *postoje* $a \in A$ *i* $b \in B$ *tako da je* $g=a$, $g=b$. *Odnosno,* $a=b=a_1 b_1$, *što nije tačno.*

2.4. Dokazati da je modularna grupa M[1] slobodan proizvod cikličnih grupa C_2 i C_3 .

Rešenje: Preslikavanja $a(z)=-\frac{1}{z}$ *i* $b(z)=\frac{z-1}{z}$ $(z \neq 0)$ *su generatorni elementi grupe M; označimo ih, kraće, sa a i b (videti zadatak 3.2.6.b)).*
Kako je za a i b ispunjeno $a^2=1$, $b^3=1$, *to se svaki element iz M predstavlja u obliku*

$$a^{\alpha_1} b^{\beta_1} a b^{\beta_2} a \ldots a b^{\beta_k} a^{\alpha_2} \qquad (1)$$

gde su $\alpha_1, \alpha_2 \in \{0,1\}$, $\beta_i \in \{1,2\}$ *za* $i \in \{1,\ldots,k\}$.
Dokazujemo jedinstvenost predstavljanja (1).

---

[1] Videti zadatak 3.2.6.

Ako postoji element iz M sa nejedinstvenim zapisom

$$a^{\alpha'_1}b^{\beta'_1}a\ldots ab^{\beta'_n}a^{\alpha'_2} = a^{\alpha''_1}b^{\beta''_1}a\ldots ab^{\beta''_m}a^{\alpha''_2} \qquad (2)$$

gde je $n\neq m$ *ili nisu svi* $\alpha'_i=\alpha''_i$ $(i=1,2)$, $\beta'_j=\beta''_j$ $(j=1,\ldots,n)$, *tada (2) možemo zapisati u obliku*

$$ab^{\gamma_1}a\ldots ab^{\gamma_k}=1 \quad , \quad \gamma_i\in\{1,2\} \ , \ i\in\{1,\ldots,k\} \qquad (3)$$

Dokazuje se, medjutim, da je za svako k

$$ab^{\gamma_1}a\ldots ab^{\gamma_k}\neq 1 \qquad (4)$$

Prema zadatku 3.2.6.c), M je homomorfna slika $\phi(M_1)$ *grupe* M_1 *celobrojnih matrica reda 2 sa determinantom jednakom 1. Pri tom je* $\ker\phi=\{E,F\}$ *gde je*

$E=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $F=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$,

Treba dakle dokazati da su pri homomorfizmu ϕ, *izrazi* $ab^{\gamma_1}a\ldots ab^{\gamma_k}$, *za* $\gamma_i\in\{1,2\}$ *slike matrica različitih od E i F.*

Prema definiciji preslikavanja ϕ *iz zad. 3.2.6.c) je*

$$\phi\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}=a \ , \quad \phi\begin{pmatrix}1 & -1\\ 1 & 0\end{pmatrix}=b$$

Kako je $ab=\phi\begin{pmatrix}-1 & 0\\ 1 & -1\end{pmatrix}$ *i* $ab^2=\phi\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}$, *to je za k=1 dokazano* $ab^{\gamma}\neq 1$ $(\gamma=1,2)$.

Primećujemo da su matrice $\begin{pmatrix}-1 & 0\\ 1 & -1\end{pmatrix}$ *i* $\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}$ *sa svojstvom: elementi na glavnoj dijagonali su oba sa znakom - , a na sporednoj oba sa suprotnim znakom (nuli se može dodeliti proizvoljan znak).*

Pretpostavimo, stoga, da je

$ab^{\delta_1}a\ldots ab^{\delta_k}\neq 1$, *tj.* $ab^{\delta_1}a\ldots ab^{\delta_k}=\phi\begin{pmatrix}a & b\\ c & d\end{pmatrix}$.

gde su a i d jednog, a b i c drugog, suprotnog znaka; pri tom, c i d nisu oba jednaki nuli (jer je ad-bc=1). Tada je

$$\phi\left(\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}-1 & 0\\ 1 & -1\end{pmatrix}\right)=\phi\begin{pmatrix}b-a & -b\\ d-c & -d\end{pmatrix}=ab^{\delta_1}a\ldots ab^{\delta_k}ab \qquad i$$

$$\phi\left(\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}\right)=\phi\begin{pmatrix}-a & a-b\\ -c & c-d\end{pmatrix}=ab^{\delta_1}a\ldots ab^{\delta_k}ab^2 \ .$$

U oba slučaja su dobijene matrice sa gore navedenim svojstvom. Napr. ako su a i d sa znakom +, a b i c sa znakom - , tada je $b-a<0$ *i* $d-c>0$. *U suprotnom je* $b-a>0$ *i* $d-c<0$, *itd.*

Dakle, $d-c\neq 0$ *pa* $\begin{pmatrix}b-a & -b\\ d-c & -d\end{pmatrix}\notin\ker\phi$;

slično, iz $a-b\neq 0$ *sledi da* $\begin{pmatrix}-a & a-b\\ -c & c-d\end{pmatrix}\notin\ker\phi$

Time je (4) u potpunosti dokazano.

Dakle, elementi iz M se jedinstveno predstavljaju pomoću $1,a,b,b^2$,

pa je $M\simeq C_2*C_3$.

2.5.Neka je grupa F slobodno generisana skupom X i neka je $X=\bigcup_{i\in I}X_i$ gde su

X_i medjusobno disjunktni skupovi. Dokazati da su podgrupe $H_i = \langle X_i \rangle$ slobodno generisane sa X_i i da je $F = \prod_{i\in I}^{*} H_i$.

Rešenje: $F = \langle X \rangle_s$ pa ne postoji netrivijalna strukturna jednakost nad elementima iz X (zad. 1.1.), dakle ni nad elementima iz X_i za proizvoljno $i\in I$; otuda, $H_i = \langle X_i \rangle_s$. Dalje, $F = \langle H_i \mid i\in I \rangle$ jer je $X = \bigcup_i X_i$, pa je proizvoljni element g iz F moguće predstaviti proizvodom elemenata iz H_i :

$$g = h_1 h_2 \ldots h_m \qquad (1)$$

($h_i \in H_{j_i}$, $i=1,\ldots,m$; h_i i h_{i+1} nisu u istoj podgrupi H_{j_i}).
Prema gornjem, svaki od h_i se jedinstveno predstavlja elementima iz X_i; dakle, g se izražava pomoću elemenata iz X, i to jedinstveno (zbog $F = \langle X \rangle_s$) pa je i predstavljanje (1) jedinstveno. Stoga $F = \prod_{i\in I}^{*} H_i$.

<u>Napomena</u>: *Slobodna grupa je, dakle, slobodan proizvod beskonačnih cikličnih grupa. Takodje, F_n se može razložiti u slobodan proizvod i na sledeći način:*

$$F_n = F_2 * F_{n-2} \quad (n \geqslant 2,\ F_0 = \{1\})$$

$$F_n = F_2 * F_1 * F_{n-3} \quad (n \geqslant 3),\ \text{itd.; uopšte}$$

$$F_n = F_{i_1} * F_{i_2} * \ldots * F_{i_k}$$

gde je $1 \leqslant k \leqslant n$, $i_1+i_2+\ldots+i_k=n$, tj.

$$\operatorname{rang} F_n = \sum_{j=1}^{k} \operatorname{rang} F_{i_j} \qquad (2)$$

Da (2) važi i za slobodan proizvod proizvoljnih grupa, dokazuje se u zadatku 2.23.

2.6.Ako su grupe G_1 i G_2 odredjene redom prezentacijama

$$\Pi_1 = \langle a_1, a_2, \ldots;\ R_1=1, R_2=1, \ldots \rangle ,\quad \Pi_2 = \langle b_1, b_2, \ldots;\ Q_1=1, Q_2=1, \ldots \rangle$$

dokazati da je $\Pi = \langle a_1, a_2, \ldots, b_1, b_2, \ldots;\ R_1=1, R_2=1, \ldots, Q_1=1, Q_2=1, \ldots \rangle$ prezentacija grupe $G_1 * G_2$.

Rešenje: Dokaz ovog tvrdjenja dat je u odeljku 12.1. (zadatak 12.1.45.).

2.7.Odrediti prezentaciju slobodnog proizvoda grupa A i B, ako je

a) $A = C_3$, $B = C_\infty$, b) $A = \langle a,b \rangle$, $B = \langle a,b,c \rangle$,

c) $A = \langle a,b,c;\ a^2=c^2, ab=c \rangle$, $B = \langle d,e;\ de^2=1 \rangle$.

Rešenje: Koristeći prethodni zadatak, slobodni proizvod $A * B$ ima predstavljanje:

a) $A * B = \langle a,b;\ a^3=1 \rangle$, b) $A * B = \langle a,b,c,d,e \rangle$,

c) $A * B = \langle a,b,c,d,e;\ a^2=c^2, ab=c,\ de^2=1 \rangle$.

2.8.Dokazati da je za proizvoljne grupe G_i ($i\in I$) ispunjeno:

a) $G_1 * G_2 = G_2 * G_1$, b) $(G_1 * G_2) * G_3 = G_1 * (G_2 * G_3)$,
c) Ako je $G = \prod_{i\in I}^{*} G_i$ i ako je $(\forall i \in I) G_i = \prod_{j\in J_i}^{*} H_{ij}$, tada $G = \prod_{\substack{i\in I \\ j\in J_i}}^{*} H_{ij}$.

Rešenje: Koristeći zad. 2.6.

2.9. Ispitati koje se od sledećih svojstava grupa prenosi slobodnim proizvodom:
a) Biti slobodna grupa , b) Konačna , c) Abel-ova ,
d) Konačno generisana , e) Periodična , f) Lokalno beskonačna

Rešenje: a) Ako su G_1 i G_2 slobodne grupe, prema zad. 1.1. i 2.6. slobodna je i grupa $G_1 * G_2$.

b) $G_1 * G_2$ je beskonačna grupa ako su G_1, G_2 netrivijalne grupe; (element ab, $a \in A$ i $b \in B$, je beskonačnog reda); dakle, slobodnim proizvodom se konačnost ne održava.

c) Grupa $C_\infty * C_\infty$ nije Abel-ova, iako C_∞ jeste.

d) $G_1 * G_2$ je konačno generisana, ako su takve G_1 i G_2 (v.zad. 2.6.).

e) Grupa $C_3 * C_2 = \langle a,b;\ a^3=1, b^2=1 \rangle$ nije periodična; element ab je beskonačnog reda.

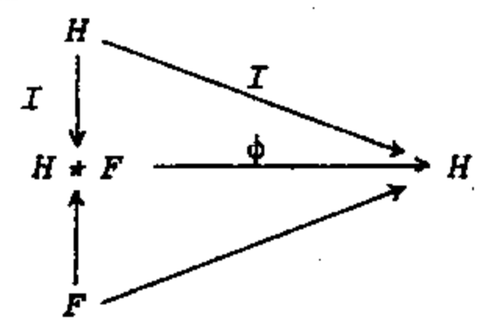
f) Ako su G_1 i G_2 netrivijalne lokalno beskonačne grupe (svi elementi izuzev 1 su beskonačnog reda), tada je i $G_1 * G_2$ lokalno beskonačna.

2.10. Ako je $G = \prod_{i\in I}^{*} G_i$ i ako su H_i prave podgrupe grupa G_i $(i \in I)$, tada za podgrupu $H = \langle H_i \mid i \in I \rangle$ važi: $H = \prod_{i\in I}^{*} H_i$. Dokazati.

Rešenje: Slično kao u rešenju zadatka 2.5., element $h \in H$, $H = \langle H_i \mid i \in I \rangle$ predstavlja se sa $h = h_1 h_2 \ldots h_n$, $h_i \in H_{j_i}$; kako je $h \in G$, gornji zapis je u svedenom obliku i jedinstven.

2.11. Ako je $G = H * F$ i ako je N najmanja normalna podgrupa u G koja sadrži F, tada je $H \cong G/N$. Dokazati.

Rešenje: Ako je $G = H * F$, prema definiciji 2.1., postoji preslikavanje ϕ takvo da dijagram



komutira. Kako je identičko preslikavanje $I : H \to H$ <u>na</u> preslikavanje, to je i ϕ <u>na</u>, pa je $(H * F)/\ker \phi \cong H$.

Neka je w proizvoljni element iz $H * F$ čiji je jedinstveni zapis

$$w = h_0 f_1 h_1 \ldots f_k h_k \qquad (h_i \in H,\ f_j \in F) .$$

Tada je

$w=h_0 f_1 h_0^{-1}(h_0h_1)f_2(h_0h_1)^{-1}\ldots(h_0h_1\ldots h_{k-1})f_k(h_0h_1\ldots h_{k-1})^{-1}h_0h_1\ldots h_k$

$=n\cdot h$

gde je $n=h_0 f_1 h_o^{-1}\ldots(h_0h_1\ldots h_{k-1})f_k(h_0h_1\ldots h_{k-1})^{-1}$ *element iz* $N=[F]^G$,
a $h=h_0h_1\ldots h_k$ *element iz H.*
Neka je $w\in\ker\phi$ *; tada :* $\phi(n\,h)=\phi(n)\cdot\phi(h)=\phi(h)=1$
① *jer je* $N\subseteq\ker\phi$

Medjutim, $\phi(h)=1$ *samo za* $h=1$, *pa je* $w=n$, *odnosno* $w\in N$. *Dakle,* $\ker\phi=N$.

2.12.Ako je $A*B=A*C$, da li je $B\simeq C$?

Rešenje: Prema zad. 2.11., $B\simeq C$.

Napomena: Iz $A*B\simeq A*C$ *ne sledi* $B\simeq C$. *Na primer,* $F_\infty * F_1\simeq F_\infty * F_2\simeq F_\infty$.

2.13.Dokazati da je $A*B$ $(A,B\neq\{1\})$ beskonačna grupa bez (netrivijalnog) centra.

Rešenje: $A*B$ *je beskonačna grupa (v.zad. 2.9.).*
Da je $Z(A*B)=\{1\}$ *dokazuje se kao u zadatku 1.10.*

2.14.Dokazati da su podgrupe A i B $(A,B\neq\{1\})$ beskonačnog indeksa u grupi $A*B$.

Rešenje: Elementi $(ab)^n$ *i* $(ab)^m$, *gde je* $a\in A$, $b\in B$ *su, zbog jedinstvenosti zapisa, različiti ako je* $n\neq m$. *Stoga su i razredi* $A(an)^n$ *i* $A(ab)^m$ *različiti.*

2.15.Dokazati da su sledeće grupe nerazložive u slobodni proizvod:
a) Abel-ove , b) Periodične , c) Konačne , d) Proste .

Rešenje: Uporediti sa zadatkom 2.9.
d) Neka je $G=A*B$ *prosta grupa* $(A,B\neq\{1\})$. *Tada je, prema zad. 2.11.,* $A\simeq G/N$ *gde je* $N=[B]^G$. *Dakle, G ima pravu normalnu podgrupu, suprotno pretpostavci da je prosta.*

2.16.Ispitati koje se od sledećih grupa mogu razložiti u slobodan proizvod:
a) $G=<a,b,c;\ a^3=1,b^5=1,c^4=1>$, b) $G=<a,b,c;\ a^3=b,c^7=1>$,
c) $G=<x,y;\ x^4=1,y^6=1,x^2=y^3>$, d) $G=<a,b;\ abab=1,b^2=1>$.

Rešenje: a) $G\simeq C_3*C_5*C_4$,
b) $G\simeq G_1*C_7$, *gde je* $G_1=<a,b;\ a^3=b>$.
c) Grupa G ima netrivijalan centar ($x^2\in Z(G)$), *pa prema zad. 2.13., G ne može biti slobodan proizvod.*
d) $G\simeq C_2*C_2$ *(videti zadatak 12.1.40.b)).*

2.17.Dokazati da je proizvoljni element konačnog reda grupe $A*B$ konjugovan odgovarajućem elementu konačnog reda iz A ili iz B.

Rešenje: Neka je $G = A * B$ *i* $g \in G$, *čiji je jedinstveni neskrativi zapis*

$$g = g_1 g_2 \cdots g_n \qquad (1)$$

Dokaz se može izvesti indukcijom po dužini $l(g)=n$.

Za $l(g)=0$ *(tj.* $g=e$*) ili* $l(g)=1$, *tvrdjenje je očigledno tačno.*

Neka je svaki element g konačnog reda u G, za koji je $l(g) < n$, *konjugovan izvesnom elementu konačnog reda u nekom od slobodnih činilaca A ili B.*

Neka je g sa zapisom (1) (tj. $l(g)=n$*) i neka je konačnog reda. To znači da* g_1 *i* g_n *pripadaju istoj grupi, A ili B (inače je* $g^k = g_1 \cdots g_n g_1 \cdots g_n \cdots g_1 \cdots g_n$ *neskrativ zapis, za svako k, pa je g beskonačnog reda). Odnosno*

$$g_1^{-1} g g_1 = g_2 \cdots (g_n g_1)$$

tj. $l(g_1^{-1} g g_1) \leqslant n-1$ *, pa je po pretpostavci njemu konjugovan element u A ili u B, odakle*

$$g_1^{-1} g g_1 = x t x^{-1} \quad \text{za neki } t \text{ iz } A \text{ ili } B \text{ pa je}$$

$$g = g_1 x t (g_1 x)^{-1} \quad \text{što je i trebalo dokazati.}$$

2.18. Neka je $G = \prod_{i \in I}^{*} G_i$ gde su G_i $(i \in I)$ konačne grupe. Tada je svaka konačna podgrupa grupe G izomorfna podgrupi neke grupe G_i. Dokazati.

Rešenje: Neka je H konačna podgrupa grupe G, i neka su $a, b \in H$. *Elementi a i b su konačnog reda, pa su prema zadatku 2.17. konjugovani elementima konačnog reda iz nekih od podgrupa* G_i $(i \in I)$. *Neka su a i b konjugovani elementima konačnog reda, c i d, redom iz podgrupa* G_j *i* G_k *, tj.*

$$a = g^{-1} c g \,, \quad b = h^{-1} d h \quad \text{za neke } g, h \in G.$$

Element ab pripada H i konačnog je reda, tj. postoji k tako da je

$$\underbrace{(g^{-1} c g h^{-1} d h)(g^{-1} c g h^{-1} d h) \cdots (g^{-1} c g h^{-1} d h)}_{k} = 1$$

Odavde $g=h$ *, tj.* $g^{-1}(cd)^k g = 1$, *odnosno* $(cd)^k = 1$.

Kada bi bilo $G_j \neq G_k$ *, tada bi element* $cd \in G_j * G_k$ *bio beskonačnog reda, suprotno izvedenom. Dakle,* $G_j = G_k$ *. Odnosno, svaka dva elementa a,b iz H pripadaju grupi* $g^{-1} G_j g$ *, za neko j.*

2.19. Neka je $G = G_1 * G_2$ i neka su $H_1 \lhd G_1$, $H_2 \lhd G_2$. Dokazati:

$$(G_1 * G_2)/H \simeq G_1/H_1 * G_2/H_2$$

gde je H normalna podgrupa grupe $G_1 * G_2$ generisana sa H_1 i H_2 .

Rešenje: Ako je $G_1 = \langle a_1, \ldots ; R_1 = 1, \ldots \rangle$, $G_2 = \langle b_1, \ldots ; S_1 = 1, \ldots \rangle$, *i ako su* H_1 *i* H_2 *normalne podgrupe generisane redom skupovima elemenata* $\{u_1, \ldots\}$, $\{v_1, \ldots\}$, *tada je, prema zad. 12.1.11.*

$$G_1/H_1 = \langle a_1, \ldots ; R_1 = 1, \ldots, u_1 = 1, \ldots \rangle ,$$

$$G_2/H_2 = \langle b_1,\ldots;\ S_1=1,\ldots,v_1=1,\ldots\rangle\ .$$

Odnosno,

$$G_1/H_1 * G_2/H_2 = \langle a_1,\ldots,b_1,\ldots;\ R_1=1,\ldots,u_1=1,\ldots,S_1=1,\ldots,v_1=1,\ldots\rangle$$

(videti zad. 2.6.).

S druge strane je $G_1 * G_2 = \langle a_1,\ldots,b_1,\ldots;\ R_1=1,\ldots,S_1=1,\ldots\rangle$ *, a podgrupa* H *je generisana sa* $\{u_1,\ldots,v_1,\ldots\}$*, pa je*

$$(G_1 * G_2)/H = \langle a_1,\ldots,b_1,\ldots;\ R_1=1,\ldots,S_1=1,\ldots,u_1=1,\ldots,v_1=1,\ldots\rangle$$

2.20. Neka je u grupi $G = G_1 * G_2$, $[G_1,G_2]$ podgrupa generisana komutatorima oblika $aba^{-1}b^{-1}$ $(a\in G_1,\ b\in G_2)$. Dokazati da je $[G_1,G_2]\lhd G$ i da je

$$\frac{G_1 * G_2}{[G_1, G_2]} \simeq G_1 \times G_2\ .$$

Rešenje: $[G_1,G_2] = \langle aba^{-1}b^{-1} \mid a\in G_1, b\in G_2\rangle$. *Neka je* $g_1\in G_1$. *Tada*

$$g_1(aba^{-1}b^{-1})g_1^{-1} = (g_1ab)a^{-1}(b^{-1}g_1^{-1}) = (g_1ab)(a^{-1}g_1^{-1}b^{-1}bg_1)(b^{-1}g_1^{-1})$$

$$= (g_1a)b(g_1a)^{-1}b^{-1}(bg_1b^{-1}g_1^{-1}) \underset{①}{=} (a_1ba_1^{-1}b^{-1})(bg_1b^{-1}g_1^{-1}) \underset{②}{\in} [G_1,G_2]$$

① $g_1\in G_1$, pa $a_1 = g_1a\in G_1$

② $a_1ba_1^{-1}b^{-1}\in [G_1,G_2]$, $bg_1b^{-1}g_1^{-1} = (g_1bg_1^{-1}b^{-1})^{-1}\in [G_1,G_2]$.

Slično, ako je $g_2\in G_2$.

Kako je $G = \langle G_1,G_2\rangle$, *to je* $g(aba^{-1}b^{-1})g^{-1}\in [G_1,G_2]$ *za sve* $g\in G$ *i sve* $a\in G_1$, $b\in G_2$.

Količnička grupa $(G_1 * G_2)/[G_1,G_2]$, *prema zad. 12.1.11. ima prezentaciju* $\langle a_1,\ldots,b_1,\ldots;\ R_1=1,\ldots,S_1=1,\ldots,a_1b_1a_1^{-1}b_1^{-1}=1,\ldots\rangle$ *, a to je, prema zadatku 12.1.44.a) prezentacija grupe* $G_1\times G_2$.

2.21. Neka je $[G_1,G_2]$ podgrupa grupe $G_1 * G_2$ kao u zadatku 2.20. Dokazati da je $[G_1,G_2]$ slobodna grupa.

Rešenje: Neka je $X = \{x_{[a,b]} \mid a\in A,\ b\in B\}$ *i* $w = x_1^{\varepsilon_1}\ldots x_k^{\varepsilon_k}$ $(x_i\in X)$ *jedinstveni neskrativi izraz po elementima iz* X. *Nakon zamene svakog* x_i *odgovarajućim elementom* $a_i^{-1}b_i^{-1}a_ib_i$, *dobijeni izraz* w', *koji predstavlja element iz* $G_1 * G_2$, *je u neskrativom obliku, i počinje sa* $a_1^{-1}b_1^{-1}$ *ili* $b_1^{-1}a_1^{-1}$, *što se lako proverava.*

2.22. Dokazati da je komutant slobodne grupe F_n $(n\geq 2)$ beskonačno generisana slobodna grupa.

Rešenje: I način. *Schreier-ova transverzala za komutant* K *grupe* $F_2 = \langle a,b\rangle$ *je* $\{a^mb^n \mid m,n\in Z\}$, *slobodni generatori za* K *su*

$$\{a^ib^jab^{-j}a^{-i-1} \mid i\in Z,\ j\in Z\setminus\{0\}\}$$

II način. Neka je $F_2 = G_1 * G_2$, gde je $G_1 \simeq G_2 \simeq C_\infty$, i neka je K komutant od F_2. Ako je $[G_1,G_2] = \langle aba^{-1}b^{-1} \mid a \in G_1, b \in G_2 \rangle$, tada je $[G_1,G_2] \subseteq K$. Prema zad. 2.20. je $F_2/[G_1,G_2] \simeq C_\infty \times C_\infty$. Dakle, $F_2/[G_1,G_2]$ je Abel-ova grupa, pa $K \subseteq [G_1,G_2]$. Stoga, $K = [G_1,G_2]$. Prema zad. 2.21. K je slobodna grupa slobodno generisana sa $\{aba^{-1}b^{-1} \mid a \in G_1, b \in G_2\}$, pa je K beskonačnog ranga.

2.23. Dokazati da je $\operatorname{rang}(A * B) = \operatorname{rang} A + \operatorname{rang} B$.

Rešenje: Neka je $\operatorname{rang}(A * B) = n$, $\operatorname{rang} A = m$, $\operatorname{rang} B = k$. Prema zad. 1.6., $A * B$ je homomorfna slika grupe F_n , tj. postoji homomorfizam $f : F_n \to A * B$. Prema teoremi Gruško-Neumann-a, $F_n = F' * F''$ gde je $A = f(F')$, $B = f(F'')$.

Za ove grupe važi

$$\operatorname{rang} A \leqslant \operatorname{rang} F', \qquad \operatorname{rang} B \leqslant \operatorname{rang} F''$$

(f je homomorfizam), tj. $m + k \leqslant \operatorname{rang} F' + \operatorname{rang} F''$, odakle, koristeći da je $\operatorname{rang} F' + \operatorname{rang} F'' = \operatorname{rang} F_n$ (videti napomenu zadatka 2.5.)

$$m + k \leqslant n \qquad (1)$$

S druge strane je

$$\operatorname{rang}(A * B) \leqslant \operatorname{rang} A + \operatorname{rang} B \qquad (2)$$

(jer je $A * B$ generisana sa A i B), tj.

$$n \leqslant m + k \qquad (2')$$

Iz (1) i (2') sledi $n = m + k$.

Neka je rang jedne od grupa A,B beskonačan. Tada je

$$\max(\operatorname{rang} A, \operatorname{rang} B) \geqslant \operatorname{rang} A + \operatorname{rang} B \qquad (3)$$

S druge strane,

$$\operatorname{rang}(A * B) \geqslant \operatorname{rang} A \ , \qquad \operatorname{rang}(A * B) \geqslant \operatorname{rang} B$$

tj.

$$\operatorname{rang}(A * B) \geqslant \max(\operatorname{rang} A, \operatorname{rang} B)$$

odakle, prema (3)

$$\operatorname{rang}(A * B) \geqslant \operatorname{rang} A + \operatorname{rang} B \qquad (4)$$

Iz (4) i (2) sledi tvrdjenje.

2.24. Dokazati sledeće, zajedničke osobine direktnog i slobodnog proizvoda grupa (simbol $\circ$ označava operaciju direktnog odnosno slobodnog proizvoda):

a) Za proizvoljne grupe G_1 i G_2 postoji grupa koja se označava sa $G = G_1 \circ G_2$ i koja sadrži podgrupe G_1' i G_2' takve da $G_1 \simeq G_1'$, $G_2 \simeq G_2'$ i $G = \langle G_1', G_2' \rangle$,

b) $[G_1]^G \cap G_2 = \{1\}$, $[G_2]^G \cap G_1 = \{1\}$,

c) $G_1 \circ G_2 \simeq G_2 \circ G_1$, d) $(G_1 \circ G_2) \circ G_3 \simeq G_1 \circ (G_2 \circ G_3)$,

e) Ako je $G = G_1 \circ G_2$ i ako $H_1 \lhd G_1$, $H_2 \lhd G_2$, tada
$G_1/H_1 \circ G_2/H_2 \simeq G/([H_1]^G \cdot [H_2]^G)$,

f) Ako je $G = G_1 \circ G_2$ i ako $H_1 < G_1$, $H_2 < G_2$, tada za podgrupu $H < G$, $H = \langle H_1, H_2 \rangle$ važi : $H \simeq H_1 \circ H_2$.

Rešenje: Videti odgovarajuće zadatke ovog poglavlja i poglavlja 5 o direktnom proizvodu.

2.25. Dokazati da nijedna netrivijalna grupa nije istovremeno slobodan i direktan proizvod netrivijalnih grupa.

Rešenje: Neka je, naprotiv, $G = A * B = C \times D$, $(A,B,C,D \neq \{1\})$. *Uočimo element g grupe G za koji je* $g=ab$, $a \in A$, $b \in B$, $a \neq 1$, $b \neq 1$ *(takav g, s obzirom na pretpostavke, sigurno postoji). Elementi*

$$ab,\ (ab)^2,\ (ab)^3,\ (ab)^4,\ldots$$

su svi različiti i medjusobno komutiraju. Zbog jedinstvenosti (neskratovog) zapisa, to su ujedno i jedini elementi komutativni sa ab, tj. g. Dakle, za centralizator $C_G(g)$ *elementa g u grupi G važi:*

$$C_G(g) = C_\infty \qquad (1)$$

Ako je, s druge strane, $g \in C \times D$, *tada je za neke* $c \in C$, $d \in D$: $g=(c,d)$. *U ovom slučaju za* $C_G(g)$ *važi sledeće:*

$$\begin{aligned} C_G(g)=C_G(c,d) &= \{(x,y) \mid x \in C,\ y \in D,\ (x,y)(c,d)=(c,d)(x,y)\} \\ &= \{(x,y) \mid x \in C,\ y \in D,\ (xc,yd)=(cx,dy)\} \\ &= \{(x,y) \mid (x \in C \wedge xc=cx) \wedge (y \wedge D \wedge yd=dy)\} \\ &= \{(x,y) \mid x \in C_C(c),\ y \in C_D(d)\} = \\ & C_C(c) \times C_D(d) \end{aligned}$$

gde su, očigledno, $C_C(c)$ *i* $C_D(d)$ *različiti od trivijalne grupe.*

Dakle, koristeći (1) je

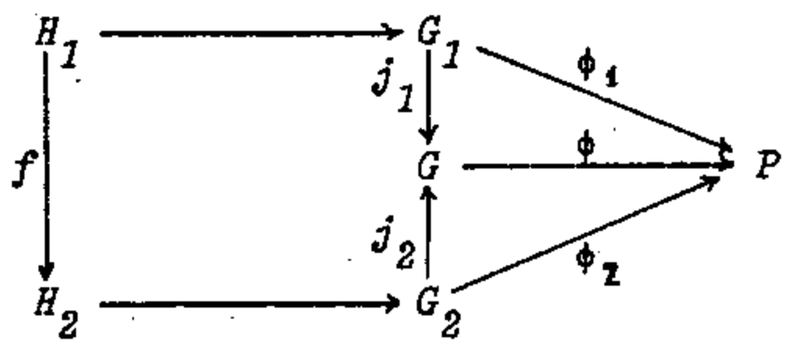
$$C_\infty = C_C(c) \times C_D(d)$$

Što nije tačno, jer C_∞ *nije razloživa u netrivijalan direktan proizvod (videti zadatak 5.3.5.a)).*

11.3. SLOBODAN PROIZVOD SA ZAJEDNIČKOM PODGRUPOM

Jedna dalja generalizacija slobodnih grupa je slobodan proizvod sa zajedničkom podgrupom.

3.1. *Definicija:* *Neka su G_1 i G_2 grupe, $H_1 < G_1$, $H_2 < G_2$ i $f : H_1 \to H_2$ je izomorfizam. Slobodan proizvod grupa G_1 i G_2 sa zajedničkom (amalgamiranom) podgrupom je grupa G sa utapanjima $j_1 : G_1 \to G$ i $j_2 : G_2 \to G$ takva da za svaku grupu P i svaki par homomorfizama $\phi_1 : G_1 \to P$ i $\phi_2 : G_2 \to P$ za koje komutira dijagram*



postoji jedinstveni homomorfizam $\phi : G \to P$ za koji je $\phi \circ j_1 = \phi_1$, $\phi \circ j_2 = \phi_2$.

Koriste se oznake : $G = G_1 \underset{f}{*} G_2$ ili $G = G_1 \underset{H}{*} G_2$ (ako je $H_1 = H_2 = H$) ili $G = *(G_1, G_2, H_1, H_2, f)$.

Napomena: U prethodnoj definiciji se ne mora zahtevati da homomorfizmi j_1 i j_2 budu 1-1 (ta se svojstva za preslikavanja j_1, j_2 dokazuju); videti rešenje zadatka 3.2.). Izabrana je ovakva formulacija zbog analogije sa definicijom 2.1.

Slobodan proizvod je, dakle, poseban slučaj slobodnog proizvoda sa zajedničkom podgrupom (zajednička podgrupa je trivijalna grupa {1}).

Kao i u slučaju slobodnog proizvoda, dokazuje se egzistencija grupe $G_1 \underset{f}{*} G_2$ (za proizvoljne G_1, G_2, f) kao i njena jedinstvenost (do na izomorfizam) - videti zadatke 3.2. i 3.2.

3.2. *Teorema:* *Neka su G_1 i G_2 grupe sa izomorfnim podgrupama redom H_1 i H_2, i izomorfizmom $f : H_1 \to H_2$. Tada je grupa $G_1 \underset{f}{*} G_2$ izomorfna grupi $(G_1 * G_2)/N$ gde je N normalna podgrupa grupe $G_1 * G_2$ generisana sa $\{h \cdot f(h^{-1}) \mid h \in H_1\}$.*

(Podsetimo da možemo pretpostaviti da su G_1 i G_2 podgrupe grupe $G_1 * G_2$.)

Ova teorema omogućuje novu, očiglednu, definiciju amalgamiranog proizvoda.

Moguće je, naravno, operaciju $\underset{H}{*}$ definisati za proizvoljnu familiju

grupa. Neka su G_i $(i \in I)$ grupe i $H_i < G_i$ koje su sve izomorfne nekoj grupi H, sa izomorfizmima $f_i : H_i \to H$. Izomorfizmi $g_{ij} : H_i \to H_j$ odredjeni su sa $g_{ij} = f_j^{-1} \circ f_i$. Slobodan proizvod grupa G_i $(i \in I)$ sa zajedničkom podgrupom H je faktor grupa G slobodnog proizvoda $\prod_{i \in I}^{*} G_i$ po normalnoj podgrupi N generisanoj sa $\{x \cdot g_{ij}(x^{-1}) \mid x \in H_i,\ i,j \in I\}$.

Kao i u slučaju slobodnih grupa F i slobodnih proizvoda $G_1 * G_2$, i ovde, kod slobodnih proizvoda $G_1 \underset{f}{*} G_2$ sa zajedničkom podgrupom, svaki element se može jedinstveno predstaviti izrazom u odgovarajućem svedenom obliku.

Neka su grupe G_1 i G_2 razbijene na desne razrede po podgrupama redom H_1 i H_2 $(H_1 \simeq H_2 \simeq H)$, i neka su izabrani predstavnici tih razreda, uz uslov da su predstavnici za H_1 i H_2 jedinični elementi.

Označimo sa $\bar{g}_i$ predstavnika razreda $H_i g_i$ $(g_i \in G_i,\ i=1,2)$, tj.

$$g_i = h_i \bar{g}_i \quad \text{za neko } h_i \in H_i \quad (i=1,2). \tag{1}$$

Izraz

$$h \bar{g}_1 \bar{g}_2 \dots \bar{g}_k \quad (k \geq 0) \tag{***}$$

gde je $h \in H_1$, $\bar{g}_i$ i $\bar{g}_{i+1}$ $(i=1,\dots,k-1)$ su predstavnici, različiti od 1, koji nisu oba u G_1 ili oba u G_2, je u *svedenom* obliku u grupi $G_1 \underset{H}{*} G_2$.

U zadatku 3.1. je dokazano da se svaki element grupe $G_1 \underset{f}{*} G_2$ jedinstveno prikazuje svedenim izrazom (***).

Ako su H_1 i H_2 trivijalne grupe, tj. proizvod $G_1 \underset{f}{*} G_2$ se svodi na obični slobodni proizvod $G_1 * G_2$, svedeni oblik (**) iz 11.2. je ujedno i oblika (***).

Primeri i zadaci

3.1. Neka su G_1 i G_2 grupe sa izomorfnim podgrupama redom H_1 i H_2 i izomorfizmom $f : H_1 \to H_2$, i neka je $G = (G_1 * G_2)/N$ gde je N normalna podgrupa generisana sa $\{h \cdot f(h^{-1}) \mid h \in H_1\}$. Dokazati da se svaki element g iz G jedinstveno predstavlja izrazom u svedenom obliku (***), tj. izrazom

$$g = h \bar{g}_1 \bar{g}_2 \dots \bar{g}_k$$

gde je $h \in H_1$, $\bar{g}_i$ su predstavnici $(\neq 1)$ desnih razreda po H_1 u G_1 ili po H_2 u G_2, pri čemu su $\bar{g}_i$ i $\bar{g}_{i+1}$ u različitim grupama (G_1 ili G_2).

Rešenje: Najpre dokazujemo da za svaki element $g \in G_1 * G_2$ čiji je jedinstveni neskrativi zapis $g = g_1 g_2 \dots g_k$, postoji izraz $g_s = h \bar{g}_1 \dots \bar{g}_n$ oblika (***) tako da

$$\pi(g) = g_s N, \quad \text{gde je } \pi : G_1 * G_2 \to (G_1 * G_2)/N \text{ prirodni homomorfizam.}$$

Dokaz izvodimo indukcijom po k , tj. dužini elementa g.

Neka je $k=1$, tj. $g=g_1$, dakle $g_1 \in G_1$ ili $g_1 \in G_2$. Tada je $\pi(g)=h_i\bar{g}_i N$ za neki $h_i \in H_i$, gde je $\bar{g}_i$ predstavnik desnog razreda $H_i g_1$ ($i=1$ ili $i=2$). Ako je $i=1$ tada je $g_s=h_1 g_1$ u traženom obliku.
Neka je $i=2$. Tada $\pi(g)=h_2\bar{g}_2 N$, pa za neki $h_1 \in H_1$ $f(h_1)=h_2$. Kako je $h_1 \cdot f(h_1^{-1}) \in N$ to $h_1 N=f(h_1)N$, odakle nalazimo

$$f(h_1)\bar{g}_2 N=f(h_1)N\bar{g}_2=h_1 N\bar{g}_2=h_1\bar{g}_2 N$$

pa možemo uzeti $g_s=h_1\bar{g}_2$.

Sada dokazujemo induktivni prelaz sa k na $k+1$. Neka je $g \in G_1 * G_2$ dužine $k+1$, recimo $g=vg_1 \ldots g_k$. Primetimo da je $\pi(g)=\pi(v)\pi(g_1 \ldots g_k)$. Prema induktivnoj pretpostavci za neke $h, h_1 \in H_1$ i predstavnike $\bar{v}_1, \bar{g}_1, \ldots, \bar{g}_n$ desnih razreda grupa H_1, H_2 respektivno u G_1, G_2 imamo

$$v_s=h_1\bar{v}_1 \ , \quad (g_1 \ldots g_k)_s=h\,\bar{g}_1 \ldots \bar{g}_n \ .$$

Neka je $w=\bar{v}_1 h$. Tada postoje ove mogućnosti:
1° $\bar{v}_1$ je predstavnik desnog razreda podgrupe H_1 u G_1 , tj. za neki $h_2 \in H_1$ i $x \in G_1$ $\bar{v}_1=h_2 x$. Tada $w \in G_1$ pa po induktivnoj hipotezi (slučaj $k=1$) postoji $h_3 \in H_1$ tako da $w_s=h_3\bar{w}_1$.
2° $\bar{v}_1$ je predstavnik desnog razreda podgrupe H_2 u G_2 , tj. za neki $h_3 \in H_2$ i $y \in G_2$ $\bar{v}_1=h_3 y$. Kako je $hN=f(h)N$, imamo $\pi(w)=h_3 yhN=h_3 yf(h)N$, tj. za $u=h_3 yf(h)$ $\pi(w)=\pi(u)$. Kako je $u \in G_2$, to po induktivnoj hipotezi (slučaj $k=1$) za neki $h_4 \in H_1$ $u_s=h_4\bar{u}_1$, dakle možemo uzeti $w_s=h_4\bar{w}_1$, gde $\bar{w}_1=\bar{u}_1$.
Prema 1° i 2° postoji $h^* \in H_1$ tako da $w_s=h^*\bar{w}_1$, pa

$$gN=vg_1 \ldots g_k N=vNg_1 \ldots g_k N=h_1\bar{v}_1 Nh\bar{g}_1 \ldots \bar{g}_n N=h_1\bar{v}_1 hN\bar{g}_1 \ldots \bar{g}_n N$$
$$=h_1 wN\bar{g}_1 \ldots \bar{g}_n N=h_1 h^* w_1 N\bar{g}_1 \ldots \bar{g}_n N=h'\bar{w}_1\bar{g}_1 \ldots \bar{g}_n N$$

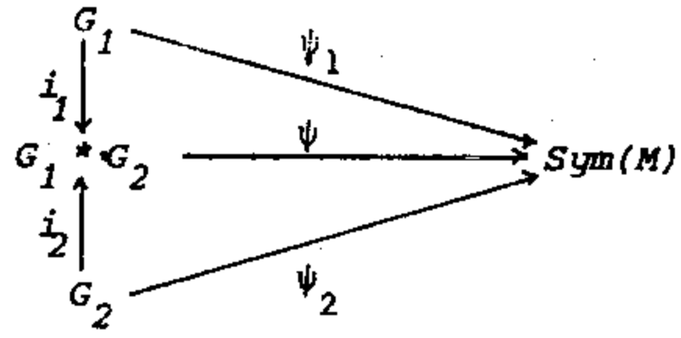
gde $h'=h_1 h^*$. Dakle, ako $\bar{w}_1, \bar{g}_1$ pripadaju različitim grupama G_1, G_2 onda možemo uzeti $g_s=h'\bar{w}_1\bar{g}_1 \ldots \bar{g}_n$
Ako $\bar{w}_1, \bar{g}_1$ pripadaju istoj grupi, recimo G_i , onda $\bar{w}_1\bar{g}_1 \in G_i$, pa po induktivnoj hipotezi (slučaj $k=1$) za neki $h'' \in H_i$ i predstavnik $\bar{a}$ desnog razreda grupe H_i u G_i važi $\bar{w}_1\bar{g}_1=h''\bar{a}$, pa možemo uzeti $g_s=h'''\bar{a}\bar{g}_1 \ldots \bar{g}_n$. gde $h'''=h'h''$.

Dokazujemo sada jedinstvenost ovakvog predstavljanja.
Neka je M skup svih izraza u svedenom obliku (***). Svakom elementu $x \in G_i$ pridružimo funkciju $\theta_x : M \xrightarrow[na]{1-1} M$, na sledeći način

$$\theta_x(h\,\bar{g}_1 \ldots \bar{g}_m)=(h\,\bar{g}_1 \ldots \bar{g}_m x)_s$$

(gde je $(h\bar{g}_1 \ldots \bar{g}_m x)_s$ svedeni izraz oblika (***), koji prema prethodnom razmatranju postoji; izraz $h\bar{g}_1 \ldots \bar{g}_m x$ se prvo dovede na neskrativ oblik u $G_1 * G_2$).

Lako se pokazuje (kao u zadatku 2.2.) da je ovako uvedenim preslikavanjem $x \longmapsto \theta_x$ $(x \in G_i)$ *odredjeno utapanje* $\psi_i : G_i \to Sym(M)$ $(i=1,2)$. *Neka je* ψ *jedinstveni homomorfizam* $G_1 * G_2 \to Sym(M)$ *za koji dijagram*



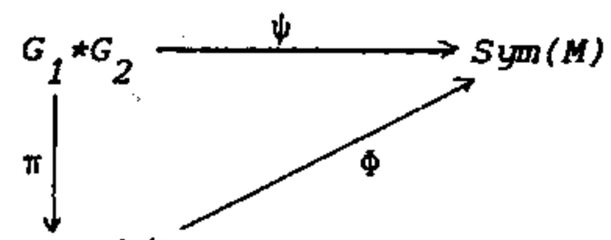
komutira (i_1 *i* i_2 *su utapanja* G_1 *i* G_2 *tim redom u* $G_1 * G_2$).
Dakle,

$$\psi(g_1 \ldots g_k) = \theta_{g_1}\theta_{g_2}\ldots\theta_{g_k} \quad (g_1 \ldots g_k \text{ je iz } G_1 * G_2) .$$

Označimo sa π *prirodni homomorfizam* $\pi : G_1 * G_2 \to (G_1 * G_2)/N$. *Dokazujemo da je* $\ker \pi \subseteq \ker \psi$. *Kako je* $N=\ker \pi$ *najmanja normalna podgrupa od* $G_1 * G_2$ *koja sadrži skup* $\{h \cdot f(h^{-1}) \mid h \in H_1\}$ *dovoljno je dokazati da za sve* $h \in H_1$ $\psi(h)=\psi(f(h))$. *Dakle, neka je* $h \in H_1$. *Tada* $f(h) \in H_2$ *i* $\psi(f(h))=\theta_{f(h)}$. *Otuda za proizvoljni element čiji je svedeni oblik* $h\bar{g}_1 \ldots \bar{g}_m$ *važi*

$h\bar{g}_1 \ldots \bar{g}_m f(h)N = h\bar{g}_1 \ldots \bar{g}_m hN$, *dakle* $(h\bar{g}_1 \ldots \bar{g}_m f(h))_s = (h\bar{g}_1 \ldots \bar{g}_m h)_s$, *tj.* $\theta_{f(h)} = \theta_h$. *Stoga* $\psi(f(h))=\psi(h)$, *što je i trebalo dokazati.*

Dakle, postoji **homomorfizam** Φ *koje produžuje* ψ *na sledeći način*



Tada je $\Phi(Ng_1 \ldots g_k) = \theta_h \theta_{\bar{g}_1} \ldots \theta_{\bar{g}_m}$ *gde je* $h\bar{g}_1 \ldots \bar{g}_m$ *predstavljanje elementa* $g_1 \ldots g_k$. *Najzad je*

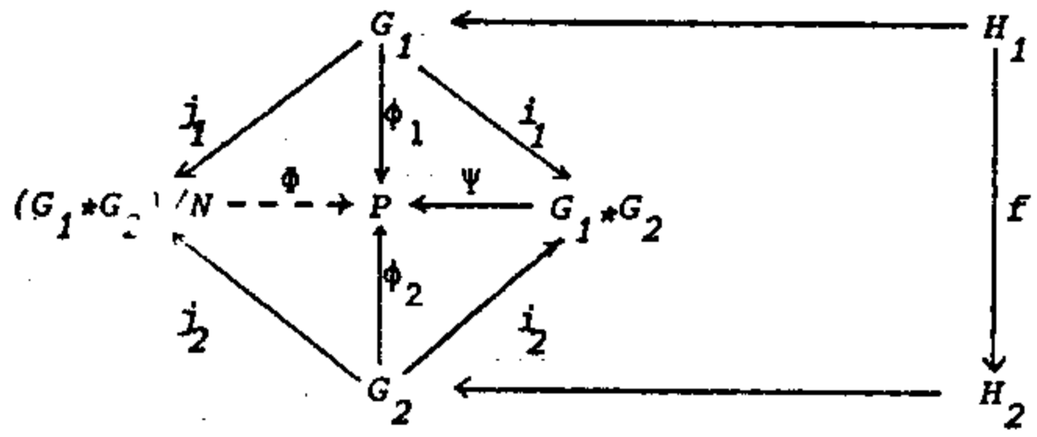
$$(\theta_h \theta_{\bar{g}_1} \ldots \theta_{\bar{g}_m})(1) = h\bar{g}_1 \ldots \bar{g}_m ,$$

tj. različitim izrazima oblika (***) odgovaraju različite funkcije iz Sym(M), odakle sledi tražena jedinstvenost.

3.2. Neka su G_1 i G_2 grupe sa izomorfnim podgrupama H_1 i H_2 i izomorfizmom $f : H_1 \to H_2$. Dokazati da je grupa $(G_1 * G_2)/N$, gde je N normalno zatvorenje skupa $\{hf(h^{-1}) \mid h \in H_1\}$, slobodan proizvod grupa G_1 i G_2 sa zajedničkom podgrupom H ($\simeq H_1 \simeq H_2$), u smislu definicije 3.1.

Rešenje: Neka su i_1 *i* i_2 *utapanja redom grupa* G_1 *i* G_2 *u grupu* $G_1 * G_2$ *i neka je* $\pi : G_1 * G_2 \to (G_1 * G_2)/N$ *prirodni homomorfizam. Definišimo preslikavanja* $j_k : G_k \to (G_1 * G_2)/N$ $(k=1,2)$ *na sledeći način:* $j_k = \pi \circ i_k$.
Neka je P proizvoljna grupa i $\phi_k : G_k \to P$ $(k=1,2)$ *homomorfizmi.*

Bez gubljenja opštosti, možemo uzeti da su preslikavanja i_1, i_2 inkluzivna.



Dalje, prema osobini slobodnog proizvoda, postoji (jedinstven) homomorfizam $\Psi : G_1 * G_2 \to P$ *tako da* $\Psi \circ i_1 = \phi_1$, $\Psi \circ i_2 = \phi_2$. *Prema prethodnom zadatku, svaki član x grupe* $(G_1 * G_2)/N$ *predstavlja se na jedinstven način svedenim izrazom* $h\bar{g}_1 \ldots \bar{g}_m$ *vida (***), tj.* $x = h\bar{g}_1 \ldots \bar{g}_m N$. *Neka je* $\Phi : (G_1 * G_2)/N \to P$ *definisano na sledeći način*

$$\Phi(h\bar{g}_1 \ldots \bar{g}_m N) = \Psi(h)\Psi(\bar{g}_1)\ldots\Psi(\bar{g}_m) \qquad (1)$$

Ovako definisano preslikavanje Φ *je homomorfizam grupe* $(G_1 * G_2)/N$ *u grupu P i navedeni dijagram komutira.*

Preslikavanje Φ *je jedinstveno odredjeno, jer ako je* Φ' *neko drugo preslikavanje koje čini komutativnim dijagram iz definicije amalgamiranog proizvoda, onda (1) važi i za* Φ' *(umesto* Φ *je* Φ'*), odakle* $\Phi = \Phi'$.

3.3. Dokazati da je grupama G_1 i G_2 i izomorfizmom $f : H_1 \to H_2$ njihovih podgrupa, jedinstveno (do na izomorfizam) odredjena grupa $G_1 *_f G_2$.

Rešenje: Prema zadatku 3.2. i definiciji 3.1.

3.4. Ako su G_1 i G_2 predstavljene sa $G_1 = \langle a_1, \ldots; R_1, \ldots \rangle$, $G_2 = \langle b_1, \ldots; S_1, \ldots \rangle$ i ako je $H_1 = \langle u_1, \ldots \rangle$, $H_2 = \langle v_1, \ldots \rangle$ $(H_i < G_i,\ i=1,2)$, gde je $f(u_j) = v_j$ $(j=1,2,\ldots)$, dokazati da je

$$G_1 *_f G_2 = \langle a_1, \ldots, b_1, \ldots; R_1, \ldots, S_1, \ldots, u_1 = v_1, \ldots \rangle .$$

Rešenje: Direktno prema zadacima 3.2. i 12.1.11., 12.1.45.

3.5. Odrediti $*(G_1, G_2, H_1, H_2, f)$ ako je $G_1 = \langle a;\ a^4 = 1 \rangle$, $G_2 = \langle b;\ b^6 = 1 \rangle$, $H_1 = \langle a^2;\ (a^2)^2 = 1 \rangle$, $H_2 = \langle b^3;\ (b^3)^2 = 1 \rangle$, $f(a^2) = b^3$.

Rešenje: $G_1 = \{1, a, a^2, a^3\}$, $G_2 = \{1, b, b^2, b^3, b^4, b^5\}$; $H_1 \simeq C_2$, $H_2 \simeq C_2$ tj. $H_1 \simeq H_2$ *gde je* $f(a^2) = b^3$. *Prema zad. 3.4. grupa* $G = *(G_1, G_2, H_1, H_2, f)$ *je sa postavkom* $G = \langle a, b;\ a^4 = 1, b^6 = 1, a^2 = b^3 \rangle$.

3.6. Za sledeće grupe (sa izomorfnom podgrupom) odrediti slobodan proizvod sa zajedničkom podgrupom:

a) $G_1 = \langle a;\ a^4 \rangle$, $G_2 = \langle b;\ b^6 \rangle$, $G_3 = \langle c;\ c^{10} \rangle$,
$H_1 = \langle a^2 \rangle$, $H_2 = \langle b^3 \rangle$, $H_3 = \langle c^5 \rangle$; $f: H_1 \to H_2$, $f(a^2)=b^3$; $g: H_1 \to H_3$, $g(a^2)=c^5$

b) $G_1 = *(A,B,A_1,B_1,f)$ i G_2, gde su $A = \langle a \rangle$, $B = \langle b \rangle$, $A_1 = \langle a^2 \rangle$, $B_1 = \langle b^3 \rangle$, $f(a^2)=b^3$; $G_2 = \langle c \rangle$, $H_2 = \langle c^7 \rangle$; $H_1 = \langle b^5 \rangle$, $g(b^5)=c^7$.

Rešenje: H_1, H_2 i H_3 su izomorfne grupe ($\simeq C_2$), pa je

$$G = *(G_1,G_2,G_3,H_1,H_2,H_3,f,g) = \langle a,b,c;\ a^4=1, b^6=1, c^{10}=1, a^2=b^3, a^2=c^5 \rangle$$

b) $G_1 = \langle a,b;\ a^2=b^3 \rangle$, $G_2 = \langle c \rangle$. Obe grupe imaju kao svoju podgrupu, grupu C_∞ Zaista, $H_1 = \langle b^5 \rangle \simeq C_\infty$, $H_2 = \langle c^7 \rangle \simeq C_\infty$. Stoga je

$$G = *(G_1,G_2,H_1,H_2,g) = \langle a,b,c;\ a^2=b^3, b^5=c^7 \rangle .$$

3.7. Neka je $G = G_1 *_f G_2$ slobodan proizvod sa zajedničkom podgrupom, sa izomorfizmom $f : H_1 \to H_2$. Dokazati da je $G \simeq \langle G_1, G_2 \rangle$ i $G_1 \cap G_2 \simeq H_1$.

Rešenje: $G = G_1 *_f G_2$ je generisana podgrupama (izomorfnim sa) G_1 i G_2, jer je $G \simeq (G_1 * G_2)/N$, $N = \left[hf(h^{-1}) \mid h \in H_1 \right]$. Neka je, dalje, $g \in G_1 \cap G_2$; tada

$$g = h_1\bar{g}_1 \quad (h_1 \in H_1,\ \bar{g}_1 \in G_1), \quad g = h_2\bar{g}_2 \quad (h_2 \in H_2,\ \bar{g}_2 \in G_2) , \text{ tj.}$$

$g = f(h^*)\bar{g}_2$ $(h^* \in H_1,\ f(h^*)=h_2)$, odakle zbog $Nf(h^*)=Nh^*$ sledi

$$h_1\bar{g}_1 = h^*\bar{g}_2 .$$

Iz jedinstvenosti predstavljanja elemenata iz G (v.zad. 3.1.) sledi $\bar{g}_1=\bar{g}_2=1$, $h_1=h^*$ tj. $g \in H_1$ (ne može biti $\bar{g}_1=\bar{g}_2 \neq 1$, jer je u slobodnom proizvodu $G_1 * G_2$ ispunjeno $G_1 \cap G_2 = \{1\}$). Obratno, neka je $g \in H_1$. Tada je $f(g) \in H_2$, tj. $g \in H_2$. Zbog $H_1 < G_1$, $H_2 < G_2$ je $g \in G_1 \cap G_2$.

3.8. Neka je g element konačnog reda u grupi $G_1 * G_2$. Dokazati da je g u grupi konjugovanoj sa G_1 ili sa G_2 .

Uputstvo: Slično zadatku 2.17.

3.9. Ako je $H_1 \lhd G_1$, $H_2 \lhd G_2$ i $G = *(G_1,G_2,H_1,H_2,f)$, dokazati da je

$$Z(G) = H_1 \cap Z(G_1) \cap Z(G_2) .$$

Rešenje: Da je $H_1 \cap Z(G_1) \cap Z(G_2) \subseteq Z(G)$ sledi iz činjenice da G_1 i G_2 generišu grupu G.

Neka je $g \in Z(G)$ i neka je $g = h\bar{g}_1\bar{g}_2 \ldots \bar{g}_n$ (jedinstveni) svedeni izraz za g (tj. $h \in H_1$, $\bar{g}_i$ i $\bar{g}_{i+1}$ nisu u istoj grupi G_j, $j=1,2$).

Za $n=0$ je $g=h$; ako $h \notin Z(G_1) \cap Z(G_2)$, napr. $h \notin Z(G_1)$, tada $hg_1 \neq g_1h$ za neko $g_1 \in G_1$. Odavde, $h \notin Z(G)$, suprotno pretpostavci.

Neka je $n > 0$ i napr. $\bar{g}_n \in G_1$; uočimo tada $g' \in G_2 \setminus H_2$. Izraz za gg' je tada u svedenom obliku: $(gg')_s = h\bar{g}_1\bar{g}_2 \ldots \bar{g}_n g'$. Za $g'g = g'h\bar{g}_1 \ldots \bar{g}_n$ se posle dovo-

djenja na svedeni oblik (kao u zad. 3.1.) dobija izraz različit od izraza za gg^* (prvi se završava sa $\bar{g}_n \in G_1$, a drugi sa $g^* \in G_2$). Dakle, $g^*g \neq gg^*$, suprotno pretpostavci.

Prema tome, $g \notin H_1$. Zbog $g \in Z(G)$ je $g \in Z(G_1)$ i $g \in Z(G_2)$, pa je $Z(G) \leq H_1 \cap Z(G_1) \cap Z(G_2)$.

3.10. Neka je $A = \star(G_1, G_2, H_1, H_2, f)$ i $B = \star(G_1, G_2, H_1, H_2, g)$ gde su f i g različita izomorfna preslikavanja podgrupa H_1 i H_2. Dokazati da nije uvek $A \simeq B$.

Rešenje: Kontraprimer: $G_1 = \langle a,b;\ a^4=1, b^2=1, ab=ba^{-1} \rangle$, $H_1 = \langle a^2, b \rangle$,
$G_2 = \langle c,d;\ c^4=1, d^2=1, cd=dc^{-1} \rangle$, $H_2 = \langle c^2, d \rangle$;
$f: H_1 \to H_2$, $f(a^2)=c^2$, $f(b)=d$
$g: H_1 \to H_2$, $g(a^2)=d$, $g(b)=c^2$.
Grupe A i B su predstavljene sa

$$A = \langle a,b,c,d;\ a^4=1, b^2=1, ab=ba^{-1}, c^4=1, d^2=1, cd=dc^{-1}, a^2=c^2, b=d \rangle$$
$$B = \langle a,b,c,d;\ a^4=1, b^2=1, ab=ba^{-1}, c^4=1, d^2=1, cd=dc^{-1}, a^2=d, b=c^2 \rangle .$$

Dokazuje se da je grupa A sa netrivijalnim centrom ($a^2 \in Z(A)$), dok je B grupa bez centra. Dakle, $A \neq B$.

3.11. Neka je $G = \star(G_1, G_2, H_1, H_2, f)$ i neka s(G) označava: a) G je konačna grupa, b) G je Abel-ova grupa. Dokazati

$$s(G) \Leftrightarrow s(G_1) \wedge s(G_2) \wedge (G_1 = H_1 \vee G_2 = H_2) .$$

Rešenje: a) ($\Rightarrow$) Ako je jedna od grupa G_1, G_2 beskonačna, tada je (koristeći jedinstvenost zapisa) i G beskonačna. Ako su $G_1 \neq H_1$ i $G_2 \neq H_2$, tj. postoje elementi $g_1 \in G_1 \setminus H_1$ i $g_2 \in G_2 \setminus H_2$, tada je $g_1 g_2$ beskonačnog reda u G.
($\Leftarrow$) Neka su $G_1 = \langle a_1, \ldots, a_n;\ R_1, \ldots, R_k \rangle$, $G_2 = \langle b_1, \ldots, b_m;\ S_1, \ldots, S_1 \rangle$ konačne grupe, i neka je $G_1 = H_1$. Tada je G sa predstavljanjem

$$G = \langle a_1, \ldots, a_n, b_1, \ldots, b_m;\ R_1, \ldots, R_k, S_1, \ldots, S_1, a_1 = f(a_1), \ldots, a_n = f(a_n) \rangle$$

Kako su $f(a_i) \in H_2$ $(i=1,\ldots,n)$, tj. $f(a_i)$ su izrazi nad $b_1, \ldots, b_m$, to je, primenjujući Tietze-ove transformacije tipa (T4) (videti odeljak 12.2.)

$$G = \langle b_1, \ldots, b_m;\ R_1', \ldots, R_k', S_1, \ldots, S_1 \rangle$$

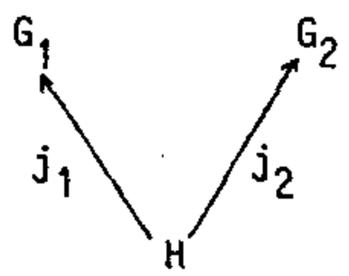
gde je R_i' $(i=1,\ldots,k)$ izraz dobijen od R_i zamenom svih slova a_j odgovarajućim izrazima $f(a_j)$ $(j=1,\ldots,n)$. Kako je G_2 konačna grupa, konačna je i njena faktor-grupa G.

b) ($\Rightarrow$) Direktno pomoću zadatka 3.9.

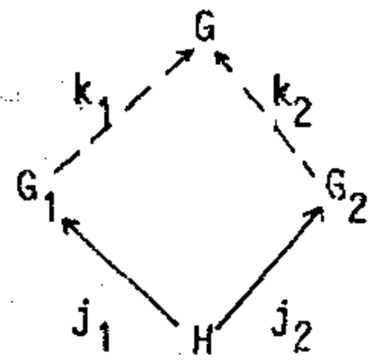
($\Leftarrow$) Kao pod a) ($\Leftarrow$ deo).

3.12. Dokazati da klasa grupa ima sledeće svojstvo amalgamacije:

Svaki dijagram vida (1), sa utapanjima j_1, j_2, ima dopunu do komutativnog



(1)

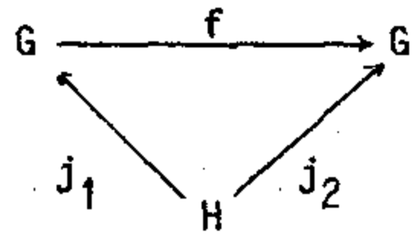


(2)

dijagrama (2), sa utapanjima k_1, k_2 .

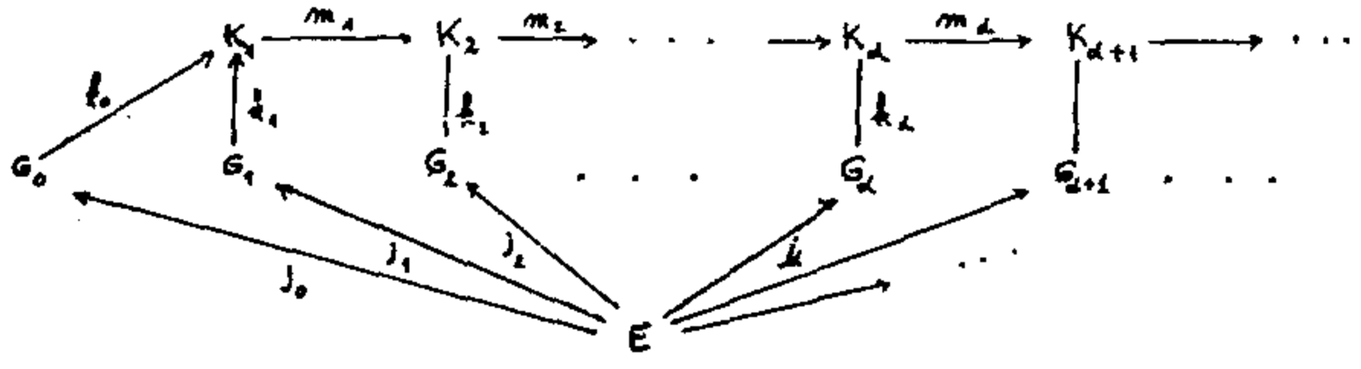
Rešenje: Neka je $f : H \to H$ *identičko preslikavanje i G slobodan proizvod grupa* G_1 , G_2 *po podgrupi H , tj.* $G = *(G_1, G_2, H, H, f)$.

3.13. Grupa G je *univerzalna* ako se svaka grupa kardinalnosti α, $\alpha \leq |G|$ utapa u G.
Grupa G je *homogena* ako za svaku grupu H , $|H| < |G|$ i svaka dva utapanja $j_1, j_2 : H \to G$ postoji $f \in \mathrm{Aut}\, G$ tako da $f \circ j_1 = j_2$.
Grupa G je *homogeno-univerzalna* ako je G homogena i univerzalna.

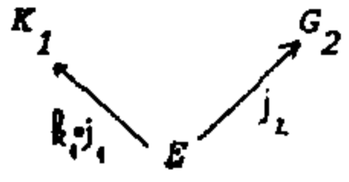


Dokazati: Ako pretpostavimo hipotezu kontinuuma (CH), onda postoji homogeno-univerzalna grupa moći kontinuuma.

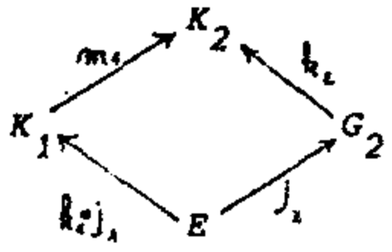
Rešenje: Uz (CH), ***prvi neprebrojivi kardinalni broj jednak je*** $\aleph_1$.
Kako postoji kontinuum (do na izomorfizam) prebrojivih grupa, to se one mogu poredjati u niz $G_0, G_1, \ldots, G_\alpha, \ldots$, $\alpha < \omega_1$.
Neka je E trivijalna grupa. Koristeći svojstvo amalgamacije za klasu grupa (videti prethodni zadatak) može se odrediti sledeći niz grupa $K_1, K_2, \ldots$, *tako da naredni dijagram komutira*



($j_0, j_1, \ldots$ *su trivijalna utapanja).*
Prvo se odredi amalgamirani proizvod K_1 , *kao i utapanja* k_0, k_1. *Zatim se amalgamira dijagram*



do dijagrama



, *itd.*

Za granične ordinale α *uzima se grupa* $K_\alpha = \bigcup_{\beta<\alpha} K_\beta$.

(Može se uzeti da su preslikavanja m_α *inkluzije, s obzirom da su utapanja. Strože,* $K_\alpha = \varinjlim(K_\beta; m_\beta, \beta<\alpha)$.*)*

Najzad, $K = \bigcup_{\alpha<\omega_1} K_\alpha$ *je grupa sa traženim svojstvima.*

Zaista, svojstvo univerzalnosti na primer, grupe K, sledi iz činjenice da svaka grupa G moći ω_1 *može da se predstavi u obliku* $G = \bigcup_{\alpha<\omega_1} H_\beta$ *, gde je svaka grupa* H_β *prebrojiva.*

12. PREDSTAVLJANJE GRUPA

12.1. GENERATORI I STRUKTURNE JEDNAKOSTI

I u ovom poglavlju, u velikoj meri koristimo osnovne pojmove, definicije i rezultate poglavlja 10.

Neka su jezik L i klasa algebarskih zakona Z (nad L) kao u prethodnom poglavlju. Neka je, dalje, A skup simbola konstanti i R neki skup formula oblika u=v, gde su u,v zatvoreni termi jezika $L \cup A$. Podsetimo se da je uredjeni par $\Pi = \langle A;R \rangle$ *predstavljanje*, *prezentacija* ili *postavka* slobodne algebre A_Π jezika $L \cup A$ klase zakona $Z \cup R$, sa skupom slobodnih generatora $X = \emptyset$ i da prema teoremi 5.3. iz 10.5. važi sledeća

1.1. Teorema: Za svaki skup konstanti A i skup zakona R postoji jedinstvena (do na izomorfizam) algebra A_Π odredjena predstavljanjem $\Pi = \langle A; R \rangle$.

Pri tome, algebra A_Π zadovoljava zakone Z, tj. A_Π je grupa; za nju se najčešće koristi oznaka G_Π.

Ako su A i R konačni ili prebrojivi skupovi

$$A = \{a_1,\ldots,a_n,\ldots\} , \quad R = \{u_1=v_1,\ldots,u_k=v_k,\ldots\} ,$$

postavku Π pišemo i u obliku

$$\Pi = \langle a_1,\ldots,a_n,\ldots; u_1=v_1,\ldots,u_k=v_k,\ldots \rangle .$$

Kako je grupa G_Π generisana skupom A (tj. interpretacijama slova iz A, videti napomenu 6.3.1 iz 10.6.), elemente iz A nazivamo njenim *generatornim elementima*. Elemente skupa R nazivamo *strukturnim jednakostima*.

Jednakost u=v pišemo često u obliku $uv^{-1}=1$; stoga u postavci Π pišemo, kraće

$$\Pi = \langle a_1,\ldots,a_n,\ldots; u_1v_1^{-1},\ldots,u_kv_k^{-1},\ldots \rangle$$

Izrazi $u_iv_i^{-1}$ nazivaju se još i : *strukturne reči* ili *odrednici (relatori)* .

U cilju skraćivanja zapisa, često ćemo, umesto "G_Π je grupa odredjena postavkom $\Pi = \langle A; R \rangle$", pisati samo $G = \langle A; R \rangle$.

Prema prethodnom, za svako predstavljanje Π postoji grupa G_Π. Koristeći Napomenu 10.6.3.3°, grupa G_Π odredjena sa $\Pi = \langle A;R \rangle$ je $G_\Pi = F/N$ gde je F slobodna grupa sa skupom slobodnih generatora A, a N najmanja normalna podgrupa u F koja sadrži sve izraze r za koje je $(r=1) \in R$ (podrazumevamo da su svi za

b) Ispitivanjem da li za svaki par različitih elemenata m_1 i m_2 iz M postoji **homomorfizam** *$\phi : M \to G$ (gde je G grupa), tako da je $\phi(m_1) \neq \phi(m_2)$. Ako takva preslikavanja postoje, elementi iz M su neekvivalentni.*

A. se nekim od gornja dva načina dokaže da ne važi (1), iz skupa M treba izbaciti "višak" ekvivalentnih markera (tako da i dalje važe uslovi iz 3^0), i ponoviti korak 4^0. Postupak se nastavlja (sve dok skup M ne bude sa svojstvom (1)).

U opštem slučaju, ovaj postupak se ne mora završiti; odnosno, grupa G_Π može biti sa nerešivim problemom reči (videti odeljak 12.3.).

5^0 Ispituje se da li je $(M, \cdot, ^{-1})$ grupa. Ako jeste, to je tražena grupa $(\simeq) G_\Pi$.

Napomena: Ako se dokaže egzistencija preslikavanja ϕ u koraku 4 b) koje je uz to 1-1 i na, tj. izomorfizam, postupak je završen. Odnosno, $G_\Pi \simeq G$.

1.2. Ispitati da li su sledeći skupovi izraza, skupovi neekvivalentnih markera za prezentaciju $\Pi = \langle a,b;\ a^2=1, b^3=1, ba=ab^2 \rangle$

a) $\{1,a,b\}$, b) $\{1,a,b,b^2,ab,ab^2,a^2b\}$, c) $\{1,a,b,b^2,ab,ab^2\}$,
d) $\{1,a,b,b^5,ab^2\}$, e) $\{1,a,b,b^3,ab,ab^5\}$.

Rešenje: a) Skup $M_1=\{1,a,b\}$ nije skup markera u smislu definicije 10.6.1. Pokazuje se, naime, da postoji izraz nad $\{a,b\} \cup L$ koji nije ekvivalentan nijednom od izraza 1,a,b. Jedan takav izraz je ab.

Zaista, uočimo preslikavanje $f : \{a,b\} \to S_3$ definisano sa

$$f(a)=(1\ 2),\qquad f(b)=(1\ 2\ 3).$$

Označimo $(1\ 2)=p$, $(1\ 2\ 3)=q$. Kako je $p^2=I$, $q^3=I$, $qp=pq^2$, f se proširuje do homomorfizma $\phi : M \to S_3$ (v.zad. 1.10.). Zbog $pq \neq I$, $pq \neq p$ i $pq \neq q$, izraz ab nije ekvivalentan nijednom od izraza 1,a,b.

Rešenje sledi i prema zadatku 1.15., jer $G_\Pi \simeq S_3$ a $|M_1| < |G_\Pi|$.

b) Skup $M_2=\{1,a,b,b^2,ab,ab^2,a^2b\}$ jeste skup markera za postavku Π. Medjutim, odgovarajuća skoro-tablica nije slegnuta. Jer, izrazi b i a^2b su različiti (kao reči), ali su ekvivalentni (zbog $a^2=1$).

	1	a	b	b^2	ab	ab^2	a^2b
1	1	a	b	b^2	ab	ab^2	a^2b
a	a	1	ab	ab^2	b	b^2	ab
b^2	b	ab^2	b^2	1	a	ab	b^2
b^2	⋮	⋮					
⋮							

c) Skup $\{1,a,b,b^2,ab,ab^2\}$ je dobar skup markera. Skoro-tablica (data na narednoj strani) je slegnuta. Rešavajuća struktura je S_3.

	1	a	b	b^2	ab	ab^2
1	1	a	b	b^2	ab	ab^2
a	a	1	ab	ab^2	b	b^2
b	b	ab^2	b^2	1	a	ab
b^2	b^2	ab	1	b	ab^2	a
ab	ab	b^2	ab^2	a	1	b
ab^2	ab^2	b	a	ab	b^2	1

d),e) Navedeni skupovi nisu "dobri" skupovi markera.

1.3.Za data predstavljanja Π, ispitati medjusobnu ekvivalentnost sledećih izraza u Π :

a) $\Pi = \langle x,y;\ x^2=y^2 \rangle$, $\{(xy)^3, x^3y^3, x^{-1}yx^6\}$,

b) $\Pi = \langle x,y;\ x^4, y^3, (xy)^2 \rangle$, $\{y, xyx^{-1}, y^{-1}x^2, x^{-1}y^{-1}x^{-1}\}$.

Rešenje: a) Medju posledicama skupa formula $Z_{\{x,y\}} \cup \{x^2=y^2\}$ *u jednakosnoj logici J su*

$$x^{-1}yx^6 = x^{-1}y^3x^4 = x^{-1}x^2yy^2x^2 = x^3yx^2 = x^3y^3 \ , \text{ tj. } x^{-1}yx^6 \sim x^3y^3 \ .$$

Medjutim, $(xy)^3 \not\sim x^3y^3$. *Dovoljno je uočiti preslikavanje* $\phi : \{x,y\} \to S_3$ *odredjeno sa* $\phi(x)=(1\ 2)$, $\phi(y)=(1\ 3)$, *koje se, zbog* $(1\ 2)^2=(1\ 3)^2$ *proširuje do homomorfizma. Slike izraza* $(xy)^3$ *i* x^3y^3 *su redom: I, (1 2 3). Kako je* $I \neq (1\ 2\ 3)$, *to je:* $(xy)^3 \not\sim x^3y^3$, $(xy)^3 \not\sim x^{-1}yx^6$.

b) Polazeći od $Z_{\{x,y\}} \cup \{x^4=1, y^3=1, (xy)^2=1\}$, *u logici J je*

$$(xy)^2=1 \ , \quad xy=y^{-1}x^{-1} \ , \quad xyx^{-1}=y^{-1}x^2 \ , \text{ tj. } xyx^{-1} \sim y^{-1}x^2 \ .$$

Slično, $(xy)^2=1$, $y^{-1}x^{-1}=xy$, $x^{-1}y^{-1}x^{-1}=y$, *tj.* $x^{-1}y^{-1}x^{-1} \sim y$.

Ostali izrazi su medjusobno neekvivalentni. Zaista, uočimo preslikavanje $\phi : \{x,y\} \to S_4$: $\phi(x)=(1\ 2\ 3\ 4)$, $\phi(y)=(1\ 3\ 2)$. *Dalje kao pod a)* .

1.4.Odrediti bar jedan skup markera za sledeću postavku Π:

a) $\Pi = \langle x,y;\ x^2, y^2, (xy)^4 \rangle$, b) $\Pi = \langle x,y;\ x^2=y^2, xy=y^{-1}x \rangle$,

c) $\Pi = \langle x,y,z;\ x^{-1}yx=z, x^{-1}zx=y, y^{-1}xy=z, y^{-1}zy=x, z^{-1}xz=y, z^{-1}yz=x \rangle$

Ispitati da li odgovarajuće rešavajuće strukture zadovoljavaju zakone Z.

Rešenje: a) $M=\{1,x,y,xy,yx,xyx,yxy,xyxy\}$. *Svaki izraz iz* Π, *zbog* $x^2=y^2=1$ *ekvivalentan je izrazu oblika* $a^\alpha bab...ab^\beta$ $(\alpha,\beta=0,1)$. *Zbog* $(xy)^4=1$ *je* $xyxy=yxyx$, $xyxyx=yxy$, $yxyxy=xyx$ *itd. Dakle, svaki izraz iz* Π *ekvivalentan je jednom od izraza iz M. Preslikavanjem* $\phi : \{x,y\} \to S_4$ *odredjenom sa*

$$\phi(x)=(1\ 2)(3\ 4)=f \ , \quad \phi(y)=(1\ 3)=g$$

je, zbog $f^2=I$, $g^2=I$, $(fg)^4=I$, *odredjen homomorfizam* $\Psi : G_\Pi \to S_4$. *Lako se pokazuje da je* Ψ *1-1 preslikavanje* G_Π *na podgrupu H grupe* S_4 *koja je gene-*

risana sa (1 2)(3 4) i (1 3).

Da markeri iz M obrazuju grupu može se dokazati i neposrednom proverom.

b) $M=\{x^{\varepsilon}y^{k} \mid \varepsilon\in\{0,1\},\ k\in Z\}$. *Indukcijom po dužini izraza, dokazuje se da je svaki izraz iz* Π *ekvivalentan nekom izrazu iz M.*

Ako je dužina izraza 0, tada je $1=x^{0}y^{0}$.

Za dužinu 1: $x=x^{1}y^{0}$, $y=x^{0}y^{1}$, $x^{-1}=xy^{-2}$, $y^{-1}=x^{0}y^{-1}$.

Ako proizvoljni izraz $x^{\varepsilon}y^{k}$ *pomnožimo sa nekim od* x,y,x^{-1},y^{-1} *dobijamo ponovo izraz iz M . Zaista*

$$x^{\varepsilon}y^{k}y=x^{\varepsilon}y^{k+1}\ ,\quad x^{\varepsilon}y^{k}y^{-1}=x^{\varepsilon}y^{k-1}\ ;$$

ako je $k=2m$: $x^{\varepsilon}y^{k}x=x^{\varepsilon}xx^{2m}=x^{\varepsilon+1}y^{2m}=\begin{cases}y^{2(m+1)} & za\ \varepsilon=1\\ xy^{2m} & za\ \varepsilon=0\end{cases}$

ako je $k=2m+1$: $x^{\varepsilon}y^{k}x=x^{\varepsilon}x^{2m}yx=x^{\varepsilon}x^{2m}xy^{-1}=x^{\varepsilon}xx^{2m}y^{-1}$

$$=x^{\varepsilon+1}y^{2m-1}=\begin{cases}y^{2m+1} & za\ \varepsilon=1\\ xy^{2m-1} & za\ \varepsilon=0\end{cases}$$

Slično za $x^{\varepsilon}y^{k}x^{-1}$.

c) $M=\{x^{2k},x^{2k}x,x^{2k}y,x^{2k}z,x^{2k}xy,x^{2k}yx \mid k\in Z\}$.

Indukcijom po dužini izraza iz Π, *kao pod b).*

1.5. Neka je M konačan skup markera postavke Π. Dokazati da se efektivno, u konačno mnogo koraka, može odrediti grupa G_{Π}.

Rešenje: Videti zadatak 1.1.

1.6. Dokazati da je sledećim postavkama odredjena jedinična grupa:

a) $\Pi=<a,b;\ a^{-1}ba=b^{2},b^{-1}ab=a^{2}>$, b) $\Pi=<a,b,c;b^{2}=1,c^{3}=1,aba^{-1}=bcb^{-1},ab=c>$

Rešenje: a) Iz $a^{-1}ba=b^{2}$ *je* $b=b^{-1}a^{-1}ba$, *a iz* $b^{-1}ab=a^{2}$ *je* $a=a^{-1}b^{-1}ab$; *odavde* $ab=a^{-1}b^{-1}abb^{-1}a^{-1}ba=1$, *tj.* $b=a^{-1}$. *Stoga je* $a=bb^{-1}ab$ *tj.* $b=1$; *takodje,* $a=a^{-1}a=1$.

b) Iz $aba^{-1}=bcb^{-1}$ *sledi* $ab^{2}a^{-1}=bc^{2}b^{-1}$, *tj. (zbog* $b^{2}=1$*),* $c^{2}=1$, *odakle je (zbog* $c^{3}=1$*)* $c=1$. *Sada je iz* $aba^{-1}=b1b^{-1}$ *i* $b=1$, *a zbog* $ab=c$ *je* $a=1$.

1.7. Neka je $\Pi=<a_1,\ldots,a_n;\ a_i^2=1,\ (a_ia_j)^2=1 \mid i,j\in\{1,\ldots,n\}>$. Dokazati da je G_{Π} konačna grupa.

Rešenje: Zbog $(a_ia_j)^2=1$ *tj.* $a_ia_j=a_ja_i$, *svaki izraz iz* Π *ekvivalentan je izrazu oblika* $a_1^{\alpha_1}a_2^{\alpha_2}\ldots a_n^{\alpha_n}$, *gde je zbog* $a_i^2=1$ $(i=1,\ldots,n)$, $\alpha_i\in\{0,1\}$. *Dakle,* G_{Π} *je konačna grupa;* $|G_{\Pi}|=2^{n}$.

1.8. Odrediti grupu G_{Π} ako je :

a) $\Pi=<a,b;\ a^3=1,b^2=1,ab=ba>$, b) $\Pi=<a,b;\ a^2=1,b^2=1,aba=bab>$,

c) $\Pi = \langle a,b,c;\ a^3=1, b^3=1, c^4=1, ac=ca^{-1}, aba^{-1}=bcb^{-1} \rangle$

d) $\Pi = \langle a,b,c;\ a^3=1, b^2=1, c^2=1, ab=ba^2, ac=ca, bc=cb \rangle$.

Rešenje: a) Prema shemi navedenoj u zadatku 1.1. konstrukciju G_Π *obavljamo na sledeći način:*

1° *T je skup svih izraza nad* $\{a,b,1,\cdot,^{-1}\}$

2° $u \sim v \overset{def}{\Longleftrightarrow} Z_{\{a,b\}} \cup \{a^3=1, b^2=1, ab=ba\} \vdash_J u=v$

3° *Proizvoljni izraz* $t \in T$ *ekvivalentan je izrazu oblika* $a^\alpha b^\beta$, *gde je* $\alpha \in \{0,1,2\}$, $\beta \in \{0,1\}$. *Za skup markera, dakle, biramo* $M = \{1,a,a^2,b,ab,a^2b\}$ *(ispunjena su oba uslova iz* 3° *zadatka 1.1.).*

4° *Jedna skoro-tablica* $\mathcal{P}$ *za M je*

	1	a	a^2	b	$\overline{ab}$	a^2b
1	1	a	a^2	b	ab	a^2b
a	a	a^2	1	ab	a^2b	b
a^2	a^2	1	a	a^2b	b	ab
b	b	ab	a^2b	1	a	a^2
ab	ab	a^2b	b	a	a^2	1
$\overline{a^2b}$	a^2b	b	ab	a^2	$\overline{1}$	a

Na primer, važi: $(a^2b)(ab) \sim a^3b^2 \sim 1$, *itd.*

Preslikavanje $f : M \to \mathbb{Z}_6$ *definisano sa* $f = \begin{pmatrix} 1 & a & a^2 & b & ab & a^2b \\ 0 & 2 & 4 & 3 & 5 & 1 \end{pmatrix}$ *je izomorfizam grupa* G_Π *i* Z_6 .

b) Skup markera je $\{1,a,b,ab,ba,aba\}$. *Grupa odredjena sa* Π *je nekomutativna grupa reda 6.*

c) Iz $aba^{-1}=bcb^{-1}$ *sledi* $c=b^{-1}aba^{-1}b$. *Stoga je*

$$c^3=b^{-1}aba^{-1}bb^{-1}aba^{-1}bb^{-1}aba^{-1}b=b^{-1}abbba^{-1}b=b^{-1}aa^{-1}b=1 .$$

Iz $c^4=1$ *i* $c^3=1$ *sledi* $c=1$. *Iz* $aba^{-1}=bcb^{-1}$, *tj.* $aba^{-1}=1$ *sledi* $b=1$.

Takodje, iz $ac=ca^{-1}$ *i* $c=1$ *sledi* $a=a^{-1}$, *odakle* $a^2=1$; *zbog* $a^3=1$ *je i* $a=1$.

Dakle, prezentacijom Π *je odredjena jedinična grupa.*

d) Grupa reda 12 čiji su elementi: $1,a,a^2,b,ba,ba^2,c,ac,bc,a^2c,abc,bac$.

1.9.a) Dokazati da je grupa G_Π, odredjena postavkom $\Pi = \langle A;R \rangle$, izomorfna grupi F/N gde je F slobodna grupa ranga |A| a N je najmanja normalna podgrupa u F koja sadrži elemente odredjene sa $\{uv^{-1} \mid (u=v) \in R\}$,

b) Opisati podgrupu N kongruencijski i odrediti joj generatorne elemente.

Rešenje: a) Direktno prema Napomeni 10.6.4.3 .

b) Neka je $Q = \{uv^{-1} \mid (u=v) \in R\}$; *tada,* $N = [Q]$. *Označimo sa H podgrupu u F generisanu sa* $\{w^{-1}qw \mid w \in F,\ q \in Q\}$. *Očigledno, H je najmanja normalna podgrupa u F koja sadrži Q , pa je* $N = H = \langle w^{-1}qw \mid w \in F,\ q \in Q \rangle$.

Napomena: Umesto "N je najmanja normalna podgrupa koja sadrži R" ili "N je

normalno zatvorenje skupa R", kaže se i kraće: "N je normalna podgrupa generisana sa R".

Podgrupi N odgovara kongruencija $\sim$ *odredjena sa*

$$\sim \overset{def}{=} \bigcap \{\rho \mid \rho \text{ je kongruencija i } \{(u,v) \mid (u=v) \in R\} \in \rho\}$$

ili

$$u \sim v \overset{def}{\Longleftrightarrow} Z_A \cup R \underset{J}{\vdash} u=v \ .$$

1.10.a) Neka su grupe G_1 i G_2 odredjene redom postavkama

$$\Pi_1 = < a_1,\ldots; R_1,\ldots > , \quad \Pi_2 = < b_1,\ldots; S_1,\ldots > .$$

Dokazati da se preslikavanje $a_i \mapsto U_i(b_1,\ldots)$ $(i=1,2,\ldots)$ proširuje do homomorfizma $\phi : G_1 \to G_2$ akko je $\phi(R_i)=1$ $(i=1,2,\ldots)$.

b) Ako je grupa G odredjena postavkom Π_1, dokazati da je grupa H, sa postavkom $\Pi' = < a_1,\ldots; R_1,\ldots,Q_1,\ldots >$ homomorfna slika grupe G.

Rešenje: a) $(\Leftarrow)$ *Direktno prema Napomeni 6.4. iz odeljka 10.6.*

$(\Rightarrow)$ *Ako se preslikavanje* $f : \{a_1,\ldots,a_n,\ldots\} \to G_{\Pi_2}$ *proširuje do homomorfizma* $\phi : G_{\Pi_1} \to G_{\Pi_2}$, *tada je* $\phi(R_i)=1$ *zbog* $R_i=1$ *(za sve* $i=1,2,\ldots$*).*

b) Prema a).

Napomena: Koristeći b) i zadatak 1.36. sledi još jednom zadatak 11.1.6. (poglavlja o slobodnim grupama): Svaka grupa je homomorfna slika neke slobodne grupe.

1.11. Ako je G odredjena postavkom $\Pi = < a_1,\ldots; R_1,\ldots >$ i ako je N normalno zatvorenje podgrupe u G generisane sa $\{Q_1,\ldots\}$, dokazati da je postavkom $<a_1,\ldots; R_1,\ldots,Q_1,\ldots>$ odredjena grupa G/N.

Rešenje: Grupa G je odredjena postavkom $< a_1,\ldots; R_1,\ldots >$; *dakle, postoji homomorfizam* $\phi_1 : F \xrightarrow{na} G$ *(v.zad.1.9.) gde je F slobodna grupa generisana sa* $\{a_1,\ldots\}$ *i pri tom je* $\ker \phi_1 = \left[R_1,\ldots\right]^F$.

Neka je H grupa odredjena postavkom $< a_1,\ldots; R_1,\ldots,Q_1,\ldots >$. *Tada takodje postoji homomorfizam* $\phi_2 : F \xrightarrow{na} H$, *gde je* $\ker \phi_2 = \left[R_1,\ldots,Q_1,\ldots\right]^F$.

Kako u H važe strukturne jednakosti iz G, prema zad. 1.10., postoji homomorfizam $\phi : G \xrightarrow{na} H$ *i pri tom je* $\phi \circ \phi_1 = \phi_2$.

Dalje je

$$\phi_1(\ker \phi_2) = \{\phi_1(y) \mid y \in F,\ y \in \ker \phi_2\} = \{\phi_1(y) \mid y \in F,\ \phi_2(y)=1_H\}$$

$$= \{g \mid g \in G,\ g=\phi_1(y),\ \phi(\phi_1(y))=1_H\} = \{g \mid g \in G, \phi(g)=1_H\}$$

$$= \ker \phi .$$

S druge strane je

$$\phi_1(\ker \phi_2) = \phi_1 \left[R_1,\ldots,Q_1,\ldots\right]^F \underset{①}{=} \left[\phi_1(\{R_1,\ldots,Q_1,\ldots\})\right]^G$$

$$\underset{②}{=} \left[\{1\} \cup \phi_1(\{Q_1,\ldots\})\right]^G = \left[\phi_1(\{Q_1,\ldots\})\right]^G$$

① *prema zadatku 3.2.3 .)*

② *jer je* $R_1,\ldots \in \ker \phi_1$

Dakle, $\ker \phi = \left[\phi_1(\{Q_1,\ldots\}) \right]^G$.

Klase $\phi_1(Q_1),\phi_1(Q_2),\ldots$ *su jedinstveno odredjene u* G *sa* $Q_1,Q_2,\ldots$, *pa je (u skladu sa dogovorom iz uvodnog dela)* $\ker \phi = \left[Q_1,\ldots \right]^G = N$.

Stoga je $G/N \simeq H$.

1.12. Dokazati da je : a) $< a,b;\ a^7=1, b^3=1, ba=a^3b > \simeq C_3$

b) $< a,b;\ a^2,b^3,a^{-1}b^{-1}ab > \simeq C_6$, c) $< a,b;\ a^2b^2,a^3b^3,\ldots > \simeq C_\infty$

Rešenje: a) Kako je $\sigma_{b^{-1}}(a) = a^3$, *to je* $\sigma^3_{b^{-1}}(x) = \sigma_{b^{-3}}(x) = \sigma_1(x) = I(x)$, *odakle* $a = I(a) = \sigma^3_{b^{-1}}(a) = a^{27}$. *Dakle,* $a^{26}=1$, *odnosno* $a^5=1$, *odakle* $a^2=1$. *Najzad,* $1 = a^7 = a\cdot(a^2)^3 = a$, *pa je*

$$< a,b;\ a^7=1, b^3=1, ba=a^3b > \simeq < b;\ b^3=1 > \simeq C_3 .$$

b) Prema zadatku 1.44. je

$$< a,b;\ a^2=1, b^3=1, a^{-1}b^{-1}ab=1 > \simeq < a;\ a^2=1 > \times < b;\ b^3=1 > \simeq C_2 \times C_3 \simeq C_6.$$

c) Iz $a^2b^2=1$ *i* $a^3b^3=1$ *sledi* $a^{-3}=b^3=b^2\cdot b=a^{-2}b$, *tj.* $b=a^{-1}$.

Kako iz $b=a^{-1}$ *slede jednakosti* $b^k=a^{-k}$ $(k\in N)$ *to je*

$$< a,b;\ a^2b^2,\ a^3b^3,\ldots > \simeq < a,b;\ b=a^{-1} > \simeq < a > ,$$

(primenom Tietze-ovih transformacija; videti odeljak 12.2.) .

1.13. Odrediti grupu G_Π ako je $\Pi = < a,b;\ a^3=1, b^4=1, (ab)^2=1 >$.

Rešenje: Neka je u grupi G_Π, H *podgrupa generisana sa* b , *tj.* $H = \{1,b,b^2,b^3\}$. *Ispitajmo koliko ima najviše napr. desnih razreda po* H *(i time odredimo gornju granicu za* $|G_\Pi|$*). S obzirom na strukturne jednakosti iz* Π, *podjimo od sledećih razreda*

$$H\ ,\ Ha\ ,\ Ha^2\ ,\ Ha^2b\ ,\ Ha^2b^2\ ,\ Ha^2b^2a \qquad (*)$$

(Nije naveden Hab , *jer je* $ab=b^{-1}a^{-1}=b^3a^2$ *pa je* $Hab = Ha^2$.)

Lako se proverava da su u (*) navedeni svi mogući razredi, tj. ima ih najviše 6. Provera se obavlja množeći razrede iz (*) generatornim elementima a *i* b . *Napr.* $(Ha^2b)a = Ha^2a^2b^3 = Ha^2b^2$, *itd.*

Zbog $|H|=4$, $|G_\Pi : H| \leqslant 6$, *zaključujemo* $|G_\Pi| \leqslant 24$.

Uočimo preslikavanje $\phi : \{a,b\} \to S_4$ *odredjeno sa*

$$\phi(a) = f = (1\ 2\ 3\ 4)\ ,\quad \phi(b) = g = (1\ 3\ 2)\ .$$

Kako je $S_4 = \left[f,g \right]$, *i* $f^4=I$, $g^3=I$, $(fg)^2=I$, *to se* ϕ *produžava do homomorfizma* $\Psi : G_\Pi \to S_4$. *Otuda ,* $|G_\Pi| \geqslant 24$. *Prema gornjem je, dakle,* $|G_\Pi|=24$, *tj.* $G_\Pi \simeq S_4$.

1.14.Dokazati da su grupe odredjene predstavljanjima
$\Pi_1 = \langle a,b;\ a^3=1, b^7=1, ba=ab^2 \rangle$ i $\Pi_2 = \langle c,d;\ c^3=1, d^7=1, dc=cd^4 \rangle$ izomorfne.

Rešenje: Kako je $dc^{-1}=c^{-1}d^2$ *i* $ba^{-1}=a^{-1}b^2$ *, to se preslikavanja*

$\phi = \begin{pmatrix} a & b \\ c^{-1} & d \end{pmatrix}$ *i* $\psi = \begin{pmatrix} c & d \\ a^{-1} & b \end{pmatrix}$ *produžavaju do homomorfizama*

$\Phi : G_{\Pi_1} \to G_{\Pi_2}$ *i* $\Psi : G_{\Pi_2} \to G_{\Pi_1}$ *(zadatak 1.10.a)).*

Preslikavanja Φ *i* Ψ *su uzajamno inverzna, pa je* $G_{\Pi_1} \simeq G_{\Pi_2}$.

1.15.Odrediti bar dva predstavljanja za svaku od sledećih grupa:
a) Klein-ove grupe V , b) S_3 , c) Grupe kvaterniona K , d) A_4 .

Rešenje: a) Jedno, tzv. trivijalno predstavljanje, je tablično. Na osnovu tablice grupe V (gde je $a(x)=x$, $b(x)=-x$, $c(x)=\frac{1}{x}$, $d(x)=-\frac{1}{x}$ *) je*

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\Pi_1 = \langle a,b,c,d;\ aa=a, ab=b, ac=c,$
$ad=d, ba=b, bb=a, bc=d, bd=c, ca=c, cb=d, cc=a, cd=b, da=d, db=c, dc=b, dd=a \rangle$.

2° Za odredjivanje druge postavke koristimo se činjenicom da se funkcije a i d mogu dobiti proizvodom funkcija b i c. Dakle, generatorni elementi su b i c, i za njih važi : $b^2=1,\ c^2=1,\ bc=cb$ *(1)*

Lako se pokazuje da nema drugih strukturnih jednakosti nad b i c, a koje nisu posledice jednakosti (1). Zaista, neka je

$$b^{\beta_1}c^{\gamma_1}\dots b^{\beta_k}c^{\gamma_k}=1 \quad (\beta_i,\gamma_i \in Z) \qquad (2)$$

Zbog (1) je izraz sa leve strane jednakosti (2) ekvivalentan izrazu $b^\alpha c^\beta$, $\alpha,\beta \in \{0,1\}$, *odakle* $b^\alpha c^\beta = 1$. *Kako je* $b\neq 1$, $c\neq 1$ *i* $bc\neq 1$, *to je* $\alpha=\beta=0$; *odnosno, jednakost (2) postaje 1=1.*

Dakle, drugo predstavljanje za V je

$$\Pi_2 = \langle b,c;\ b^2=1, c^2=1, bc=cb \rangle .$$

b) $_1^\circ$ *Prema zad. 4.1.20.c) grupa* S_n *je generisana elementima (1 2 ... n),(1 2). Dakle,* S_3 *je generisana sa (1 2 3) i (1 2). Za ove elemente je ispunjeno*

$$(1\ 2\ 3)^3=I\ ,\ (1\ 2)^2=I\ ,\ (1\ 2\ 3)(1\ 2)=(1\ 2)(1\ 2\ 3)^2 .$$

Stoga uočavamo postavku

$$\Pi_1 = \langle a,b;\ a^3=1, b^2=1, ab=ba^2 \rangle .$$

Lako se pokazuje da je $G_{\Pi_1} \simeq S_3$. *Zaista, markeri za* Π_1 *su* $M_1=\{1,a,a^2,b,ab,a^2b\}$. *Preslikavanje* $\phi : G_{\Pi_1} \to S_3$ *odredjeno sa* $\phi(a^\alpha b^\beta)=(1\ 2\ 3)^\alpha(1\ 2)^\beta$, $\alpha \in \{0,1,2\}$, $\beta \in \{0,1\}$, *je traženi izomorfizam.*

2° Slično, $\Pi_2 = \langle a,b;\ a^2=1, b^2=1, (ab)^3=1 \rangle$ *je takodje postavka za* S_3 . *Do nje se dolazi iz činjenice da je* S_3 *generisana elementima (1 2) i (1 3) (videti*

zadatak 4.1.20.a)), za koje je ispunjeno: $(1\ 2)^2=I$, $(1\ 3)^2=I$, $((1\ 2)(1\ 3))^2=I$ Markeri postavke Π_2 su, prema zad. 1.8.b) (jer iz $a^2=1, b^2=1, (ab)^3=1$ sledi $aba=bab$), $M_2=\{1,a,b,ab,ba,aba\}$.

c) 1° Tablica grupe kvaterniona K je data u zadatku 2.12.f). Na osnovu nje je lako konstruisati tabličnu postavku Π_1 .

2° S obzirom na veze izmedju i,j,k date u tablici, imamo: $i^4=1$, $i^2=j^2$, $iji=j$. Uočava se stoga postavka

$$\Pi_2 = < a,b;\ a^4=1, b^2=a^2, aba=b >\ .$$

Njeni markeri su $M_2=\{1,a,a^2,a^3,b,ab,a^2b,a^3b\}$. Preslikavanje $f(a)=i$, $f(b)=j$ proširuje se do izomorfizma $G_{\Pi_2} \to K$.

3° Kako je $ij=j^{-1}i$, $ji=i^{-1}j$, to je i

$$\Pi_3 = < a,b;\ ab=b^{-1}a, ba=a^{-1}b >$$

postavka grupe K . Pokazuje se da su strukturne jednakosti iz Π_2 posledice jednakosti iz Π_3 , i obratno.

(Zaista, iz $ba=a^{-1}b$ sledi $aba=b$; iz $ba=a^{-1}b$ i $ab=b^{-1}a$ sledi $a^2=abb^{-1}a=abab=aa^{-1}bb=b^2$; takodje, $a^4=abba=b^{-1}aa^{-1}b=1$.

Obratno, iz $aba=b$ sledi $ba=a^{-1}b$; iz $aba=b$ i $a^2=b^2$ sledi $abab=a^2$, tj. $ab=b^{-1}a$.)

Stoga je $G_{\Pi_2} \simeq G_{\Pi_3}$.

d) 1° Pored tablične postavke, za grupu A_4 postoje i naredne. Naime, A_4 je generisana permutacijama $(2\ 3\ 4)$ i $(1\ 2)(3\ 4)$ za koje je ispunjeno:

$$(2\ 3\ 4)^3=I\ ,\ ((12)(3\ 4))^2=I\ ,\ ((2\ 3\ 4)(1\ 2)(3\ 4))^3=I\ .$$

Neka je, stoga, $\Pi_1 = < a,b;\ a^3=1, b^2=1, (ab)^3=1 >$.

Svaki izraz iz Π_1 ekvivalentan je jednom od izraza $a^{\alpha_1}b^{\beta_1}a^{\alpha_2}b^{\beta_2}$, $\alpha_i \in \{0,1,2\}$, $\beta_i \in \{0,1\}$ $(i=1,2)$, gde α_1 i β_2 nisu istovremeno različiti od nule, tj. $M_1=\{1,a,a^2,ab,a^2b,aba,a^2ba,aba^2,a^2ba^2,b,ba,ba^2\}$. Preslikavanje $f(a)=(2\ 3\ 4)$, $f(b)=(1\ 2)(3\ 4)$ se proširuje do izomorfizma $G_{\Pi_1} \to A_4$.

2° A_4 ima i postavku

$$\Pi_2 = < a,b,c;\ a^3=1, b^2=1, c^3=1, acb=1 >$$

(iz jednakosti postavke Π_1 slede jednakosti za Π_2 i obratno).

1.16. Za sledeće grupe G i njihove normalne podgrupe N, odrediti homomorfne slike G/N : a) $G = < a,b;\ a^2=1, b^5=1, ba=ab^4 >$, $N = [b^4ab^{-2}a^{-1}]$,

b) $G = F_2$, N je normalno zatvorenje skupa izraza parne dužine ,

c) $G = S_4$, $N = \{I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Rešenje: a) $G/N = < a,b;\ a^2=1, b^5=1, ba=ab^4, b^4ab^{-2}a^{-1}=1 >$. Kako je $ba=ab^4$, tj. $b^4a=ab$, to je $abb^{-2}a^{-1}=1$ odakle $b=1$. Dakle, $G/N = < a\ ;\ a^2=1 >$, tj. $G/N \simeq C_2$.

b) Ako su $u,v \in G$ elementi parne dužine, i w proizvoljni element iz G, tada su $uv, u^{-1}, w^{-1}uw$ takodje parne dužine. Dakle, N je skup svih elemenata parne

dužine iz G. Dva elementa neparne dužine su u istom razredu po H, pa je $|G:N|=2$. *Dakle,* $G/N=C_2$.

c) $S_4/N \simeq S_3$.

1.17.Ako je $<A;R>$ predstavljanje grupe G , tada je $<A;R\cup\{[a,b] \mid a,b\in A\}>$ ($[a,b]$ su komutatori), predstavljanje grupe G/G'. Dokazati.

Rešenje: *Normalno zatvorenje N skupa* $S=\{[a,b] \mid a,b\in A\}$ *pripada komutantu G': Grupa* $\langle A;R\cup\{ab=ba \mid a,b\in A\}\rangle$ *je Abelova pa N sadrži komutant. Dakle,* $N=G'$ *i prema z. 1.11* G/G' *ima postavku* $\langle A;\ R\cup S\rangle$.

1.18.Odrediti grupu G/G' ako je : a) $G=F_2$, b) $G=<a,b;\ a^6,b^2,(ab)^2>$, c) $G=<a,b;\ a^4,a^2=b^2,ba=a^3b>$, d) $G=<a,b;\ a^6,b^2=(ab)^2=a^3>$.

Rešenje: a) Prema prethodnom zadatku je $F_2/F_2'\simeq<a,b;ab=ba>$ *a koristeći zadatak 1.44.a) je* $F_2/F_2'\simeq<a>\times<b>$, *tj.* $F_2/F_2'\simeq C_\infty\times C_\infty$.

b) $G/G'\simeq<a,b;\ a^6,b^2,(ab)^2,ab=ba>$. *Iz* $(ab)^2=1$ *i* $ab=ba$, $b^2=1$ *sledi* $a^2=1$. *Dalje, iz jednakosti* $a^2=1$, $b^2=1$, $ab=ba$ *slede ostale jednakosti* $a^6=1$, $(ab)^2=1$ *pa ih je , prema zadatku 12.2. 1 .) moguće izostaviti. Drugim rečima,*

$$G/G'\simeq<a,b;\ a^2=1,b^2=1,ab=ba>\simeq C_2\times C_2 .$$

c) $G/G'\simeq<a,b;\ a^4=1,a^2=b^2,ba=a^3b,aba^{-1}b^{-1}=1>$. *Kako je* $ab=ba$ *to je* $ab=a^3b$ *tj.* $a^2=1$; *stoga je i* $b^2=1$. *Neposredno se proverava da iz jednakosti* $a^2=1$, $b^2=1$, $ab=ba$ *slede sve strukturne jednakosti grupe G . Stoga je*

$$G/G'\simeq<a,b;\ a^2=1,b^2=1,ab=ba>\simeq C_2\times C_2$$

d) $G/G'\simeq<a,b;\ a^6=1,b^2=(ab)^2=a^3,ab=ba>$. *Koristeći rezultate odeljka 12.2. izvršimo sledeće transformacije ove postavke. Iz* $(ab)^2=b^2$ *i* $ab=ba$ *sledi* $a^2=1$ *a odavde* $b^2=a$; *dalje je* $b^4=a^2=1$. *Gornjoj prezentaciji* Π *stoga možemo dodati strukturnu jednakost* $b^4=1$, *a da se grupa* G_Π *ne promeni. Dalje, zamenjujući a sa* b^2 , *izostavljamo generator a iz* Π *i sve jednakosti transformišemo koristeći* $a=b^2$ *Tako je dobijena postavka* $\Pi'=<b;\ b^{12}=1,b^2=b^6=b^6,b^3=b^3,b^4=1>$. *Izostavljajući trivijalne jednakosti i jednakost* $b^{12}=1$ *koja je posledica jednakosti* $b^4=1$, *dolazimo do postavke* $\Pi''=<b;\ b^4=1>$ *za koju je* $G_{\Pi''}=G/G'$. *Odnosno,* $G/G'\simeq C_4$.

1.19.Ako je F slobodna grupa, dokazati da je F/F' slobodna Abel-ova grupa ranga $|F|$.

Rešenje: Neka je $F=<A>_S$; *tada je* $F/F'\simeq G=<A;\{[a,b] \mid a,b\in A\}>$.
Neka je S slobodna Abel-ova grupa nad skupom generatora $A'=\{a' \mid a\in A\}$.
Preslikavanje $a\to a'$ $(a\in A)$ *produžuje se do homomorfizma* $\Phi: G\to S$, *jer su slike izraza* $[a,b]$ *jedinica u S .*
Preslikavanje $a'\to a$ $(a\in A)$ *produžuje se do homomorfizma* $\Psi: S\to G$, *jer je S slobodna Abel-ova, a G Abel-ova grupa.*

Kako su Φ i Ψ medjusobno inverzni, to je $G \cong S$.

Odrediti grupe sa sledećim strukturnim jednakostima (generatori su samo ona slova koja se pojavljuju u navedenim jednakostima):

1.20.a) $a^3=b^2=1$, $ab=ba$, b) $a^3=b^2=1$, $ab=ba^2$

Rešenje: Grupe reda 6 (v.zad. 8.2.8.)

1.21.a) $a^4=b^2=1$, $a^b=a^3$, b) $a^4=b^4=1$, $a^2=b^2$, $aa^b=a^3$

Rešenje: Sve nekomutativne grupe reda 8 (v.zad. 8.2.9.)

1.22.a) $a^5=b^2=1$, $ab=ba$, b) $a^5=b^2=1$, $a^b=a^4$

Rešenje: Grupe reda 10 (v.zad. 8.2.10.)

1.23.a) $a^2=b^2=c^2=1$, $ab=ba$, $ac=ca$, $bc=cb$, b) $a^4=b^3=1$, $ab=ba$,
c) $a^3=b^4=1$, $a^b=a^{-1}$, d) $a^3=b^2=c^2=1$, $ab=ba$, $a^c=a^{-1}$, $bc=cb$,
e) $a^2=b^2=c^3=1$, $b^c=ab$, $a^c=ab$.

Rešenje: Grupe reda 12 (v.zad. 8.2.12.)

a) $C_2^2 \times C_3$, b) $C_4 \times C_3$, c) Grupa M iz zadatka 8.2.12. ,
d) D_6 , e) A_4

1.24.a) $a^p=b^2=1$, $ab=ba$, b) $a^p=b^2=1$, $a^b=a^{-1}$ (p je prost broj)

Rešenje: Grupe reda 2p (v.zad. 8.2.13.)

a) C_{2p} , b) D_p .

1.25.Neka je p prost broj. a) $a^p=b^4=1$, $ab=ba$,
b) $a^b=b^2=c^2=1$, $ab=ba$, $ac=ca$, $bc=cb$, c) $a^p=b^4=1$, $a^b=a^{p-1}$,
d) $a^p=b^2=c^2=1$, $ab=ba$, $a^c=a^{-1}$, $bc=cb$,
e) Ako je $p=1 \pmod 4$ i $i \neq 1$, $i^2 \neq 1 \pmod p$, $i^4=1 \pmod p$, $a^p=b^4=1$, $ab=ba^i$.

Rešenje: Sve grupe reda 4p (v.zad. 8.2.14.)

1.26.Neka su p,q prosti brojevi, $p < q$.
$a^p=b^q=1$, $b^a=b^k$ gde je $k=1$ ako $p \nmid q-1$; $k^{p-1}=1 \pmod q$ i $1<k\leq q-1$, inače.

Rešenje: Sve grupe reda pq (v.zad. 8.2.15.)

1.27.a) $a^p=b^p=c^p=1$, $ab=ba$, $ac=ca$, $bc=cb$, b) $a^{p^2}=b^p=1$, $ab=ba$,
c) $a^{p^3}=1$, d) $a^p=b^p=c^p=1$, $ac=ca$, $bc=cb$, $a^b=ac$,
e) $a^{p^2}=b^p=1$, $a^b=a^{p+1}$, p je prost broj .

Rešenje: Sve grupe reda p^3 (v.zad. 8.2.16.)

1.28.a) $a^2=b^3=c^3=1$, $ab=ba$, $ac=ca$, $bc=cb$, b) $a^2=b^9=1$, $ab=ba$,
c) $a^2=b^9=1$, $b^a=b^{-1}$, d) $a^2=b^3=c^3=1$, $b^a=b$, $c^a=c^{-1}$, $bc=cb$,
e) $a^2=b^3=c^3=1$, $b^a=b^{-1}$, $c^a=c^{-1}$.

Rešenje: Sve grupe reda 18 (v.zad. 8.2.18.)

1.29.a) $a^3=b^7=1$, $ab=ba$, b) $a^3=b^7=1$, $b^a=b^2$.

Rešenje: Sve grupe reda 21 (v.zad. 8.2.20.)

1.30.a) $a^3=b^3=c^3=1$, $ac=ca$, $bc=c$,$a^b=ac$, b) $a^9=b^3=1$, $a^b=a^4$.

Rešenje: Sve nekomutativne grupe reda 27 (v.zad. 8.2.21.)

1.31.a) $a^2=b^2=c^7=1$, $ab=ba$, $ac=ca$, $bc=cb$, b) $a^4=b^7=1$, $ab=ba$,
c) $a^7=b^4=1$, $a^b=a^{-1}$, d) $a^7=b^2=c^2=1$, $ab=ba$, $bc=cb$, $a^c=a^{-1}$.

Rešenje: Sve grupe reda 28 (v.zad. 8.2.22.)

1.32.a) $a^{15}=b^2=1$, $a^b=a$, b) $a^{15}=b^2=1$, $a^b=a^4$, c) $a^{15}=b^2=1$, $a^b=a^{11}$,
d) $a^{15}=b^2=1$, $a^b=a^{-1}$.

Rešenje: Sve grupe reda 30 (v.zad. 8.2.23.)

1.33.a_1) $a^3=b^8=1$, $ab=ba$,
a_2) $a^3=b^4=c^2$, $ab=ba$, $ac=ca$, $bc=cb$,
a_3) $a^3=b^2=c^2=d^2$, $ab=ba$, $ac=ca$, $ad=da$, $bc=cb$, $bd=db$, $cd=dc$,
b_1) $a^b=a$, $a^c=a$, $a^d=a^{-1}$, $a^3=b^2=c^2=d^2=1$, $bc=cb$, $bd=db$, $cd=dc$,
b_2) $a^3=b^2=c^4=1$, $bc=cb$, $a^b=a$, $a^c=a^{-1}$,
b_3) $a^3=b^2=c^4=1$, $bc=cb$, $a^b=a^{-1}$, $a^c=a$,
b_4) $a^3=b^8=1$, $a^b=a^{-1}$,
b_5) $a^3=b^4=c^2=1$, $b^c=b^{-1}$, $a^b=a$, $a^c=a$,
b_6) $a^3=b^4=c^2=1$, $a^b=a$, $a^c=a^{-1}$, $b^c=b^{-1}$,
b_7) $a^3=b^4=c^2=1$, $b^c=b^{-1}$, $a^b=a^{-1}$, $a^c=a$,
b_8) $a^3=b^4=c^4=1$, $b^2=c^2$, $b^c=b^{-1}$, $a^b=a$, $a^c=a$,
b_9) $a^3=b^4=c^4=1$, $a^b=a$, $a^c=a^{-1}$,
c_1) $a^3=b^2=c^2=d^2=1$, $bc=cb$, $bd=db$, $cd=dc$, $b^a=c$, $c^a=bc$, $d^a=d$,
c_2) $a^3=b^4=c^4=1$, $b^2=c^2$, $b^c=b^{-1}$, $b^a=c$, $c^a=b$,
d_1) $a^3=b^4=1$, $(ab)^2=1$.

Rešenje: Sve grupe reda 24 (v.zad. 8.2.24.)

a_i) komutativne , b_i) grupe u tački A zadatka 8.2.24.
c_i) grupe u tački B zadatka 8.2.24., d_i) grupe u tački C zadatka 8.2.24.

1.34.a_1) $a^{16}=1$,

b_1) $a^2=b^2=c^2=d^2$, $ab=ba$, $ac=ca$, $ad=da$, $bc=cb$, $bd=db$, $cd=dc$,

c_1) $a^8=b^2=1$, $a^b=a$,

c_2) $a^8=b^2=1$, $a^b=a^5$,

c_3) $a^8=b^2=1$, $a^b=a^3$,

c_4) $a^8=b^2=1$, $a^b=a^7$,

c_5) $a^8=b^4=1$, $b^2=a^4$, $a^b=a^7$,

d_1) $a^2=b^4=c^2=1$, $a^b=a$, $a^c=a$, $b^c=b$,

d_2) $a^2=b^4=c^2=1$, $a^b=a$, $a^c=a$, $b^c=ab$,

d_3) $a^2=b^4=c^4=1$, $a^b=a$, $a^c=a$, $b^c=b$,

d_4) $a^2=b^4=c^4=1$, $a^b=a$, $a^c=a$, $b^c=ab$, $c^2=a$,

d_5) $a^4=b^2=c^2=1$, $a^b=a^{-1}$, $ac=ca$, $bc=cb$,

d_6) $a^4=b^4=c^2=1$, $a^2=b^2$, $a^b=a^3$, $ac=ca$, $bc=cb$,

d_7) $a^4=b^4=c^4=1$, $a^2=b^2=c^2$, $a^b=a^3$, $a^c=a$, $b^c=b$.

Rešenje: Sve grupe reda 16 (v.zad. 8.2.25.)

a_i) tipa A , b_i) tipa B , c_i) tipa C , d_i) tipa D .

1.35.Neka je $\underline{G}=(G,*)$ grupa, F slobodna grupa generisana skupom G i $h:\underline{F}\to\underline{G}$ homomorfizam odredjen preslikavanjem $f(a)=a$ $(a\in G)$. Dokazati da je $\ker h$ najmanja normalna podgrupa u F generisana sa $S=\{abc^{-1} \mid a,b,c\in G \text{ i } a*b=c\}$.

Rešenje: Ako je $[S]^F=N$, dokažimo da je $N=\ker h$.

1^o $N\subseteq\ker h$.

Dovoljno je dokazati da je $S\subseteq\ker h$. Neka je $abc^{-1}\in S$; tada zaista

$$h(abc^{-1})=h(a)*h(b)*h(c)^{*1}=a*b*c^{*1}=1 .$$

2^o $\ker h\subseteq N$.

Neka je $g\in\ker h$, $g=a_1^{\alpha_1}\dots a_k^{\alpha_k}$ $(a_i\in G,\ \alpha_i=\pm 1)$.

Ako je $a^{-1}=b$ u G, tada je $Na^{-1}=N(b\cdot a\cdot 1^{-1})^{-1}b=Nb$, jer $b\cdot a\cdot 1^{-1}\in S$.

Neka su b_i $(i=1,\dots,k)$ elementi iz G takvi da je $b_i=a_i^{\alpha_i}$. Imamo, dakle,

$$Ng=Na_1^{\alpha_1}\dots Na_k^{\alpha_k}=Nb_1\dots Nb_k=Nb_1\dots b_k .$$

Neka su c_i $(i=1,\dots,k)$ elementi iz G takvi da je $c_i=b_1*\dots*b_i$.

Očigledno $c_{i-1}b_ic_i^{-1}\in S$ za svako $i=2,\dots,k$. Kako je $b_1\dots b_kg^{-1}\in N$, $N\subseteq\ker h$ i $g\in\ker h$, to je $b_1\dots b_k\in\ker h$, odnosno $c_k=1$. Sada imamo

$$b_1\dots b_k=c_1b_2c_2^{-1}\cdot c_2b_3c_3^{-1}\dots c_{k-1}b_kc_k^{-1} .$$

Na desnoj strani je element iz N, pa je $b_1\dots b_k$, a s njim i g , takodje element iz N .

1.36.Dokazati: a) Svaka grupa ima bar jedno predstavljanje ll ,

b) Svaka konačna grupa ima konačno predstavljanje.

Rešenje: Direktno prema zadatku 1.35., $G \simeq F/N$. Koristeći zad. 1.11., $G \simeq G_{\Pi}$ *gde je* $\Pi = \langle G;\ \{abc^{-1} \mid a,b,c \in G\ ;\ a*b=c\} \rangle$.

Napomena: Ovako dobijena postavka je tzv. tablična postavka grupe G. Ona nije i jedina za G. Dokazaće se kasnije (v.zad. 12.3.7.) da ih G ima beskonačno mnogo. U zadacima odeljka 12.2. opisan je postupak prelaska sa jedne konačne postavke grupe G na drugu.

II način: Kako je svaka grupa G izomorfna faktor-grupi slobodne grupe (v. zad. 11.1.6.), prema zad. 1.11., svaka grupa ima predstavljanje.

1.37. Dokazati da sledeće grupe imaju konačno predstavljanje :

a) Slobodne grupe konačnog ranga , b) Konačno generisane Abel-ove grupe .

Rešenje: a) Jedno konačno predstavljanje za grupu F_n $(n < \infty)$ *je*

$$F_n \simeq \langle a_1,\dots,a_n \rangle .$$

b) Konačno generisana Abel-ova grupa je faktor-grupa A/N slobodne Abel-ove grupe A konačnog ranga. Kako je svaka podgrupa grupe A konačno generisana, to je i N konačno generisana, pa A/N ima predstavljanje sa konačno mnogo strukturnih jednakosti.

II način: Svaka konačno generisana Abel-ova grupa je direktan proizvod konačno mnogo cikličnih grupa. Koristiti dalje zad. 1.44. o predstavljanju direktnog proizvoda.

1.38. Dokazati da aditivna grupa racionalnih brojeva ima sledeće predstavljanje

$$\Pi = \langle a_1,\dots,a_n,\dots;\ a_1=a_2^2,\ a_2=a_3^3,\ \dots,\ a_n=a_{n+1}^{n+1},\ \dots \rangle .$$

Rešenje:

Lema: Za svaki racionalni broj $x \in (0,1)$ *postoji tačno jedan prirodan broj n i jedinstveni prirodni brojevi* $x_1,x_2,\dots,x_n$ *takvi da je*

$$x = \frac{x_1}{1!} + \frac{x_2}{2!} + \dots + \frac{x_n}{n!} \quad i \quad (\forall i<n)(0 \leqslant x_i < i),\ x_n \neq 0 \qquad (*)$$

Dokaz: Dokazujemo najpre jedinstvenost:

Ako su $m,n,x_1,\dots,x_m,y_1,\dots,y_n$ *prirodni brojevi takvi da*

$$x = \sum_{1 \leqslant i \leqslant m} \frac{x_i}{i!} = \sum_{1 \leqslant j \leqslant n} \frac{y_j}{j!} = y \quad i \quad 0 \leqslant x_i, y_i < i \qquad (1)$$

$(1 \leqslant i \leqslant n,m)$ *, tada* $(\forall i<n)x_i=y_i$

Zaista, pretpostavimo da nije za svaki i (koji je manji od m i n) $x_i=y_i$. *Tada postoji najmanji prirodan broj k takav da* $x_k \neq y_k$ *; recimo da je* $x_k > y_k$, *tj.* $x_k \geqslant y_k+1$ *. Otuda*

$$x \geqslant \sum_{i<\kappa} \frac{x_i}{i!} = \sum_{i<k} \frac{x_i}{i!} + \frac{x_k}{k!} = \sum_{i<k} \frac{y_i}{i!} + \frac{x_k}{k!} \geqslant \sum_{i<k} \frac{y_i}{i!} + \frac{y_k}{k!} + \frac{1}{k!}$$

pa $$x \geq \sum_{i \leq k} \frac{y_i}{i!} + \frac{1}{k!} \qquad (2)$$

Dalje, $$\sum_{k<j\leq n} \frac{y_j}{j!} \leq \sum_{k<j\leq n} \frac{j-1}{j!} = \sum_{k<j\leq n} \frac{j}{j!} - \sum_{k<j\leq n} \frac{1}{j!} = \sum_{k\leq j\leq n} \frac{1}{(j-1)!} -$$

$\sum_{k<j\leq n} \frac{1}{j!} = \frac{1}{k!} - \frac{1}{n!} < \frac{1}{k!}$, pa iz (2) i prethodnog sledi

$$x > \sum_{i \leq k} \frac{y_i}{i!} + \sum_{k<j\leq n} \frac{y_j}{j!} = y ,$$

što je suprotno pretpostavci da je $x=y$. Ovim je (1) dokazano.

Dokazujemo sada da svaki racionalni broj $x \in (0,1)$ ima predstavljanje oblika (*). Neka je n odredjen prirodan broj i

$$X = \{ \frac{x}{n!} \mid 0 \leq x < n! \} , \qquad Y = \{ \frac{x_1}{1!} + \ldots + \frac{x_n}{n!} \mid (\forall i \leq n)(0 \leq x_i < i) \} .$$

Prema (1) skup Y ima članova koliko i n-torki prirodnih brojeva $(x_1,\ldots,x_n)$ takvih da $0 \leq x_i < i$ $(1 \leq i \leq n)$. Ovakvih nizova ima $n!$, dakle $|Y|=n!$. Dalje, očigledno $|X|=n!$. Najzad, ako je $y \in Y$, tada $0 \leq y$ i

$$y = \sum_{i \leq n} \frac{y_i}{i!} < \sum_{i=1}^{\infty} \frac{i-1}{i!} = 1 ,$$

tj. y je racionalan broj za koji je $0 \leq y < 1$.

Dalje, za svaki $i \leq n$ $i!$ deli $n!$; dakle y se može predstaviti u obliku raz lomka $y = \frac{m}{n!}$. Kako je $0 \leq y < 1$, to $m < n!$ pa $y \in X$. Dakle, $Y \subseteq X$. Kako su X i Y jednakobrojni konačni skupovi, to $Y = X$.

Najzad, svaki racionalni broj $c \in (0,1)$ može se napisati u obliku $z = \frac{a}{b}$, tj. $z = \frac{a \cdot (b-1)!}{b!}$, pa za neki n $(=b)$ $z \in X$, čime je lema dokazana . ∇

Prema prethodnoj lemi neposredno sledi:

Za svaki racionalan broj z postoji jedinstven ceo broj y,
jedinstven prirodan broj n i jedinstveni prirodni brojevi
$x_1,\ldots,x_n$ takvi da $0 \leq x_i < i$ $(1 \leq i < n)$ (**)

$$z = y + \frac{x_1}{1!} + \frac{x_2}{2!} + \ldots + \frac{x_n}{n!}$$

Vratimo se sada prezentaciji II.

Zbog $a_1a_2 = a_2^2a_2 = a_2a_1$, $a_1a_3 = a_2^2a_3 = a_3a_3^3a_3^3 = a_3a_1$,... itd. sledi da je G_{II} komutativna .

Neka je z element Q koji je razložen u oblik (**). Definišimo preslikavanje $\phi : Q \to G$ na sledeći način

$$\phi(z) = a_1^y a_2^{x_2} a_3^{x_3} \ldots a_n^{x_n}$$

Tada je ϕ izomorfizam grupa $(Q,+)$ i G_{II} .

1.39. Dokazati da je za simetričnu grupu S_n jedno predstavljanje

$$\Pi = \langle a_1, \ldots, a_{n-1};\ P, Q, R \rangle .$$

gde su $P = \{a_i^2 \mid 1 \leqslant i \leqslant n-1\}$, $Q = \{(a_i\ a_{i+1})^3 \mid 1 \leqslant i \leqslant n-2\}$,
$R = \{ [a_i, a_j] \mid 1 \leqslant i < j-1 \leqslant n-2\}$.

Rešenje: Grupa S_n je generisana sa (1 2), (2 3),...,(n-1 n) . Označimo sa a_i transpoziciju (i i+1). Pokazuje se da u S_n važe jednakosti tipa P,Q,R. Zaista,

$$(i\ \ i+1)^2 = \begin{pmatrix} 1 \ldots & i & i+1 & n \\ 1 \ldots & i+1 & i & \ldots n \end{pmatrix}^2 = I \qquad (i=1,\ldots,n-1)$$

$$((i\ \ i+1)(i+1\ \ i+2))^3 = \begin{pmatrix} \cdots & i & i+1 & i+2 & \cdots \\ & i+2 & i & i+1 & \end{pmatrix} = I \quad (i=1,2,\ldots,n-2)$$

$$(i\ \ i+1)(j\ \ j+1) = (j\ \ j+1)(i\ \ i+1) \qquad (1\ \ i\ \ j-1\ \ n-2)$$

tj. $[(i\ \ i+1),(j\ \ j+1)] = I$.

Dakle, G_Π ima bar n! elemenata. Treba još dokazati da G_Π ima najviše n! elemenata.

1.40. a) Odrediti predstavljanja dijedarskih grupa D_n $(n \in N)$,
b) Dokazati da je grupa $\langle a,b;\ b^2=1, ba=a^{-1}b \rangle$ beskonačna[1].

Rešenje: a) Dijedarska grupa D_n je grupa simetrije pravilnog n-tougla (v. zad. 2.1.17.); dakle $D_n < S_n$ i posmatraju se samo izometrije n-tougla na sebe. Primetimo da se prilikom ovakvih preslikavanja skup temena preslikava na sebe. Neka su temena 1,2,...,n obeležena u smeru skazaljke na satu. Tražena preslikavanja su rotacije u ravni Oxy oko centra (0,0) tog n-tougla, za ugao $2\pi/n$, $4\pi/n$,...$2n\pi/n$, i refleksije oko osa simetrije n-tougla. Primetimo da se svaka ovakva refleksija oko ose l može dobiti rotacijom oko ose l, u prostoru, za ugao π.

Rotacija za ugao $2\pi/n$ se može predstaviti sa

$$a = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ 2 & 3 & \ldots & n & 1 \end{pmatrix} = (\ 1\ \ 2\ \ 3\ \ldots\ n-1\ \ n)$$

Tada su ostale rotacije u ravni redom $a^2, a^3, \ldots, a^n$, gde je $a^n=1$.

Rotacija oko Ox za α, tj. refleksija, može se predstaviti sa

$$b = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix}$$

Pri tom je $b^2=1$. Sve ostale refleksije mogu se prikazati kao proizvodi refleksije b i rotacija a^k $(k=1,\ldots,n)$. Medju preslikavanjima a i b postoji sledeća veza:

---

[1] Ova grupa, u oznaci D_∞ je *beskonačna dijedarska* grupa.

$$ba = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 1 & n & \dots & 4 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & 1 & 2 & \dots & n-2 & nn \end{pmatrix}\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 1 & n & \dots & 3 & 2 \end{pmatrix} = a^{-1}b$$

Odavde, svaki element grupe simetrije je oblika $a^i b^j$ $(i\in\{0,1,\dots,n-1\}$, $j\in\{0,1\})$. *Na taj način, dakle, predstavljeni su svi elementi iz* D_n *(ima ih* $2n$, *v.zad. 2.2.15.), pa je*

$$D_n \simeq \langle a,b;\ a^n=1, b^2=1, ba=a^{-1}b \rangle .$$

b) Prema zad. 1.11., svaka grupa D_n *je homomorfna slika grupe*

$$D_\infty = \langle a,b;\ b^2=1, ba=a^{-1}b \rangle ,$$ *pa*

pa je D_∞ *zaista beskonačna grupa.*

Primetimo da je $D_\infty = C_2 * C_2$. *Naime, iz* $ba=a^{-1}b$ *i* $b^2=1$ *sledi* $(ba)^2=1$, *pa je*

$$\langle a,b;\ b^2=1, ba=a^{-1}b \rangle \overset{①}{\simeq} \langle a,b;u;\ b^2=1, ba=a^{-1}b, (ba)^2=1, u=ba \rangle$$

$$\overset{②}{\simeq} \langle a,b,u;\ b^2=1, (ba)^2=1, a=b^{-1}u \rangle \overset{③}{\simeq} \langle b,u;\ b^2=1, u^2=1 \rangle$$

① *primenom transformacija* T_1 *i* T_3 *(videti odeljak 12.2. i zad. 12.2.1.)*

② *primenom transformacije* T_2, *jer je* $ba=a^{-1}b$ *posledica jednakosti* $(ba)^2=1$ *i* $b^2=1$,

③ *primenom transformacije* T_4 .

Tvrdjenje sledi prema zad. 1.45.

1.41. Dokazati da je grupa linearnih transformacija oblika $f(x)=cx+d$ $(c\neq 0\ ;\ x,c, d\in Z_p)$, u odnosu na proizvod preslikavanja, odredjena predstavljanjem

$$\Pi = \langle a,b;\ a^p=1, b^{p-1}=1, ab=ba^q \rangle ,$$

gde je p prost broj a q je u grupi $(Z_p, \cdot_p)$ reda p-1 .

Rešenje: Kako je $ab=ba^q$, *svi izrazi nad* $\{a,b\}$ *su ekvivalentni izrazima oblika*

$$b^i a^j \text{ , gde je } 0 \leqslant i \leqslant p-1 \text{ , } 0 \leqslant j < p .$$

Dakle, grupa G_Π *je najviše reda* $p(p-1)$.

S druge strane, grupa L linearnih transformacija nad $(Z_p, \cdot_p)$ *je reda* $p(p-1)$.

Osim toga, svi elementi iz L se mogu predstaviti kompozicijom sledeće dve transformacije:

$$f_1(x)=x+1 \text{ , } f_2(x)=qx .$$

Kako u grupi L važe jednakosti

$$f_1^p = I,\ f_2^{p-1} = I,\ f_1 f_2 = f_2 f_1^q ,$$

to grupa G_Π *ima bar* $p(p-1)$ *elemenata. Prema tome,* G_Π *ima tačno* $p(p-1)$ *elemenata. Preslikavanje* ϕ *odredjeno sa*

$$\phi(a)=f_1 \text{ , } \phi(b)=f_2$$

proširuje se do izomorfizma grupa L i G_Π.

1.42. Neka je M modularna grupa (v.zad. 3.2.6.). Dokazati:

a) $\langle x,y;\ x^2,y^3 \rangle$ je postavka grupe M ,

b) M je homomorfna slika multiplikativne grupe matrica $\underline{M}_1$, gde je $M_1 = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in Z\ ;\ ad-bc=1 \}$; odrediti postavku grupe M_1 ,

c) Komutant grupe M je slobodna grupa ,

d) Postoje grupe u M koje su slobodne grupe proizvoljnog konačnog ranga .

Rešenje: a) Kako je $M \simeq C_2 * C_3$, *to je prema zad. 1.45.* $M \simeq \langle x,y;\ x^2=1, y^3=1 \rangle$.

b) Preslikavanje $\phi : M_1 \to M$ *definisano sa* $\phi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \dfrac{az+b}{cz+d}$ *je homomorfizam grupe* M_1 *u grupu M sa*

$$\ker \phi = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \} \quad \text{(v.zad. 3.2.6.c))}$$

M_1 *je generisana elementima*

$$x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \quad z = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

za koje je $x^2=z$, $y^3=z$, $z^2=E$ *(E - jedinična matrica reda 2).*

Tražena postavka je $\langle x,y;\ x^4=1, x^2=y^3 \rangle$.

I odavde se neposredno utvrdjuje da je M homomorfna slika grupe M_1 . *Naime, postavka grupe M dobija se iz postavke grupe* M_1 *dodavanjem* $x^2=1$.

c) $M = C_2 * C_3$. *Podgrupa* $K = [C_2, C_3]$ *grupe M generisana sa* $\{ [a,b] \mid a \in C_2, b \in C_3 \}$ *je normalna u M (v.zad.11.2.20.). Ako sa K' označimo komutant grupe M , tj. K' je podgrupa generisana sa* $\{ [a,b] \mid a,b \in C_2 * C_3 \}$ *tada je očigledno* $K \leq K'$. *S druge strane je* $(C_2 * C_3)/K \simeq C_2 \times C_3$ *(v.zad. 11.2.20.) pa iz komutativnosti grupa* C_2 *i* C_3 *sledi komutativnost grupe* $(C_2 * C_3)$, *tj. grupe* $(C_2 * C_3)/K$. *Prema zad. 3.2.12.,* K K'. *Dakle,* $K = K'$. *Da je K slobodna grupa dokazano je u zad. 11.2.21.*

Napomena: Jedino svojstvo grupa C_2 *i* C_3 *koje se koristi u prethodnom dokazu je da su one Abel-ove grupe. U stvari, može se dokazati jače tvrdjenje: Komutant grupe A*B , gde su A,B Abel-ove grupe, je slobodna grupa.*

d) Grupa M ima slobodnu grupu F_2 *kao podgrupu (prema c)) a* F_2 *ima slobodne podgrupe proizvoljnog ranga (v.zad. 11.1.18.).*

1.43. Odrediti konačne postavke za sledeće grupe:

a) $\underline{M}_1 = (M_1, \cdot)$, gde je $M_1 = \{ \begin{pmatrix} \varepsilon & x \\ 0 & 1 \end{pmatrix} \mid \varepsilon = \pm 1\ ,\ x \in Z_n \}$

b) $\underline{M}_2 = (M_2, \cdot)$, gde je $M_2 = \{ \begin{pmatrix} \varepsilon & z \\ 0 & 1 \end{pmatrix} \mid \varepsilon = \pm 1\ ,\ z \in Z \}$

c) $\underline{M}_3 = (M_3, \cdot)$, gde je $M_3 = \{ \begin{pmatrix} x & 0 \\ y & 1 \end{pmatrix} \mid x,y \in Z_5\ ,\ x \neq 0 \}$

d) A_5

Rešenje: a) $M_1 \simeq \langle a,b;\ a^n=1, b^2=1, ba=a^{-1}b \rangle \simeq D_n$;

izomorfizam je odredjen sa $f(a)=\begin{pmatrix}1&1\\0&1\end{pmatrix}$, $f(b)=\begin{pmatrix}-1&0\\0&1\end{pmatrix}$.

b) $M_2 \simeq \langle a,b;\ b^2=1, ba=a^{-1}b\rangle \simeq D_\infty$;
izomorfizam je odredjen sa $g(a)=\begin{pmatrix}1&1\\0&1\end{pmatrix}$, $g(b)=\begin{pmatrix}-1&0\\0&1\end{pmatrix}$.

c) $M_3 \simeq \langle a,b;\ a^5=1, b^4=1, ab=ba^2\rangle$;
preslikavanje $h(a)=\begin{pmatrix}1&0\\1&1\end{pmatrix}$, $h(b)=\begin{pmatrix}2&0\\0&1\end{pmatrix}$ *odredjuje izomorfizam.*

d) $A_5 \simeq \langle a,b;\ a^5=1, b^3=1, (ab)^2=1\rangle$.

1.44.a) Neka su grupe G_1 i G_2 odredjene redom prezentacijama

$$\Pi_1 = \langle a_1,\ldots;\ R_1,\ldots\rangle, \quad \Pi_2 = \langle b_1,\ldots;\ Q_1,\ldots\rangle;$$

dokazati da je

$$\Pi = \langle a_1,\ldots,b_1,\ldots;\ R_1,\ldots,Q_1,\ldots,a_ib_j=b_ja_i,\ldots\rangle \quad (i,j=1,2,\ldots),$$

prezentacija grupe $G_1 \times G_2$.

b) Odrediti prezentacije grupa $C_2 \times C_2$ i $S_3 \times K$.

Rešenje: a) Neka su skupovi generatornih elemenata grupa G_1 *i* G_2 *disjunktni (ako nisu, izvršiti preimenovanje). Tada su i skupovi strukturnih reči iz* Π_1 *i* Π_2 *disjunktni. Neka je, dalje, prezentacijom* Π *odredjena grupa* G.
Dokazujemo da je $G \simeq G_1 \times G_2$.
Preslikavanje $a_i \mapsto a_i$ *može se, prema zad. 1.10.a) proširiti do homomorfizma* $\phi_1 : G_1 \to G$, *jer se strukturne reči iz* Π_1 *preslikavaju u jedinicu grupe* G.
Takodje, preslikavanje $b_i \to b_i$ *proširujemo do homomorfizma* $\phi_2 : G_2 \to G$.
Dokažimo da je preslikavanje $\phi : G_1 \times G_2 \to G$ *definisano sa*

$$\phi((u,v))=\phi_1(u)\phi_2(v) \qquad (u\in G_1,\ v\in G_2)$$

homomorfizam. Neka su $(u_1,v_1),(u_2,v_2)\in G_1 \times G_2$. *Tada*

$$\phi((u_1,v_1)(u_2,v_2))=\phi((u_1u_2,v_1v_2))=\phi_1(u_1u_2)\phi_2(v_1v_2)$$
$$=\phi_1(u_1)\phi_1(u_2)\phi_2(v_1)\phi_2(v_2).$$

Elementi a_i *i* b_j *komutiraju u* G *(zbog relacija* $a_ib_j=b_ja_i$; $i,j=1,2,\ldots$*), pa kako su* $u_2\in G_1$, $v_1\in G_2$ *(tj.* $u_2=a_{i_1}a_{i_2}\ldots a_{i_k}$, $v_1=b_{j_1}b_{j_2}\ldots b_{j_k}$*), komutiraju u* G *i elementi* $\phi_1(u_2)$ *i* $\phi_2(v_1)$. *Stoga je*

$$\phi((u_1,v_1)(u_2,v_2))=\phi_1(u_1)\phi_2(v_1)\phi_1(u_2)\phi_2(v_2)=\phi((u_1,v_1))\phi((u_2,v_2)).$$

Preslikavanje $a_i \mapsto (a_i,1)$, $b_j \mapsto (1,b_j)$ *proširuje se do homomorfizma* $\Psi : G \to G_1 \times G_2$, *jer se strukturne reči iz* Π *preslikavaju u jedinicu grupe* $G_1 \times G_2$.
Kako su preslikavanja ϕ *i* Ψ *uzajamno inverzna, to su grupe* G *i* $G_1 \times G_2$ *izomorfne.*

b) $C_2 = \langle a;\ a^2=1\rangle$, $C_2 \times C_2 = \langle a,b;\ a^2=1, b^2=1, ab=ba\rangle$;
$S_3 = \langle a,b;\ a^3=1, b^2=1, ab=ba^2\rangle$ *(v. zad. 1.15.b))*
$K = \langle a,b;\ ab=b^{-1}a, ba=a^{-1}b\rangle$ *(v. zad. 1.15.c)).*
$S_3 \times K = \langle a,b,c,d;\ a^3=1, b^2=1, ab=ba^2, cd=d^{-1}c, dc=c^{-1}d, ac=ca, ad=da, bc=cb, bd=db\rangle$.

1.45.Ako su grupe G_1 i G_2 odredjene redom prezentacijama

$\Pi_1 = \langle A;R \rangle = \langle a_1,\ldots; R_1,\ldots \rangle$, $\Pi_2 = \langle B;Q \rangle = \langle b_1,\ldots; Q_1,\ldots \rangle$ $(A \cap B = \emptyset)$, dokazati da je $\Pi = \langle a_1,\ldots,b_1,\ldots; R_1,\ldots,Q_1,\ldots \rangle$ prezentacija grupe $G_1 * G_2$.

Rešenje: Neka je G grupa odredjena prezentacijom $\Pi = \langle A \cup B;\ R \cup Q \rangle$, *i neka su preslikavanja* $j_i : G_i \to G$ $(i=1,2)$ *proširenja identičkih preslikavanja* ***skupova A, B.*** *Kako se izrazi* $R_1,\ldots,Q_1,\ldots$ *preslikavaju u 1, to su prema zad. 1.10.a),* j_1 *i* j_2 *homomorfizmi.*

Lako se pokazuje da su j_1 *i* j_2 *1-1 preslikavanja.*

Neka su, dalje, $f_i : G_i \to H$ $(i=1,2)$ *homomorfizmi u proizvoljnu grupu H .*

Definišimo preslikavanje $\phi : A \cup B \to H$ *tako da je* $\phi\restriction_A = f_1\restriction_A$, $\phi\restriction_B = f_2\restriction_B$.

Za proizvoljni izraz $R_i(a_{i_1},\ldots,a_{i_n})$ *iz R je*

$$R_i(f_1(a_{i_1}),\ldots,f_1(a_{i_n})) = 1_H \text{ , pa je i } R_i(\phi(a_{i_1}),\ldots,\phi(a_{i_n})) = 1_H .$$

Slično je i $Q_j(\phi(b_{j_1}),\ldots,\phi(b_{j_m})) = 1_H$ *za proizvoljni* Q_j *iz Q .*

Dakle, ϕ *se proširuje do homomorfizma* $\psi : G \to H$ *i dijagram iz definicije 11.2.1. komutira. Kako je* ϕ *jedinstveno odredjeno preslikavanjima* f_1 *i* f_2, *to je jedinstveno i njegovo homomorfno proširenje* ψ .

1.46.Ako je G grupa čije su dve podgrupe A i B izomorfne, sa izomorfizmom f, dokazati da postoji grupa H , $G \prec H$, i element $h \in H$ tako da je

$$(\forall x \in A) f(x) = h^{-1}xh .$$

Rešenje: Konstrukcija grupe H može se ostvariti na sledeći način.

Neka su $H_1 = G * \langle c \rangle$, $H_2 = G * \langle d \rangle$, *gde su* $\langle c \rangle$ *i* $\langle d \rangle$ *beskonačne ciklične grupe. Uočimo u grupama* H_1 *i* H_2 *redom podgrupe* L_1 *i* L_2 *generisane sa* $L_1 = \langle G , c^{-1}Ac \rangle$, $L_2 = \langle G , d^{-1}Bd \rangle$. *Prema Kuroš-evoj teoremi o podgrupama (videti odeljak 11.2.) je*

$$L_1 = G * c^{-1}Ac \text{ ,} \qquad L_2 = G * d^{-1}Bd \tag{1}$$

((1) sledi i neposredno, na osnovu jedinstvenosti predstavljanja elemenata iz H_1 *i* H_2 *; napr.* $g_1c^{-1}a_1cg_2c^{-1}a_2c\ldots g_kc^{-1}a_kc$, *gde su* $g_i, a_i \in G$ *a* $c \in \langle c \rangle$, *je jedinstveni zapis u* H_1, *pa i u podgrupi* L_1*).*

Neka je $\phi : L_1 \to L_2$ *homomorfno proširenje preslikavanja* ψ *odredjenog sa*

$$(\forall g \in G)\psi(g) = g \text{ ,} \qquad (\forall x \in A)\psi(c^{-1}xc) = d^{-1}f(x)d .$$

Kako su preslikavanja $\phi\restriction_G : G \to G$ *i* $\phi\restriction_{c^{-1}Ac} : c^{-1}Ac \to d^{-1}Bd$ *izomorfizmi, to je i* $\phi : G * c^{-1}Ac \to G * d^{-1}Bd$ *izomorfizam . Može se stoga konstruisati slobodan proizvod grupa* H_1 *i* H_2 *sa zajedničkom podgrupom L* $(\cong L_1 \cong L_2)$ *u odnosu na preslikavanje* ϕ*:*

$$H = H_1 \underset{L}{*} H_2$$

Prema zadatku 11.2.3. H sadrži kao podgrupu H_1 (tj. njen izomorfni lik), pa stoga i grupu G .

Element $h = cd^{-1}$ grupe H je sa traženim svojstvom. Zaista, u H važe jednakosti (v.zad. 11.3.2.)

$$c^{-1}xc = \phi(c^{-1}xc) \quad \text{za sve } x \in A ,$$

tj. $c^{-1}xc = d^{-1}f(x)d$, *odakle* $(cd^{-1})^{-1}x(cd^{-1}) = f(x)$.

1.47. Dokazati da se svaka prebrojiva grupa G može potopiti u grupu $\bar{G}$ sa dva generatora [1].

Rešenje: Neka je G prebrojiva grupa sa generatorima $g_0=1, g_1, g_2, \ldots, g_n, \ldots$

Ako je $F_2 = \langle x,y \rangle_s$, konstruišimo grupu $L = G * F_2$, i nadjimo u njoj dve izomorfne podgrupe (tako da možemo primeniti konstrukciju prethodnog zadatka).

Prema zad. 11.1.9. skup $\{y, x^{-1}yx, \ldots, x^{-n}yx^n, \ldots\}$ slobodno generiše podgrupu F' u grupi F_2 , tj. u grupi L . Uočimo skup $\{x, g_1y^{-1}xy, \ldots, g_ny^{-n}xy^n, \ldots\}$ i podgrupu F'' generisanu njim. Kako je $\{x, y^{-1}xy, \ldots, y^{-n}xy^n, \ldots\}$ skup slobodnih generatora u L, a u L nema strukturnih jednakosti koje povezuju g_i (g_i su iz G) sa elementima iz F_2 , to gornji skup slobodno generiše podgrupu F'' .

Dakle, $f(g_iy^{-i}xy^i) = x^{-i}yx^i$ je izomorfizam podgrupa F' i F'' .

Neka je, prema prethodnom zadatku, H grupa koja sadrži L i u kojoj postoji element h za koji je $(\forall x \in F')f(x) = h^{-1}xh$.

Najzad, neka je $\bar{G}$ podgrupa grupe H generisana sa $\{x,h\}$. Tada $G < \bar{G}$.

Zaista,

$$f(g_iy^{-i}xy^i) = h^{-1}g_iy^{-i}xy^ih = x^{-i}yx^i .$$

Kako je $y \in \bar{G}$ (jer je za i=0 $f(g_0y^0xy^0 = f(x) = y = h^{-1}xh$), to je $x^{-i}yx^i \in \bar{G}$, pa i $h^{-1}g_iy^{-i}xy^ih \in \bar{G}$ odakle $g_i \in \bar{G}$.

1.48. Neka je F slobodna grupa i $w \in F$, $w \neq 1$. Dokazati da postoji u F normalna podgrupa N konačnog indeksa, koja ne sadrži w .

Rešenje: Neka je $F = \langle a_1, \ldots, a_n, \ldots \rangle$ i neka je $w = a_{i_1}^{\varepsilon_1}a_{i_2}^{\varepsilon_2}\ldots a_{i_k}^{\varepsilon_k}$, gde je $\varepsilon_j \in \{1,-1\}$, $a_{i_j} \in \{a_1, a_2, \ldots, a_n\}$, $j=1,\ldots,k$, $a_{i_j} \neq a_{i_{j+1}}$ $(w \neq 1)$.

Pretpostavili smo, dakle, da u svedenom obliku za w učestvuje n različitih slova - oznaka za generatore $a_1, \ldots, a_n$.

Odredimo homomorfizam ϕ grupe F u neku konačnu grupu G, tako da bude $\phi(w) \neq 1$.

---

[1] Rezultati zadataka 1.46. i 1.47. pripadaju autorima G.Higman, B.H.Neumann, H.Neumann, 1949 .

Izaberimo za G simetričnu grupu S_{k+1} . Dovoljno je, dakle, preslikati $a_1,\dots,a_n$ u permutacije $f_1,\dots,f_n$ tako da permutacija $f_{i_1}^{\alpha_1}f_{i_2}^{\alpha_2}\dots f_{i_k}^{\alpha_k}$ ($i_j\in\{1,\dots,n\}$) bude različita od identične, I . Ostalim generatorima u F, pridružimo preslikavanjem ϕ upravo identičku permutaciju I . Odredjenije, definišimo ϕ tako da $\phi(a_{i_1}^{\alpha_1}\dots a_{i_k}^{\alpha_k})=f_{i_1}^{\alpha_1}f_{i_2}^{\alpha_2}\dots f_{i_k}^{\alpha_k}=\begin{pmatrix}1 & \dots & k+1\\ k+1 & \dots & \end{pmatrix}$.

Proučimo mogućnost konstruisanja takvog homomorfizma na jednom primeru. Neka je $w=x_1^{-1}x_2x_1x_3^{-1}$. Preslikavamo F u S_5 (jer je $|w|=4$) tako da slovima x_1,x_2,x_3 (koja učestvuju u w) pridružujemo $f_1,f_2,f_3\in S_5$ (koje su različite od I), a ostalim x_j (j=3,4,...) permutaciju I . Ako želimo da je $\phi(x_1^{-1}x_2x_1x_3^{-1})=f_1^{-1}f_2f_1f_3^{-1}=\begin{pmatrix}1 & \dots & 5\\ 5 & \dots & .\end{pmatrix}$ definišimo ϕ tako da $\phi(x_1^{-1})=\begin{pmatrix}1 & \dots\\ 2 & \dots\end{pmatrix}$, $\phi(x_2)=\begin{pmatrix}. & 2 & \dots\\ . & 3 & \dots\end{pmatrix}$, $\phi(x_1)=\begin{pmatrix}.. & 3.. & \\ .. & 4.. & \end{pmatrix}$, $\phi(x_3^{-1})=\begin{pmatrix}\dots & 4 & .\\ \dots & 5 & .\end{pmatrix}$. To se ostvaruje ako je

$$f_1=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 4 & & & \end{pmatrix},\quad f_2=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ & 3 & & & \end{pmatrix},\quad f_3\ \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ & & & & 4\end{pmatrix}$$

Ostale elemente u f_1,f_2,f_3 popunimo proizvoljno.

Slično možemo postupiti u opštem slučaju. Definišimo preslikavanje $\psi:\{a_1,a_2,\dots\}\to S_{k+1}$ na sledeći način:

$$\psi(a_{i_j})=f_{i_j}=\begin{cases}\begin{pmatrix}\dots & j & \dots\\ \dots & j+1 & \dots\end{pmatrix}, & \text{ako je } \varepsilon_j=1\\ \begin{pmatrix}\dots & j+1 & \dots\\ \dots & j & \dots\end{pmatrix}, & \text{ako je } \varepsilon_j=-1\end{cases}$$

($i_j\in\{1,\dots,n\}$, $j\in\{1,\dots,k\}$).

Time je postignuto da bude

$$\psi(a_{i_j})^{\varepsilon_j}=f_{i_j}^{\varepsilon_j}=\begin{pmatrix}\dots & j & \dots\\ \dots & j+1 & \dots\end{pmatrix}.$$

Ovo se preslikavanje na jedinstven način produžava do homomorfizma $\phi:F\to S_{k+1}$, odredjenog sa

$$\phi(a_{i_1}^{\varepsilon_1}\dots a_{i_k}^{\varepsilon_k})=\psi(a_{i_1})^{\varepsilon_1}\dots\psi(a_{i_k})^{\varepsilon_k}=f_{i_1}^{\varepsilon_1}\dots f_{i_k}^{\varepsilon_k}\ .$$

Prema definiciji preslikavanja ψ je

$$\phi(a_{i_1}^{\varepsilon_1}\dots a_{i_k}^{\varepsilon_k})=\begin{pmatrix}1 & \dots\\ 2 & \dots\end{pmatrix}\dots\begin{pmatrix}\dots & k & \dots\\ \dots & k+1 & \dots\end{pmatrix}=\begin{pmatrix}1 & \dots\\ k+1 & \dots\end{pmatrix}\neq I$$

Dakle, $w\notin\ker\phi$ ($\ker\phi=N$), a $\phi(F)$ je konačna grupa ($\phi(F)<S_{k+1}$), što je i trebalo dokazati.

1.49. Dokazati da ne postoji zakon u=v koji zadovoljavaju sve konačne grupe, a koji nije posledica teorije grupa.

Rešenje: Neka zakon u=v nije posledica teorije grupa i neka u njemu učestvuju slova $x_1,\dots,x_n$ (i slova jezika $L=\{\cdot,^{-1},1\}$). Tada je $uv^{-1}\neq 1$ u slobodnoj grupi $F_n=\langle x_1,\dots,x_n\rangle_S$. Neka je N normalna podgrupa u F_n, konačnog indeksa, koja ne sadrži uv^{-1} (a koja, prema prethodnom zadatku postoji).

Dakle, u konačnoj grupi F_n/N ne važi zakon $u=v$.

1.50. Neka je S podgrupa simetrične grupe S_Z koja se sastoji od svih permutacija skupa Z (celih brojeva) koje premeštaju samo konačno mnogo elemenata iz Z. Da li postoji netrivijalna strukturna jednakost koju zadovoljava grupa S ?

Rešenje: Grupa S sadrži izomorfne likove svih konačnih grupa, pa prema prethodnom zadatku u S ne važi ni jedan netrivijalni zakon.

1.51. Dokazati: a) Postoji prebrojivo mnogo konačno predstavljivih grupa ,
b) Postoji $2^{\aleph_0}$ neizomorfnih grupa sa dva generatora .

Rešenje: a) Neka je $A=\{a_1,a_2,\ldots\}$ prebrojiv skup slova. Svaku konačnu postavku Π' možemo transformisati do postavke $\Pi=<a_1,\ldots,a_n;\ r_1,\ldots,r_m>$ tako da je $G_{\Pi}\simeq G_{\Pi}$. (preimenovanjem generatornih elemenata iz Π' i sledstvenim preimenovanjem strukturnih jednakosti).
S druge strane Π je konačan niz prebrojivog skupa $X=A\cup\{<,>,\cdot,^{-1},,\}$. S obzirom da konačnih nizova prebrojivog skupa ima prebrojivo mnogo, sledi da prezentacija Π ima takodje prebrojivo mnogo.

b) U dokazu se koristi sledeća činjenica: postoji $2^{\aleph_0}$ različitih podskupova skupa prostih brojeva. Svakom takvom skupu P pridružimo direktnu sumu $G_P=\sum_{p\in P} C_p$ cikličnih grupa reda p ($p\in P$). Prema zad. 1.47., postoji grupa $\bar{G}_p$ sa dva generatora koja sadrži izomorfni lik grupe G_p. Koristeći konstrukciju zad. 1.46. i 1.47. je:

$$G_P<\bar{G}_P<H \quad , \text{ gde je } \quad H\simeq(G_P*F_2*<c>)\underset{L}{*}(G_P*F_2*<d>)$$
$$L\simeq<G_P*F_2,c^{-1}F'c>\simeq<G_P*F_2,d^{-1}F''d> \ .$$

Proizvoljni element konačnog reda grupe H je, prema zad. 11.3.8., u podgrupi konjugovanoj sa $G_P*F_2*<c>$ ili sa $G_P*F_2*<d>$. Kako su F_2, $<c>$ i $<d>$ slobodne grupe, tj. bez elemenata konačnog reda, zaključujemo (prema zadatku 11.2.17.) da H ima element nekog konačnog reda akko takav element ima G_P. Odnosno, G_P ima element reda p akko $\bar{G}_P$ ima element reda p .(S druge strane, G_P ima element reda p akko $p\in P$.)
Dakle, izomorfnih grupa $\bar{G}_p$ ima onoliko koliko i skupova P , tj. $2^{\aleph_0}$.

12.2. TIETZE-OVE TRANSFORMACIJE

Kao što je već istaknuto u 12.1., jedna grupa ima beskonačno mnogo postavki. Mogu se stoga razmatrati sledeća pitanja:

- Kakva je veza medju postavkama jedne iste grupe G ?
- Može li se i kako od jedne postavke Π grupe G_Π , dobiti druga ?
- Može li se za dve postavke Π_1 i Π_2 utvrditi odredjuju li istu grupu ?

itd.

Odgovor (negativan) na treće pitanje dat je u odeljku 12.3. Za razmatranja prva dva problema pogodno je uvesti transformacije postavki grupa, kojima se od postavke Π grupe G dobija postavka Π' iste te grupe. Jedan primer ovakvih transformacija su tzv. Tietze-ove transformacije.

Koristićemo u daljem sledeće oznake: za jednakost u=v za koju je $Z_A \cup R \underset{J}{|\!\!-\!\!-} u=v$, kažemo da je *posledica* [1] skupa jednakosti R u postavci $\Pi = \langle A; R \rangle$; pored gornje, koriste se još i oznake:

$$R \;|\!\!-\!\!-\; u=v\,, \qquad \Pi \;|\!\!-\!\!-\; u=v\,, \ (\text{ili } \underset{\Pi}{|\!\!-\!\!-} u=v), \qquad G_\Pi |\!\!-\!\!-\; u=v\,, \qquad u \underset{\Pi}{\sim} v\,.$$

Za izraze u i v za koje je $\Pi \;|\!\!-\!\!-\; u=v$ kažemo da su *ekvivalentni u* Π.
Za izraz w nad azbukom $L \cup A$, gde je $L=\{\cdot, ^{-1}, 1\}$ i $\Pi = \langle A;R \rangle$, pisaćemo i kraće: $w \in \Pi$.

2.1. *Definicija:* *Neka je* $\Pi = \langle A;R \rangle$. *Tietze-ove transformacije predstavljanja* Π *tipa* T_1 - T_4 *su:*

(i) $T_1(\Pi) = \langle A;\ R \cup \{u=1\} \rangle$, *ako je* $\Pi \;|\!\!-\!\!-\; u=1$,

(ii) $T_2(\Pi) = \langle A;\ R \setminus \{u=1\} \rangle$, *ako je* $\langle A;\ R \setminus \{u=1\} \rangle \;|\!\!-\!\!-\; u=1$

(iii) $T_3(\Pi) = \langle A \cup \{a\};\ R \cup \{a=u\} \rangle$, *ako je u izraz nad* $A \cup L$, *i* $a \notin A$,

(iv) $T_4(\Pi) = \langle A \setminus \{a\};\ (R \setminus \{a=u\})^c \rangle$, *ako je* $R = R' \cup \{a=u\}$ *i* $(a=u) \notin R'$, *gde je u izraz nad* $(A \setminus \{a\}) \cup L$, *i* $(R')^c$ *označava skup jednakosti iz* R' *u kojima su sva pojavljivanja slova a zamenjena izrazom u* .

Drugim rečima, (višestruke) primene transformacija gornjih tipova sastoje se u sledećem:

- strukturnim jednakostima R se dodaju posledice tih jednakosti (T_1) ,
- iz R se izostavljaju one strukturne jednakosti koje su posledice preostalih jednakosti iz R (T_2) ,

---

[1] Videti uvodni deo odeljka 10.5.

- generatornim elementima A se dodaju novi elementi a,b,... (a,b,... nisu iz A), a strukturnim jednakostima R nove jednakosti a=u, b=v,... gde su u,v,... izrazi nad $A \cup L$ (tj. u njima ne učestvuju slova a,b,... (T_3) ,
- ako u R postoje jednakosti oblika a=u, b=v,... gde su a,b,... iz A a u, v,... izrazi nad $(A \setminus \{a,b,...\}) \cup L$, tada se iz A izostavljaju elementi a,b,..., iz R jednakosti a=u, b=v,..., a u preostalim jednakostima iz R se a,b,... redom zamene sa u,v,... (T_4) .

Umesto " transformacija tipa T_i " , pisaćemo, kraće, " transformacija T_i " (i=1,2,3,4).

Na osnovu zadatka 2.1. sledi : $(\forall i \in \{1,2,3,4\})\ G_\Pi \simeq G_{T_i(\Pi)}$.

Uvodjenjem ovakvih transformacija se u mnogome olakšava rad sa postavkama grupa.

Primeri i zadaci

2.1. Ako je postavka Π' dobijena od postavke Π primenom Tietze-ovih transformacija, dokazati da je $G_\Pi \simeq G_{\Pi'}$.

Rešenje: Neka je $\Pi = \langle A;R \rangle$. *Ako je* $\Pi' = T_1(\Pi)$ *ili* $\Pi' = T_2(\Pi)$, *tada je*

$$u \underset{\Pi}{\sim} v \iff u \underset{\Pi'}{\sim} v \qquad (1)$$

jer su, u jednakosnoj logici J, skupovi posledica klase zakona $Z_A \cup R$ *i* $Z_A \cup R \cup \{w=1\}$, *jednaki, ako je* $Z_A \cup R \vdash w=1$.

Ako je $\Pi' = T_3(\Pi)$, *tada* $u \underset{\Pi}{\sim} v \Leftrightarrow u' \underset{\Pi'}{\sim} v'$, *gde svakom izrazu u' iz* Π' *odgovara izraz u iz* Π *tako što se a zameni sa w. Slično za* T_4 .

Dakle, klase zakona $Z_A \cup R$ *i* $Z_{A \cup \{a\}} \cup R \cup \{a=w\}$ *imaju jednake skupove posledica u jednakosnoj logici J, ako je w izraz nad A* [1] *(ne sadrži slovo a). Naime, svaki izraz t' nad* $A \cup \{a\}$ *je moguće, zbog a=w, svesti na izraz t nad A, za koji je t=1 ili ne, zavisno od jednakosti u R .*

2.2. Odrediti transformacije T_i^{-1} , inverzne transformacijama T_i (i=1,2,3,4).

Rešenje: Transformaciji tipa T_1 *je inverzna transformacija tipa* T_2 , *što zapisujemo, kraće :* $T_1^{-1} = T_2$. *Zaista,* $T_2(T_1(\Pi)) = \Pi$.

---

[1] Za izraze jezika $L \cup A$, gde je $L = \{\cdot, ^{-1}, 1\}$, kažemo često da su izrazi nad A, ne naglašavajući uvek prisutni deo jezika, L .

Takodje je $T_2^{-1}=T_1$ *jer je* $T_1(T_2(\Pi))=\Pi$, *i* $T_3^{-1}=T_4$ *jer je* $T_4(T_3(\Pi))=\Pi$.

Odredimo, najzad, tipove transformacija koje $T_4(\Pi)$ *dovode do* Π.

Ako je $\Pi=<A;R>$, *tada je* $T_4(\Pi)=<A\setminus\{a\};R'>$, *gde je* $R'=R\setminus\{a=u\}$, $(a=u)\notin R'$ *i u* R' *nema pojavljivanja slova a. Stoga i u postavci* $T_3(T_4(\Pi))=<A;\ R'\cup\{a=u\}>$, *u* R' *nema pojavljivanja slova a. Primenjujemo sada transformacije tipa* T_1 *dodajući jednakosti v=w iz R, u kojima se pojavljuje a (to su neke od jednakosti v'=w' iz R' u kojima je izraz u zamenjen sa a); očigledno je v=w posledica jednakosti v'=w' i a=u. Konačno, primenjujući transformacije tipa* T_2 *treba izostaviti sve one jednakosti v'=w' za koje postoje odgovarajuće posledice v=w dodate transformacijama tipa* T_1. *Stoga*

$$T_4^{-1}=\underbrace{T_2\circ\ldots\circ T_2}_{k}\circ\underbrace{T_1\circ\ldots\circ T_1}_{k}\circ T_3$$

2.3. Neka su $\Pi_1=<a_1,a_2,\ldots;\ R_1,R_2,\ldots>$ i $\Pi_2=<b_1,b_2,\ldots;\ Q_1,Q_2,\ldots>$ dve prezentacije grupe G. Dokazati da postoji niz Tietze-ovih transformacija koji prevodi jednu prezentaciju u drugu.

Rešenje: *Označimo* $R=\{R_1=1,R_2=1,\ldots\}$, $Q=\{Q_1=1,Q_2=1,\ldots\}$, $A=\{a_1,a_2,\ldots\}$ $B=\{b_1,b_2,\ldots\}$. *Neka je*

$$F_1=<A>_S\ ,\qquad F_2=<B>_S\ ;$$

tada $G\simeq F_1/[R]\simeq F_2/[Q]$, *tj. postoje* **homomorfizmi**

$$\phi_1:\ F_1\xrightarrow{na}G\ ,\qquad \phi_2:\ F_2\xrightarrow{na}G\ .$$

S obzirom da je $\phi_1(F_1)=G=\phi_2(F_2)$ *to za svaki izraz u nad A postoji izraz v nad B tako da* $\phi_1(u)=\phi_2(v)$.

Dakle, mogu se uvesti preslikavanja $x\longmapsto u_x$ *skupa A u* F_2 *i* $y\longmapsto v_y$ *skupa B u* F_1 *tako da je*

$$(\forall x\in A)\phi_1(x)=\phi_2(u_x)\ ,\qquad (\forall y\in B)\phi_2(y)=\phi_1(v_y)\ .$$

Označimo sa S i T sledeće skupove jednakosti:

$$S=\{(x=u_x)\mid x\in A,\ u_x\in F_2,\ \phi_1(x)=\phi_2(u_x)\}$$
$$T=\{(y=v_y)\mid y\in B,\ v_y\in F_1,\ \phi_2(y)=\phi_1(v_y)\}$$

Možemo sada transformisati postavku $\Pi_1=<A;R>$ *do postavke* $\Pi_2=<B;Q>$ *na sledeći način:*

$$<A;R>\ \xrightarrow[①]{}\ <A\cup B;\ R\cup T>\ \xrightarrow[②]{}\ <A\cup B;\ R\cup T\cup Q>$$
$$\xrightarrow[③]{}\ <A\cup B;\ R\cup T\cup Q\cup S>\ \xrightarrow[④]{}\ <B;\ R\cup T\cup Q>\ \xrightarrow[⑤]{}\ <B;\ Q>$$

① *primenjujući transformacije* T_3

② $Z_{A\cup B}\cup R\cup T \mid\frac{}{J} Q_i=1$, *za svako i jer je* $<A\cup B;\ R\cup T>\simeq G$, *a u G važe jednakosti Q nad* $b_1, b_2, \ldots$; *stoga se mogu primeniti transformacije tipa* T_1

③ *primenom transformacija* T_1 , *jer* $Z_{A\cup B}\cup R\cup Q \mid\frac{}{J} S$, *tj. u G važe jednakosti S*

④ *primenom* T_4

⑤ *primenom* T_2 , *jer je* $<B;\ R\cup T\cup Q>\simeq G$, *tj.* $Z_B\cup Q \mid\frac{}{J} R\cup T$ *(ako bi u* $R\cup T$ *bilo novih strukturnih jednakosti koje nisu posledice jednakosti iz Q, tada bi* $<B;\ R\cup T\cup Q>$ *bila prava homomorfna slika od G)*

Napomene: 1) Ako su postavke Π_1 *i* Π_2 *konačne, tj.*

$$\Pi_1=<a_1,\ldots,a_n;\ R_1,\ldots,R_m>,\quad \Pi_2=<b_1,\ldots,b_k;\ Q_1,\ldots,Q_l>$$

tada se prelaz sa Π_1 *na* Π_2 *obavlja u tačno*

$$k+l+n+n+m+k=2(k+n)+(l+m)$$

koraka (tj. primena transformacija tipa $T_1 - T_4$*).*

2) Opisani postupak ne rešava problem izomorfizma za konačno predstavljive grupe. Ne postoji efektivni postupak kojim se za proizvoljne dve postavke Π_1 *i* Π_2 *utvrdjuje da li je* $G_{\Pi_1}\simeq G_{\Pi_2}$ *ili ne (videti odeljak 12.3.).*

2.4. Ako je $\Pi=<a_1,\ldots,a_n;\ R_1,\ldots,R_m>$ konačna postavka grupe G , dokazati da se svaka postavka te grupe sa konačno generatora $\Pi'=<b_1,\ldots,b_k;Q_1,Q_2,\ldots>$ može transformisati u konačnu postavku primenjujući samo Tietze-ove transformacije tipa T_1 .

Rešenje: Postavke $\Pi=<A;\ R>$ *i* $\Pi'=<B;\ Q>$ *odredjuju izomorfne grupe, sa izomorfizmom* $f: G_\Pi \to G_{\Pi'}$. *Tada je*

$$(\forall i\in\{1,\ldots,m\})f(R_i)=1\ ,\quad (\forall j\in N)f^{-1}(Q_j)=1\ .$$

Prema zad. 1.9.b) svaki od izraza $f(R_i)$ *se predstavlja u obliku*

$$u_1^{-1}Q_{i_1}u_1\ldots u_l^{-1}Q_{i_l}u_l \qquad (1)$$

$(u_1,\ldots,u_l\in F_k\ ,\ F_k=<b_1,\ldots,b_k>_s\ ,\ Q_{i_1},\ldots,Q_{i_l}\in Q\ ).$

Slično, svaki od izraza $f^{-1}(Q_j)$ *se predstavlja u obliku*

$$v_1^{-1}R_{j_1}v_j\ldots v_p^{-1}R_{j_p}v_p \qquad (2)$$

$(v_1,\ldots,v_p\in F_n\ ;\ F_n=<a_1,\ldots,a_n>_s\ ,\ R_{j_1},\ldots,R_{j_p}\in R\ ).$

Kako izraza R_i ima konačno mñogo (m), i kako se svaki $f(R_i)$ predstavlja pomoću (1) u kome ima konačno mnogo izraza iz Q, to se s v i $f(R_i)$ predstavljaju pomoću (1) i nekog konačnog skupa

$$S=\{Q_{i_1},Q_{i_2},\ldots,Q_{i_s}\}$$

Sada je, za svaki Q_i ($i\in N$)

$$Q_i=f\circ f^{-1}(Q_i)=f(w_1^{-1}R_1^{\bullet}w_1\ldots w_t^{-1}R_t^{\bullet}w_t)$$

$$=f(w_1)^{-1}(x_1^{-1}Q_1^{\bullet}x_1\ldots x_t^{-1}Q_t^{\bullet}x_t)f(w_1)\ldots f(w_t)^{-1}(y_1^{-1}Q_1^{\bullet\bullet}y_1\ldots y_r^{-1}Q_r^{\bullet\bullet}y_r)f(w_t)$$

gde su $R_1^{\bullet},\ldots,R_t^{\bullet}\in R$; $Q_1^{\bullet},\ldots,Q_t^{\bullet},\ldots,Q_1^{\bullet\bullet},\ldots,Q_r^{\bullet\bullet}\in S$; $w_1,\ldots,w_t\in F_n$; $x_1,\ldots,x_t,\ldots,y_1,\ldots,y_r\in F_k$.

Dakle, svaki Q_i se predstavlja proizvodom elemenata konjugovanih elementima iz S , tj. $Q_i\in[S]$, Drugim rečima skupovi posledica zakona $Z_B\cup Q$ i $Z_B\cup S$ su jednaki.

Stoga se izostavljanjem skupa jednakosti $\{r=1 \mid r\in Q\setminus S\}$ iz $\Pi^{\bullet}$ dobija konačna postavka $\Pi^{\bullet\bullet}$ koja takodje odredjuje grupu (=) G_{Π}.

2.5. Dokazati da je grupa sa postavkom $\Pi=\langle A;\ a_1a_2\ldots a_k=a_{k+1}\ldots a_n\rangle$ gde su $a_1,\ldots,a_n$ različiti elementi iz A, slobodna.

Rešenje: $\Pi=\langle A;\ a_1=a_{k+1}\ldots a_n(a_2\ldots a_k)^{-1}\rangle \xrightarrow[T_4]{} \langle A\setminus\{a_1\}\rangle$

2.6. Dokazati da sledeća predstavljanja odredjuju (do na izomorfizam) istu grupu G:

a) $\Pi_1=\langle a,b,c;\ a^3,c^2,abc\rangle$, $\Pi_2=\langle x,y;\ x^3y^2\rangle$

b) $\Pi_1=\langle x,y;\ x^2y^2,y^2\rangle$, $\Pi_2=\langle x,y;\ x^2,y^2\rangle$

c) $\Pi_1=\langle a,b;\ aba=bab\rangle$, $\Pi_2=\langle x,y;\ x^3=y^2\rangle$,
$\Pi_3=\langle a,b,c;\ a^{-1}b^{-1}cb,b^{-1}c^{-1}ac,c^{-1}a^{-1}ba\rangle$

d) $\Pi_1=\langle a,b,c;\ (ab)^2ab^2\rangle$, $\Pi_2=\langle x,y\rangle$

Rešenje: $\Pi_1=\langle a,b,c;\ a^3,c^2,abc\rangle \xrightarrow[T_4]{} \langle a,c;\ a^3,c^2\rangle=\Pi_2$.

b) $\Pi_2=\langle x,y;\ x^2=1,\ y^2=1\rangle \xrightarrow[T_1]{} \langle x,y;\ x^2=1,y^2=1,x^2y^2=1\rangle$

$$\xrightarrow[T_2]{} \langle x,y;\ x^2y^2=1,y^2=1\rangle=\Pi_1$$

c) Primenjujemo postupak naveden u dokazu zadatka 2.3.

$\Pi_1=\langle a,b;\ aba=bab\rangle \xrightarrow[T_3]{} \langle a,b,x,y;\ aba=bab,x=ab,y=bab\rangle \xrightarrow[T_1]{}$

① $\langle a,b,x,y;\ aba=bab,\ x=ab,y=bab,a=x^{-1}y,b=y^{-1}x^2\rangle \xrightarrow[T_1]{}$

$\langle a,b,x,y;aba=bab,x=ab,y=bab,a=x^{-1}y,b=y^{-1}x^2,y^2=x^3\rangle$

②

$\xrightarrow[T_4]{} \langle x,y;\ y^2=x^3,x=x^{-1}yy^{-1}x^2,y=y^{-1}x^2x^{-1}yy^{-1}x^2\rangle \xrightarrow[T_2]{} \langle x,y;\ y^2=x^3\rangle=\Pi_2$

① *jer iz* $xa=y$ *sledi* $a=x^{-1}y$, *i iz* $b=a^{-1}x$ *sledi* $b=y^{-1}x^2$

② *jer iz* $aba=bab$, *zamenjujući* a *i* b *sledi* $x^{-1}yy^{-1}x^2x^{-1}y=y^{-1}x^2x^{-1}yy^{-1}x^2$, *tj.* $y=y^{-1}x^3$ *ili* $y^2=x^3$

Dalje je

$$\Pi_3=\langle a,b,c;\ cb=ba,ac=cb,ba=ac\rangle \xrightarrow[T_2]{} \langle a,b,c;\ c=bab^{-1},c=a\ \ ba\rangle$$

$$\xrightarrow[T_1]{} \langle a,b,c;\ c=bab^{-1},c=a^{-1}ba,aba=bab\rangle \xrightarrow[T_4]{} \langle a,b;\ bab^{-1}=a^{-1}ba,aba=bab\rangle$$

$$\xrightarrow[T_2]{} \langle a,b;\ aba=bab\rangle = \Pi_1$$

d) $\Pi_2=\langle x,y\rangle \xrightarrow[T_3]{} \langle x,y,a;\ a=x^{-2}\rangle \xrightarrow[T_1]{} \langle x,y,a;\ a=x^{-2},x^2a=1\rangle$

$$\xrightarrow[T_2]{} \langle x,y,a;\ x^2a=1\rangle \xrightarrow[T_3]{} \langle x,y,a,b,c;\ x^2a=1,b=x^{-1}a,c=xa^{-1}x\rangle$$

$$\xrightarrow[T_1]{} \langle x,y,a,b,c;\ x^2a=1,b=x^{-1}a,c=xa^{-1}x,x=cb,a=cb^2\rangle \xrightarrow[T_2]{}$$

③ $\langle x,y,a,b,c;\ x^2a=1,x=cb,a=cb^2\rangle$

$$\xrightarrow[T_1]{} \langle x,y,a,b,c;\ x^2a=1,x=cb,a=cb^2,(cb)^2cb^2=1\rangle$$

$$\xrightarrow[T_2]{} \langle x,y,a,b,c;\ x=cb,a=cb^2,(cb)^2cb^2=1\rangle \xrightarrow[T_4]{} \langle c,b,y;\ (cb)^2cb^2=1\rangle = \Pi_1$$

③ *jer iz* $xb=cb^2$ *i* $a=cb^2$ *sledi* $b=x^{-1}a$, *a iz* $x=cb$ *i* $b=x^{-1}a$ *sledi* $c=xa^{-1}x$.

2.7. Dokazati da za svaku konačno generisanu grupu G postoji predstavljanje tipa $\langle a_1,\ldots,a_n;\ P_1=1,P_2=1,\ldots\rangle$ gde su $P_1,P_2,\ldots$ izrazi nad $\{a_1,\ldots,a_n\}\cup\{1,\cdot\}$ (tj. svi eksponenti slova $a_1,\ldots,a_n$ u $P_1,P_2,\ldots$ su pozitivni).

Rešenje: Neka je $\Pi=\langle b_1,\ldots,b_m;\ R_1,R_2,\ldots\rangle$ *proizvoljna postavka sa* m *generatora, grupe* G *. Svaki podizraz oblika* b_i^{-1} *zamenjujemo izrazom* c_i , *tj.*

$$\langle b_1,\ldots,b_m;\ R_1,R_2,\ldots\rangle \xrightarrow[T_3]{} \langle b_1,\ldots,b_m,c_1,\ldots,c_m;\ R_1,R_2,\ldots,b_1c_1=1,\ldots,$$

$$b_mc_m=1\rangle \longrightarrow \langle b_1,\ldots,b_m,c_1,\ldots,c_m;\ R_1^*,R_2^*,\ldots,b_1c_1=1,\ldots,b_mc_m=1\rangle$$

gde su R_i^* *izrazi dobijeni od* R_i *zamenom svakog pojavljivanja* b_j^{-1} *izrazom* c_j.

2.8. Dokazati (pomoću Tietze-ovih transformacija) da ciklična grupa C_{mn} , gde je $(m,n)=1$, ima postavku $\langle a,b;\ a^m=1,b^n=1,ab=ba\rangle$.

Rešenje: $C_{mn}\simeq \langle c;\ c^{mn}=1\rangle \xrightarrow[T_3]{} \langle c,a,b;\ c^{mn}=1,a=c^n,b=c^m\rangle$

$$\xrightarrow[T_1]{} \langle c,a,b;\ c^{mn}=1,a=c^n,b=c^m,a^m=1,b^n=1.ab=ba\rangle$$

Kako je $(m,n)=1$, *to postoje* α *i* β *iz* N *tako da je* $\alpha n+\beta m=1$. *Odavde,* $c^{\alpha n+\beta m}=c$ *tj,* $a^\alpha b^\beta=c$. *Stoga je, daljc*

$\xrightarrow[T_1]{} < c,a,b;\ c^{mn}=1, a=c^n, b=c^m, a^m=1, b^n=1, ab=ba, c=a^{\alpha}b^{\beta} >$

$\xrightarrow[T_4]{} < a,b;\ (a^{\alpha}b^{\beta})^{mn}=1, a=(a^{\alpha}b^{\beta})^n, b=(a^{\alpha}b^{\beta})^m, a^m=1, b^n=1, ab=ba >$

$\xrightarrow[T_2]{} < a,b;\ a^m=1, b^n=1, ab=ba >$

2.9. Ako je $< a_1,\dots,a_n;\ r_1,\dots,r_m >$ postavka konačne grupe, dokazati da je $n \leqslant m$.

Rešenje: *Neka je grupa* $G=< A;R > = < a_1,\dots,a_n;\ r_1,\dots,r_m >$ *konačna, reda k. Tada je podgrupa* $N=[R]$ *indeksa k u* F_n. *Prema zad. 11.1.16., N je konačno generisana, sa* $k(n-1)+1$ *slobodnih generatora.*

S druge strane, prema zad. 12.1.9. N je generisana sa

$$\{w^{-1}rw \mid w \in F_n,\ r \in R\} \qquad (1)$$

Kako je $(\forall w \in F_n)(\exists_1 m \in M)\ Z_A \cup R \mid\!\frac{}{J}\ w=m$

gde je M skup svedenih, kardinalnosti k, to iz beskonačnog skupa generatora (1), možemo izdvojiti konačni, od km elemenata $(m=|R|)$.

Kako slobodna grupa ranga j ne može biti generisana sa manje od j generatora (sledi prema zad. 11.1.6.b)), to je

$$k(n-1)+1 \leqslant km$$

odnosno, $n-m \leqslant \varepsilon$, *gde je* $0 \leqslant \varepsilon < 1$.

Kako su $n,m \in N$, *odavde* $n \leqslant m$, *što je i trebalo dokazati.*

2.10. Dokazati (pomoću Tietze-ovih transformacija) da grupa $G=< a,b;\ b^{-1}a^2b=a^3 >$ nije Hopf-ova.

Rešenje: *Dokazuje se da* $Z_{\{a,b\}} \cup \{b^{-1}a^2b=a^3\} \not\mid\!\frac{}{J}\ a=(a^{-1}b^{-1}ab)^2$,

a zatim, Tietze-ovim transformacijama da je

$$< a,b;\ b^{-1}a^2b=a^3 > \simeq < a,b;\ b^{-1}a^2b=a^3, a=(a^{-1}b^{-1}ab)^2 >,$$

odnosno, da je G izomorfna svojoj pravoj faktor-grupi.

12.3. ALGORITAMSKI PROBLEMI KOD GRUPA

Pre razmatranja najvažnijih primera problema odlučivosti u teoriji grupa, ukazujemo na neke pojmove i rezultate teorije algoritama, koji se ovde koriste.

Neka je Z neki matematički zadatak. *Problem odlučivosti* ili *problem algoritamske rešivosti* za Z je problem egzistencije efektivnog postupka, algoritma, koji rešava zadatak Z.

Intuitivni pojam algoritma u gornjem iskazu može se zameniti nekom od postojećih formalizacija ovog pojma - rekurzivnim funkcijama, mašinama Turing-a, normalnim algoritmima Markova, itd. Kako se svaki problem Z u matematici može preformulisati tako da se svede na izračunavanje neke posebne, tim problemom odredjene funkcije f_Z, to se zbog mogućnosti aritmetizacije nadalje mogu, sa gledišta izračunljivosti, tretirati samo brojevne funkcije.

3.1. *Definicija: Problem odlučivosti za zadatak Z je rekurzivno rešiv ako je funkcija f_Z rekurzivna. Inače je rekurzivno nerešiv.*

Ekvivalentno, možemo govoriti o rešivosti i nerešivosti po Turing-u, itd.
Za sve dosad uvedene formalizacije pojma algoritma, tj. efektivno izračunljive funkcije, dokazano je da su medjusobno ekvivalentne. Ako se uz to prihvati sledeći predlog

3.2. *Teza Church-a: Funkcija je efektivno izračunljiva akko je rekurzivna,*

u definiciji 3.1. se reč "rekurzivno" može izostaviti ili zameniti sa "algoritamski" tj. "efektivno". U tom smislu, uz prihvatanje teze Church-a, rešivost odnosno nerešivost su apsolutni.
Za problem Z se kaže još i, kraće, da je *odlučiv* odnosno *neodlučiv*.

Nećemo ovde uvoditi formalizam rekurzivnosti. **Elementi ove teorije mogu se naći u bilo kojem udžbeniku iz matematičke logike.**
Rekurzivnost relacije $R(x_1,\ldots,x_n)$ $(x_i \in N)$ se definiše pomoću rekurzivnosti njene karakteristične funkcije

$$c_R(x_1,\ldots,x_n) = \begin{cases} 0, & \text{ako } R(x_1,\ldots,x_n) \\ 1, & \text{ako } R(x_1,\ldots,x_n) \end{cases}$$

Dakle, neki skup S, $S \subseteq N$, je *rekurzivan*, ako se za proizvoljni prirodni broj n može efektivno utvrditi da li je $n \in S$ (tj. da li je $c_S(n)=0$) ili nije.
Drugim rečima, problem pripadnosti (rekurzivnom) skupu S je rešiv.

Pored rekurzivnih, u svetlu efektivnosti, od značaja su i *rekurzivno-prebrojivi* skupovi. Intuitivno, to su skupovi za koje postoje algoritmi koji ih u nekom redosledu prebrojavaju, generišu. Drugim rečima, skup S je rekurzivno-prebrojiv ako je oblast vrednosti neke rekurzivne funkcije.
Svaki rekurzivni skup je rekurzivno-prebrojiv. Obratno nije tačno, tj. važi sledeća

3.3. *Teorema: Postoji nerekurzivni, rekurzivno prebrojivi skup T .*

Pored navedene, često se koristi i sledeća

3.4. *Teorema (Post): Skup S je rekurzivan akko su S i njegov komplement $\bar{S}$ rekurzivno-prebrojivi*

Možemo sada proširiti pojam konačnosti, kojim su dosad razvrstavane prezentacije grupa, pojmom rekurzivnosti.

3.5. *Definicija: Postavka $\langle A ; R \rangle$ je rekurzivna ako je skup A konačan a R rekurzivno-prebrojiv.*

Prema zadatku 3.1., $\langle A ; R \rangle$ je rekurzivna akko je R rekurzivan skup, pa je naziv u definiciji 3.5. opravdan.
Grupa G je *rekurzivno predstavljiva* ako postoji rekurzivna postavka Π takva da je $G_\Pi \simeq G$.
Ovaj pojam ima bitnu ulogu kod opisa prezentacija podgrupa grupe G . Naime, poznato je da podgrupa konačno predstavljive (k.p.) grupe ne mora biti čak ni konačno generisana (v.zad.11.1.9.a)). Dakle, od interesa je pre svega ispitati konačno generisane podgrupe k.p. grupa. Odgovor na ovo pitanje daje sledeća

3.6. *Teorema (Higman): Konačno generisana grupa G se može potopiti u k.p. grupu H akko je G rekurzivno predstavljiva.*

U teoriji grupa su od posebnog interesa sledeća dva tipa problema odlučivosti:
A) Problem egzistencije algoritma koji za neku odredjenu grupu utvrdjuje koji od njenih elemenata zadovoljavaju uočeni uslov C. Takvi su napr. problem reči, problem konjugacije, stepeni problem, itd.
Ovi problemi, koji se tiču *elemenata* pojedinačnih grupa, su problemi odlu-

čivosti I reda.

B) Problem egzistencije algoritma koji za proizvoljnu prezentaciju Π utvrdjuje da li grupa G_Π zadovoljava uočeni uslov C ili ne. Takvi su napr. problem izomorfizma, zatim problem ispitivanja cikličnosti, konačnosti, komutativnosti itd. proizvoljne grupe G_Π, zadate konačnom prezentacijom Π. Ovi problemi, koji se tiču prezentacija i osobina koje ima grupa kao algebarska struktura *u celini*, su problemi odlučivosti II reda.

Razmatramo malo detaljnije najvažnije primere oba navedena tipa problema.

Prve zadatke algoritamske prirode u teoriji grupa, postavio je M.Dehn 1912 godine. To su problem reči (PR), problem konjugacije (PK) i problem izomorfizma (PI). Sva tri ova problema postavljena su u razmatranjima u topologiji (kao što je, u ostalom, i sam pojam konačno predstavljive grupe; recimo, to je fundamentalna grupa zatvorene diferencijabilne n-tostrukosti, $n \geq 4$).

Neka je $\Pi = \langle A ; R \rangle$.

3.7. *Definicija: Problem postojanja algoritma kojim se za proizvoljna dva izraza u i v nad $A \cup L$ utvrdjuje da li je $u \underset{\Pi}{\sim} v$, tj. predstavljaju li oni isti element grupe G_Π ili ne, je problem reči za predstavljanje* Π

(Ili, ekvivalentno, kojim se za proizvoljni izraz w ($w=uv^{-1}$) utvrdjuje da li je $\Pi \vdash w=1$.)

Ako takav algoritam postoji, PR je rešiv; inače je (algoritamski) nerešiv.

Odnosno, prema prethodnom, PR je rešiv za Π akko je skup

$$\{w \mid w \in \Pi \wedge \Pi \vdash w=1\}$$

rekurzivan.

3.8. *Definicija: Problem postojanja algoritma kojim se za proizvoljna dva izraza u i v nad $A \cup L$ utvrdjuje predstavljaju li oni konjugovane elemente u G_Π ili ne, je problem konjugovanosti za* Π.

Kao i gore, PK je rešiv za Π akko je skup

$$\{(u,v) \mid u,v \in \Pi \wedge (\exists r \in \Pi)(\Pi \vdash u=r^{-1}vr)\}$$

rekurzivan.

Označimo sa $\sim^C$ relaciju konjugovanosti medju elementima iz Π, tj.

$$u \underset{\Pi}{\sim}^C v \overset{def}{\Longleftrightarrow} (\exists r \in \Pi)\, \Pi \vdash u=r^{-1}vr .$$

Oba navedena problema definisana su, dakle, za prezentacije grupa. Medjutim, (ne)rešivost problema PR i PK za prezentaciju Π_1 konačno generi-

sane grupe G prenosi se na svaku drugu prezentaciju π_2 te grupe (v.zad.3.3.), Stoga je opravdano govoriti o problemu reči, odnosno problemu konjugovanosti *grupe* G .

Postoje grupe sa rešivim problemima PR i PK (videti zadatke 3.4., 3.6. i 3.8.), kao i one kod kojih su ovi problemi nerešivi. To je za k.p. grupe dokazao P.S.Novikov : 1954 godine je konstruisao k.p. grupu sa nerešivim problemom konjugovanosti, a 1955 god. k.p. grupu sa nerešivim problemom reči.

Na ovu temu postoje i mnogi drugi interesantni rezultati. Pomenimo na primer teoremu W.Magnus-a (1932) o rešivosti problema reči za sve grupe sa jednom strukturnom jednakošću, teoremu A.W.Mostowski-V.H.Dyson-a (1964) o rešivosti problema reči za sve rezidualno-konačne [1] k.p. grupe i teoremu G.Baumslag-a (1965) o nerešivosti problema konjugacije za neke rezidualno-konačne grupe, itd.

Zadatkom 3.5. je pokazano da rešivost PK povlači rešivost PR. Da ne važi obratno dokazao je A.A.Fridman (1960) konstrukcijom k.p. grupe sa rešivim PR i nerešivim PK .

Pomenimo još neke algoritamske probleme prve vrste.

3.9. *Definicija: Neka je u grupi G podgrupa H generisana sa* $H = \langle w_1, w_2, \ldots \rangle$ *Problem egzistencije algoritma kojim se za proizvoljni element u iz G utvrdjuje da li je u H ili ne, je generalisani problem reči za H u G.*

Ovaj problem, koji skraćeno zapisujemo sa GPR, definisao je W.Magnus. Rešiv je napr. za konačno generisane Abel-ove grupe, itd. Očigledno, PR za grupu G je GPR za trivijalnu podgrupu {1} u grupi G.

D.J.Collins (1973) je dokazao egzistenciju k.p. grupe G sa nerešivim *stepenim* problemom - za proizvoljna dva elementa u i v utvrditi da li je jedan stepen drugoga (podrazumevajući da je 1 nulti stepen svakog elementa iz G). Odnosno, konstruisao je grupu G za koju je skup

$$\{(u,v) \mid u,v \in \Pi \wedge (\exists k \in Z)\ \Pi \vdash\!\!\!- u = v^k\}$$

nerekurzivan.

Stepeni problem za grupu G je, u stvari, GPR za ciklične podgrupe u G .

---

[1] Grupa G je *residualno-konačna* ako za svako $w \in G$ $(w \neq 1)$ postoji normalna podgrupa N koja ne sadrži w i za koju je G/N konačna grupa (tj. presek svih normalnih podgrupa H za koje je G/H konačna grupa, je {1}).

Medju problemima II vrste najistaknutiji je treći M.Dehn-ov, problem izomorfizma.

3.10. *Definicija: Neka je* $\mathcal{L}=\{\Pi_i \mid i\in I\}$ *proizvoljni rekurzivni skup konačnih predstavljanja grupa. Problem egzistencije algoritma koji za proizvoljne* $i,j\in I$ *utvrdjuje da li je* $G_{\Pi_i} \simeq G_{\Pi_j}$ *ili ne, je problem izomorfizma za* $\mathcal{L}$.

Da bi problem bio dobro definisan, neophodno je pretpostaviti rekurzivnost skupa $\mathcal{L}$.

S.I.Adyan (1955) i M.Rabin (1958) su dokazali da je problem PI nerešiv za skup $\mathcal{P}$ svih konačnih prezentacija grupa.

Interesantno je i pitanje raspoznatljivosti nekih važnijih svojstava grupa, kao što su konačnost, komutativnost, cikličnost, rešivost, itd. Kako je postavkom Π grupa G_Π odredjena *do na izomorfizam*, to su sa gledišta algoritamske raspoznatljivosti od interesa samo ona svojstva grupe G_Π, zadate sa Π, koja se prenose izomorfizmom - tzv. *algebarska* svojstva.

Medju svim algebarskim, posebno su važna *markovska* [1] svojstva grupa.

Skup svih k.p. grupa označimo sa $\mathcal{K}$.

3.11. *Definicija: Algebarsko svojstvo s k.p. grupa je markovsko ako je ispunjeno:*

(i) $(\exists G_1\in\mathcal{K})\ s(G_1)$, *tj. svojstvo s je neprazno ,*

(ii) $(\exists G_2\in\mathcal{K})(\forall G\in\mathcal{K})(\forall H<G)\neg(s(G)\wedge H\simeq G_2)$,

tj. postoji k.p. grupa G_2 *koja ne može biti potopljena ni u jednu k.p. grupu sa svojstvom s .*

Markovska su napr. sledeća svojstva: biti trivijalna grupa, konačna, ciklična, slobodna, Abel-ova, rešiva, lokalno-beskonačna, itd.

Poseban slučaj markovskih su i tzv. *nasledna* svojstva - sa grupe G prenose se na sve njene podgrupe.

3.12. *Teorema (Adyan,Rabin): Neka je s proizvoljno markovsko svojstvo. Skup*

$$S_s = \{\Pi \mid \Pi\in\mathcal{P}\wedge s(G_\Pi)\}$$

svih konačnih prezentacija grupa sa svojstvom s, nije rekurzivan.

---

[1] Prema sovjetskom matematičaru A.A.Markovu, koji je ovakva svojstva definisao za polugrupe.

Drugim rečima, svako markovsko svojstvo grupa je algoritamski neraspoznatljivo.

Pomenimo najzad i to da su mnogi rezultati o neodlučivosti kod grupa uopšteni u odnosu na *stepene nerešivosti* . Napr. dokazano je da postoji k.p. grupa čiji je problem reči proizvoljnog stepena nerešivosti (A.A.Fridman 1962, C.R.J.Clapham 1964), zatim da postoji k.p. grupa sa rešivim PR čiji je PK proizvoljnog stepena nerešivosti (D.J.Collins 1969), itd. W.W.Boone je (1968) uopštio i teoremu 3.12. tako da važi za proizvoljni stepen nerešivosti.

Ova problematika, koja predstavlja još jednu vezu izmedju teorije grupa (i to tzv. kombinatorne teorije grupa) i matematičke logike, i dalje je veoma aktuelna.

Primeri i zadaci

3.1. Ako je grupa G odredjena postavkom $\Pi = \langle a_1,\ldots,a_n; R \rangle$ gde je R rekurzivno prebrojiv skup, dokazati da postoji postavka $\langle b_1,\ldots,b_m; Q \rangle$ te grupe, takva da je skup Q rekurzivan.

Rešenje: Neka je $R = \{R_1, R_2, \ldots\}$ *rekurzivno prebrojivi skup izraza nad* $A = \{a_1, a_2, \ldots, a_n\}$. *Dakle, postoji efektivno izračunljiva funkcija* $F : N \to \mathcal{T}$ *gde je* $\mathcal{T}$ *skup svih izraza nad A, takva da je*

$$F(i) = R_i \ , \quad i=1,2,\ldots$$

Uočimo postavku $\Pi_1 = \langle a_1,\ldots,a_n,b \ ; \ b=1, bR_1=1, b^2R_2=1,\ldots,b^nR_n=1,\ldots \rangle$
S obzirom na Tietze-ove transformacije, očigledno je

$$G_\Pi \simeq G_{\Pi_1} \ .$$

Ispitujemo da li je skup $Q = \{b, bR_1, b^2R_2, \ldots\}$ *rekurzivan . Neka je* $\mathcal{T}^*$ *skup svih izraza nad* $A \cup \{b\}$. *Za proizvoljni izraz w iz* $\mathcal{T}^*$ *lako se efektivno utvrdjuje da li je oblika* $b^i v$, *gde je v neki izraz nad A. Ako w nije tog oblika, tada* $w \notin Q$. *U suprotnom ispitujemo da li je* $v = F(i)$; *ako jeste,* $w \in Q$, *inače* $w \notin Q$. *Dakle, postoji efektivni postupak kojim se rešava problem pripadnosti skupu Q , tj. Q je rekurzivan skup .*

3.2. Neka je G konačno predstavljiva grupa i H njena podgrupa. Ako je H konačno generisana, tada je H rekurzivno predstavljiva. Dokazati.

Rešenje: Ako je $G = \langle a_1,\ldots,a_n ; R_1,\ldots,R_m \rangle$ *tada je skup svih jednakosti koje važe u G sledeći:*

$$S = \{g_1^{-1}R_{i_1}^{\varepsilon_1}g_1 g_2^{-1}R_{i_2}^{\varepsilon_2}g_2\ldots g_j^{-1}R_{i_j}^{\varepsilon_j}g_j=1 \mid R_{i_j}\in\{R_1,\ldots,R_m\},\ g_j\in\langle a_1,\ldots,a_n\rangle,\ \varepsilon_j\in\{1,-1\},\ j=1,2,\ldots\}$$

Skup S je rekurzivno prebrojiv, jer $F=\langle a_1,\ldots,a_n\rangle_s$ *je efektivno prebrojiv skup a* $\{R_1,\ldots,R_m\}$ *konačan, pa se mogu efektivno poredjati u niz* $f(1),f(2),\ldots$ *svi izrazi sa levih strana jednakosti iz S* [1].

Neka je $H<G$ *i* $H=\langle u_1,\ldots,u_k\rangle$ *gde su* $u_i\in\langle a_1,\ldots,a_n\rangle_s$ $(i=1,\ldots,k)$.

Označimo sa $W=\{w_1,w_2,\ldots\}$ *skup svih izraza u svedenom obliku nad slovima* $\bar{u}_1,\ldots,\bar{u}_k$, *a sa* $\bar{W}=\{\bar{w}_1,\bar{w}_2,\ldots\}$ *skup izraza u svedenom obliku nad slovima* $a_1,\ldots,a_n$ *dobijenih od izraza iz W zamenom svih slova* $\bar{u}_i$ *izrazima* $u_i(a_1,\ldots,a_n)$. *Podgrupa H tada ima postavku*

$$H = \langle u_1,\ldots,u_k ; V\rangle$$

gde je $V=\{w_i \mid w_i\in W \wedge \bar{w}_i\in S\}$. *Dakle,*

$$w\in V \Leftrightarrow \bar{w}\in\bar{W}\cap S ,$$

tj. $c_1=c_2\circ\phi$, *gde su sa* c_1 *i* c_2 *označene redom karakteristične funkcije skupova V i* $\bar{W}\cap S$, *a* ϕ *je efektivna funkcija prelaska od izraza* $w\in W$ *do izraza* $\bar{w}\in\bar{W}$. *Kako je* $\bar{W}\cap S$ *rekurzivno prebrojiv skup, takav je i skup V, pa je podgrupa H rekurzivno predstavljiva.*

3.3. Neka je G konačno generisana grupa. Ako su za jednu njenu postavku $\Pi_1=\langle a_1,\ldots,a_n ; S_1,\ldots\rangle$ rešivi problem reči i problem konjugacije, dokazati da su ti problemi rešivi i za svaku drugu postavku Π_2 grupe G, sa konačnim brojem generatora.

Rešenje: Neka je $\Pi_2=\langle b_1,\ldots,b_m ; Q_1,\ldots\rangle$ *i neka su* $\mathcal{A}_1$ *i* $\mathcal{A}_2$ *algoritmi koji u postavci* Π_1 *rešavaju redom problem reči i problem konjugacije.*

Kako je G generisana sa $a_1,\ldots,a_n$, *kao i sa* $b_1,\ldots,b_m$, *to se svaki element* b_i $(i=1,\ldots,m)$ *može predstaviti izrazom nad* $a_1,\ldots,a_n$, *tj.*

$$b_1=B_1(a_1,\ldots,a_n),\ \ldots,\ b_m=B_m(a_1,\ldots,a_n)$$

Drugim rečima, postoji preslikavanje $f:\{b_1,\ldots,b_m\}\to F_n$, $F_n=\langle a_1,\ldots,a_n\rangle_s$ *odredjeno sa*

$$f(b_i)=B_i(a_1,\ldots,a_n) \qquad i=1,\ldots,m \qquad (1)$$

Neka je ϕ *jedinstveno homomorfno proširenje za f, tj. neka je* $\phi:F_m\to F_n$,

---

[1] Slično, S je rekurzivo prebrojiv i kada je skup strukturnih jednakosti $R_1=1, R_2=1,\ldots$ grupe G, rekurzivno prebrojiv.

$F_m = \langle b_1,\ldots,b_m \rangle_s$; tada je za proizvoljni izraz $R(b_1,\ldots,b_m)$ iz F_m

$$\phi(R(b_1,\ldots,b_m)) = R(B_1(a_1,\ldots,a_n),\ldots,B_m(a_1,\ldots,a_n)) \ .$$

Preslikavanje ϕ je rekurzivno, tj. za svaki izraz R iz F_m, koristeći (1), efektivno se može odrediti $\phi(R)$.

Neka su sada R_1 i R_2 proizvoljni izrazi iz F_m. Koristeći postupak $\mathcal{A}_1$, efektivno utvrdjujemo da li je $\phi(R_1) \overset{\sim}{\Pi_1} \phi(R_2)$.

Kako R_1 i $\phi(R_1)$ (kao i R_2 i $\phi(R_2)$) odredjuju iste elemente grupe G (jer b_i i B_i odredjuju iste elemente u G), to je:

$$R_1 \overset{\sim}{\Pi_2} R_2 \Leftrightarrow \phi(R_1) \overset{\sim}{\Pi_1} \phi(R_2) \ .$$

Takodje

$$R_1 \overset{\sim}{\Pi_2}{}^{C} R_2 \Leftrightarrow \phi(R_1) \overset{\sim}{\Pi_1}{}^{C} \phi(R_2)$$

(pri tom $(\forall d \in F_n)(\exists c \in F_m) d = \phi(c)$), pa se algoritmom $\mathcal{A}_2$ i efektivnim preslikavanjem ϕ, rešava i problem konjugovanosti u Π_2 .

3.4. Konstruisati algoritme koji rešavaju problem reči i problem konjugacije za grupu:

a) $G_1 \simeq \langle a,b ; a^5, b^2, ab=ba^{-1} \rangle$, b) $G_2 \simeq \langle a,b ; a^5, b^4, ab=ba^2 \rangle$

c) $G_3 \simeq \langle a,b,c ; ab=ba, bc=ca, ba=cb, cb=ac \rangle$.

Rešenje: Ako algoritam koji za proizvoljna dva izraza r_1 i r_2 iz prezentacije Π utvrdjuje da li je $r_1 \overset{\sim}{\Pi} r_2$ postoji, jedna mogućnost njegove konstrukcije je sledeća: odredi se skup neekvivalentnih markera M za Π (koji je rekurzivan), i konstruiše algoritam kojim se za proizvoljni r iz Π odredjuje m iz M takav da je $r \overset{\sim}{\Pi} m$. Sada je $r_1 \overset{\sim}{\Pi} r_2$ akko $m_1 = m_2$, ($r_1 \overset{\sim}{\Pi} m_1$, $r_2 \overset{\sim}{\Pi} m_2$).

a) Skup markera je $M_1 = \{a^i b^j \mid 0 \leq i < 5,\ 0 \leq j < 2\}$; dakle, M_1 je konačan, pa je i rekurzivan. Za svaki izraz $a^{\alpha_1} b^{\beta_1} \ldots a^{\alpha_k} b^{\beta_k}$ ($\alpha_i, \beta_i \in Z$) iz Π_1 se efektivno, u konačno koraka odredjuje njemu ekvivalentan izraz iz M_1 (primenom $a^5=1$, $b^2=1$, tj. $a^{-1}=a^4$, $b^{-1}=b$ dolazi se do izraza

$a^{p_1} b^{q_1} \ldots a^{p_k} b^{q_k}$, $p_i, q_i \in N \cup \{0\}$, tj. do izraza $a^{r_1} b^{s_1} \ldots a^{r_k} b^{s_k}$, gde je $r_i \in \{0,1,2,3,4\}$, $s_i \in \{0,1\}$, $i=1,\ldots,k$; treba zatim primeniti $ab=ba^{-1}$, itd.).

Preostaje još da se dokaže neekvivalentnost izraza iz M_1. Napr. konstrukcijom homomorfizma takvog da se svaka dva elementa iz M_1 preslikavaju u različite elemente (videti poglavlje 8). Napr. preslikavanje $f : \{a,b\} \to \underline{M}$ gde je $\underline{M} = (M, \cdot)$ multiplikativna grupa matrica reda 2 sa elementima iz $(Z_5, +_5, \cdot_5)$ odredjeno sa $f(a) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $f(b) = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}$ se proširuje do homomorfizma sa traženim svojstvom.

Slično se može konstruisati i algoritam $\mathfrak{B}$ koji rešava problem konjugovanosti u ovoj grupi. Konstruiše se (rekurzivni) skup izraza K_1 tako da je svaki r iz Π_1 konjugovan nekom elementu iz K_1 , i svi elementi iz K_1 su međusobno nekonjugovani (tj. K_1 je skup predstavnika klasa konjugacija).

Lako se dokazuje da je za grupu G_1 , $K_1 = \{1, a, a^2, ab\}$.

Zaista, $(a^i b)a^\alpha (a^i b)^{-1} \sim a^{-\alpha}$

$a^i a^\alpha a^{-i} \sim a^\alpha$ $\quad (i,\alpha \in \{0,1,2,3,4\})$,

tj. $a \sim^C a^4$, $a^2 \sim^C a^3$.

Elementi b, ab, a^2b, a^3b, a^4b iz M_1 su svi konjugovani elementu ab (napr. $b \sim a^5 b \sim a^4 ba^{-1} \sim a^3 ba^{-2} \sim a^2(ab)a^{-2}$, $a^3 b \sim a(ab)a^{-1}$, *itd.)*

Koristeći neekvivalentnost izraza iz M_1, sada se lako dokazuje nekonjugovanost izraza iz K_1.

Na primer, neka je $ab \sim^C a$, tj. $ab \sim r^{-1}ar$ za neko $r \in \Pi_1$; kako je r ekvivalentan nekom izrazu iz M_1 , to je:

za $r \sim a^k$ $(k=0,1,2,3,4)$, $ab \sim a^{-k}aa^k$ tj. $ab \sim a$, što nije tačno ,

za $r \sim a^k b$ $(k=0,1,2,3,4$, $ab \sim b^{-1}a^{-k}aa^k b$ tj. $ab \sim a^4$, itd.

b) Slično kao pod a). Grupa G_{Π_2} je reda 20.

Napomena: Traženi algoritmi postoje za grupe G_{Π_1} i G_{Π_2} i na osnovu zadatka 3.10.

c) $M_3 = \{a^{2z}, a^{2z}a, a^{2z}b, a^{2z}c, a^{2z}ab, a^{2z}ba \mid z \in Z\}$

$K_3 = \{a^{2z}, a^{2z}a, a^{2z}ab \mid z \in Z\}$.

3.5. Dokazati: ako je za grupu G rešiv problem konjugacije, rešiv je i problem reči.

Rešenje: $u \underset{\Pi}{\sim} v \Leftrightarrow uv^{-1} \underset{\Pi}{\sim}^C 1$, *odnosno algoritmom koji rešava PK može se ispitivati konjugovanost sa 1, tj. ekvivalentnost.*

Obratno ne važi (videti uvodni deo).

3.6. Dokazati da slobodne grupe imaju rešiv problem reči i problem konjugacije.

Rešenje: Problem reči u slobodnoj grupi $F = \langle X \rangle_s$, $X = \{x_1, x_2, \ldots\}$ je trivijalno rešiv: jedini izraz u svedenom obliku nad $x_1, x_2, \ldots$ koji je jednak 1 je upravo 1. Rešivost ovog problema sledi i iz rešivosti problema konjugacije (v.zad. 3.5.).

Dokaz o egzistenciji algoritma kojim se u slobodnoj grupi F rešava problem konjugacije, može se izvesti u dva koraka:

1^0 *Dokazom da je dovoljno odrediti algoritam primenljiv na one elemente* $w=x_1^{\varepsilon_1}\dots x_n^{\varepsilon_n}$ *iz* F $(x_i\in X,\ \varepsilon_i=\pm 1,\ x_i=x_{i+1}\Rightarrow\varepsilon_i\neq-\varepsilon_{i+1})$ *za koje je*

$$x_n^{\varepsilon_n}x_1^{\varepsilon_1}\neq 1 \qquad (s)$$

2^0 *Konstrukcijom algoritma kojim se za proizvoljna dva elementa sa svojstvom (s), utvrdjuje da li su ti elementi konjugovani u* F *ili ne.*

1^0 *Dokažimo prvo da se za svaki element* $w\in F$, $w\neq 1$, *može efektivno odrediti element* $v\in F$ *sa svojstvom (s), tako da je* $w\sim^C v$.

Zaista, ako je $w=x_1^{\varepsilon_1}\dots x_n^{\varepsilon_n}$ *i ako je* $x_n^{\varepsilon_n}x_1^{\varepsilon_1}=1$, *tada*

$$x_1^{-\varepsilon_1}wx_1^{\varepsilon_1}=x_2^{\varepsilon_2}\dots x_{n-1}^{\varepsilon_{n-1}}\ .$$

Dalje, ako je

$x_{n-1}^{-1}x_2^{\varepsilon_2}=1$, *tada* $x_2^{-\varepsilon_2}x_1^{-\varepsilon_1}wx_1^{\varepsilon_1}x_2^{\varepsilon_2}=x_3^{\varepsilon_3}\dots x_{n-2}^{\varepsilon_{n-2}}$, *itd.*

Kako je $w\neq 1$, *postoji* j $\left(1\leq j<\left[\frac{n+1}{2}\right]\right)$ *tako da je*

$$x_j^{-\varepsilon_j}\dots x_1^{-\varepsilon_1}wx_1^{\varepsilon_1}\dots x_j^{\varepsilon_j}=x_{j+1}^{\varepsilon_{j+1}}\dots x_{n-j}^{c_{n-j}}\ ;$$

dobijeni izraz je sa svojstvom (s).

Dakle, ako su $u,v\in F$ $(u\neq 1,\ v\neq 1)$, *postoje* u', v' *iz* F *sa svojstvom (s) tako da je* $u\sim^C u'$, $v\sim^C v'$.

Sada je

$$u\sim^C v \Leftrightarrow u'\sim^C v'$$

(*iz* $u=r_1^{-1}u'r_1$, $v=r_2^{-1}v'r_2$, $u=r_3^{-1}vr_3$ *sledi* $u'=(r_2r_3r_1^{-1})^{-1}v'(r_2r_3r_1^{-1})$).

2^0 *Neka su* $u=u_1^{\varepsilon_1}\dots u_m^{\varepsilon_m}$, $v=v_1^{\delta_1}\dots v_k^{\delta_k}$ $(u_i,v_j\in\{x_1,x_2,\dots\},\ \varepsilon_i,\delta_j=\pm 1,$ $i=1,\dots,m\ ;\ j=1,\dots,k)$ *elementi iz* F, *predstavljeni izrazima u svedenom obliku sa svojstvom (s). Dokažimo tvrdjenje:*

<u>(T1)</u>: $u\sim^C v \Leftrightarrow$ *postoji ciklična permutacija* p *skupa* $\{1,\dots,n\}$ *tako da je* $u=v_{p_1}^{\delta_{p_1}}\dots v_{p_k}^{\delta_{p_k}}$.

<u>Dokaz</u>: ($\Leftarrow$) *Očigledno*

($\Rightarrow$) *indukcijom po dužini* $d(r)$ *elementa* r *iz* F *za koji je* $u=r^{-1}vr$.

Ako je $d(r)=1$, *tada iz* $u_1^{\varepsilon_1}\dots u_m^{\varepsilon_m}=r^{-1}v_1^{\delta_1}\dots v_k^{\delta_k}r$ *i uslova (s), sledi da je* $r^{-1}v_1^{\delta_1}=1$ *ili* $v_k^{\delta_k}r=1$ (*nisu ispunjena oba uslova, jer bi iz* $r=v_1^{\delta_1}=v_k^{-\delta_k}$ *sledilo* $v_k^{\delta_k}v_1^{\delta_1}=1$ *suprotno uslovu (s)*). *Dakle je*

$$u_1^{\varepsilon_1}\dots u_m^{\varepsilon_m}=v_2^{\delta_2}\dots v_k^{\delta_k}v_1^{\delta_1} \quad \text{ili} \quad u_1^{\varepsilon_1}\dots u_m^{\varepsilon_m}=v_k^{\delta_k}v_1^{\delta_1}\dots v_{k-1}^{\delta_{k-1}}\ .$$

Kako su u *i* v *u svedenom obliku,* $d(u)=d(v)$, *pa je* u *ciklična permutacija od* v.

Neka je tvrdjenje tačno za sve r *za koje je* $d(r)<n$ *i neka je* $r=a_1^{\alpha_1}\dots a_n^{\alpha_n}$ $(\alpha_i=\pm 1,\ a_i\in X,\ i=1,\dots,n)$. *Tada*

$$u_1^{\varepsilon_1}\dots u_m^{\varepsilon_m} = a_n^{-\alpha_n}(a_1^{\alpha_1}\dots a_{n-1}^{\alpha_{n-1}})^{-1} v_1^{\delta_1}\dots v_k^{\delta_k}(a_1^{\alpha_1}\dots a_{n-1}^{\alpha_{n-1}})a_n^{\alpha_n} ,$$

tj. prema dokazanom, $u_1^{\varepsilon_1}\dots u_m^{\varepsilon_m}$ *se dobija cikličnom permutacijom iz*

$$(a_1^{\alpha_1}\dots a_{n-1}^{\alpha_{n-1}})^{-1} v_1^{\delta_1}\dots v_k^{\delta_k}(a_1^{\alpha_1}\dots a_{n-1}^{\alpha_{n-1}})$$

pa prema indukcijskoj pretpostavci i iz $v_1^{\delta_1}\dots v_k^{\delta_k}$. ∇

Najzad, kako se za svaka dva elementa iz F može efektivno utvrditi da li je jedan ciklična permutacija drugog ili nije, s obzirom na 1^o *i* 2^o *sledi da je problem konjugacije algoritamski rešiv.*

3.7. Dokazati da je u slobodnoj grupi F , relacija R definisana sa

$$R(x,y) \overset{def}{\Longleftrightarrow} x\cdot y = y\cdot x \qquad (x,y\in F,\ x,y\neq 1)$$

rekurzivna relacija ekvivalencije.

Rešenje: Očigledno je ispunjeno

$$(\forall x\in F)R(x,x) \quad i \quad (\forall x,y\in F)\left[R(x,y)\Rightarrow R(y,x)\right].$$

Neka je

$$x\cdot y = y\cdot x \quad i \quad y\cdot z = z\cdot y \qquad (1)$$

Uočimo podgrupe $H_1 = \langle x,y\rangle$ *i* $H_2 = \langle y,z\rangle$ *. One su slobodne i rang im je 1 ili 2. Zbog (1) sledi da su obe ranga 1, tj. beskonačne ciklične grupe. (Zaista, ako je rang* $H_1 = 2$ *, tada je* $\{x,y\}$ *skup slobodnih generatora za* H_1*; medjutim, u slobodnoj grupi generatori ne komutiraju.)*

Neka je $H_1 = \langle a\rangle$, $H_2 = \langle b\rangle$ *. Tada postoje* $n,m,k,l\in Z\setminus\{0\}$ *tako da je*

$$x = a^n , \quad y = a^m , \quad y = b^k , \quad z = b^l \qquad (2)$$

Iz $a^m = b^k$ *sledi* $a^m b^k = b^k a^m$ *, pa je, slično,* $H_3 = \langle a,b\rangle$ *beskonačna ciklična grupa, recimo* $H_3 = \langle c\rangle$ *. Dakle, postoje* $i,j\in Z\setminus\{0\}$ *tako da je* $a = c^i$, $b = c^j$. *Prema (2) je*

$$x = a^n = (c^i)^n = c^{ni} , \quad z = b^l = (c^j)^l = c^{lj} , \text{ odakle } x\cdot z = c^{ni+lj} = z\cdot x.$$

Rekurzivnost sledi na osnovu prethodnog zadatka:

$$R(x,y) \text{ akko } F \vdash xyx^{-1}y^{-1} = 1 .$$

3.8. Dokazati da su problem reči i problem konjugacije rešivi za slobodne Abelove grupe.

Uputstvo: Slično dokazu zadatka 3.6.; koristiti jedinstveni neskrativi zapis elemenata slobodne Abel-ove grupe (videti poglavlje 7.)

3.9. Konstruisati program (na nekom od programskih jezika) kojim se generiše niz Cayley-evih tablica konačnih grupa $G_1, G_2, \dots$ tako da za $i < j$ važi $|G_i| \leqslant |G_j|$, i za $i\neq j$ $G_i \not\cong G_j$.

3.10. Ako je Π prezentacija konačne grupe, dokazati da su za grupu G_Π rešivi problem reči i problem konjugacije.

Rešenje: <u>*Problem reči:*</u> *Neka je* $\Pi = \langle \{a_1,\dots,a_n\} ; R \rangle$ *i* w *reč za koju ispitujemo da li u* G_Π *važi* $w=1$. *Za svaku konačnu grupu efektivno se može utvrditi da li su za neki izbor (od n) generatora zadovoljene jednakosti iz R. Dakle, efektivno se može generisati niz konačnih grupa* $G_1, G_2, \dots$ *u kojima, za neki izbor generatora, važe jednakosti iz R. Primetimo da su sve grupe* G_i *homomorfne slike grupe* G_Π. *Sada možemo generisati niz reči*

$u_o, v_o, u_1, v_1, u_2, v_2, \dots$ *tako da*

(1) $R \vdash u_o=1, u_1=1, \dots$, *i (2)* v_i *je vrednost reči* w *u* G_i. *Tada*

A. Ako u G_Π *važi* $w=1$ *onda* $R \vdash w=1$, *dakle* $w=u_i$ *za neki* i.

B. Ako u G_Π *ne važi* $w=1$, *tj. nije* $R \vdash w=1$, *tada u nekoj grupi* G_i *takodje ne važi* $w=1$, *pa za neki* i $v_i \neq 1$.

<u>*Problem konjugacije:*</u> *Koristeći prethono rešenje, može se efektivno odrediti tablica grupe* G_Π, *kao i reči* $g_1,\dots,g_n$ *takve da* $G_\Pi = \{g_1,\dots,g_n\}$. *Tada*

$$a \sim^c b \Leftrightarrow b=a^{g_1} v \dots v\ b=a^{g_n}.$$

3.11. Dokazati da su za konačno generisane Abel-ove grupe rešivi problem reči i problem konjugacije.

Rešenje: Abel-ova grupa G sa n generatora je direktan proizvod m konačnih cikličnih grupa i n-m beskonačnih cikličnih grupa (videti teoremu 7.3.1.). Prema zad. 3.10. problem reči je rešiv za konačne ciklične grupe, a prema zad. 3.6. i za grupu C_∞ *(tj.* F_1*). Najzad, prema zad. 3.14., ovaj problem je rešiv i za samu grupu G.*

Primetimo da je problem konjugovanosti kod Abel-ovih grupa ekvivalentan problemu reči.

3.12. Ispitati da li je rešiv problem reči za sledeće grupe:

a) $\langle a,b ; a^7=1, b^6=1, ab=ba^3 \rangle$,

b) $\langle a_1,\dots,a_n,\dots ; a_1=a_2^2,\ a_2=a_3^2,\ \dots, a_n=a_{n+1}^2 \dots \rangle$

Da li je u njima rešiv problem konjugacije?

Rešenje: a) Data grupa je konačna, reda 42 (markeri su oblika $b^\beta a^\alpha$, $\beta \in \{0,1,2,3,4,5\}$, $\alpha \in \{0,1,\dots,6\}$*), pa su navedeni problemi rešivi (videti zadatak 3.10.)*

b) Ovako predstavljena grupa G_Π je Abel-ova. Zaista, dokazuje se da je za proizvoljne $i,j\in N$, $a_i a_j = a_j a_i$. Neka je $i<j$, tj. $j=i+k$ za neko $k\in N$; tada

$$a_i a_{i+k} = a_{i+1}^2 a_{i+k} = (a_{i+2})^4 a_{i+k} = (a_{i+3})^8 a_{i+k} = \ldots = (a_{i+k})^{2^k} a_{i+k}$$

$$= a_{i+k}(a_{i+k})^{2^k} = a_{i+k}(a_{i+k}^2)^{2^{k-1}} = a_{i+k}(a_{i+k-1})^{2^{k-1}} = \ldots = a_{i+k} a_i .$$

Dakle, dovoljno je dokazati rešivost problema reči za G_Π. Slično gornjem izvodjenju, lako se pokazuje da je za proizvoljni izraz $w(a_{i_1}^{\alpha_1} a_{i_2}^{\alpha_2} \ldots a_{i_k}^{\alpha_k})$ iz Π, gde je $i_1 < i_2 < \ldots < i_k$, $\alpha_i \in Z\setminus\{0\}$, ispunjeno:

$$w \underset{\Pi}{\sim} a_{i_k}^{\beta} \quad \text{za neki } \beta\in Z .$$

Koristeći strukturne jednakosti iz Π, ako je β paran broj, tada je $w \underset{\Pi}{\sim} a_1^{\nu}$ (za neki $\nu\in Z$) ili je $w \underset{\Pi}{\sim} a_{i_j}^{\mu}$ (za neki neparan broj μ; $j<k$). Dakle

$$\{a_1^{\nu} \mid \nu\in Z\} \cup \{a_i^{\mu} \mid i>1 \wedge \mu\in 2Z+1\}$$

je skup markera; nalaženjem odgovarajućeg homomorfizma lako se pokazuje njihova neekvivalentnost. Odavde sledi rešivost PR .

3.13. Dokazati da rekurzivno predstavljiva prosta grupa ima rešiv problem reči[1]:

Rešenje: Neka su $x_1,\ldots,x_n$ generatori grupe G_Π. Tada:

1° $w=1$ u G_Π ako se $w=1$ javlja na listi posledica od $\Pi = \langle A ; R\rangle$.

2° $w\neq 1$ u G_Π ako se na listi posledica od $\Pi_w = \langle A ; R\cup\{w=1\}\rangle$ javljaju sve jednakosti $x_1=1,\ldots,x_n=1$.

Jedan od ova dva slučaja mora da nastupi, jer je G_Π prosta grupa.

3.14. Ako su grupe G_1 i G_2 sa rešivim problemom reči (konjugacije), dokazati da grupa $G_1 \times G_2$ ima rešiv problem reči (konjugacije).

Rešenje: Neka je $\Pi_1 = \langle A ; R\rangle$, $\Pi_2 = \langle B ; Q\rangle$, $G_{\Pi_1} \simeq G_1$, $G_{\Pi_2} \simeq G_2$; tada je grupa $G_1 \times G_2$ sa postavkom $\Pi = \langle A,B ; R,Q,\{[a\ b^1] = 1 \mid a\in A,\ b\in B\}\rangle$.
Svaki izraz koji predstavlja element grupe $G_1 \times G_2$ ekvivalentan je izrazu $w_1 w_2$, gde je $w_1\in\Pi_1$, $w_2\in\Pi_2$. Kako je

$$\Pi \vdash\!\!\!- w_1 w_2 = 1 \quad \text{akko} \quad (\Pi_1 \vdash\!\!\!- w_1 = 1 \ \text{ i } \ \Pi_2 \vdash\!\!\!- w_2 = 1),$$

znajući algoritme $\mathcal{A}_1$ i $\mathcal{A}_2$ koji rešavaju PR redom za G_1 i G_2, lako je konstruisati algoritam $\mathcal{A}$ koji taj problem rešava i za grupu $G_1 \times G_2$.
Slično za problem konjugacije.

---

[1] Rezultat A.V.Kuznecova .

3.15. Neka su G_1 i G_2 konačno generisane grupe. Dokazati:

a) Ako je problem reči rešiv za G_1 i G_2, rešiv je i za grupu $G_1 * G_2$;

b) Ako je problem konjugacije rešiv za G_1 i G_2, rešiv je i za $G_1 * G_2$.

Rešenje: a) Neka su $G_1 = \langle a_1,\ldots,a_n; R_1,\ldots\rangle$, $G_2 = \langle b_1,\ldots,b_m; S_1,\ldots\rangle$ *grupe, za koje postoje algoritmi* $\mathcal{A}_1$ *i* $\mathcal{A}_2$ *kojima se za proizvoljne izraze redom nad* $L\cup\{a_1,\ldots,a_n\}$ *i* $L\cup\{b_1,\ldots,b_m\}$ *utvrdjuje da li su oni ekvivalentni 1 ili ne.*

Proizvoljni element w grupe $G_1 * G_2 = \langle a_1,\ldots,a_n,b_1,\ldots,b_m; R_1,\ldots,S_1,\ldots\rangle$ *se jedinstveno zapisuje u svedenom obliku :* $w=g_1\ldots g_k$. *Kako* g_i *i* g_{i+1} *nisu oba iz* G_1 *ili iz* G_2 , *i kako u predstavljanju za* $G_1 * G_2$ *nema strukturnih jednakosti koje povezuju izraze nad* $\{a_1,\ldots,a_n\}$ *i* $\{b_1,\ldots,b_m\}$, *to je*

$$(\Pi \vdash\!\!\!- w=1) \iff (\Pi_1 \vdash\!\!\!- g_1=1 \wedge \Pi_2 \vdash\!\!\!- g_2=1 \wedge \ldots \wedge \Pi_k \vdash\!\!\!- g_k=1)$$

gde je Π *predstavljanje grupe* $G_1 * G_2$, *a* Π_i *je predstavljanje grupe* G_{j_i} *kojoj pripada element* g_i $(i=1,\ldots,k\ ;\ j_i=1,2)$.

Dakle, pomoću algoritama $\mathcal{A}_1$ *i* $\mathcal{A}_2$ *lako se konstruiše algoritam* $\mathcal{A}$ *kojim se za svako* $w\in G_1 * G_2$ *utvrdjuje da li je* $\Pi \vdash\!\!\!- w=1$ *ili ne.*

b) Neka su $\mathcal{B}_1$ *i* $\mathcal{B}_2$ *algoritmi kojima se rešavaju problemi konjugacije redom kod grupa* G_1 *i* G_2. *Kao kod slobodnih grupa (v.zad. 3.6.), lako se dokazuje da je proizvoljni* $w\in G_1 * G_2$ *konjugovan elementu* $w^*\in G_1 * G_2$ *koji ima jedinstveni neskrativi zapis oblika*

$$w^* = g_1 g_2 \ldots g_k\ , \quad g_1 \text{ i } g_k \text{ nisu oba u } G_1 \text{ ili oba u } G_2 \qquad (\theta)$$

Pri tom je prelaz sa w na w^* *efektivan.*

Konstruišimo sada algoritam $\mathcal{B}$ *kojim se za proizvoljne* $u=u_1u_2\ldots u_i$ *i* $v=v_1v_2\ldots v_j$ *sa svojstvom* (θ) *ispituje da li je* $u \overset{c}{\sim} v$ *ili nije.*

Ako je $u=1$ *i* $u \overset{c}{\sim} v$, *tada je* $v=1$. *Odnosno, ako je* $u=1$ *(što se utvrdjuje pomoću* $\mathcal{B}_1$*), treba ispitati da li je* $v=1$ *(pomoću* $\mathcal{B}_2$*) ili ne.*

Ako je, dalje, $u=u_1$ *i* u_1 *pripada recimo* G_1, *i ako je* $u \overset{c}{\sim} v$, *tada postoji* $r=r_1\ldots r_s$ *tako da*

$$v = r_s^{-1}\ldots r_1^{-1} u_1 r_1 \ldots r_s \qquad (1)$$

Po pretpostavci, v je sa svojstvom (θ), *pa je izraz sa desne strane jednakosti (1) skrativ. Dakle,* $r_1\in G_1$, *tj.* $r_1^{-1}u_1r_1=u_1^*$, $u_1^*\in G_1$; *slično, dalje*

$$r_2^{-1}u_1^*r_2=u_2^*\ ,\ u_2^*\in G_1\ ,\ldots,\ \text{itd.}\quad v=r_s^{-1}u_{s-1}^*r_s=u_s^*\ ,\ u_s^*\in G_1\ .$$

Prema tome, ako je $u=u_1$, *tada treba proveriti (pomoću* $\mathcal{B}_1$*) da li je* $v \overset{c}{\sim} u_1$.

Neka je, najzad $u=u_1\ldots u_i$ $(i>1)$.

Kao kod slobodnih grupa, dokazujemo

(T1): $u \overset{c}{\sim} v \iff$ *(u se dobija cikličnom permutacijom iz v)* .

(Dokaz indukcijom po dužini d(r) izraza za koji je $u=r^{-1}vr$).

Kako je relacija sa desne strane ekvivalencije iz (T1) efektivno proverljiva (jer su G_1 i G_2 sa rešivim PR), to je problem konjugovanosti za $G_1 * G_2$ rešiv.

3.16. Dokazati da postoji konačno predstavljiva grupa G sa nerešivim problenom reči.

Rešenje: Dokaz se zasniva na teoremi 3.6. Higman-a i teoremi 3.3. o egzistenciji nerekurzivnog rekurzivno prebrojivog skupa T.

Neka je f(x) rekurzivna funkcija za koju je $\{f(n) \mid n\in N\} = T$, i neka je

$$G' = \langle x,y,u,v;\ \{x^{-f(n)}yx^{f(n)}=u^{-f(n)}vu^{f(n)} \mid n\in N\}\rangle .$$

Kako je G' rekurzivno predstavljiva grupa, ona se može potopiti u konačno predstavljivu grupu G. Problem reči za G' je rešiv ako se za proizvoljna dva izraza w_1 i w_2 može utvrditi da li je $\vdash_{G'} w_1=w_2$. No tada se to može utvrditi i za izraze oblika $x^{-k}yx^k$ i $u^{-k}vu^k$. Medjutim,

$$\vdash_{G'} x^{-k}yx^k=u^{-k}vu^k \iff (\exists m\in N)f(m)=k \iff k\in T$$

Kako je T nerekurzivan skup, to je PR nerešiv u G'. Stoga je nerešiv i u nadgrupi G .

3.17. Neka je G proizvoljna k.p. grupa. Dokazati da je skup svih prezentacija grupe G nerekurzivan [1] .

Rešenje: Neka je $\mathcal{P}$ skup svih konačnih prezentacija i

$$\mathcal{P}_G = \{\Pi \mid \Pi\in\mathcal{P} \wedge G_\Pi \simeq G\} .$$

Dalje, neka je G data jednom svojom postavkom $\Pi_1 = \langle A_1 ; R_1\rangle$. Ako je $\Pi = \langle A ; R\rangle$ proizvoljna postavka iz $\mathcal{P}$, konstruišimo $\Pi' = \langle A_1 \cup A ; R_1 \cup R\rangle$, tj. grupu $G_{\Pi'} \simeq G * G_\Pi$. Kako je, prema zad. 11.2.23.

$$rang\ G_{\Pi'} = rang\ G + rang\ G_\Pi$$

to je

$$G_{\Pi'} \simeq G \iff G_\Pi \simeq \{1\} .$$

Dakle, ako postoji algoritam kojim se za svaku prezentaciju Π' utvrdjuje da li je $\Pi' \in \mathcal{P}_G$ (tj. $G_{\Pi'} \simeq G$), tada se za proizvoljnu prezentaciju Π može utvrditi da li je $G_\Pi \simeq \{1\}$, suprotno teoremi 3.12.

---

[1] Rezultat M.Rabin-a

13. A D D E N D U M

Teorija grupa ima primene u različitim oblastima matematike. Mi smo se ovde ograničili na dva slučaja: Teoriju brojeva i Teoriju polja. U prvom slučaju navodimo i neke rezultate teorije brojeva koje smo dosada slobodno koristili.

13.1. BROJEVI

Izmedju ostalog, u ovoj knjizi koriste se neka elementarna svojstva prirodnih i celih brojeva. Kroz sledeće definicije, primere, teoreme i zadatke dajemo pregled tih osobina, ali isto tako i tvrdjenja koja se mogu dobiti kao neposredne posledice odredjenih teorema teorije grupa.

Struktura prirodnih brojeva je struktura $\underline{N}=(N,+,\cdot,\leqslant,0,1)$ gde je $N=\{0,1,2,...\}$ skup prirodnih brojeva a $+$, $\cdot$ uobičajene operacije sabiranja i množenja prirodnih brojeva. Obe operacije zadovoljavaju komutativni i asocijativni zakon, dok je operacija $\cdot$ distributivna prema $+$. Element 0 je neutralan za sabiranje a 1 je neutralni element za $\cdot$. Takodje važe sledeći zakoni skraćivanja (kancelacije):

$$x+z = y+z \Rightarrow x=y, \quad \text{i za} \quad z\neq 0 \quad xz = yz \Rightarrow x=y.$$

Relacija $\leqslant$ je uobičajeno uredjenje prirodnih brojeva. Važi:

$$x\leqslant y \Leftrightarrow (\exists z\in N)\ y = x+z,\quad x\leqslant y \Rightarrow x+z \leqslant y+z,\quad x\leqslant y \rightarrow xz\leqslant yz.$$

Uredjenje $\leqslant$ zadovoljava sledeći princip najmanjeg elementa (tj. $(N,\leqslant)$ je dobro uredjenje):

(PN) Ako je $X\subseteq N$ i $X\neq\emptyset$ tada postoji najmanji element u skupu X.

Struktura celih brojeva je struktura $\underline{Z} = (Z,+,\cdot,\leqslant,0,1)$ gde je $Z = \{...,-2,-1,0,1,2,...\}$ skup celih brojeva, $+$ i $\cdot$ redom sabiranje i množenje celih brojeva i $\leqslant$ uredjenje celih brojeva. Važi:

$\underline{Z}$ je komutativan uredjen prsten sa jedinicom.

Dakle, $(Z,+,0)$ je komutativna grupa, $(Z,\cdot,1)$ komutativan monoid i $\underline{Z}$ važi $x(y+z) = x\cdot y + x\cdot z$. Takodje, $(Z,\leqslant)$ je linearno uredjenje saglasno sa operacijama $+$ i $\cdot$. Prsten $\underline{Z}$ ima i ova svojstva:

$\underline{Z}$ je domen tj. $(\forall x,y\in Z)(xy=0 \Rightarrow x=0 \vee y=0)$.

$(\forall x\in Z)(x\in N \vee -x\in N)$. Dakle, za $x\in Z$ važi $|x|\in N$.

Definicija 1.1. *Neka su* $a,b \in Z$. *Tada* $a|b \Leftrightarrow (\exists z \in Z)\ b=az$.

Formulu a|b čitamo "a deli b". Ako je $a \neq 0$ ili $b \neq 0$, najveći zajednički delilac brojeva a,b je najveći prirodan broj koji deli a i b. Najveći zajednički delilac brojeva a,b označava se sa (a,b) ili NZD(a,b). Najmanji zajednički sadržilac brojeva a,b je najmanji prirodan broj deljiv sa a,b. Ovaj broj se označava sa NZS(a,b). Prirodan broj $p>1$ je prost broj ako $\forall x \in N$ $(x|p \Rightarrow x=1 \vee x=p)$.

Teorema 1.2. *Neka su* $a,b \in Z$, $b \neq 0$. *Tada postoje jedinstveni* $q \in Z$ $r \in N$ *takvi da* $a=bq+r$, $0 \leq r < |b|$.

Brojevi $a,b \in Z$ su uzajamno prosti ukoliko NZD(a,b)=1. Sledeća teorema daje potreban i dovoljan uslov da brojevi a,b budu uzajamno prosti:

Teorema 1.3. *Neka su* $a,b \in Z$. *Tada* $(\exists x,y \in Z)\ ax+by=1 \Leftrightarrow NZD(a,b)=1$.

Definicija 1.4. *Neka su* $a,b \in Z$, $n \in N-\{0\}$. *Tada* $a=b(\mathrm{mod}n) \Leftrightarrow n|a-b$. *Ukoliko je* $a=b(\mathrm{mod}n)$ *kažemo da je a kongruentno b modulo n. Takodje se koristi oznaka* $a \equiv_n b$.

Teorema 1.5. *Neka je* $n \in N-\{0\}$. *Tada je* $\equiv_n$ *kongruencija prstena celih brojeva, tj.* $\equiv_n$ *je relacija ekvivalencije i* $\equiv_n$ *saglasna je sa operacijama* $+, \cdot$ *u* $\underline{Z}$.

U najvažnije metode dokazivanja u matematici spada dokazivanje matematičkom indukcijom. Neka je F(n) matematička formula gde je domen promenljive n skup prirodnih brojeva.

Teorema matematičke indukcije. ***Ako su formule*** $F(0)$ ***i*** $(\forall n \in N)(F(n) \Rightarrow F(n+1))$ ***tačne, tada je i formula*** $(\forall n)F(n)$ ***tačna.***

Ukoliko je dokaz za $(\forall n)F(n)$ izveden primenom teoreme matematičke indukcije, kažemo da je $\forall n$ F(n) dokazana matematičkom indukcijom.

Teorema potpune indukcije. ***Ako za svaki prirodan broj*** m ***važi*** $((\forall n<m)F(n)) \Rightarrow F(m)$, ***tada je formula*** $\forall n$ $F(n)$ ***tačna.***

Ukoliko je dokaz za $\forall n$ F(n) izveden primenom teoreme potpune indukcije, kažemo da je $\forall n$ F(n) dokazana potpunom indukcijom.

Zadaci

1.1. Dokazati Teoremu 1.2.

Rešenje: Neka su $a,b \in N$, $b \neq 0$ i $X=\{x \in N : bx>a\}$. $X \neq \emptyset$ budući da $a+1 \in X$, te prema principu najmanjeg broja postoji $m \in N$, m je minimum skupa X. Kako je $m>1$ to je $q=m-1$ prirodan broj i $bq \leq a$. Otuda postoji $r \in N$ da $a=bq+r$. Ako je $r \geq b$ onda za neki $r' \geq 0$ $r=b+r'$, odakle $a=b(q+1)+r'$ tj. $b(q+1) \leq a$, pa $bm \leq a$, suprotno izboru broja m. Dakle, $r<b$. Dokazujemo da su brojevi q,r sa datim svojstvom jedinstveni. Neka su $q',r' \in N$ takvi da $a=bq'+r'$, $0 \leq r'<b$. Prema jednakosti $a=bq+r$ tada sledi $b(q-q')=r'-r$, odakle $b \mid r'-r$. Kako je $|r'-r|<b$ onda $r'-r=0$, tj. $r'=r$.

Neka su a,b ma koji celi brojevi, $b \neq 0$. Prema prethodnom postoje jedinstveni q_o, r_o takvi da $|a| = |b| q_o + r_o$, $r_o < |b|$. Tada $a=bq_o^* + r_o^*$ gde $q_o^* \in \{q_o, -q_o\}$, $r_o^* \in \{r_o, -r_o\}$. Ako je $r_o^* = r_o$ tada $q=q_o^*$, $r=r_o^*$. Ako je $r_o^* < 0$ i, recimo, $b>0$ tada $a=b(q_o^*-1)+b-r_o$, dakle $q=q_o^*-1$, $r=b-r_o^*$.

1.2. Dokazati da za sve $a,b \in Z - \{0\}$ postoji: a) NZS(a,b)
b) NZD(a,b)

Rešenje: Bez gubljenja opštosti možemo pretpostaviti $a,b \in N$, $a,b \neq 0$, s obzirom da se sličan dokaz izvodi za $|a|$, $|b|$.
a) Neka je $X=\{x \in N : a \mid x, \ b \mid x\}$. $X \neq \emptyset$ jer $ab \in X$, pa prema principu najmanjeg broja postoji minimum skupa X. Neka je $m=\min X$. Očigledno m je najmanji sadržalac brojeva a,b.
b) Neka je m najmanji zajednički sadržalac brojeva a,b. Dokazujemo
1^o Ako $a \mid c$ i $b \mid c$ tada $m \mid c$.

Neka je $c \in N$, $a \mid c$, $b \mid c$. Tada $m \leq c$ i prema Teoremi 1. postoje $q,r \in N$ takvi da $c=mq+r$, $0 \leq r<m$. Kako $a \mid c$, $a \mid m$ to onda $a \mid r$. Slično $b \mid r$. Otuda, prema izboru broja m sledi $m \leq r$ ili $r=0$. Kako je $r<m$ to $r=0$, dakle, $c=mq$ pa 1^o važi.

Dalje, kako $a \mid ab$, $b \mid ab$, prema prethodnom $m \mid ab$. Neka je
2^o $d=ab/m$.

Dokazujemo da je d najveći zajednički delilac brojeva a,b. Iz 2^o sledi $a=(m/b)d$, dakle $d \mid a$. Slično $d \mid b$. Dalje, neka $c \mid a$, $c \mid b$. Tada za neke $x,y \in N$ $a=cx$, $b=cy$. Otuda $cxy=ay=bx$ tj. $a \mid cxy$, $b \mid cxy$ pa prema 1^o $m \mid cxy$. Kako je $ab=c^2xy$ sledi

ab/m = (cxy/m)c, tj. d=(cxy/m)c pa c|d. Otuda d je najveći zajednički delilac brojeva a,b.

Napomena: Prema prethodnom važi NZS(a,b)NZD(a,b)=ab.

Postojanje NZD(a,b) može se i ovako utvrditi: Skup X=
={x∈N : x|a, x|b} je konačan te ima najveći element d.

1.3. Iz PN izvesti Teoremu matematičke indukcije.

Rešenje: Neka je F(0) i ∀n(F(n) ⇒ F(n+1)). Pretpostavimo da nije ∀nF(n). Tada je skup X ={n∈N : ⁊F(n)} neprazan pa prema principu najmanjeg broja postoji najmanji prirodan broj m, m∈X. Kako je F(0) to m>0. Neka je q=m-1. Prema izboru broja m F(q) važi. Kako ∀n(F(n) ⇒ F(n+1)) to F(q)⇒F(q+1), te po modus ponensu F(q+1) tj. F(m), kontradikcija.

1.4. Dokazati Teoremu potpune indukcije na osnovu: a) PN,
b) Teoreme matematičke indukcije.

Rešenje: a) Neka za svaki m∈ N važi ((∀n<m)F(n))⇒F(m). Pretpostavimo nije ∀nF(n). Tada skup X={n∈N:F(n)} nije prazan te prema principu najmanjeg broja postoji najmanji prirodan broj m takav da ⁊F(m). Iz ((∀n<m)F(n)⇒F(m) kontrapozicijom sledi ⁊F(m)⇒(∃n<m)⁊F(n), te po modus ponensu ∃n<m ⁊F(n). Dakle za neki prirodan broj n<m važi ⁊F(n), suprotno izboru broja m.

b) Neka je F(x) formula, a x promenljiva čiji je domen skup prirodnih brojeva. Dokazujemo

(PI) $\forall x((\forall y<x)F(y) \Rightarrow F(x)) \Rightarrow \forall x F(x)$

na osnovu (F'(x) je proizvoljna formula):

(I) $F'(0) \wedge \forall x(F'(x) \Rightarrow F'(x+1)) \Rightarrow \forall x F'(x)$

i elementarnih svojstava aritmetičkih operacija i uredjenja skupa N. Neka je G(x) formula (∀y<x)F(y) i H(x) formula (∀y<x)F(y) ⇒ F(x). Tada

1^{o} $G(0)$

2^{o} $G(x+1) \Leftrightarrow G(x) \wedge F(x)$

3^{o} $H(x) \Rightarrow (G(x) \Rightarrow F(x))$.

Iz 2^{o} *i* 3^{o} *sledi*

4^{o} $H(x) \Rightarrow (G(x) \Rightarrow G(x+1))$, *odakle*

5^{o} $\forall x H(x) \Rightarrow \forall x(G(x) \Rightarrow G(x+1))$.

Prema 1^{o}, 5^{o} *primenom sheme (I) na formulu G(x) sledi (PI).*

1.5. Neka su $a,b\in Z$. Tada: a) $(\exists x,y\in Z)ax + by = 1 \Leftrightarrow (a,b) = 1$, v.Teoremu 1.3. b) $(\exists x,y\in Z)ax + by = (a,b)$.

Rešenje: ($\Rightarrow$) Neka za neke $x,y\in Z$ važi $ax+by=1$. Ako je $d=(a,b)$ tada $d|a$, $d|b$, te na osnovu navedene jednakosti $d|1$, tj. $d=1$. ($\Leftarrow$) Prethodno dokazujemo sledeće tvrdjenje:

1^o Ako $(a,b)=1$ tada za sve $x,y\in Z$ $ax=by$ povlači $a|y$, $b|x$.

Dokaz za 1^o: Neka $(a,b)=1$ i $ax=by$. Tada $a|ax$, $b|ax$, te prema z. 1.2. $c|ax$, gde $c=NZS(a,b)$. Dalje, prema istom zadatku $c\cdot(a,b)=a\cdot b$, pa kako je $(a,b)=1$ to $c=ab$, stoga $ab|ax$. Dakle, za neki $m\in Z$ $ax=abm$, te $abm=by$, tj. $am=y$, pa $a|y$. Slično se dokazuje da $b|x$.

Kao neposrednu posledicu prethodnog za $a,b,c,d\in Z$ imamo:

2^o Ako je $(a,b)=1$ i $ac=ad(modb)$ tada $c=d(modb)$. Zaista, ako je $(a,b)=1$ i $ac=ad(modb)$ tada za neki $x\in Z$ $a(c-d)=bx$ pa prema 1^o $b|c-d$ tj. $c=d(modb)$.

Neka su $a,b\in Z$, $(a,b)=1$. Ako je $|a|=1$ ili $|b|=1$ tvrdjenje je trivijalno, zato pretpostavimo $|a|,|b|\neq 1$. Bez gubljenja opštosti možemo pretpostaviti $a,b\in N$. Neka je $F:N\rightarrow \{0,1,\ldots,b-1\}$, $F(x)=y \Leftrightarrow \exists q(x=qb+y)$. Prema Teoremi 1.2. funkcija F je dobro definisana. Kako je $a>1$, skup $X = \{1,a,a^2,\ldots\}$ je beskonačan dok je $F(X)\subseteq\{0,1,\ldots,b-1\}$, dakle konačan. Otuda za neke m,n, $m>n$ $F(a^m) = F(a^n)$, tj. $a^m=a^n$ $modb$. Prema 2^o sledi $a^{m-1}=a^{n-1}$ $modb,\ldots,$ $a^{m-n}=1$ $modb$, tj. za $k=m-n$ $a^k=1$ $modb$ i $k>0$. Tada za neki $z\in Z$ $a\cdot a^{k-1}-1= bz$, tj. $ax + by = 1$ za $x=a^{k-1}$, $y=-z$.

Napomena: Prema prethodnom za diofantovsku jednačinu $ax+by=1$ postoji rešenje (x,y) u kojem $x=a^k$ za neki $k\in N$. Može se uzeti $k=\varphi(b)-1$ gde je $\varphi(b)$ Eulerova funkcija, sa obzirom da je $(A,\cdot_b)$ grupa, $A=\{x\in N: x<b, (x,b)=1\}$. Red ove grupe je $\varphi(b)$ i $a\in A$, te prema Langrangeovoj teoremi $a^{\varphi(b)}=1$ gde je stepenovanje u smislu operacije $\cdot b$. Otuda $a^{\varphi(b)}=1$ $modb$, dakle za neki $y\in Z$ $a\cdot a^{\varphi(b)-1}+by=1$.

b) Svesti na slučaj pod (a) uzimajući $a'=a/(a,b)$, $b'=b/(a,b)$.

1.6. Neka su $a,b,c\in Z$. Tada: a) $(a,b)=1\wedge(a,c)=1\Rightarrow(a,bc)=1$,
b) $(a,b)=1\Rightarrow(\forall n\in N)\ (a,b^n)=1$, c) $(a,b)=1\ \ a|bc\Rightarrow a|c$,
d) $a|c\wedge b|c\wedge(a,b)=1\Rightarrow ab|c$.

Rešenje: a) Neka $(a,b)=1$, $(a,c)=1$. Tada prema Teoremi 2.3.

za neke $x_1, x_2, y_1, y_2 \in Z$ $ax_1+by_1=1$, $ax_2+cy_2=1$ *odakle* $bcy_1y_2 = (1-ax_1)(1-ax_2)$ *tj.* $a(x_1+x_2-ax_1x_2)+bcy_1y_2=1$, *dakle jednačina* $ax+bcy=1$ *ima rešenje u Z. Otuda prema Teoremi 1.3.* $(a,bc)=1$.

b) Prema (a) indukcijom po n.

c) Neka $(a,b)=1$ *i* $a \mid bc$. *Prema Teoremi 1.3. za neke* $x,y \in Z$ $ax+by=1$, *te* $c=acx+bcy$. *Po pretpostavci a deli desnu stranu ove jednakosti pa* $a \mid c$.

d) Neka $(a,b)=1$, $a \mid c$, $b \mid c$. *Tada prema rešenju z. 1.2.* $m \mid c$, *gde* $m=NZS(a,b)$. *Prema istom zadatku* $m=ab/(a,b)$, *te* $m=ab$. *Otuda* $ab \mid c$.

1.7. Neka je p prost broj i $a_1, a_2, \ldots, a_n \in Z$. Tada:

a) $p \mid a_1a_2\ldots a_n \Rightarrow p \mid a_1 \vee \ldots \vee p \mid a_n$,

b) $(\forall n \geq 1)\ (p \mid a^n \Rightarrow p \mid a)$.

Rešenje: a) Neka je p prost broj i $a_1, \ldots, a_n \in Z$. *Tada p nije uzajamno prost sa* a_i *akko* $p \mid a_i$, *tj. p je uzajamno prost sa* a_i *akko* $\neg p \mid a_i$. *Pretpostavimo* $p \nmid a_1, \ldots, a_n$. *Tada je p uzajamno prost sa* $a_1, \ldots, a_n$ *te prema z. 1.6. p je uzajamno prost sa* $a_1a_2\ldots a_n$, *dakle* $p \mid a_1a_2\ldots a_n$.

b) Uzeti u (a) $a_1=\ldots=a_n=a$.

1.8. (Teorema o predstavljanju prirodnih brojeva preko prostih) Neka je $n \in N$, $n>2$. Tada postoje jedinstveni prosti brojevi $p_1<p_2<\ldots<p_k$ i jedinstveni pozitivni prirodni brojevi $u_1, \ldots, u_k$ takvi da $n=p_1^{u_1} \cdot p_2^{u_2} \cdot \ldots \cdot p_k^{u_k}$.

Rešenje: Potpunom indukcijom dokazujemo da je svaki $m \in N$ *proizvod prostih brojeva. Neka je* $m>1$ *i pretpostavimo tvrdjenje za sve* $n<m$. *Ako je m prost broj dokaz je završen. Pretpostavimo da je m složen, dakle za neke* $n,k \in N$ $m=nk$ *i* $k,n \neq m$. *Dakle* $k,n<m$ *te po induktivnoj hipotezi k,n su proizvodi prostih brojeva, dakle i m je proizvod prostih brojeva.*

Neka je $X=\{p: p \text{ je prost broj}, p \mid n\}$, $n \in N$. *Očigledno X je konačan* $(|X| \leq n)$, *te se može uzeti* $X=\{p_1, \ldots, p_k\}$ *i* $p_1<\ldots<p_k$. *Neka je za* $p \in X$ α *najveći prirodan broj takav da* $p^{\alpha} \mid n$. *Prema z. 1.6. za* $i \neq j$ $(p_i^{\alpha_i}, p_j^{\alpha_j})=1$, *te kako* $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k} \mid n$ *sledi* $p_1^{\alpha_1}\ldots p_k^{\alpha_k} \mid n$. *Neka je* $m \in N$ *takav da* $n=mp_1^{\alpha_1}\ldots p_k^{\alpha_k}$. *Ako*

je $m>1$ tada postoji prost broj q, $q|m$. Tada $q|n$, dakle $q\in X$ tj. za neki $i\leq k$ $q=p_i$. Tada $p_i^{\alpha+1}|n$, suprotno pretpostavci o broju α_i. Dakle $m=1$. Pretpostavimo $n=q_1^{\beta_1}\dots q_r^{\beta_r}$, q_i su prosti brojevi, $q_1<\dots<q_r$. Tada prema definiciji skupa X $\{q_1,\dots,q_r\}\subseteq X$. S druge strane $p_i|n$ te $p_i|q_1^{\beta_1}\dots q_r^{\beta_r}$ pa prema z. 1.6. $p_i|q_j^{\beta_j}$ za neki j, dakle $p_i=q_j$. Otuda $X\subseteq\{q_1,\dots,q_r\}$, stoga $X=\{q_1,\dots,q_r\}$. Prema tome $r=k$ pa iz uslova monotonosti nizova p_i, q_i sledi $p_1=q_1,\dots,p_k=q_k$. Dalje, prema definiciji brojeva α_i, $\beta_i\leq\alpha_i$. Kako je $n=p_1^{\beta_1}\dots p_k^{\beta_k}$ i $p_1^{\alpha_1}|n$, $(p_1^{\alpha_1},p_i^{\beta_i})=1$ za $i\neq1$, prema z.1.6. $p_1^{\alpha_1}|p_1^{\beta_1}$ tj. $p_1^{\beta_1}=xp_1^{\alpha_1}$ za neki $x\in N$. Sa obzirom na zakon kancelacije za množenje sledi $\alpha_1\leq\beta_1$, dakle $\alpha_1=\beta_1$.

1.9. Dokazati da je $(Z,|)$ parcijalno uredjenje. Kako se mogu interpretirati NZD(x,y), NZS(x,y)?

Rešenje: $NZD(x,y)=inf(x,y)$, $NZS(x,y)=sup(x,y)$, gde su inf i sup u smislu uredjenja $|$.

1.10. Dokazati Teoremu 1.5.

Rešenje: Relacija $\equiv_n$ je relacija ekvivalencije, dokažimo npr. tranzitivnost. Ako $x\equiv_n y$ i $y\equiv_n z$, tada $n|x-y$, $n|y-z$, odakle $n|(x-y)+(y-z)$, stoga $n|x-z$, tj. $x\equiv_n z$. Dalje, $\equiv_n$ saglasna je sa operacijom množenja: Ako $x_1\equiv_n y_1$, $x_2\equiv_n y_2$ tada $n|x_1-y_1$, $n|x_2-y_2$ te za neke $u,v\in Z$ $x_1-y_1=un$, $x_2-y_2=vn$. Otuda $x_1x_2=(y_1+un)(y_2+vn)$ tj. $x_1x_2-y_1y_2=n(uvn+uy_2+vy_1)$, dakle $n|x_1x_2-y_1y_2$ pa $x_1x_2\equiv_n y_1y_2$. /Slično se dokazuje da je $\equiv_n$ saglasna sa operacijom sabiranja.

1.11. Neka su $Z_n=\{0,1,\dots,n-1\}$, $+_n$, $\cdot_n$ redom sabiranje i množenje celih brojeva modulo n. Dokazati da je $\underline{Z}_n=(Z_n,+_n,\cdot_n,0,1)$ komutativan prsten sa jedinicom.

Rešenje: Prethodno dokazujemo

1° $\forall x,y,z\in\{0,1,\dots,n-1\}$ $(z=x\cdot_n y \Leftrightarrow z\equiv_n xy)$. Zaista, ako je $z=x\cdot_n y$ tada za neki $q\in Z$ $xy=qn+z$, dakle $xy\equiv_n z$. Sa druge strane ako je $z\equiv_n xy$ tada postoji $q\in Z$ takav da $xy=qn+z$. Kako je po pretpostavci $x,y,z\in\{0,1,\dots,n-1\}$, tj. $z<n$, to je po definiciji operacije $\cdot_n$ $z=x\cdot_n y$. Dalje važi

2° $a\equiv_n xu \wedge u\equiv_n yz \Rightarrow a\equiv_n xyz$. Zaista, neka je $a\equiv_n xu$, $u\equiv_n yz$. Prema Teoremi 1.5. $\equiv_n$ je kongruencija prstena celih brojeva, dakle saglasna je sa množenjem. Otuda iz $u\equiv_n yz$ sledi $xu\equiv_n x(yz)$, te prema tranzitivnosti relacije $\equiv_n$ sledi $a\equiv_n xyz$.

Prema z.2.2.2. $(\{0,1,\ldots,n-1\},+_n,0)$ je Abelova grupa. Dokazujemo asocijativnost operacije $\cdot_n$. Neka je $a=x\cdot_n(y\cdot_n z)$ $b=(x\cdot_n y)\cdot_n z$, $x,y,z,a,b\in\{0,1,\ldots,n-1\}$. Tada

$$a=x\cdot_n(y\cdot_n z) \Rightarrow \exists u(a=x\cdot_n u \wedge u=y\cdot_n z) \quad \text{prema } 1^{\circ}$$
$$\Rightarrow \exists u(a\equiv_n xu \wedge u\equiv_n yz) \quad \text{prema } 2^{\circ}$$
$$\Rightarrow \exists u(a\equiv_n x(yz))$$
$$\Rightarrow a\equiv_n xyz.$$

Dakle, $a\equiv_n xyz$. Slično $b=x\cdot_n(y\cdot_n z)\Rightarrow b\equiv_n xyz$, te $b\equiv_n xyz$. Prema prethodnom $a\equiv_n b$, tj. $n\,|\,a-b$. Kako $|a-b|<n$, to $a-b=0$, tj. $a=b$. Na sličan način se dokazuje distributivnost operacije $\cdot_n$ prema $+_n$. Neka su $x,y,z,a,b\in\{0,1,\ldots,n-1\}$, $a=x\cdot_n(y+_n z)$, $b=(x\cdot_n y)+_n(x\cdot_n z)$. Tada

$$a=x\cdot_n(y+_n z) \Rightarrow \exists u(a=x\cdot_n u \wedge u=y+_n z)$$
$$\Rightarrow \exists u(a\equiv_n xu \quad u\equiv_n y+z)$$
$$\Rightarrow a\equiv_n x(y+z)$$

dakle $a\equiv_n x(y+1)$. Slično $b=_n xy+xz$, stoga $a\equiv_n b$ te $n\,|\,a-b$ pa $a=b$. Na sličan način se dokazuje da u $\underline{Z}_n$ važe i ostali zakoni.

1.12. Dokazati $Z/\equiv_n = Z_n$.

Rešenje: Neka je $F:\underline{Z}_n\to\underline{Z}/\equiv_n$ preslikavanje definisano sa $F(x)=x/\sim$ gde $x/\sim=\{y\in Z: y\equiv_n x\}$, tj. $x/\sim$ je klasa ekvivalencije elementa x u odnosu na $\equiv_n$. F je 1-1: Neka $F(x)=F(y)$. Dakle $x/\sim=y/\sim$, te $x\equiv_n y$, tj. $n\,|\,x-y$. Kako za $x,y\in Z_n$ $|x-y|<n$, to onda $x-y=0$. F je <u>na</u>: Neka je $a\in Z$ i $0\le x<n$ tako da $a=qn+x$, $q\in Z$. Tada $a\equiv_n x$, tj. $a/\sim=x/\sim$. Dakle $F(x)=a/\sim$, pa je F <u>na</u>.

F je homomorfizam: Dokazujemo da je $F(x+_n y)=x/\sim\,\dot{+}\,y/\sim$, gde je $\dot{+}$ operacija prstena $Z/\equiv_n$. Neka je $u=x+_n y$, $x,y,u\in\{0,1,\ldots,n-1\}$. Tada $u\equiv_n x+y$, te $u/\sim=(x+y)/\sim$. Kako je $x/\sim\,\dot{+}\,y/\sim=(x+y)/\sim$ to $u/\sim=x/\sim\,\dot{+}\,y/\sim$. Dakle $F(x+_n y)=x/\sim\,\dot{+}\,y/\sim$.

Slično se dokazuje $F(x\cdot_n y)=x/\sim\,\dot{\cdot}\,y/\sim$, gde je $\dot{\cdot}$ operacija množenja prstena $Z/\equiv_n$.

1.13. Dokazati Kinesku Teoremu o ostacima: Neka su $c_1,\dots,c_n \in Z$ takvi da za $i\neq j$ $(c_i,c_j)=1$. Tada za sve $a_1,\dots,a_n \in Z$ postoji $x\in Z$ takav da $x=a_i \pmod{c_i}$, $i=1,\dots,n$.

Rešenje: Neka su c_i, a_i kao u iskazu teoreme. Tada $(c_1, c_2c_3 \dots c_n)=1$, $(c_2, c_1c_3 \dots c_n)=1$, $\dots$, $(c_n, c_1c_2 \dots \dots c_{n-1})=1$. Otuda prema Teoremi 1.3 postoje x_i, y_i takvi da $x_1c_1 + y_1c_2c_3\dots c_n=1$, $x_2c_2 + y_2c_1c_3\dots c_n=1,\dots,x_nc_n + + y_nc_1c_2\dots c_{n-1}=1$. Dakle,

$$x_1c_1a_1 + y_1a_1c_2c_3\dots c_n=a_1,\dots,x_nc_na_n + y_na_nc_1c_2\dots c_{n-1}=a_n .$$

Otuda za odgovarajuće x_i', y_i'

$$x_1'c_2c_3\dots c_n = y_1'c_1 + a_1,\dots,x_n'c_1c_2\dots c_{n-1}=y_n'c_n+a_n .$$

Neka je $x=x_1'c_2c_3\dots c_n + c_n+x_2'c_1c_3\dots c_n+x_n'c_1c_2\dots c_{n-1}$. Tada

$$x=x_1'c_2c_3\dots c_n \bmod c_1 = (y_1'c_1+a_1) \bmod c_1 = a_1 \bmod c_1.$$

Slično za sve $i\leqslant n$ $x=a_i \bmod c_i$.

1.14. Neka je $n=p_1^{u_1}\dots p_k^{u_k}$ dekompozicija prirodnog broja n na proste faktore. Dokazati $Z_n \cong Z_{p_1^{u_1}}x\dots xZ_{p_k^{u_k}}$.

Rešenje: Neka je $F:\underline{Z}_{p_1^{u_1}}x\dots x\underline{Z}_{p_k^{u_k}} \to \underline{Z}_n$ definisano sa $x=F(x_1,\dots,x_k)$ akko x je najmanji prirodan broj takav da $x=x_1 \bmod p_1^{u_1}$, $\dots$, $x=x_k \bmod p_k^{u_k}$. Kako su $p_i^{u_i}$, $p_j^{u_j}$ uzajamno prosti za $i\neq j$, prema kineskoj Teoremi o ostacima F je dobro definisano preslikavanje. Dalje, ako je $z=x_i \bmod p_i^{u_i}$, $i=1,\dots,k$ tada prema Teoremi 1.3. postoji $x\geqslant 0$ takav da $x<n$ i $z=x \bmod n$. Otuda za neke $v, w_i \in Z$ $z-x_i=w_ip_i^{u_i}$, $z-x=vn$, te $x-x_i=w_ip_i^{u_i}-vn$, dakle $x=x_i \bmod p_i^{u_i}$. Prema tome $F(x_1,\dots,x_n)\in Z_n$. Takodje

1^o F je <u>na</u>:

Zaista, za $m\in Z_n$ neka su $x_i=m \bmod p_i^{u_i}$, $0\leqslant x_i<p_i^{u_i}$. Tada $F(x_1,\dots,x_k)=m$.

2^o F je 1-1:

Sledi na osnovu $|Z_n|=|Z_{p_1^{u_1}}x\dots xZ_{p_k^{u_k}}|$.

3^o F je homomorfizam:

Neka je $F(x_1,\dots,x_k)=x$, $F(y_1,\dots,y_k)=y$, $z_i=x_i+y_i$, $F(z_1,\dots,z_k)=z$.

Tada $x=x_i \ mod p_i^u i$, $y=y_i \ mod p_i^u i$, *te* $x+y=(x_i+y_i) \ mod p_i^u i=z_i \ mod p_i^u i$, $i=1,\ldots,k$. *Kako je* $z=z_i mod p_i^u i$ *to* $x+y=z \ mod p_i^u i$, $i=1,\ldots,k$. *Za* $i\neq j$ $p_i^u i$, $p_j^u j$ *su uzajamno prosti, dakle,* $x+y=z \ mod p_1^u 1 \ldots p_k^u k$, *v.z. 1.6. tj.* $x+y=z \ mod n$, *pa* $z=x+_n y$, *odnosno* $F(x_1+y_1,\ldots,x_k+y_k)=F(x_1,\ldots,x_k)+_n F(y_1,\ldots,y_k)$. *Slično se dokazuje jednakost* $F(x_1y_1,\ldots,x_ky_k)=F(x_1,\ldots,x_k)\cdot_n F(y_1,\ldots,y_k)$. *Napominjemo da smo u prethodnom razmatranju pisali* $+$, $\cdot$ *umesto* $+_{p_i^u i}$, $\cdot_{p_i^u i}$.

1.15. Dokazati da je $\underline{Z}_n$ polje akko je n prost broj.

Rešenje: ($\Rightarrow$) *Neka je* $\underline{Z}_n$ *polje. Ako n nije prost broj tada za neke* $a,b\in N$ $n=ab$, $1<a$, $b<n$. *Tada* $a,b\in Z_n$ *i* $ab=0 \ mod n$, *tj.* $a\cdot_n b=0$. *Kako* $a,b\neq 0$, $\underline{Z}_n$ *ima, dakle, delitelje nule, suprotno pretpostavci da je* $\underline{Z}_n$ *polje.*

($\Leftarrow$) *Neka je* $a\in Z_n$, $a\neq 0$. *n je prost broj te* $(a,n)=1$, *dakle za neke* $x,y\in Z$ $ax+ny=1$. *Otuda* $ax=1 \ mod n$, *tj.* $a\cdot_n b=1$ *za* $b=x \ mod n$, $b\in Z_n$. *Prema prethodnom a ima inverzan.*

1.16. Neka je $k:Z\to Z/\equiv_n$ kanonski homomorfizam i $J=\ker(k)=\{x\in Z: k(x)=0\}$.
Dokazati: a) $J=nZ$, b) $(J,+,0)$ je grupa i $JZ\subseteq J$,
c) Neka je $J\subseteq Z$ koji zadovoljava uslove pod (b). Tada postoji $n\in N$ takav da $J=nZ$.

Rešenje: a) $k(x)=0$ *akko* $x=0 \ mod n$ *akko* $n|x$.
b) Neka su $j\in J$, $z\in Z$. *Tada* $k(j)=0$, *dakle* $k(jz)=k(j)k(z)=0\cdot k(z)=0$, *te* $jz\in J$. *Prema tome* $JZ\subseteq J$.
c) Neka J zadovoljava uslove pod (b). $J\neq\emptyset$ *jer* $0\in J$. *Ako je* $J=\{0\}$ *tada* $J=0Z$. *Neka postoji* $a\in J$, $a\neq 0$. *Tada J sadrži pozitivan broj jer* $x\in J \Rightarrow -x\in J$. *Prema principu najmanjeg broja J sadrži najmanji pozitivan prirodan broj n. Neka je* $z\in Z$. *Ako je* $z>0$ *tada* $nz=n+\ldots+n$ *(z puta), te* $nz\in J$. *Ako je* $z<0$ *tada* $nz=-w$, *gde* $w=n+\ldots+n$ *(-z puta), te* $nz\in J$ *jer je* $(J,+,0)$ *grupa. Očigledno* $0\cdot z\in J$.
Dakle $nZ\subseteq J$.

Neka je $j\in J$. *Prema Teoremi 1.2. postoji r,* $0\leq r<n$, *takav da za neki* $q\in Z$ $j=qn+r$. $(J,+,0)$ *je grupa,* $j,qn\in J$ *te* $j-qn\in J$, *dakle* $r\in J$. *Kako je* $0\leq r<n$ *prema izboru broja*

n sledi r=0. Dakle j=qn, tj. j∈nZ. Prema tome J⊆nZ, te kako je nZ⊆J sledi J=nz.

1.17. Dokazati da za svaki prost broj p postoji polje koje ima tačno p^2 elemenata.

Rešenje: Ako je p=2 tada je F=(F,+,.,0,1) polje, gde F={0,1,2,3} i

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Primetimo da u ovom polju jednačine $x^2+1=0$, $x^2+x+1=0$ imaju rešenje. Neka je p>2 prost broj i f:{1,2,...,p-1}→{1,2,...,p-1} definisano jednakošću $f(x)=x^2$. Tada f(1)=f(-1), dok 1≠-1 u $\underline{Z}_p$, dakle f nije 1-1, prema tome nije ni na. Dakle, za neki a∈{1,2,...,p-1} ∀x∈Z_p $x^2\neq a$. Neka je F skup svih linearnih izraza nad jezikom {+,}∪{0,1,...,p-1}∪{c}, c je novi simbol konstante, tj. F = {i+jc:0≤i,j≤p-1}. Tada je F=(F,+,·,0,1) polje, gde za u=i+jc, v=i'+j'c, $u+v=(i+_p i')+(j+_p j')c$, $u\cdot v=(i\cdot_p i'+_p a\cdot_p j\cdot_p j')+(i\cdot_p j'+i'\cdot_p j)c$ (dakle u·v je proizvod izraza i+jc, i'+j'c po modulu $c^2=a$). Primetimo da je $c^{-1}=bc$ gde $a\cdot_p b=1$, dok je za x=i+jc, x≠0, $x^{-1}=i/(i^2-aj^2)+(j/(i^2-aj^2))c$, gde su algebarski izrazi $i/(i^2-aj^2)$, $j/(i^2-aj^2)$ sračunati u polju $\underline{Z}_p$.

1.18. Ako je $\underline{F}=(F,+,\cdot,0,1)$ konačno polje tada postoji prost broj p i prirodan broj n≥1 takvi da $|F|=p^n$.

Rešenje: Neka je $\underline{F}=(F,+,\cdot,0,1)$ konačno polje. Ako je m=|F|, sa obzirom da je (F,+,0) grupa, prema Langrangeovoj Teoremi m·1=0, dakle postoji najmanji prirodan broj p>1 takav da p·1=0. Tada

1^o p je prost broj.

Zaista, ako je p=uv, u,v>1, iz uslova p·1=0 sledi (u·v)·1=0, tj. (u·1)·(v·1)=0, odakle u·1=0 ili v·1=0, suprotno izboru broja p. Dalje, (F,+,0) je vektorski prostor nad poljem $\underline{Z}_p$ ukoliko se za proizvod vektora x∈F i skalara a∈Z_p uzme ax=x+...+x (a puta). F je konačan skup, pa je ovaj vektorski prostor konačno-dimenzion, recimo dimF=n. Tada je ovaj prostor, prema stavu iz linearne algebre, izomorfan prostoru $(Z_p,+,0)^n$, dakle $|F|=p^n$. Takodje $(F,+,0)=C_p^n$.

1.19. Ako je $\underline{F}=(F,+,\cdot,0,1)$ polje i $G<(F-\{0\},\cdot)$ konačna podgrupa, tada je G ciklična.

Rešenje: Neka je $|G|=n$ *i* $H=\{x\in F: x^n=1\}$. *Prema Langrangeovoj Teoremi* $\forall x\in G\ x^n=1$, *dakle* $G<H$. *Prema T.6.1.5. dovoljno je dokazati da je H ciklična grupa. H je konačan skup (ima najviše n elemenata jer polinom n-tog stepena u polju ima najviše n korena) pa prema stavu o dekompoziciji konačnih Abelovih grupa važi* $H=C_{m_1}^{k_1}x\ldots xC_{m_r}^{k_r}$ *gde su* $m_1,\ldots,m_r$ *dva po dva uzajamno prosti brojevi i* $k_1,\ldots,k_r\geq 1$. *Otuda postoji* $K<H$ *tako da* $C_{m_1}^{k_1}=K$. *Svaki* $x\in C_{m_1}^{k_1}$ *zadovoljava* $x^{m_1}=1$, *dakle* $\forall x\in K\ x^{m_1}=1$. *Polinom* $x^{m_1}-1$ *ima najviše* m_1 *korena u polju* $\underline{F}$, *stoga* $|K|\leq m_1$. *S druge strane* $|K|=|C_{m_1}^{k_1}|=m_1^{k_1}$, *dakle* $m_1^{k_1}\leq m_1$, *tj.* $k_1=1$. *Slično se dokazuje da je* $k_2=\ldots=k_r=1$. *Dakle* $H=\underline{C}_{k_1}x\ldots x\underline{C}_{k_r}$. *Neka su* $a_1,\ldots,a_r$ *redom generatori grupa* $\underline{C}_{k_1},\ldots,\underline{C}_{k_r}$. *Tada je* $a=(a_1,\ldots,a_r)$ *generator grupe* $\underline{C}_{k_1}x\ldots x\underline{C}_{k_r}$ *(v.z.6.2.3.), dakle H je ciklična.*

1.20. Neka je $\Phi_n=\{i\geq 1: i<n, (i,n)=1\}$. Dokazati da je $(\Phi_n,\cdot_n)$ grupa i odrediti $|\Phi_n|$.

Rešenje: Dokazujemo: $x,y\in\Phi_n\Rightarrow x\cdot_n y\in\Phi_n$.
Neka su $x,y\in\Phi_n$. *Tada* $(x,n)=1$, $(y,n)=1$, *te prema z. 1.6.* $(xy,n)=1$. *Neka je* $z=x\cdot_n y$. *Tada* $xy=qn+z$, $1\leq z<n$, *te iz uslova* $(xy,n)=1$ *sledi* $(z,n)=1$, *tj.* $x\cdot_n y\in\Phi_n$. *Prema prethodnom i z. 1.11. sledi da je* $(\Phi_n,\cdot_n)$ *semigrupa sa jedinicom.*

Neka je $a\in\Phi_n$. *Tada* $(a,n)=1$ *te prema Teoremi 1.3. postoje* $x,y\in Z$ *takvi da* $ax+ny=1$, *tj.* $ax=1\ mod n$. *Otuda* $a\cdot_n b=1$, *gde* $x=qn+b$, $1\leq b<n-1$. *Dakle svaki element iz* Φ_n *ima inverzan, pa je* $(\Phi_n,\cdot_n)$ *grupa.*

$|\Phi_n|=\varphi(n)$, *$\varphi(n)$ je Eulerova funkcija.*

1.21. Dokazati: a) (Fermat-ova Teorema) Ako je p prost broj tada $(n,p)=1\Rightarrow n^{p-1}=1(mod p)$; b) $(\forall x\in Z)((x,n)=1\Rightarrow x^{\varphi(n)}=1(mod n))$, $\varphi(n)$ je Euler-ova funkcija.

Rešenje: a) Pretpostavimo $(n,p)=1$, *p je prost broj. Neka je* $a\in Z_p$ *takav da* $n=a\ mod p$. *Tada* $n^{p-1}=a^{p-1}\ mod p$ *i takodje* $a^{p-1}=$

$=a\cdot_p \ldots \cdot_p a$ (**modp**) . *Kako je* $a \in Z_p-\{0\}$ *i red grupe* $(Z_p-\{0\},\cdot_p)$ *je p-1, prema Langrangeovoj Teoremi* $a\cdot_p \ldots \cdot_p a$ *(p-1 puta)=1 , tj.* $a^{p-1}=1$ *modp, dakle* $n^{p-1}=1$ *modp.*

b) Izvesti slično razmatranje kao pod (a), ali sada sa grupom Φ_n *iz prethodnog zadatka.*

1.22. Dokazati Wylson-ovu Teoremu: n je prost broj akko (n-1)! = -1(modn).

Rešenje: ($\Rightarrow$) *Neka je n prost broj. Tada je prsten* $\underline{Z}_n$ *polje, v.z. 1.15. Jednačina* $x^2=1$ *ima tačno dva rešenja u* $\underline{Z}_n$, *to su 1,n-1, te* $1\cdot_n 2\cdot_n \ldots \cdot_n (n-1)=n-1$, *jer se u proizvodu* $1\cdot_n 2\cdot_n \ldots \cdot_n (n-1)$ *za svaki x pojavljuje i njegov inverzni, tj.* x^{-1}. *Otuda* $1\cdot 2\cdot \ldots \cdot (n-1)=n-1$ *modn, tj.* $n!=-1$ *modn.*

($\Leftarrow$) *Ako je* $(n-1)!=-1$ *modn tada za neki* $x \in Z$ $(n-1)!(-1)+nx=1$, *te prema Teoremi 2* $((n-1)!,n)=1$. *Otuda n nije deljiv ni sa jednim* $i<n$, $i\neq 1$, *dakle n je prost broj.*

1.23. Neka su $a\in N$, $b,c\in Z$, $b\neq 0,1,-1$, $(a,b)=1$, $(b,c)=1$. Dokazati da postoji $n\in N$ takav da ab^n+c nije prost broj.

Rešenje: Neka je $A_n=ab^n+c$. *Bez gubljenja opštosti može se pretpostaviti da je* $a>0$, $b>0$, *inače se ovaj dokaz izvodi za* $B_n=sgn(a)A_{2n}$.

Očigledno $A_n = ab(b^{n-1}-1)+ab+c$. *Razlikujemo sledeće slučajeve:*

1^o *Neka je* $|ab+c|>1$. *Tada postoji prost broj p takav da* $p|ab+c$. *Kako je* $(a,c)=1$, $(b,c)=1$, *prema z. 1.6.* $(ab,c)=1$, *te* $(p,b)=1$. *Otuda, prema maloj Fermatovoj Teoremi* $p|b^{p-1}-1$, *dakle* $p|A_p$.

2^o *Neka je* $|ab+c|=1$. *Tada za* $d=ab+c$ *(dakle* $d=\pm 1$*)* $A_{n+2}=ab^3(b^{n-1}-1)+ab(b^2-1)+d$. *Tada* $ab(b^2-1)+d>1$, *te postoji prost broj p takav da* $p|ab(b^2-1)+d$, *tj.* $p|ab^3+c$. *Kako je* $(ab^3,c)=1$ *to p ne deli b, dakle prema maloj Fermatovoj Teoremi* $p|b^{p-1}-1$, *stoga* $p|A_{p+2}$.

1.24. Dokazati da za svaki polinom p nad $\underline{Z}$, $st(p)\geq 1$, postoji $n\in N$ takav da p(n) nije prost broj.

Rešenje: Za svaki ceo broj a postoji polinom q(x) sa celo-

brojnim koeficijentima takav da p(x)=(x-a)q(x)+p(a). Ako je za neki a∈N p(a)=0 tvrdjenje neposredno sledi. Zato neka je a∈N takav da p(a)>1 (ili p(a)<-1). Tada za dovoljno veliki m∈N za x_o=a+mp(a) q(x_o)≠0 (polinom q(x) ima najviše konačno mnogo korena) i 1+mq(x_o)≠0,1,-1. Tada p(x_o)=p(a)(mq(x_o)+1), tj. p(x_o) je složen broj.

Napomena: J. Matijaševič (1970), sovjetski matematičar, dokazao je da postoji polinom $p(x_1,\ldots,x_{10})$ sa celobrojnim koeficijentima čiji je skup pozitivnih vrednosti upravo skup prostih brojeva.

1.25. Neka je n∈N, n>1 i n nije stepen broja 10. Dokazati da je log(n) iracionalan broj.

Rešenje: Neka je x=logn i pretpostavimo da je za neke uzajamno proste u,v∈N x=u/v. Tada $n=10^x$, tj. $n^v=2^u5^u$. Dalje, neka je $n=p_1^{s_1}\ldots p_k^{s_k}$ razlaganje broja n na proste faktore. Tada $p_1^{s_1v}\ldots p_k^{s_kv}=2^u5^u$. Prema teoremi o predstavljanju prirodnih brojeva preko prostih, v.z. 1.8., sledi k=2, $p_1=2$, $p_2=5$, $s_1v=u$, $s_2v=u$, dakle $s_1=s_2$. Otuda $n=2^{s_1}5^{s_1}=10^{s_1}$, suprotno pretpostavci da n nije potencija broja 10.

1.26. Neka je c iracionalan broj. Dokazati: a) Z+cZ={x+cy:x,y∈Z} je gust u skupu realnih brojeva R; b) {xc-[xc]: x∈N} je gust u [0,1].

Rešenje: Možemo pretpostaviti c>0. a) 1° Neka je f:N→[0,1] preslikavanje definisano jednakošću f(x)=xc-[xc]. f je 1-1; zaista ako je $f(x_1)=f(x_2)$ tada $(x_1-x_2)c=[x_2c]-[x_1c]$. Ukoliko bi bilo $x_1-x_2\neq 0$, onda $c=([x_2c]-[x_1c])/(x_1-x_2)$, suprotno pretpostavci da je c iracionalan broj. Dakle $x_1=x_2$.

2° Neka je n∈N, n>0. Preslikavanje g:N→{0,1,...,n} definisano je na sledeći način: g(x)=najmanji i∈N takav da f(x)∈[i/(n+1), (i+1)/(n+1)]. Prema prethodnom i 1° ako je $g(x_1)=g(x_2)$, sledi $0\leq|f(x_1)-f(x_2)|\leq 1/(n+1)<1/n$. Otuda za $v=x_1-x_2$, $u=[x_2c]-[x_1c]$, $|u+vc|<1/n$. Neka je d=u+vc. Možemo pretpostaviti da je d>0, inače biramo d=(-u)+(-v)c. Dakle 0≤d<1/n i d∈Z+cZ.

3^{o} *Neka su* $x,y \in R$, $0<x<y$ *i* $1/n<y-x$, $n \in N$. *Prema* 2^{o} *postoji* $d \in Z+cZ$ *takav da* $0<d<1/n$. *Neka je* $m \in N$ *najveći prirodan broj takav da* $md<x$. *Tada* $x<md+d<x+1/n<y$. *Dakle za* $a=md+d$ $x<a<y$ *i* $a \in Z+cZ$. *Slično se dokazuje da postoji* $a \in Z+cZ$ $x<a<y$ *i u slučajevima* $x<0<y$ *ili* $x<y<0$.

b) 1^{o} *Dokazujemo da je skup* $S=\{cy-x : x,y \in N\}$ *gust u* $[0,1]$. *Sa obzirom na dokaz u (a),* 3^{o} *dovoljno je dokazati da za svaki* $d \in R$, $d>0$, *postoji* $s \in S$ *takav da* $0<s<d$. *Pretpostavimo suprotno: za neki* $d>0$.

(1) $S \cap [0,d] = \emptyset$.

Prema (a) skup $Z+cZ$ *je gust u* $[0,1]$, *pa kako iz* $0<x+cy<1$ *sledi da su* x,y *različitog znaka, to prema (1)* $[0,d] \cap (Z+cZ) = \{x-cy : x,y \in N$ *i* $x-cy \in [0,d]\}$ *i ovaj skup je gust u* $[0,d]$.

Neka je $a=\underline{x}-c\underline{y}$, $0<a<d$. *Ako je* $z \in Z+cZ$, $-a<z<0$, *onda* $0<-z<a$, *te za neke* $u,v \in N$ $-z=u-vc$, *tj.* $z=vc-u$, *dakle*

(2) $[-a,0] \cap (Z+cZ) = \{vc-u : v,u \in N$ *i* $vc-u \in [-a,0]\}$ *i ovaj skup je gust u* $[-a,0]$. *Članovi* u,v *u* $vc-u$ *su neograničeni kada* $vc-u$ *prolazi kroz* $[-a,0]$, *tj. za svaki* $m>0$ *postoje* $u,v>m$ *takvi da* $vc-u \in [-a,0]$. *Zaista, ukoliko bi za neki* $u_o \in N$ *za sve* $vc-u \in [-a,0]$ *bilo* $u \leq u_o$, *onda iz* $vc-u<0$ *sledi* $vc \leq u_o$, *te je i* v *ograničen, što znači da u* $[-a,0]$ *ima konačno mnogo članova oblika* $vc-u$, *a to je kontradikcija prema (2). Slično se dokazuje da ni* v *ne može biti ograničen.*

Za $0>vc-u>-a$ $(\underline{x}-u)+(v-\underline{y})c=a+vc-u>0$ *i prema prethodnom za neke dovoljno velike* $\underline{u},\underline{v} \in N$ *važi* $0>\underline{v}c-\underline{u}>-a$, $\underline{v}-\underline{y}>0$, $\underline{x}-\underline{u}<0$, *tj. za* $x=\underline{x}-\underline{u}$, $y=\underline{v}-\underline{y}$ *važi* $0<yc-x<a<d$, $x,y \in N$, *što je suprotno pretpostavci (1). Dakle S je gust u* $[0,1]$.

2^{o} *Neka je* $0<cy-x<1$, $x,y \in N$. *Tada* $cy=x+r$, $0<r<1$, *odakle* $[cy]=x$, *prema tome* $cy-x=cy-[cy]$. *Dakle* $\{cy-x : x,y \in N, 0<cy-x<1\} = \{nc-[nc] : n \in N\}$, *pa prema* 1^{o} *tvrdjenje sledi.*

1.27. Neka su $a,b \in N$, $a,b \neq 0$, a nije potencija broja 10. Tada postoje prirodni brojevi n,c takvi da $a^{n}=b*c$, * je operacija konkatenacije (dopisivanja) reči.

Rešenje: Neka je $b'=10b+1$ *i* $m \in N$, $1<b'/10^{m}<10$. *Prema prethodnim zadacima loga je iracionalan broj, stoga skup* $\{nloga-[nloga] : n \in N\}$ *je gust u* $[0,1]$. *Otuda za neki* $n \in N$ $(b'+1)/10^{m}>10^{nloga-[nloga]}>b'/10^{m}$ *i* $[nloga]>m$. *Neka je*

$k=[n\log a]-m$. Tada $b'+1>10^{n\log a-k}>b'$, tj. $10^k(b'+1)>a^n>10^k b'$. Otuda za neki $c'<10^k$ $a^n=10^k b'+c'$, odakle $a^n=10^{k+1}b+10^k+c'$, te $a^n=b*c$, gde $c=10^k+c'$.

1.28. Jednačina $x^4-1=0$ ima četiri različita rešenja u polju $\underline{Z}_p$ akko $p=1(\mathrm{mod}4)$, p je prost broj. Dokazati!

Rešenje: Videti dokaz tvrdjenja T.1. u rešenju z. 8.2.14.

1.29. Neka je p prost broj. Dokazati da jednačina $x^2+1=0$ ima koren u polju $\underline{Z}_p$ akko $p=1(\mathrm{mod}4)$.

Rešenje: Jednačina $x^2+1=0$ ima rešenje u polju $\underline{Z}_p$ akko jednačina $x^4-1=0$ ima četiri različita rešenja u $\underline{Z}_p$, dakle tvrdjenje sledi prema prethodnom zadatku.

1.30. Neka su p,q prosti brojevi. Dokazati: jednačina $x^p-1=0$ ima koren $x\neq 1$ u $\underline{Z}_p$ akko $p|q-1$.

Rešenje: Videti dokaz tvrdjenja T.1. u rešenju z.8.2.15.

1.31. Rešiti diofantovsku jednačinu $x^p+y^p=qz$, p,q su prosti brojevi.

Rešenje: <u>Slučaj p=2</u>: Dokazujemo da ova jednačina ima netrivijalno rešenje $x\neq y \bmod q$ akko $q=1 \bmod 4$. ($\Rightarrow$) Neka su $\underline{x},\underline{y},\underline{z}\in Z$, $\underline{x}^2+\underline{y}^2=qz$, $q\nmid \underline{x},\underline{y}$. Tada $\underline{x}^2+\underline{y}^2=0 \bmod q$, stoga $t\in Z_q$, $t=\underline{x}\underline{y}^{-1}$, jeste rešenje jednačine $x^2+1=0$ u $\underline{Z}_q$. Otuda, prema z. 1.29 sledi $q=1 \bmod 4$. ($\Leftarrow$) Neka je $q=1 \bmod 4$. Tada prema z. 1.29 jednačina $x^2+1=0$ ima rešenje u $\underline{Z}_q$, neka su to $t_1,t_2\in \underline{Z}_q$. Tada za neke $m_1,m_2\in N$ $t_i^2+1=m_i q$. Netrivijalna rešenja diofantske jednačine su $x=yt_i$, $z=m_i y^2$.

<u>Slučaj p∉2N+1:</u> Rešenje x,y,z diofantske jednačine nazvaćemo trivijalnim ukoliko $y=-x$ ili $q|x,y$. Dokazujemo da ova diofantska jednačina ima netrivijalno rešenje akko $p|q-1$. ($\Rightarrow$) Neka su $\underline{x},\underline{y},\underline{z}$ netrivijalna rešenja diofantske jednačine. Tada je $t=-xy^{-1}$ netrivijalno rešenje jednačine $x^p=1$ u $\underline{Z}_q$, te prema z. 1.3o $p|q-1$.
($\Leftarrow$) Neka $p|q-1$. Tada prema z. 1.3o. jednačina $x^p=1$ ima netrivijalno rešenje u $\underline{Z}_q$. Otuda postoji $t\in \underline{Z}_q$ takav da su sva rešenja jednačine $x^p=1$ u $\underline{Z}_q$ potencije od t, neka su to $t_1,\ldots,t_p$. Tada $t_i^p-1=m_i q$ za neke m_i, odakle $x=-t_i y$, $z=-m_i y^p$ jeste rešenje diofantske jednačine.

1.32. Rešiti diofantovske jednačine: a) $x^3+y^3=5z$,b) $x^3+y^3=7z$.

Rešenje: a) $3\nmid 5-1$, pa prema prethodnom zadatku opšte rešenje je $x=5m$, $y=5n$, $z=25(m^3+n^3)$, $m,n\in Z$.

b) $3\mid 7-1$, te prema prethodnom zadatku ova diofantovska jednačina ima netrivijalno rešenje. Koristeći notaciju iz istog zadatka imamo $t_1=2$, $m_1=1$, $t_2=4$, $m_2=9$, te su sva rešenja oblika: $x=-2y$, $z=-y^3$, $x=-4y$, $z=-9y^3$, $x=7m$, $y=7n$, $z=49(m^3+n^3)$, $m,n\in Z$.

1.33. Dokazati da jednačina $x^2+3=0$ ima rešenje u $\underline{Z}_p$ akko $x^3-1=0$ ima rešenje $x\neq 1$ u $\underline{Z}_p$, p je prost broj.

Rešenje: Jednačina $x^3-1=0$ ima rešenje $x\neq 1$ u $\underline{Z}_p$ akko $x^2+x+1=0$ ima rešenje u $\underline{Z}_p$. Dalje, $x^2+x+1=0$ akko $((x+1/2)/(1/2))^2+3=0$.

1.34. Ako jednačina $x^4+1=0$ ima rešenje u $\underline{Z}_p$, tada i jednačina $x^2-2=0$ ima rešenje u $\underline{Z}_p$, p je prost broj.

Rešenje: Neka je a rešenje jednačine $x^4+1=0$ u $\underline{Z}_p$. Tada $a^4+1=0$, te $a^2+a^{-2}=0$. Otuda $(a+a^{-1})^2 = a^2+2+a^{-2}$, tj. $(a+a^{-1})^2-2=0$, dakle $a+a^{-1}$ jeste rešenje jednačine $x^2-2=0$ u $\underline{Z}_p$.

1.35. Dokazati da jednačina $x^4+1=0$ ima rešenje u $\underline{Z}_p$ akko $8\mid p-1$, p je prost broj.

Rešenje: ($\Rightarrow$) Neka je a rešenje jednačine $x^4+1=0$ u $\underline{Z}_p$. Tada $a^4=-1$ i $a^8=1$, stoga $red(a)=8$ u multiplikativnoj grupi $(\underline{Z}_p-\{0\},\cdot_p)$ polja $\underline{Z}_p$. Prema Langrangeovoj Teoremi sledi $red(a)\mid p-1$, tj. $8\mid p-1$.

($\Leftarrow$) Neka $8\mid p-1$. Multiplikativna grupa $(Z_p-\{0\},\cdot_p)$ polja $\underline{Z}_p$ je ciklična, v.z. 1.19., te kako $8\mid p-1$ prema z. 6.1.24 postoji $a\in Z_p-\{0\}$ reda 8. Tada je a^2 rešenje jednačine $x^4+1=0$ u $\underline{Z}_p$.

1.36. Rešiti diofantovsku jednačinu $x^4+y^4=pz$, p je prost broj.

Rešenje: Rešenje diofantske jednačine je trivijalno akko $p\mid x,y$. Ova diofantska jednačina ima netrivijalno rešenje akko $8\mid p-1$, videti prethodni zadatak. Ukoliko $8\mid p-1$ tada se rešenje može odrediti rešavanjem jednačine $x^4+1=0$ u polju $\underline{Z}_p$, videti takodje z. 1.31., 1.32.

U sledećim zadacima P označava skup prostih brojeva.

1.37. Dokazati da su sledeći skupovi beskonačni: a) $P\cap(3N-1)$, b) $P\cap(4N-1)$, c) $P\cap(6N-1)$.

Rešenje: a) Videti dokaz tvrdjenja (3) u rešenju z.8.19.
b), c) Slično kao pod (a).

1.38. Dokazati da su sledeći skupovi beskonačni: a) $P\cap(3N+1)$, b) $P\cap(4N+1)$, c) $P\cap(6N+1)$, d) $P\cap(8N+1)$.

Rešenje: a) Videti rešenje z.8.2.33.
b) 1^o $p\in P\cap(4N+1)$ *akko* $4|p-1$ *akko (prema z. 1.29) jednačina* $x^2+1=0$ *ima rešenje u* $\underline{Z}_p$.

Pretpostavimo da je $P\cap(4N+1)$ *konačan, te neka je* $P\cap(4N+1)=\{p_1,\ldots,p_k\}$ *i* $a=p_1\ldots p_k$. *Dalje, neka je* $p\in P$, $p|a^2+1$. *Tada* $a^2+1=0$ *modp, dakle jednačina* $x^2+1=0$ *ima rešenje u* $\underline{Z}_p$ *te prema* 1^o $4|p-1$. *Otuda, prema definiciji broja a sledi* $p|a$. *Kako po pretpostavci takodje* $p|a^2+1$, *to* $p|1$, *kontradikcija.*
c) Prema (a) $P\cap(3N+1)$ *je beskonačan. Neka je* $p\in P\cap(3N+1)$. *Tada za neki* $m\in N$ $p=3m+1$. *Ako je* $m=2k+1$ *onda* $p=6k+4$, *tj.* $2|p$, *kontradikcija. Dakle* $m=2k$, *tj.* $P\cap(6N+1)=P\cap(3N+1)$.
d) $p\in P\cap(8N+1)$ *akko* $8|p-1$ *akko (prema z. 1.35)* $x^4+1=0$ *ima rešenje u* $\underline{Z}_p$. *Dalje, slično kao pod (b).*

1.39. Ako je p prost broj dokazati da je $P\cap(pN+1)$ beskonačan skup.

Rešenje: 1^o $q\in P\cap(pN+1)$ *akko* $p|q-1$ *akko (prema z. 1.30) jednačina* $x^p-1=0$ *ima rešenje* $x\neq 1$ *u polju* $\underline{Z}_q$.

Pretpostavimo da je $P\cap(pN+1)$ *konačan skup i neka je* $P\cap(pN+1)=\{q_1,\ldots,q_k\}$. *Dalje, neka je* $a=q_1\ldots q_k$ *i* $q\in P$, $q|a^p-1$. *Otuda sledi* $q\nmid a$ *i* $a^p=1$ *modq. Dakle jednačina* $x^p-1=0$ *ima netrivijalno rešenje u* $\underline{Z}_q$, *te prema* 1^o $p|q-1$, *stoga, prema definiciji broja a* $q|a$, *što je kontradikcija.*

1.40. (Langrange-ova Teorema) Dokazati: Za svaki $n\in N$ postoje $m_1,m_2,m_3,m_4\in Z$ takvi da $n=m_1^2+m_2^2+m_3^2+m_4^2$.

Rešenje: Za cele brojeve $x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4$ *važi:*

$$1^o(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 +$$
$$+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 + (x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2 +$$
$$+(x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2 .$$

2^{o} *Ako je* $p>2$ *prost broj tada postoji* $n\in N$ *takav da* $1\leqslant n<p$ *i* np *je zbir četiri kvadrata prirodnih brojeva.*

Dokaz za 2^{o}: *Neka su* $0\leqslant x,y<(p-1)/2$ *i* $x^2=y^2$ *modp. Tada* $p|(x-y)(x+y)$, *te* $p|x-y$ *ili* $p|x+y$. *Kako je* $0\leqslant x+y\leqslant p-1$ *to* $p|x-y$. *Dalje,* $|x-y|\leqslant(p-1)/2$, *stoga* $x-y=0$, *tj. skup* $A=\{x^2 : 0\leqslant x\leqslant(p-1)/2\}$ *ima* $(p+1)/2$ *element. Slično se dokazuje da skup* $B=\{-1-y^2 : 0\leqslant y\leqslant(p-1)/2\}$ *ima takodje* $(p+1)/2$ *članova. Skup* $Z_p=\{0,1,\ldots,p-1\}$ *ima* p *članova i* $A\cup B\subseteq Z_p$, *te* $A\cap B\neq\emptyset$, *tj. postoje* $x,y\in Z$ *takvi da* $0\leqslant x,y\leqslant(p-1)/2$, $x^2\equiv -1-y^2$ *modp, dakle, za neki* $n\in N$ $np=x^2+y^2+1$. *Dalje, kako su* $0\leqslant x,y\leqslant(p-1)/2$ *to* $np\leqslant 2((p-1)/2)^2+1<p^2/2+1<p^2$, *odakle* $n<p$.

3^{o} *Ako je* p *prost broj tada je* p *zbir četiri kvadrata celih brojeva.*

Dokaz za 3^{o} : $2=1^2+1^2+0^2+0^2$, *te pretpostavimo* $p>2$. *Neka je* n *najmanji prirodan broj takav da je* np *zbir četiri kvadrata. Prema* 2^{o} $1\leqslant n<p$. *Neka je* $np=x_1^2+x_2^2+x_3^2+x_4^2$ *i pretpostavimo* $n>1$. *Pretpostavimo da je* n *paran broj. Tada je* $x_1^2+x_2^2+x_3^2+x_4^2$ *takodje paran, tako da razlikujemo sledeće slučajeve: (1) sva četiri od* x_1,x_2,x_3,x_4 *su parni, (2) dva su parna dva su neparna, (3) sva četiri su neparna. U slučaju (2) možemo pretpostaviti da su* x_1,x_2 *parni, stoga u svim slučajevima (1), (2), (3) važi*

$$(n/2)p=((x_1+x_2)^2/2)^2+((x_1-x_2)/2)^2+((x_3+x_4)/2)^2+((x_3+x_4)/2)^2$$

i pritom su svi izrazi u zagradama celi brojevi. Medjutim to je kontradikcija izboru (minimalnosti) broja n. *Dakle,* n *je neparan broj.*

Elementi skupa $S=\{y:-(n-1)/2\leqslant y\leqslant(n-1)/2\}$ *nisu uzajamno kongruentni modn i takodje* $|S|=n$. *Otuda postoje* $y_i\in S$ *takvi da* $x_i\equiv y_i$ *modn,* $i=1,2,3,4$, *te* $x_1^2+x_2^2+x_3^2+x_4^2\equiv y_1^2+y_2^2+y_3^2+y_4^2\equiv 0$ *modn, recimo* $y_1^2+y_2^2+y_3^2+y_4^2=rn$. *Tada* $r\neq 0$ *jer inače* $y_i=0$ *za* $i=1,\ldots,4$, *te* $n|x_i$ *za* $i=1,\ldots,4$, *odakle* $n^2|x_1^2+x_2^2+x_3^2+x_4^2$, *tj.* $n^2|np$, *pa* $n|p$, *kontradikcija. Takodje* $rn<4(n/2)^2=n^2$, *te* $r<n$. *Dalje,* $(nr)(np)$ *je zbir četiri kvadrata prema* 1^{o}, *a takodje se neposredno vidi da je za ovako izabrane* x_i, y_i *svaki sabi-*

rak na desnoj strani u 1^o deljiv sa n^2. Dakle, rp je zbir četiri kvadrata, dok je $0<r<n$, a to je kontradikcija prema izboru broja n.

Sada tvrdjenje sledi prema reprezentaciji prirodnih brojeva preko prostih i prema 1^o i 3^o.

1.41. Dokazati da je skup prirodnih brojeva definabilan u prstenu celih brojeva $\underline{Z}$, tj. postoji formula F jezika $\{+,\cdot\}$ tako da za sve $x\in Z$ $F(x)$ važi u $\underline{Z}$ akko $x\in N$.

Rešenje: Prema prethodnom zadatku imamo: $n\in N$ akko

$$(\exists x_1,x_2,x_3,x_4)\ n=x_1^2+x_2^2+x_3^2+x_4^2 \quad važi\ u\ \underline{Z}.$$

U sledećim zadacima uvodimo pojam determinante nad ma kojim prstenom. Ukoliko je reč o komutativnim prstenima, pokazuje se da se mnoga uobičajena svojstva determinante zadržavaju. Isto tako, uverićemo se da se mnoge osobine determinante dobijaju kao posledica iz teorije permutacijskih grupa S_n, A_n. Podsećamo na definiciju determinante.

Neka je $\underline{P}$ komutativan prsten, $m_n(P)$ skup kvadratnih matrica reda n nad $\underline{P}$ i neka je $\varepsilon:\underline{S}_n\to(\{1,-1\},\cdot)$ homomorfizam P iz odeljka 4.2. *Determinanta* matrice $A=||a_{ij}||nxn$, $A\in m_n(P)$ je

$$\det(A)\overset{def}{=}\sum_{p\in S_n}\varepsilon(p)a_{1p_1},a_{2p_2}\ldots a_{np_n}.$$

1.42. Neka je $\underline{P}$ komutativan prsten i $A\in m_n(P)$. Dokazati:

(i) Ako je $q\in S_n$ tada $\sum_{p\in S_n}\varepsilon(p)a_{q_1p_1}a_{q_2p_2}\ldots a_{q_np_n}=\varepsilon(q)\det(A)$.

(ii) Ako je A^T transponovana matrica matrice A, tada $\det(A^T)=\det(A)$.

Rešenje: 1) Neka je $A_p=a_{q_1p_1}\ldots a_{q_np_n}$ i $\varphi:S_n\to S_n$ preslikavanje definisano sa $\varphi(p)=qop$. Tada je φ 1-1 i <u>na</u>, tj. $\varphi\in Sym(S_n)$. Dalje,

$$(1)\sum_{p\in S_n}\varepsilon(poq)a_{q_1p_1}\ldots a_{q_np_n}=\sum_{p\in S_n}A_p\overset{①}{=}\sum_{p\in S_n}A_{\varphi(p)}$$ i

$$A_{\varphi(p)}=\varepsilon(poq)a_{q_1p_1(q_1)}\ldots a_{q_np(q_n)}\overset{②}{=}\varepsilon(p)\cdot\varepsilon(q)a_{q_1p(q_1)}\ldots a_{q_np(q_n)}$$

Neka je $x_i=a_{q_ip_i(q_i)}$. Tada za $I_n=\{1,2,\ldots,n\}$ važi $q^{-1}\in Sym\ I_n$ $(=S_n)$ i

$$a_{q_1p(q_1)}\ldots a_{q_np(q_n)}=\prod_{i\in I_n}a_{q_ip(q_i)}=\prod_{i\in I_n}x_i\overset{①}{=}$$

$$=\prod_{i\in I_n}x_{q^{-1}(i)}\overset{③}{=}\prod_{i\in I_n}a_{ip_i}=a_{1p_1}\ldots a_{np_n}.$$

Dakle, $A_{\varphi(p)}=\varepsilon(q)\varepsilon(p)a_{1p_1}a_{2p_2}\ldots a_{np_n}$, pa prema ①

$\sum_{p\in S_n}\varepsilon(q)\varepsilon(p)a_{q_1p_1}\ldots a_{q_np_n}=\varepsilon(q)\sum_{p\in S_n}\varepsilon(p)a_{1p_1}\ldots a_{np_n}=\varepsilon(q)\det(A)$.

① prema 1.3.12.

② ε je prema T.4.2.1. homomorfizam.

③ $x_{q^{-1}(i)}=a_{ip_i}$.

(2) Neka je $C_p=a_{p_n1}\ldots a_{p_n1}$. Tada za $q=p^{-1}$ važi

$\varepsilon(p)a_{1p_1}\ldots a_{np_n}=\varepsilon(p)a_{q_11}\ldots a_{q_nn}=\varepsilon(p^{-1})C_{p^{-1}}$ jer $\varepsilon(p)=\varepsilon(p^{-1})$ (v.z. 4.22).

Kako za $\psi: p\mapsto p^{-1}$ važi $\psi\in Sym(S_n)$, sledi

$\det A=\sum_{p\in S_n}\varepsilon(p)a_{1p_1}\ldots a_{np_n}=\sum_{p\in S_n}\varepsilon(p^{-1})C_{p^{-1}}=\sum_{p\in S_n}\varepsilon(p)C_p$.

1.43. Determinanta matrice $A\in m_n(P)$ može se shvatiti kao funkcija svojih vrsta (ili kolona). Naime, ako je $A=\|a_{ij}\|_{n\times n}$, $a_i=(a_{i1},a_{i2},\ldots,a_{in})$, $i=1,\ldots,n$, tada $\det A=\det[a_1,a_2,\ldots,a_n]$. Dokazati

1) $\det[b,c,a_3,\ldots,a_n]=-\det[b,c,a_3,\ldots,a_n]$

2) Determinanta je linearna funkcija svojih vrsta (kolona) tj. $\det[\alpha b+\beta e, a_2a_3,\ldots,a_n]=\alpha\det[b,a_2,a_3,\ldots,a_n]+\beta\det[e,a_2,a_3,\ldots,a_n]$.

Rešenje: Neka je $b=(b_1,\ldots,b_n)$, $c=(c_1,\ldots,c_n)$ i neka je $a_p=b_{p_1}c_{p_2}a_{3p_3}\ldots a_{np_n}$. Tada za transpoziciju $g=(12)$, preslikavanje $\gamma: p\mapsto pog$ pripada $Sym\ S_n$, dakle

$\det[b,c,a_3,\ldots,a_n]=\sum_{p\in S_n}\varepsilon(p)A_p=\sum_{p\in S_n}\varepsilon(pog)A_{pog}$ ① $=\varepsilon(g)\sum_p\varepsilon(p)A_{pog}$

Kako je $A_{pog}=c_{p_1}b_{p_2}a_{3p_3}\ldots a_{np_n}$, $\varepsilon(g)=\varepsilon(12)=-1$, i

$\sum_p\varepsilon(p)c_{p_1}b_{p_2}a_{3p_3}\ldots a_{np_n}=\det[c,b,a_3,\ldots,a_n]$ to

$\det[b,c,a_3,\ldots,a_n]=-\det[c,b,a_3,\ldots,a_n]$.

① ε je homomorfizam.

② Operator sumiranja Σ je aditivan i homogen operator.

1.44. Dokazati Binet-Cauchy-evu teoremu:

$\det: m_n(P)\to P$ je homomorfizam iz semigrupe $(m_n(P),\cdot)$ u semigrupu $(P,\cdot)$ tj. $(\forall A,B\in m_n(P))\det(A\cdot B)=\det A\cdot\det B$.

Rešenje: Neka je $A=\|a_{ij}\|_{n\times n}$, $B=\|b_{ij}\|_{n\times n}$ i $C=\|c_{ij}\|_{n\times n}$ gde $c_{ij}=\sum_k a_{ik}b_{kj}$. Tada

$$det(C)=\sum_{p\in S_n}\varepsilon(p)c_{1p_1}\dots c_{np_n}$$

$$c_{ip_i}=\sum_{q_i\in S_n}a_{iq_i}b_{q_ip_i},\quad i=1,\dots,n$$

Neka je $F_n=\{f\,|\,f:\{1,\dots,n\}\to\{1,\dots,n\}\}$. Tada

$$det(C)=\sum_{p\in S_n}\varepsilon(P)\sum_{q_1,\dots,q_n\in n}a_{1q_1}a_{2q_2}\dots a_{nq_n}b_{q_1p_1}\dots b_{q_np_n}$$

pa

$$det(C)=\sum_{q\in F_n}a_{1q_1}\dots a_{nq_n}\sum_{p\in S_n}\varepsilon(p)b_{q_1p_1}\dots b_{q_np_n}=X+Y\quad gde$$

$$X=\sum_{q\in S_n}a_{1q_1}\dots a_{nq_n}\sum_{p\in S_n}\varepsilon(p)b_{q_1p_1}\dots b_{q_np_n}$$

$$Y=\sum_{q\in F_n\setminus S_n}a_{1q_1}\dots a_{nq_n}\sum_{p\in S_n}\varepsilon(p)b_{q_1p_1}\dots b_{q_np_n}$$

Tada, koristeći $\varepsilon(q)\varepsilon(q)=1$.

$$X=\sum_{q\in S_n}(\varepsilon(q)a_{1q_1}\dots a_{nq_n}\,\varepsilon(q)\sum_{p\in S_n}\varepsilon(p)b_{q_1p_1}\dots b_{q_np_n})$$

$$=\sum_{q\in S_n}\varepsilon(q)a_{1q_1}\dots a_{nq_n}\,det(B)=det(A)det(B).$$

Dalje, neka je $q\in F_n\setminus S_n$ i $d_{ij}=b_{q_ij}$, $1\le i,j\le 4$. Tada

$$\sum_{p\in S_n}\varepsilon(p)b_{q_1p_1}\dots b_{q_np_n}=\sum_{p\in S_n}d_{1p_1}\dots d_{np_n}=det(D)\quad gde$$

$D=\|d_{ij}\|_{nxn}$.

Preslikavanje q nije 1-1, dakle postoje $i,k\le n$, $i\ne k$, tako da $q_i=q_k$. Neka su to, recimo, redom 1,2.

Tada $q_1=q_2$, tj. $d_{1j}=d_{2j}$, $j=1,\dots,n$, tj. prva i druga vrsta matrice D su jednake. Otuda, prema z.1.43. $det(D)=0$. Dakle,

$$Y=\sum_{q\in F_n\setminus S_n}a_{1q_1}\dots a_{nq_n}\,det\,D=0$$

pa $det(AB)=det(C)=det(A)det(B)$.

1.45. Neka je $\underline{P}$ komutativan prsten sa jedinicom i neka je $m_n(P)$ skup svih kvadratnih matrica reda n nad $\underline{P}$. Dalje, neka je $D:m_n(P)\to P$ preslikavanje sa ovim osobinama:

1) D je linearna funkcija svojih vektora vrsta

2) D je alternirajuća funkcija svojih vektora vrsta, tj.

ako je $A \in m_n(P)$, $A = \alpha_{ij}$, i $a_i = (\alpha_{i1}, \ldots, \alpha_{in})$,
$i = 1, \ldots, n$,
tada $D[a_1, \ldots, a_i, a_j, \ldots, a_n] = -D[a_1, \ldots, a_j, a_i, \ldots, a_n]$,
$1 \leq i < j \leq n$.

3) Ako je E jedinična matrica reda n, tada $D(E) = 1$.
Dokazati da je $\forall A \in m_n(P)$ $D(A) = \det(A)$.

Rešenje: Neka su $e_1 = (1, 0, .., 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, ...
$e_n = (0, \ldots, 0, 1)$ *jedinični vektori. Tada su vektori vrste* a_i *linearna kombinacija ovih vektora, tj. ako je* $A = \| \alpha_{ij} \|_{nxn}$ *onda*

$$a_i = \alpha_{i1} e_1 + \ldots + \alpha_{in} e_n , \quad i = 1, \ldots, n$$

odakle, koristeći linearnost preslikavanja D

$$D(A) = D[a_1, \ldots, a_n] = D[\alpha_{11} e_1 + \ldots + \alpha_{1n} e_n, \ldots, \alpha_{n1} e_1 + \ldots + \alpha_{nn} e_n]$$

$$= \sum_{p \in F_n} \alpha_{1p_1} \ldots \alpha_{np_n} \; D[e_{p_1}, \ldots, e_{p_n}]$$

gde je F_n *skup svih preslikavanja skupa* $\{1, \ldots, n\}$ *u samog sebe. Ako je* $p \in F_n \setminus S_n$ *tada za neke različite* $i, j < n$, *recimo da su to 1 i 2, važi* $p_1 = p_2$. *Tada, s obzirom da je D alternirajuća funkcija*

$$D[e_{p_1}, e_{p_2}, e_{p_3}, \ldots, e_{p_n}] = D[e_{p_2}, e_{p_1}, e_{p_3}, \ldots, e_{p_n}] =$$

$$= -D[e_{p_1}, e_{p_2}, e_{p_3}, \ldots, e_{p_n}]$$

odakle

$$D[e_{p_1}, e_{p_2}, \ldots, e_{p_n}] = 0$$

Otuda

$$D = \sum_{p \in S_n} \alpha_{1p_1} \ldots \alpha_{np_n} \; D[e_{p_1}, \ldots, e_{p_n}] = \sum_{p \in S_n} \alpha_{1p_1} \ldots \alpha_{np_n} \varepsilon(p)$$

jer je D alternirajuća funkcija, pa za $p \in S_n$
$D[e_1, \ldots, e_n] = \varepsilon(p)$ *gde je* ε *homomorfizam grupe* S_n *na grupu* $(\{1, -1\}, \cdot)$.

13.2. Teorija Galoisa

Do početka 19. veka osnovni je bio problem rešavanje algebarskih jednačina vida

$a_0+a_1x+\ldots+a_nx^n = 0$ (a_i dati, x nepoznat kompleksan broj)

Još u davnim vremenima znalo se za rešavanje kvadratnih jednačina. U 16. veku italijanski matematičari S. del Ferro i N. Tartaglia rešili su kubnu jednačinu, dok je Ferrari rešio jednačinu 4. stepena. Traganje za sličnim formulama za rešavanje algebarskih jednačina viših stepena nastavljeno je dalje, ali bezuspešno. Sam pojam formule rešenja bio je u ono vreme nejasan, mada se na kraju došlo do toga da ove formule treba da budu izgradjene od koeficijenata jednačina, znakova aritmetičkih operacija, kao i znakova korenovanja ($\surd$, $\surd$,...).

Abel je 1826. g. dokazao da se u opštem slučaju jednačine petog stepena ili većeg ne mogu rešiti na opisani način. Neposredno posle toga Galois je uveo grupe u matematiku, a sa njima Galoisu je bilo lako da potvrdi Abelov rezultat.

U vezi sa pitanjem algebarskog rešavanja, kaže se i rešavanje pomoću radikala (*radicus*, lat.- koren), pomenimo i sledeće. Reč je, u stvari, o veoma uslovnom rešavanju. Naime, smatrajući da su rešene sve jednačine oblika

$x^2=a$, $x^3=a$, $x^4=a$,... (a dat kompleksan broj)

traga se za odgovarajućom formulom rešenja. I pored toga što za algebarske jednačine stepena većeg od 4 ne postoje rešavajuće formule, to ne znači da se ne mogu odrediti koreni takvih jednačina. Naprotiv, postoje mnogobrojne metode (Šturmov niz, Newtnov metod i druge) pomoću kojih se koreni mogu odrediti do proizvoljnog broja decimala.

Polinomi

Neka je $\underline{F} = (F,+,\cdot,0,1)$ polje i $a_0,\ldots,a_n \in F$. Algebarski izraz vida

$$a_0 + a_1x + \ldots + a_nx^n$$

naziva se *polinomom* nad F sa koeficijentima $a_0,a_1,\ldots,a_n$. Ako je $a_n \neq 0$ tada je stepen polinoma jednak n i koristimo oznaku stp. Konstante iz F, izuzev nule, su polinomi stepena 0.

Skup svih polinoma polja $\underline{F}$ obeležavamo sa $F[x]$. Ukoliko su $+$ i $\cdot$ uobičajene operacije sabiranja i množenja, tada je $(F[x],+,\cdot,\underline{0})$ prsten. U ovom prstenu važi Euklidov algoritam, naime, za svaka dva polinoma $p,q\in F[x]$, koji nisu oba jednaka 0 jedinstveno postoje polinomi m,r tako da $p=mq+r$ i $r=0 \vee \mathrm{st}r<\mathrm{st}q$.

Otuda, najveći zajednički delilac polinoma $p,q\in F[x]$, u oznaci NZD(p,q) odredjen je nizom

$$\begin{aligned} a_0 &= m_0a_1 + a_2 && a_0 = p\ ,\ a_1 = q \\ a_1 &= m_1a_2 + a_3 && \mathrm{st}a_1>\mathrm{st}a_2>\ldots>\mathrm{st}a_{n+1} \\ &\vdots \\ a_n &= m_{n-1}a_n+a_{n+1} && a_{n+1} = \mathrm{NZD}(p,q) \\ a_n &= m_na_{n+1} \end{aligned}$$

Element $a\in F$ je *koren* polinoma $p\in F[x]$ ukoliko je $p(a)=0$.

Teorema 2.1. *Neka je $p\in F[x]$ i $a\in F$. Tada $p(a)=0$ akko $x-a$ deli $p(a)$.*

Dokaz ($\rightarrow$) $p(x)=(x-a)q(x)+r$ *za neki* $r\in F$ *i* $q\in F[x]$. *Iz uslova* $p(a)=0$ *sledi* $r=0$, *pa* $x-a$ *deli* $p(x)$. ▼

Definicija 2.2. *Neka je* $p(x)=\sum_{i\leq n} a_ix^i$ *polinom nad poljem* F.

Izvod polinoma p *je*

$$p'(x) = \sum_{i\leq n} ia_ix^{i-1}$$

Dakle, $'$ je preslikavanje prstena $F[x]$. Za izvod važe ove osobine:

Teorema 2.3. *Neka su* $p,q\in F[x]$ *i* $a\in F$. *Tada*

(i) $(a\cdot p)' = a\cdot p'$

(ii) $(p+q)' = p'+q'$.

(iii) $(p\cdot q)' = p\cdot q'+p'\cdot q$

(iv) $(x-a)^2 \mid p(x) \Leftrightarrow p(a)=0 \wedge p'(a)=0$.

Dokaz: (i) $(a\cdot p)'=(a\sum a_ix^i)'=\sum a_ix^{i-1}=ap'(x)$..

(iv) ( ) Ako $(x-a)^2$ deli $p(x)$, tada za neki m F x važi $p(x)=(x-a)^2m(x)$, pa prema (iii) nalazimo $p'(x)=2(x-a)m(x)+(x-a)^2m'(x)$, odakle sledi $p'(a)=0$.

($\leftarrow$) Kako je $p(a)=0$, prema Teoremi 2.1. $p(x)=(x-a)q(x)$ za neki $q\in F[x]$. Otuda nalazimo $p'(x)=q(x)+(x-a)q'(x)$ pa kako je takodje $p'(x)=(x-a)n(x)$ za neki $n\in F[x]$, to $p(x)=(x-a)\ p'(x) - (x-a)^2q'(x) = (x-a)^2(n(x)-q'(x))$. ▼

Posledica Neka je n>1 prirodan broj. Tada za $p \in F[x]$ i $\alpha \in F$ važi

$$(x-\alpha)^n \mid p(x) \Leftrightarrow (\forall i<n)\ p^{(i)}(\alpha)=0.$$

Ovde, $p^{(0)}(x)=p(x)$, $p^{(1)}(x)=p'(x)$, $p^{(2)}(x)=p''(x)$,...

Koren $\alpha \in F$ polinoma $p \in F[x]$ je višestruk ukoliko je za neki $n>1$ $(x-\alpha)^n \mid p(x)$. Prethodna posledica daje jedan kriterijum za višestrukost polinoma.

Definicija 2.4. *Polinom $p \in F[x]$ je* <u>*svodljiv*</u> *nad F ukoliko je p proizvod polinoma nad F stepena manjeg od st p. Polinom p je nesvodljiv nad F akko F nije svodljiv nad F.*

Ako je p polinom sa celobrojnim koeficijentima, tada postoji jednostavan uslov nesvodljivosti za p.

<u>Eisenstain-ov kriterijum 2.5.</u> Neka je $p \in Z[x]$, $p=a_0+a_1x+\ldots+a_nx^n$, i m prost broj. Ako m deli $a_0,\ldots,a_{n-1}$ i $m^2 \nmid a_0$, $m \nmid a_n$, tada je p nesvodljiv nad <u>Q</u>.

Dokaz. Najpre primetimo da je p nesvodljiv nad Q akko p nije svodljiv nad Z. Sada, pretpostavimo da je $p=q\cdot r$, st q, st r<n. Tada za $q=\sum_j b_jx^j$, $r=\sum_j c_jx^j$ važi $a_0=b_0c_0$, odakle možemo uzeti da, recimo, $m \mid b_0$ i $m \nmid c_0$. Indukcijom dobijamo da onda m deli sve koeficijente b_i polinoma q: Neka je i+1<n. Tada $a_{i+1}=b_0c_{i+1}+\ldots+b_{i+1}c_0$. Kako $m \nmid c_0$, koristeći induktivnu hipotezu nalazimo $m \mid b_{i+1}$. Kako je st q<n, to je za neki k<n $a_n=b_0c_k+\ldots+b_nc_n$, pa $m \mid a_n$, što je kontradikcija.

Rašireпja

Neka su $\underline{F}$, $\underline{K}$ polja takva da je $\underline{F} \subseteq \underline{K}$. Tada se $\underline{F}$ naziva podpoljem $\underline{K}$, dok se $\underline{K}$ naziva *rašireпjem* polja $\underline{F}$. Svako polje $\underline{L}$ za koje važi $\underline{F} \subseteq \underline{L} \subseteq \underline{K}$ naziva se *međupoljem*.

Pretpostavimo da za neki $n \in N$ u polju $\underline{F}$ važi $n \cdot 1 = 0$. Ako je n najmanji prirodan broj sa ovom osobinom, tada, s obzirom da $\underline{F}$ nema delitelja nule, broj n je prost. Ovaj broj naziva se *karakteristikom* polja F. Ako takav broj ne postoji, kažemo da je $\underline{F}$ karakteristiko nula. Primetimo da raširenje ima istu karakteristiku kao i njegovo podpolje.

Ako je $\underline{F} \subseteq \underline{K}$ tada je $\underline{K}$ vektorski prostor nad F. Dimenzija ovog prostora beleži se sa $|\underline{K} : \underline{F}|$. Ako je ova dimenzija konačna, onda je $\underline{K}$ konačno raširenje polja $\underline{F}$.

Teorema 2.6. Neka su $\underline{F}$, $\underline{L}$, $\underline{K}$ polja takva da $\underline{F} \subseteq \underline{K} \subseteq \underline{L}$. Tada

$$|\underline{K} : \underline{L}| \cdot |\underline{L} : \underline{F}| = |\underline{K} : \underline{F}|$$

Dokaz ove teoreme dajemo u zadatku .

Neka su F, K polja takva da $F \subseteq K$. Element $a \in K$ je *algebarski* nad F ukoliko je a koren nekog polinoma nad F. Element $a \in K$ je *transcedentan* nad F akko a nije algebarski nad F. Raširenje K nad F je algebarsko ukoliko je svaki $a \in K$ algebarski nad F.

Ukoliko je K generisan skupom $F \cup \{a_1, \ldots, a_n\}$, onda takodje koristimo oznaku $K = F(a_1, \ldots, a_n)$. Ako je $F \subseteq K$ i $a \in K$, broj $|F(a):F|$ nazivamo *stepenom* elementa a nad F.

Sledeće tvrdjenje ima bitnu ulogu u dokazima egzistencije nekih posebnih polja.

Lema 2.7. (Kroneoker) za svako polje F i polinom $p \in F[x]$ različit od konstante, postoji raširenje $K \supseteq F$ u kojem p ima koren.

Dokaz: Ideal prstena P je svaki skup $I \subseteq P$ koji ima osobine: (I,+,0) je grupa i za svaki $r \in P$ $rI \subseteq I$ gde je $rI = \{ri \mid i \in I\}$. Ideal I je pravi ako $I \neq P$.

Neka je $\mathcal{S}$ familija svih pravih ideala prstena F[x] koji sadrže p. Na familiju $\mathcal{S}$ može se primeniti Zornova lema pa $\mathcal{S}$ ima maksimalan član I. Tada je I maksimalan ideal u F[x] i $p \in I$. Neka je $K = F[x]/I$ količnički prsten i $k : F \to K$ kanonički homomorfizam, tj. $k : q \to q/I$. Neka su $r, q \in F[x]$ takvi da $r \cdot q \in I$. Dakle, za $q, r \in F[x]$ $q/I = \{s \in F[x] / q - s \in I\} = q + I$ $q/I + r/I = (q+r)/I$,

$(q/I)\cdot(r/I)=(qr)/I$. Nula ovog prstena je $I=0/I$.
Ako $r\notin I$, tada ideal generisan skupom $I\cup\{r\}$ nije pravi, dakle, za neki $m\in F[x]$ i $j\in I$ važi $m\cdot r+j=1$. Otuda $mrq+jq=q$, odakle sledi $q\in I$. Stoga

$$rq\in I\Rightarrow r\in I \text{ v } q\in I$$

tj. za $a,b\in K$ važi $ab=0\Rightarrow a=0$ v $b=0$ (uzmimo $a=r/I, b=r/I$). Dalje, neka je $a\in K$, $a\neq 0$. Tada za neki $q\notin I$ $a=q/I$. Otuda, ideal generisan sa $I\cup\{q\}$ jednak je $F[x]$, pa za neki $m\in F[x]$, $i\in I$, važi $mq+i=1$. S obzirom da je k homomorfizam, sledi $k(m)k(q)+k(i)=k(i)$, tj. za $b=k(m)$ važi $b\cdot a=1$, jer $k(q)=q/I=a$, i $k(i)=0$.

Ovim smo pokazali da je K polje. Primetimo da se polje F utapa u K: ako je $r\in F\setminus\{0\}$ onda iz $r\in I$ sledi $r\cdot 1/r\in I$ pa $1\in I$. Onda svaki $p\in F[x]$ pripada I jer $p=1\cdot p$, što je suprotno pretpostavci da je I pravi ideal. Otuda za $r_1,r_2\in F$, iz $r_1/I=r_2/I$ sledi $r_1-r_2\in I$ tj. $r_1=r_2$, dakle preslikavanje $r\to r/I$, $r\in I$ je utapanje, pa možemo uzeti da je K raširenje polja F.

Dakle, možemo uzeti da $p\in K[x]$. Tada za $a=x/I$ važi $p(a)=p(x/I)=p(k(x))=I=0_K$, jer $p\in I$. Prema tome, a je koren polinoma p u K. ▼

Raširenje $K\supseteq F$ je korensko polje polinoma $p\in F[x]$ ukoliko je p proizvod nekih linearnih polinoma iz K i nije proizvod linearnih polinoma ni iz jednog medjupolja.

Teorema 2.8. *Svaki polinom p ima korensko polje.*

Dokaz: Višestrukom primenom Leme 2.7 i Teoreme 2.1 nalazimo polje K u kojem se p razlaže na linearne faktore. Ako je F osnovno polje polinoma p i $\alpha_1,\ldots,\alpha_n$ svi koreni u K polinoma p, tada je $F[\alpha_1,\ldots,\alpha_n]$ korensko polje polinoma p. ▼

Polje K je *algebarski zatvoreno* ukoliko svaki nekonstantni polinom $p\in K[x]$ ima koren u K. Polje K je *algebarski zatvorenje* polja K ukoliko je K algebarsko raširenje polja F i K je algebarski zatvoreno.

Teorema 2.9. *Svako polje F ima algebarsko zatvorenje.*

Dokaz: Ovaj stav dokazaćemo primenom stava kompaktnosti.

Neka je $C=\{c_p \mid p\in F[x]\}$ skup novih simbola konstanata tako da su za različite $p,q\in F[x]$, simboli c_p i c_q takodje medjusobno različiti. Prema Lemi 2.7 skup rečenica

$$T=\text{Teorija polja} + \Delta(\underline{F}) + \{p(c_p)=0 \mid p\in F[x]\}$$

je konačno neprotivurečan[1)], pa prema stavu kompaktnosti postoji model $(\underline{H}, c_p)\ p \in F[x]$ za T. Tada se $\underline{F}$ utapa u polje $\underline{H}$ i svaki polinom $p \in F[x]$ stepena > 1, ima koren u T. Dakle, postoji niz polja

$$F = F_0 \subseteq F_1 \subseteq \ldots$$

tako da svaki $p \in F_i$ ima koren u F_{i+1}. Tada je $K = \bigcup_i F_i$ algebarski zatvoreno polje i $F \subseteq K$, a medjupolje $L = \{a \in K \mid a$ je algebarski nad $F\}$ je algebarsko zatvaranje polja K.

Konstrukcije lenjirom i šestarom

Neki geometrijski problemi mogu se prevesti na odgovarajuće probleme u algebri. U ovom slučaju koristićemo metode analitičke geometrije, tako što ćemo tačke Euklidske ravni označiti parovima realnih brojeva. Pretpostavimo da su nam na raspolaganju sve tačke sa celobrojnim koordinatama. One tačke u ravni koje se mogu dobiti primenom lenjira i šestara nazivamo *konstruktibilnim*. Realan broj x nazovimo konstruktibilnim ukoliko je par (x,0) konstruktibilan. Primetimo da par (a,b) odredjuje konstruktibilnu tačku akko su a,b konstruktibilni brojevi.

Pažljivom analizom konstrukcija lenjirom i šestarom pokazuje se da za konstruktibilne tačke važe ove osobine, kao i da su sve dozvoljene konstrukcije svodljive na ove koje navodimo:

Neka su A, B, C, D različite konstruktibilne tačke. Tada

1° ukoliko su prave AB i CD ne-paralelne, tada je presečna tačka ovih pravih konstruktibilna.

2° Ako je K krug sa centrom A i prečnikom AB takav da seče pravu CD, tada su presečne tačke kruga K i prave CD konstruktibilne.

Pretpostavimo da koordinate tačaka A, B, C, D leže u nekom podpolju F polja realnih brojeva. Koristeći se metodom analitičke geometrije neposredno nalazimo:

U slučaju 1° koordinate nove tačke leže u F.

U slučaju 2° koordinate nove tačke leže u F ili $F(\sqrt{a})$, gde

---

[1)] $\Delta(\underline{F})$ je dijagram polja $\underline{F}$, tj. skup svih rečenica vida $u=v$, $u \neq v$, gde su u,v termi jezika $\{\underline{a} \mid a \in F\} \cup \{+,\cdot,0,1\}$.

je $a \in F$ neki pozitivan broj.

Dakle, za svaki konstruktibilan broj a postoji $n \in N$ tako da $Q = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n$, i $a \in F_n$, gde je za $i \leq n$ $F_i = F_{i-1}(\sqrt{a_i})$, a_i je neki pozitivan broj iz F_{i-1}. Prema Teoremi 2.6. nalazimo da je $|F_n:Q| = 2^m$ za neki $m \in N$, pa je i $|F(a):Q|$ stepen broja 2. Otuda važi sledeća

Teorema 2.10. *Svaki konstruktibilan realan broj je algebarski nad poljem Q, i njegov stepen nad Q jednak je stepenu broja 2.*

Galois-ove grupe

Na kraju, evo nas na početku! Naime, kao što je više puta napomenuto, teorija grupa vodi svoje poreklo iz razmatranja algebarskih jednačina. U ovom poglavlju razmotrićemo neke ideje, kako se ovi i slični problemi iz teorije polja, svode na pitanja iz teorije grupa.

Neka je F polje, $p \in F[x]$ i $\sigma \in \mathrm{Aut}\ F$. Ako σ fiksira koeficijente polinoma p, tada σ preslikava korene polinoma p u korene polinoma p. Zaista, ako je $p(a)=0$, tada $\sigma(p(a))=0$, odakle $p(\sigma(a))=0$, jer je σ homomorfizam. Dakle, automorfizmu σ odgovara jedna permutacija korena polinoma p. Pod odredjenim uslovima važi i obrat, tj. nekim permutacijama korena polinoma p mogu se pridruženi automorfizmi korenskog polja polinoma p.

Neka je K proširenje polja F i $G = \{\sigma \in \mathrm{Aut}\ K \mid \forall x \in F\ \sigma(x)=x\}$. Tada se neposredno proverava da je G grupa u odnosu na slaganje funkcija. Ova grupa naziva se *Galois-ovom grupom* proširenja polja F i označava se sa G(K/F).

Definicija 2.11. Neka je K algebarsko proširenje polja F. Tada

1° K je *normalno* proširenje polja F akko svaki nesvodljiv polinom $p \in F[x]$ koji ima koren K, razlaže se na linearne faktore u K.

2° Polinom $p \in F[x]$ je *separabilan* akko p nema višestruke korene ni u jednom proširenju polja F.
Element $a \in K$ je *separabilan* nad F akko a je koren nekog separabilnog polinoma nad F.
Proširenje K je *separabilno* nad F akko je svaki element polja K separabilan nad F.

3° K je Galois-ovo rašširenje polja F akko je K separabilno i normalno rašširenje polja F.

Fundamentalni stav teorije Galoisa je sledeća

Teorema 2.12. Neka je K konačno Galois-ovo rašširenje polja F i neka je G = G(K/F). Dalje, neka je $\mathcal{F}$ skup svih medjupolja L, $F \subseteq L \subseteq K$ i neka je $\mathcal{S}$ skup svih podgrupa grupe G.

Za preslikavanje $^*: \mathcal{F} \to \mathcal{S}$, definisano sa $L^* = G(K/L)$, $L \in \mathcal{F}$, važe sledeće osobine:

*(i) Preslikavanje * je 1-1 i <u>na</u>.*

(ii) $|L^*| = |K:L|$, $|G:L^*| = |L:F|$

(iii) $L^* \triangleleft G$ akko je L normalno rašširenje polja F.

Najpre navedimo nekoliko činjenica u vezi sa prethodnom teoremom.

Preslikavanje * iz ove teoreme naziva se Galoisovim preslikavanjem. Kao i u slučaju preslikavanja *, svakoj grupi $H \in \mathcal{S}$ pridružuje se medjupolje $L = \{x \in K | (\forall \sigma \in H)\ \sigma(x) = x\}$. Za ovo medjupolje takodje ćemo koristiti znak *, tj. uzećemo $L = H^*$. Dakle, za svaku podgrupu $H < G(K/F)$, $H^* = \{x \in K | (\forall \sigma \in H)\ \sigma(x) = x\}$.

Važan slučaj primene osnovne teoreme odnosi se na korenska rašširenja polinoma. Naime, neka je $p \in F[x]$ separabilan i neka je K ⊇ F rašširenje polja F koje sadrži korensko polje $F(a_1,\ldots,a_n)$ polinoma p. *Grupa jednačine* $p(x)=0$, ili polinoma p, je Galois-ova grupa $G_p = G(F(a_1,\ldots,a_n)/F)$.

Primetili smo da svaki automorfizam $\sigma \in G_p$ odredjuje jednu permutaciju korena polinoma p, tj. ako je $\tau = \sigma|\{a_1,\ldots,a_n\}$, tada $\tau \in \mathrm{Sym}\ \{a_1,\ldots,a_n\}$. S druge strane, ako je $\varsigma \in \mathrm{Sym}\ \{a_1,\ldots,a_n\}$ tada postoji najviše jedan $\sigma \in G_p$ takav da $\sigma|\{a_1,\ldots,a_n\} = \varsigma$. Jer, ako je $a \in F(a_1,\ldots,a_n)$, tada postoji neki racionalan izraz $R(x_1,\ldots,x_n)$ nad F takav da $a = R(a_1,\ldots,a_n)$. Otuda

$$\sigma(a) = R(\sigma(a_1),\ldots,\sigma(a_n)) = R(\varsigma(a_1),\ldots,\varsigma(a_n)).$$

Dakle, grupi G pridružena je jedinstvena podgrupa $H < S_n$ takva da $G \cong H$, pa se često uzima slobodnije da je $G < S_n$.

Sada najpre dokazujemo nekoliko tvrdjenja koja pored primene u dokazu Teoreme 2.12. imaju svoj nezavisan interes, takodje.

<u>Definicija 2.13.</u> Neka je $(G,\cdot,1)$ grupa, $(F,+,\cdot,0,1)$ polje i $\sigma_j : (G,\cdot,1) \to (F\setminus\{0\},\cdot,1)$, $j=1,\ldots,n$, homomorfizmi. Preslika-

vanja $\sigma_1,\ldots,\sigma_n$ *su* <u>*nezavisna ukoliko*</u> *ne postoje* $a_1,\ldots,a_n \in F$ *takvi da*

$$(\forall x \in G) \sum_{i<n} a_i\, \sigma_i(x) = 0.$$

Sledeća dva tvrdjenja pripadaju E. Artinu.

<u>*Lema 2.14.*</u> *Neka je* $(G,\cdot,1)$ *grupa,* $(F,+,\cdot,0,1)$ *polje i* $\sigma_j : G \to (F\setminus\{0\},\cdot,1)$, $j=1,2,\ldots,n$, *medjusobno različiti homomorfizmi. Tada su oni nezavisni.*

Dokaz: Ovaj dokaz izvodimo potpunom indukcijom.

Tvrdjenje je tačno za $n=1$ jer $a_1\cdot\sigma_1(x)=0$ povlači $a_1=0$.

Neka je $n>1$ i pretpostavimo induktivnu hipotezu, tj.
(IH) svaki pravi podskup od $\{\sigma_1,\ldots,\sigma_n\}$ je nezavisan.

Sada pretpostavimo da je za neki $x\in G$

$$a_1\,\sigma_1(x) + \ldots + a_n\,\sigma_n(x) = 0 \qquad (1)$$

netrivijalna nezavisnost izmedju $\sigma_1,\ldots,\sigma_n$. Tada su zbog IH svi elementi a_i različiti od 0. Kako je $\sigma_1 \neq \sigma_n$, postoji $e \in G$ takav da $\sigma_1(e) \neq \sigma_n(e)$. Množeći jednakost (1) sa a_n^{-1} dobijamo

$$b_1\,\sigma_1(x)+\ldots+b_{n-1}\,\sigma_{n-1}(x)+\sigma_n(x)=0, \quad b_i=a_n^{-1}a_i\neq 0 \qquad (2)$$

U jednakosti (2) zamenimo x sa ex. Tada

$$b_1\,\sigma_1(e)\,\sigma_1(x)+\ldots+b_{n-1}\,\sigma_{n-1}(e)\,\sigma_{n-1}(x)+\sigma_n(e)\,\sigma_n(x)=0$$

odnosno

$$\sigma_n^{-1}(e)b_1\,\sigma_1(e)\,\sigma_1(x)+\ldots+\sigma_n(x) = 0 \qquad (2')$$

Oduzimajući jednakost (2') od jednakosti (1) dobijamo

$$(b_1-\sigma_n(e)^{-1}b_1\,\sigma_1(e))\,\sigma_1(x)+\ldots+c_{n-1}\,\sigma_{n-1}(x) = 0 \qquad (3)$$

Koeficijent uz $\sigma_1(x)$ u jednakosti (3) nije 0, jer bi inače bilo $b_1=\sigma_n(e)^{-1}b_1\,\sigma_1(e)$, ali kako je $b_1\neq 0$, imali bismo $\sigma_n(e)=\sigma_1(e)$, suprotno izboru elementa e. Dakle, jednakost (3) bila bi netrivijalna zavisnost izmedju elemenata $\sigma_1,\sigma_2,\ldots,\sigma_{n-1}$, što je suprotno induktivnoj hipotezi. ▼

Posebno interesantan slučaj primene ove leme dobijamo ukoliko za grupu G izaberemo multiplikativnu grupu nekog polja.

<u>*Teorema 2.15.*</u> *Neka je* $H=\{\sigma_1,\ldots,\sigma_n\}$ *grupa nekih automorfizama polja K, tj.* $H < Aut\ K$. *Ako je F fiksno polje za H, dakle* $F = \{x\in K \mid (\forall\sigma\in H)\ \sigma(x)=x\}$, *Tada* $|K:F| = n$.

Dokaz: 1^0 $|K : F| \geq n$: Pretpostavimo suprotno, tj. $|K : F| = m < n$. Neka je $e_1,\ldots,e_m$ baza za vektorski prostor K nad poljem F. Tada sistem homogenih linearnih jednačina

$$(S) \qquad \sum_{i\leq n} \sigma_i(e_j)x_i = 0 \quad , \quad j=1,\ldots,m$$

ima više nepoznatih nego jednačina, pa prema poznatom stavu iz linearne algebre ovaj sistem ima netrivijalno rešenje $\bar{x}_1,\ldots,\bar{x}_n$. Neka je $a \in K$ bilo koji element. Tada, s obzirom da je $< e_i | i=1,\ldots,m >$ baza, postoje $a_1,\ldots,a_m \in F$ takvi da $a=a_1e_1+\ldots+a_me_m$. Kako je F fiksno polje za H i $a_i \in F$, to $\sigma_j(a_i)=a_i$ i

$$\sigma_j(a_ie_i) = \sigma_j(a_i)\ \sigma_j(e_i) = a_i\ \sigma_j(e_i)$$

jer $\sigma_j \in \mathrm{Aut}\ K$. Stoga, množeći prvu jednačinu sistema (S) sa a_1, drugu sa a_2, itd., imamo

$$(S') \qquad \sum_{i\leq n} \sigma_i(a_je_j)\bar{x}_i = 0 \quad , \quad j=1,\ldots,m$$

Ukoliko saberemo sve ove jednačine i koristeći

$$\sum_{j\leq m} \sigma_i(a_je_j) = \sigma_i\left(\sum_j a_je_j\right) = \sigma_i(a)$$

dobijamo

$$\sum_i \sigma_i(a)\bar{x}_i = 0$$

što predstavlja netrivijalnu zavisnost izmedju automorfizma $\sigma_1,\ldots,\sigma_n$, a to je kontradikcija prema Lemi 2.14. (v. takodje napomenu iza ove leme).

2^0 $|K : F| \leq n$. Pretpostavimo suprotno, tj. $|K : F| > n$. Tada postoje $e_1,\ldots,e_{n+1} \in K$ koji su kao vektori linearno nezavisni nad poljem F. Prema već pomenutoj teoremi iz linearne algebre, sledeći sistem homogenih linearnih jednačina

$$(S) \qquad \sum_{i\leq n+1} \sigma_j(e_i)x_i = 0 \quad , \quad j=1,\ldots,n \ .$$

ima netrivijalno rešenje. Primetimo da ova rešenja leže u polju F, jer s obzirom da $I_K \in H$, recimo $\sigma_1 = I_K$, imali bismo linearnu zavisnost izmedju $e_1,\ldots,e_{n+1}$.

Neka je $a_1,\ldots,a_m,0,\ldots,0$ ono netrivijalno rešenje sistema (S) koje ima najmanji broj članova različitih od 0 (možemo uzeti $a_1,\ldots,a_m \neq 0$). Primetimo da je $m>1$ (jer $a_1 \neq 0$ i $\sigma_1(e_1)=e_1 \neq 0$). Isto tako, može se uzeti da je $a_m=1$, jer možemo dobiti takvo rešenje množeći članove datog rešenja sa a_m^{-1}. Dakle,

$$a_1\ \sigma_i(e_1) + \ldots + a_{m-1}\ \sigma_i(e_{m-1}) + \sigma_i(e_m) = 0,\ i=1,\ldots,n \quad (1)$$

Bar jedan od elemenata $a_1,\ldots,a_{m-1}$ ne pripada polju F, pa uzmimo da $a_1 \in K\setminus F$. Tada za neki $\sigma_k \in H$ važi $\sigma_k(a_1) \neq a_1$. Dalje, H je grupa, pa je $(\sigma_k\sigma_1,\ldots,\sigma_k\sigma_n)$ jedna permutacija skupa H. Primenom preslikavanja σ_k na jednakost (1) sledi

$$\sigma_k(a_1)\sigma_k\ \sigma_j(e_1)+\ldots+\sigma_k(a_{m-1})\ \sigma_k\ \sigma_j(e_{m-1})+\sigma_k\ \sigma_j(e_m)=0$$

$$j=1,\ldots,n$$

pa za $\sigma_i = \sigma_k\sigma_j$ važi

$$\sigma_k(a_1)\sigma_i(e_1)+\ldots+\sigma_k(a_{m-1})\sigma_i(e_{m-1})+\sigma_i(e_m) = 0,\ i=1,\ldots,n \quad (2)$$

Iz (1) i (2) oduzimanjem sledi

$$(a_1-\sigma_k(a_1))\ \sigma_i(e_1)+\ldots+(a_{m-1}-\sigma_k(a_{m-1}))\ \sigma_i(e_{m-1})=0,$$

$$i=1,\ldots,n$$

što znači da sistem (S) ima netrivijalno rešenje koje ima manje od m elemenata različitih od 0, suprotno izboru broja m. ▼

Posledica 2.16. *Neka je K proširenje polja F i G = G(K/F). Ako je G konačna grupa tada za svaku podgrupu H < G važi H** = H.*

Dokaz: Ako je $\sigma\in H$ i $x\in H^*$ tada $\sigma(x)=x$. Dakle, $\sigma\in H^{**}$, tj. $H < H^{**}$. Dokazujemo da je $H^{**} < H$. Prema prethodnoj teoremi za $n=|H|$ važi $[K:H^*]=n$. Pretpostavimo da postoji $\sigma\in H^{**}\setminus H$. No tada je H^* fiksiran sa skupom od n+1 automorfizama, pa prema dokazu 1° Teorema 2.15. $|K:H^*|\geq n+1$, što je kontradikcija. ▼

Lema 2.17. *Neka je σ: F → F' izomorfizam polja F, F'. Dalje, neka je $p\in F[x]$ nesvodljiv polinom nad F i $p'\in F[x]$ njemu odgovarajući polinom prema izomorfizmu σ. Ako su K = F(α) i K' = F'(α') proširenja polja F i F' redom, gde p(α) = 0 u K i p'(α') = 0 u K', onda se σ može produžiti do izomorfizma polja K i K'.*

Dokaz:

$$\begin{array}{ccc} K & \xrightarrow{\theta} & K' \\ \cup & & \cup \\ F & \xrightarrow{\sigma} & F' \end{array}$$

Neka je $I=\{q\in F[x] \mid p|q\}$. Tada je I ideal prstena F[x]. Neka su $a,b\in F[x]$ takvi da $ab\in I$. Tada $p|ab$. Pretpostavimo da $p\nmid a$. Tada su a,p uzajamno prosti, pa kako u F[x] važi Euklidov algoritam, to u F[x] takodje važi Bezuet-ov stav, tj. postoje polinomi .

$m,n\in F[x]$ takvi da $m\cdot a+n\cdot p=1$, odakle $mab+nbp=b$. Kako $p|ab$, to $p|b$. Dakle, dokazali smo

(1) $a \cdot b \in I \Rightarrow a \in I \vee b \in I$.

Dokazujemo da je I maksimalan ideal. Neka je $a \in F[x]$, $a \notin I$. Tada $p \nmid a$, pa su p i a uzajamno prosti, te postoje $m,n \in F[x]$ takvi da $m \cdot a + n \cdot p = 1$. Ali to znači da 1 pripada idealu generisanom skupom $I \cup \{a\}$, dakle,

(2) I je maksimalan ideal.

Onda, prema dokazu Leme 2.7. $L = F[x]/I$ je polje i $x+I$ je koren polinoma p u polju L. Ako je $a \in F[x]$ i $a = m \cdot p + r$, $str < stp$, onda $a/I = r/I$, dakle,

$$L = \{a/I \mid a \in F[x],\ sta < stp\}.$$

Kako je $a/I = a(x/I)$, to je za $d = x/I = x+I$, i $n = stp$

$$L = \{a(d) \mid a \in F[x],\ sta < n\}.$$

Neka je $\varphi: L \to K$ preslikavanje definisano sa $\varphi: \alpha_0 + \alpha_1 d + \ldots + \alpha_{n-1} d^{n-1} \mapsto \alpha_0 + \alpha_1 c + \ldots + \alpha_{n-1} d^{n-1}$ gde $\alpha_0, \ldots, \alpha_{n-1} \in F$. Tada se neposredno proverava da je φ izomorfizam polja L i K. Slično, neka je $\psi: L \to K'$, $\sigma : \alpha_0 + \alpha_1 d + \ldots + \alpha_{n-1} d^{n-1} \to \sigma(\alpha_0) + \sigma(\alpha_1)d + \ldots + \sigma(\alpha_{n-1}) d^{n-1}$. Tada je ψ izomorfizam polja L i K'. Otuda, $\theta = \psi \circ \varphi^{-1}$ je traženi izomorfizam. ▼

Prethodno tvrdjenje ima nekoliko posledica. Prva je

Posledica 2.18. Neka je $p \in F[x]$ nesvodljiv polinom i $K \supseteq F$ raširenje polja F tako da je $K = F(\alpha)$, i $p(\alpha) = 0$. Tada $|K : p| = stp$.

Isto tako, koristeći ovu lemu dokazuje se

Teorema 2.19. *Koreneko polje polinoma jedinstveno je do na izomorfizam.*

Teorema 2.20. *Ako je $\sigma: F_1 \to F_2$ izomorfizam polja $\underline{F}_1$, $\underline{F}_2$ tada postoji izomorfizam $\theta : K_1 \to K_2$, gde je $\sigma \subseteq \theta$, a K_1, K_2 su algebarska zatvorenja redom polja F_1, F_2.*

Elementi dokaza teorema 2.19 i 2.20. mogu se videti iz dokaza sledećeg tvrdjenja (tačka(1)).

Teorema 2.21. *Neka je K konačno Galois-ovo raširenje polja F, i neka je $G = G(K/F)$. Tada važi*

(i) $G^* = F$

(ii) *Ako je L medjupolje, tada je K Galois-ovo raširenje polja L.*

(iii) *Za svako medjupolje L važi* $L^{**} = L$.

Dokaz: (i) Neka je $\alpha_0 \in G^*$. Pretpostavimo da $\alpha_0 \notin F$. Neka je $p \in F[x]$ nesvodljiv polinom nad F takav da $p(\alpha_0)=0$ u K. Kako je K separabilno raširenje polja F, to p nema višestruke korene. S druge strane K je normalno raširenje polja F, dakle, p se razlaže na linearne faktore. Kako je st p>1, to je

$$p(x)=(x-\alpha_0)(x-\beta_0)\ldots(x-\gamma_0)$$

i $\beta_0 \neq \alpha_0$. Prema Lemi 2.17. postoji izomorfizam $\delta_0=F(\alpha_0) \to F(\beta_0)$ koji fiksira F i $\delta_0(\alpha_0)=\beta_0$. Preslikavanje δ_0 možemo produžiti do automorfizma $\delta \in \mathrm{Aut}\ K$: Neka je $\alpha_1 \in K \setminus F(\alpha_0)$ i p_1 nesvodljiv polinom nad $F(\alpha_0)$ takav da $p_1(\alpha_1)=0$ u K. Prema (ii) K je Galois-ovo raširenje, pa kao malopre nalazimo $\beta_1 \in k$ i izomorfizam $\delta_1 : F_0(\alpha_0,\alpha_1) \to F(\beta_0,\beta_1)$. Na ovaj način nalazimo niz polja

$$F \subsetneq F(d_0) \subsetneq F(\alpha_0,\alpha_1) \subsetneq \ldots$$

sadržanih u K. Kako je K konačno raširenje polja F i $|K : F| = |K : F(\alpha_0)| \cdot |F(\alpha_0) : F| = \ldots$

To je ovaj niz polja konačan, tj. za neki $n \in N$ $K = F(\alpha_0,\ldots,\alpha_n)$, pa $\delta_n \in \mathrm{Aut}\ K$, $\delta_n \supseteq \delta_0$. Kako δ_n fiksira F (jer δ_0 fiksira F), to $\delta_n \in G$. Otuda $\delta_n(\alpha_0)=\alpha_0$ (jer $\alpha_0 \in G^*$), ali to je kontradikcija pre-ma $\delta_n(\alpha_0) = \delta_0(\alpha_0) = \beta_0$ i $\alpha_0 \neq \beta_0$.

(ii) Neka je L medjupolje. Kako je F L i K je separabilan nad F, tim pre je K separabilno nad K.

Neka je $p \in L[x]$ nesvodljiv polinom nad L i pretpostavimo da je za neki $\alpha \in K$ $p(\alpha)=0$. Neka je $q \in F[x]$ nesvodljiv polinom nad F takav da $q(\alpha)=0$ (takav postoji jer je K algebarsko raširenje polja F). Tada $q \in L[x]$, pa s obzirom na nesvodljivost polinoma p u L, to $p|q$ tj. $q=a \cdot p$. Polje K je normalno raširenje, pa se q može predstaviti kao proizvod linearnih faktora u K. To očigledno daje faktorizaciju i polinoma p na linearne članove.

(iii) Neka je L medjupolje. Tada je prema (ii) K Galois-ovo raširenje polja L i prema (i) važi

$$L^{**} = G(K/L)^* = L \quad .$$

Sada smo u mogućnosti da dokažemo Osnovnu Teoremu Galois-ove teorije.

Dokaz Teoreme 2.12.

(i) Preslikavanje * je 1-1: Ako je $L_1^* = L_2^*$ tada $L_1^{**} = L_2^{**}$, odakle prema Teoremi 2.21. sledi $L_1 = L_2$. Preslikavanje * je na : Ako je $H<G(K/F)$, tada prema posledici 2.16. važi $H = H^{**}$, tj. H je slika polja H^*.

(ii) Neka je $H<G$. Tada prema Teoremi 2.15. važi $|G:H^*|=|H|$, dakle, za svako medjupolje L važi

$$|G : L| = |L^*|$$

jer $L^{**} = L$.

Otuda iz jednakosti $|K:F| = |K:L| \cdot |L:F|$ sledi

$$|F^*| = |L^*| \cdot |L:F|$$ odakle, koristeći $F^* = G$,

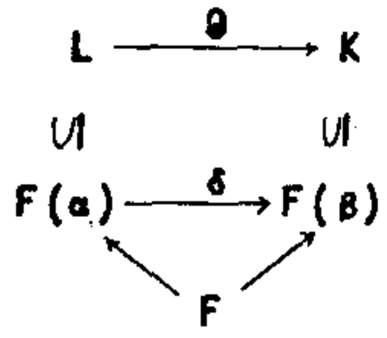
$$|L:F| = |G:L^*| .$$

(iii) Najpre dokažimo:

(*) Medjupolje L je normalno rašireњe polja F akko svako utapanje $\delta : L \to K$ koje fiksira F jeste automorfizam polja L.

($\Rightarrow$) Neka je L normalno rašireњe polja F i $\delta: L \to K$ utapanje. Neka je $\alpha \in L$ i $p \in F[x]$ nesvodljiv polinom takav da $p(\alpha) =0$. Tada $\delta(p(\alpha)) = 0$, odakle $p(\delta(\alpha)) = 0$, tj. $\delta(\alpha)$ je koren polinoma p. S druge strane, zbog normalnosti polja L, p se u K razlaže u proizvod linearnih faktora, dakle $\delta(\alpha) \in L$, tj. $\delta \in Aut\ L$.

($\Leftarrow$) Neka L nije normalno rašireњe polja F. Tada postoji $\alpha \in L$ i nesvodljiv polinom p nad K takav da $p(\alpha)=0$ u L i p se ne može predstaviti kao proizvod linearnih faktora u L. S druge strane, K je normalno rašireњe polja F, dakle p se razlaže na proizvod linearnih faktora u K (jer $p(\alpha)=0$ u K takodje), odakle sledi da postoji $\beta \in K \setminus L$ takav da $p(\beta)=0$ =0. Prema Lemi 2.17. postoji izomorfizam $\delta: F(\alpha) \to F(\beta)$. Kao u dokazu Teoreme 2.21.(i) tada dokazujemo da postoji utapanje $\theta : L \to K$ koje produžuje δ . Kako je $\theta(\alpha) = \delta(\alpha) = \beta$ i $\beta \notin L$, to $\theta \notin Aut\ L$.



Ovim je dokazano tvrdjenje (*).

Sada, neka je L normalno rašireњe polja K i neka je $G' = G(L/F)$. Prema (*) preslikavanje $\phi : \delta \to \delta|_L$ jeste homomorfizam grupe G u grupu G'. Dalje, $\delta \in Ker\ \phi$ akko $\delta|_L = I_L$ akko $\delta \in G(K/L)$, pa

$$Ker\ \phi = L^*.$$

Otuda $L^* \triangleleft G$, a takodje i $G/L^* = G(L/F)$. Sada pretpostavimo da L *nije normalno raširenje polja F. Tada postoji utapanje* $\delta : L \to K$ koje *nije* automorfizam polja L, a sa druge strane $\delta \restriction F = I_F$. Kao u dokazu Teoreme 2.21. (i) dokazujemo da postoji $\theta \in \mathrm{Aut}\, K$ takav da $\delta \subseteq \theta$. Tada je lako proveriti da važi

$$G(K/\delta(L)) = \theta\, G(K/L)\theta^{-1}.$$

Odavde sledi da L^* nije normalna u G jer $L^* \neq G(K/\delta(L))$. ▼

Posledica 2.22. Neka je K konačno Galois-ovo raširenje polja F. Tada je broj medjupolja konačan.

Dokaz: Primetimo da konačna grupa ima konačan broj podgrupa. ▼

Neka je F polje karakteristike 0. Tada je prema zadatku 2.11. svako algebarsko raširenje polja F separabilno. Dalje, neka je $p \in F[x]$ i neka je $F(\alpha_1,\dots,\alpha_n)$ korensko polje polinoma p. Tada je $F(\alpha_1,\dots,\alpha_n)$ Galois-ovo *raširenje* polja F (ovde su $\alpha_1,\dots,\alpha_n$ svi koreni polinoma p). Zaista, dovoljno je dokazati da je $F(\alpha_1,\dots,\alpha_n)$ normalno raširenje polja F.

Neka je K algebarsko zatvorenje polja $F(\alpha_1,\dots,\alpha_n)$. Prema tvrdjenju (*) u dokazu 2.12. (i), dovoljno je dokazati da je svako utapanje $\delta : F(\alpha_1,\dots,\alpha_n) \to K$ *automorfizam* polja K. Ali, to neposredno sledi, jer δ samo permutuje korene $\alpha_1,\dots,\alpha_n$, tj. $(\delta\alpha_1,\dots,\delta\alpha_n)$ je jedna permutacija skupa $\{\alpha_1,\dots,\alpha_n\}$, jer

$$p(\alpha_i) = 0 \Rightarrow \delta(p(\alpha_i)) = 0 \Rightarrow p(\delta(\alpha_i)) = 0.$$

Zadaci

2.1. Neka su *p i q prosti brojevi i* $Q_{p,q} = \{\frac{a\sqrt{p} + b\sqrt{a}}{c\sqrt{p} + d\sqrt{a}} \mid a,b,c,d \in Q, c^2+d^2 \neq 0\}$. Dokazati *da je* $(Q_{p,q},+,\cdot,0,1)$ *polje i odrediti* $|Q_{p,q}:Q|$.

Rešenje: Ako je $p=q$ *tada* $Q_{p,q}=Q$. *Neka je* $p\neq q$. *Tada* $\frac{a\sqrt{p} + b\sqrt{a}}{c\sqrt{p} + d\sqrt{q}} = \frac{a + b\sqrt{q/p}}{c + d\sqrt{q/p}}$. *Kako je* $S=\{\alpha+\beta\sqrt{q/p} \,/\, \alpha,\beta\in Q\}$ *podpolje polja realnih brojeva, to onda* $Q_{p,q}\subseteq S$. *S druge strane, očigledno* $S\subseteq Q_{p,q}$, *dakle* $S=Q_{p,q}$. *Kako je* $|S:Q|=2$, *to* $|Q_{p,q}:Q|=2$.

2.2. Dokazati da je polinom $q(x)=1+x+x^2+\ldots+x^{p-1}$, p je prost broj, nesvodljiv nad Q.

Rešenje: Dovoljno je dokazati nesvodljivost polinoma $q(x+1)$, jer $q(x)=g(x)h(x) \Rightarrow q(x+1)=g(x+1)h(x+1)$. Kako je $q(x+1) = \frac{(x+1)^p-1}{x}$ $\Rightarrow q(x+1)=\binom{p}{1}+\binom{p}{2}x+\ldots+\binom{p}{p-1}x^{p-1}+x^p$, za svaki i, $1<i<p$, $p\mid\binom{p}{i}$, pa kako $p^2\nmid p$, prema Eisenstein-ovom kriterijumu $q(x+1)$ je nesvodljiv.

2.3. Razložiti polinome x^p-x, $x^{p-1}-1$ na nesvodljive faktore u polju $\underline{Z}p$, p je prost broj.

Rešenje: U $\underline{Z}p$ važi $x^p-x=0$, dakle, <u>svi</u> elementi polja Zp su koreni polinoma x^p-x, tj. $x^p-x=x(x-1)(x-2)\ldots(x-(p-1))$.

2.4. Neka su $a_1,a_2,\ldots,a_n$ različiti celi brojevi. Dokazati da je polinom $p(x)=(x-a_1)\ldots(x-a_n)-1$ nesvodljivi nad Q.

Rešenje: Pretpostavimo da je $p(x)=g(x)h(x)$, $1\leq stg$, $sth\leq stp-1$, $g,h\in Z[x]$. Tada $g(a_i)h(a_i)=-1$ i $g(a_i)$, $h(a_i)$ su celi brojevi. Otuda, $g(a_i)+h(a_i)=0$ za $i=1,2,\ldots,n$. Dalje, polinom $g(x)+h(x)$ je stepena $\leq n$ i ima n različitih korena. Otuda, $(\forall x\in R)\ g(x)+h(x)=0$ te $h(x)=-g(x)$. Stoga, $p(x)=-g(x)^2$, što je nemoguće, jer $p(x)$ uz x^n ima koeficijent 1.

2.5. Neka su F, E, K polja takva da $F\subseteq E\subseteq K$. Dokazati:
$|K : F| = |K : E|\cdot |E : F|$.

Rešenje: Neka su A,B redom baze prostora $(K,+)$ nad E i prostora $(E,+)$ nad poljem F. Prema definiciji dimenzije vektorskog prostora važi $|K : E| = |A|$, $|E : F| = |B|$. Dokazujemo da je $C=\{ab \mid a\in A,\ b\in B\}$ baza prostora $(K,+)$ nad E.

1^o Skup C generiše K, tj. svaki $x\in K$ je linearna kombinacija vektora iz C. Zaista, neka $x\in K$. Budući da je A baza za $(K,+)$ nad E, postoji $n\in N$, $\alpha_1,\alpha_2,\ldots,\alpha_n\in E$ i $a_1,\ldots,a_n\in A$ tako da $x=\alpha_1a_1+\alpha_2a_2+\ldots+\alpha_na_n$. Kako je B baza za $(E,+)$ nad F svaki α_i je linearna kombinacija nekih vektora iz B. Kako vektora α_i ima konačno mnogo (tj. n), to postoje vektori $b_1,b_2,\ldots,b_m\in B$ tako da je svaki α_i $(1\leq i\leq n)$ linearna kombinacija vektora $b_1,\ldots,b_m$. Otuda $\alpha_i=\beta_{i1}b_1+\ldots+\beta_{in}b_n$ za neke $\beta_{i1},\beta_{i2},\ldots,\beta_{in}\in F$, $1\leq i\leq n$. Prema tome,

$$x=\beta_{11}a_1b_1+\beta_{12}a_1b_2+\ldots+\beta_{1n}a_1b_n+\beta_{21}a_1b_1+\ldots+\beta_{nm}a_nb_m\ .$$

2^{o} Vektori iz skupa C su linearno nezavisni. Zaista, neka su $\lambda_{ij} \in F$, $a_i \in A$, $b_j \in B$, $1 \leq i \leq n$, $1 \leq j \leq m$ takvi da $\sum_{i,j} \lambda_{ij} a_i b_j = 0$. Tada $\sum_i (\sum_j \lambda_{ij} b_j) a_i = 0$ i za svaki $i \in \{1,2,\ldots,n\}$ $(\sum_j \lambda_{ij} b_j) \in E$. Otuda zbog linearne nezavisnosti vektora a_i nad poljem E, važi $\sum_j \lambda_{ij} b_j = 0$, $i=1,2,\ldots,n$. Stoga, zbog linearne nezavisnosti vektora b_j (nad poljem F) sledi $\lambda_{ij}=0$, $j=1,2,\ldots,m$, $i=1,2,\ldots,n$. Prema prethodnom, C je baza proširenja $(K,+)$ nad poljem F, tj. $|K : F| = |C|$. Preslikavanje $\varphi : (a,b) \to ab$ $(a \in A, b \in B)$ je 1-1 i <u>na</u>. Zaista, ako je $ab = a'b'$, $a,a' \in A, b,b \in B$, tada $ba + (-b')a' = 0$, te kako su vektori iz skupa B linearno nezavisni i $a,a' \neq 0$ to $b'=b$ i $a=a'$. Očigledno, φ je <u>na</u>. Prema prethodnom,
$|K : F| = |C| = |A \times B| = |A||B| = |K : E| \cdot |E : F|$.

Nekoliko sledećih zadataka odnose se na pitanje, u kojim slučajevima je moguće rešiti geometrijski zadak, koristeći pri tome jedino lenjir i šestar. Ovde je od naročitog interesa paragraf o konstrukciji lenjirom i šestarom, odnosno Teorema 2.6.

2.6. Dokazati da problem udvajanja kocke nije moguće rešiti pomoću lenjira i šestara.

Rešenje: Ovaj problem svodi se na to da se konstruiše $\sqrt[3]{2}$. Polinom $x^3 - 2$ je nesvodljiv nad poljem racionalnih brojeva. Prema Posledici 2.18. tada $|Q(\sqrt[3]{2}) : Q| = 3$, pa prema Teoremi 2.6. $\sqrt[3]{2}$ nije konstruktibilan broj.

2.7. Dokazati da problem kvadrature kruga nije moguće rešiti pomoću lenjira i šestara.

Rešenje: Ovaj problem svodi se na konstrukciju broja π. Ali, broj π je transcedentan, tj. nije algebarski nad Q, (dokaz ove činjenice nije jednostavan), pa prema Teoremi 2.6. ne može se konstruisati.

2.8. Dokazati da nije moguće u svakom slučaju rešiti problem trisekcije ugla pomoću lenjira i šestara.

Rešenje: Dokazaćemo da se ne može izvršiti trisekcija ugla od 60^{o} pomoću lenjira i šestara. Ovaj zadatak očigledno je ekvivalentan konstruktibilnosti broja $\cos 20^{o}$. Kako je

$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$, za $a=2\cos\theta$ nalazimo da je $a^3-3a-1=0$. Kako je polinom x^3-3x-1 nesvodljiv nad poljem Q (jer nema racionalnih korena), to pokazuje da je a stepena 3 nad Q, pa prema Teoremi 2.6. a nije konstruktibilan.

2.9. (F.Gauss) *Konstrukcija pravilnih poligona.* Prirodan broj a je Fermat-ov ukoliko je oblika $2^{2^x}+1$ za neki $x \in N$. Dokazati: Pravilan poligon sa n stranica može se konstruisati lenjirom i šestarom akko n je proizvol nekog stepena broja 2 i Fermatovih prostih brojeva.

Rešenje: Konstrukcija pravilnog poligona sa n stranica očigledno se svodi na pitanje konstruktibilnosti broja

$$\eta = 2\cos\frac{2\pi}{n} = \varepsilon + \varepsilon^{-1}$$

gde je $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ *primitivan koren n-tog stepena iz jedinice.*

Neka je S skup svih primitivnih korena iz jedinice n-tog stepena. Dakle, S je skup generatora ciklične grupe $(\{x\in C \mid x^n=1\},\cdot)$, pa $|S| = \varphi(n)$, gde je $\varphi(x)$ Euler-ova funkcija. Neka je $\Phi_n(x) = \prod_{\tau\in S}(x-\tau)$. *Tada*

(1) $\Phi_n(x) \in Q[x]$.

Dokaz tvrdjenja (1) izvodimo indukcijom. Zaista $\Phi_1(x)=x-1$, pa tvrdjenje važi za n=1. Dalje, pretpostavimo da tvrdjenje važi za $d<n$. Tada

$$x^n-1 = \prod_{d\mid n}\Phi_d(x) = \Phi_n(x)\prod_{\substack{d\mid n\\ d<n}}\Phi_d(x)$$

Po induktivnoj pretpostavci $\prod_{\substack{d\mid n\\ d<n}}\Phi_d(x) \in Q[x]$, *odakle sledi da* $\Phi_n(x) \in Q[x]$. *Ovim je (1) dokazano.*

Dalje, ako je $\varepsilon\in S$ tada $S=\{\varepsilon^j \mid j<n,(j,n)=1\}$, dakle

(2) $Q(\varepsilon)$ je korensko polje polinoma $\Phi_n(x)$.

Polinom $\Phi_n(x)$ *je separabilan, pa*

(3) $Q(\varepsilon)$ je Galois-ovo rašireњe polja Q.

Otuda, prema Teoremi 2.12. (ii) $|Q(\varepsilon):Q| = |G(Q(\varepsilon)/Q)|$.

Ako je $\delta\in G(Q(\varepsilon)|Q)$ tada $\delta(\varepsilon)\in S$ i δ je u potpunosti odredjen sa vrednošću $\delta(\varepsilon)$, pa $G(Q(\varepsilon)/Q)\cong$Aut C_n, C_n je ciklična grupa reda n. Kako je $|\text{Aut } C_n| = \varphi(n)$, *to*

(4) $|Q(\varepsilon):Q| = \varphi(n)$.

Dalje, $G(Q(\varepsilon)/Q(\eta)) = \{\delta \in Aut\ Q(\varepsilon) \mid \delta(\eta) = \eta\} = \{1, \mu\}$, gde $1 : x \to x$, $\mu : x \to x^{-1}$, jer: ako je $\delta(\eta)=\eta$, tada

$\delta(\varepsilon)=\varepsilon^j=\cos\frac{2\pi j}{n} + i\cos\frac{2\pi j}{n}$, gde $1\le j<n$, $(j,n)=1$. Takodje

$\delta(\eta)=\frac{\delta(\varepsilon)+\delta(\varepsilon)^{-1}}{2}$, pa $\delta(\eta)=2\cos\frac{2\pi j}{n}$. Otuda $\cos\frac{2\pi j}{n}=\cos\frac{2\pi}{n}$

odakle $j \in \{1,-1\}$.

Otuda, prema osnovnoj Teoremi 2.12. (ii) i prema (4) imamo

(5) $Q(\eta) : Q = \frac{\varphi(n)}{2}$.

<u>Napomena</u>: Do jednakosti (4) i (5) može se doći i tako što se dokaže nesvodljivost polinoma $\Phi_n(x)$ nad Q, a zatim primeni Posledica 2.18.

Sada, prema Teoremi 2.6. n je konstruktibilan akko $\frac{\varphi(n)}{2}$ je stepen broja 2, dakle i $\varphi(n)$ je stepena 2. Neka je $n=2^{\lambda} \cdot q_1^{\alpha_1} \dots q_k^{\alpha_k}$ razlaganje broja n na proste faktore. Tada prema 2.6.2.3

$$\varphi(n)=2^{\lambda-1} q_1^{\alpha_1-1} \dots q_k^{\alpha_k-1}(q_1-1)\dots(q_k-1).$$

Otuda $\alpha_1=\dots=\alpha_n=1$ i $q_j=2^m+1$ za neki $m \in N$. Ako je $m=u\cdot v$ i $n \in 2N+1$, tada $(2^v+1) \mid 2^m+1$, što je suprotno činjenici da je q_j prost broj. Dakle, $m=2^r+1$.

<u>Napomena</u>: $2^{2^r}+1$ je prost broj za $r=0,1,2,3,4$. Broj $2^{2^5}+1$ deljiv je sa 641.

2.10. (F.Gauss; ovaj dokaz u osnovi pripada E.Artinu).

Dokazati da je polje kompleksnih brojeva algebarsko zatvorenje polja realnih brojeva.

Rešenje: Neka je i imaginarna jedinica, tj. $i^2=-1$. Tada $\underline{C}=\underline{R}[i]$, dakle, $\underline{C}$ je algebarsko proširenje polja realnih brojeva.

Neka je $\bar{R}$ algebarsko zatvorenje realnih brojeva. Možemo pretpostaviti da je $i \in \bar{R}$, tj. $C \subseteq \bar{R}$. Neka je $a \in \bar{R}$. Tada je a algebarski element nad R, pa neka je $p \in R[x]$ takav da je $p(a)=0$ u polju $\bar{R}$. Dalje, neka je K korensko polje polinoma $(x^2+1)p(x)$. Tada $C \subseteq K$ i K je konačno Galois-ovo proširenje polja R.

Dokažimo da je $C=K$. Neka je $G=G(K/R)$, i neka je H sylowska 2-podgrupa grupe G. Ako je $F=H^*$, prema osnovnoj teoremi teorije Galoisa nalazimo da je $|F:R| \in 2N+1$. Neka je

$\alpha \in F$. Prema Teoremi 2.6. broj $|R(\alpha):R|$ deli $|F:R|$, dakle takodje $|R(\alpha):R| \in 2N+1$. Ako je $p \in R[x]$ nesvodljiv polinom nad R, takav da je $p(\alpha)=0$ u $R(\alpha)$, tada je $stp=|R(\alpha):R|$ dakle $stp \in 2N+1$. S druge strane, svaki polinom neparnog stepena nad R je svodljiv osim polinoma prvog stepena, pa $stp=1$. Otuda $\alpha \in R$, tj. $R(\alpha)=R$. Kako je $F=\bigcup_{\alpha \in F} R(\alpha)$, to takodje $F=R$, pa $G=R^*=F=-H^{**}=H$, tj. G je sylowska 2-podgrupa.

Dalje, primetimo da je K Galois-ovo rašireni nad $C=R(i)$, pa neka je $G_1=G(K/C)$. Kako je G_1 2-grupa, ako je G_1 netrivijalna, to onda prema z.8.2.7 postoji $H_1<G_1$ tako da $|G_1:H_1|=2$. Neka je $F_1=H_1^*$. Tada $|F_1:C|=2$, tj. $F_1=C(b)$, gde je $b^2 \in C$. Ali, lako je proveriti da je polje kompleksnih brojeva zatvoreno za korenovanje, pa $b \in C$, dakle $F_1=C$ što je suprotno sa $|F_1:C|=2$. Dakle, G_1 je trivijalna grupa, pa $K=C$, pa i $a \in C$. Otuda $\bar{R}=C$.

2.11. Ako je F polje karakteristike 0 i $p \in F[x]$ je nesvodljiv polinom nad F, dokazati da je p separabilan polinom.

Rešenje: Najpre dokažimo sledeće tvrdjenje:

T1 Neka je $f \in F[x]$ nesvodljiv polinom, $K \supseteq F$ rašireni i $a \in K$ je koren polinoma f u K. Tada za $g \in F[x]$ važi $g(a)=0 \Rightarrow f|g$.

Dokaz: Neka je $r \in F[x]$ polinom najmanjeg stepena takav da $r(a)=0$. Tada za neke $m,n \in F[x]$

$$f(X)=m(x)q(x)+n(X), \qquad st\ n<st\ r$$

Kako je $f(a)=r(a)=0$, to $n(a)=0$, pa prema izboru polinoma r sledi da je n 0-polinom. Dakle, $f=m \cdot r$, pa kako je f nesvodljiv sledi da je m konstanta i $st\ r = st\ f$.

Dalje, neka je $g \in F[x]$, $g(a)=0$ i neka su $q_1, q_2 \in F[x]$ takvi da $g(X)=q_1(X)f(X)+q_2(x)$, $stq_2<stq_1$. Tada $q_2(a)=0$, pa je q_2 0-polinom. ∇

Predjimo sada na samo tvrdjenje zadatka. Ako p nije separabilan, tada u nekom rašireni $K \supseteq F$ za neki $a \in K$ $p(a)=0$, $p'(a)=0$. Tada, prema T1 $p|p'$. Kako je $st\ p'<st\ p$, to je p' 0-polinom. Ali, ako je $p(X)=\sum_i a_i x^i$ i $st\ p=n$, tada u p' ux x^{n-1} stoji $n \cdot a_n \neq 0$, pa p' nije 0-polinom.

2.12. Neka je $p(x)=x^3+mx+n$ polinom nad poljem racionalnih brojeva Q, i neka je K korensko polje ovog polinoma. Odrediti $G=G(K/Q)$.

Rešenje: Ako p(x) ima sva tri korena racionalna tada je G trivijalna grupa. Ako p(x) ima dva racionalna korena, tada je i treći koren takodje racionalan, pa pretpostavimo da p(x) ima tačno jedan koren. Tada je G ciklična grupa reda 2.

Pretpostavimo da p nema racionalnih korena. Tada je p nesvodljiv polinom nad Q (jer bi p inače imao linearan faktor). Dakle, ako je $a \in K$ koren polinoma p prema P.2.18 *$|Q(a):Q| = 3$. Kako je $|K:Q|=|K:Q(a)|\cdot|Q(a):Q|$, to 3 deli $|K:Q|$. S druge strane, svaki automorfizam $\alpha \in G$ odredjen je jedinstveno nekom permutacijom korena polinoma p, tačnije G je izomorfna nekoj podgrupi grupe S_3. Dakle, $G \tilde{=} C_3$ ili $G \tilde{=} S_3$. Primetimo da ako je $G \tilde{=} S_3$, onda je prema* T.2.12. *$H=Q(a)^*$ indeksa 3 u S_3, pa $H \trianglelefteq S_3$. Otuda ni Q(a) nije Galois-ovo rašireanje polja Q.*

Primetimo da postoji jednostavan kriterijum kojim se utvrdjuje koji od dva pomenuta slučaja nastupa. Neka je

$$d=(a_1-a_2)(a_2-a_3)(a_3-a_1), \quad D=d^2$$

gde su a_1, a_2, a_3 svi koreni polinoma p (Primetimo da su ovi koreni različiti s obzirom da je p nesvodljiv nad Q, a Q je karakteristika 0, v. Z.2.11.). Ako je $\alpha \in G$ onda $\alpha(a_i)=a_j$, pa $\alpha(d)=\pm d$, odakle sledi $\alpha(D)=D$. Dakle, $D \in G^*$ tj. $D \in Q$. Zaista, $D=-4m^3-27n^2$.

Sada, ako je G reda 3 onda s obzirom da je G izomorfna podgrupi S_3 sledi $G \tilde{=} A_3$. Otuda ($\forall \alpha \in G$) $\alpha(d)=d$ odakle sledi $d \in Q$, tj. D je potpun kvadrat.

Sa druge strane, ako G nije reda 3, onda postoji $\alpha \in G$ kojem odgovara neparna permutacija korena a_1, a_2, a_3, pa $\alpha(d)=-d$. Otuda $d \notin G^*$, tj. $d \notin Q$, dakle Q nije potpun kvadrat.

Prema prethodnom važi :

D je potpun kvadrat $\Rightarrow G \tilde{=} C_3$

D nije potpun kvadrat $\Rightarrow G \tilde{=} S_3$.

Na primer, ako je $p(x)=x^3+x+1$ onda $D=-31$, pa $G \tilde{=} S_3$.

Ako je $p(x)=x^3-3x+1$ onda $D=81$, pa $G \tilde{=} C_3$.

2.13. Neka je p prost broj i K korensko polje polinoma x^p-1 nad

poljem F. Dokazati da je G=G(K/F) Abelova grupa.

Rešenje: Ako je F polje karakteristike p onda $x^p-1=(x-1)^p$, *pa K=F, tj. G(K/F) je trivijalna grupa.*

Pretpostavimo da F nije karakteristika p. Kako je $(x^p-1)'=p\cdot x^{p-1}$, *to su onda svi koreni ovog polinoma različiti. U stvari, ako je* $\varepsilon\neq 1$ *koren polinoma, tada su* $1, \varepsilon, \varepsilon^2, \cdot, \varepsilon^{p-1}$ *svi koreni ovog polinoma, pa* $K=F(\varepsilon)$. *Otuda, svaki automorfizam* $\varphi\in G$ *je u potpunosti odredjen svojom vrednošću* $\varphi(\varepsilon)$. *Neka su* $\varphi,\psi\in G$. *Tada* $\varphi(\varepsilon)=\varepsilon^i$, $\psi(\varepsilon)=\varepsilon^j$ *za neke i,j pa* $(\varphi\circ\psi)(\varepsilon)=\varepsilon^{ij}$ *i takodje* $(\psi\circ\varphi)(\varepsilon)=\varepsilon^{ij}$. *Dakle,* $\varphi\circ\psi=\psi\circ\varphi$.

Primetimo da je $|G|=p-1$.

2.14. Neka je F polje u kojem se polinom x^n-1 razlaže na proizvod linearnih faktora. Neka je $a\in F$, i K korensko polje polinoma x^n-a nad F. Dokazati da je G=G(K/F) Abelova grupa.

Rešenje: Ako je w koren polinoma x^n-a, *tada je bilo koje drugo rešenje jednačine* $x^n-a=0$ *oblika* εw *gde je* ε *koren jedinice, dakle i* $\varepsilon\in F$. *Otuda* $K=F(w)$, *pa je svaki automorfizam* $\alpha\in G$ *u potpunosti odredjen vrednošću* $\alpha(w)$. *Neka su* $\varphi,\psi\in G$ *i* $\varphi(w)=\varepsilon w$, $\psi(w)=\eta w$ *gde su* ε, η *koreni jedinice reda n. Tada*

$$(\varphi\circ\psi)(w)=\varepsilon\eta w, \quad (\psi\circ\varphi)(w)=\eta\varepsilon w \quad \text{pa}$$

$\varphi\circ\psi=\psi\circ\varphi$, *tj. G je Abelova grupa.*

2.15. Odrediti red Galois-ove grupe polinoma x^4-a, $a\in Q^+$.

Rešenje: Pretpostavimo da a nije potpun kvadrat. Tada je prema Eisensteinovom kriterijumu x^4-a *nesvodljiv nad Q. Neka je* $c\in C$ *jedan koren ovog polinoma i neka je* $i^2=-1$. *Tada* $|Q(i):Q|=2$ *i* $|Q(c):Q|=4$ *prema P.2.18. Korensko polje ovog polinoma je* $K=Q(c,i)$, *pa* $|K:Q|=|K:Q(c)|\cdot|Q(c):Q|$. *Kako* $i\notin Q(c)$ *jer je c realan, to* $|K:Q(c)|=2$, *tj.* $|K:Q|=8$. *Takodje,* $G(K/Q)=\langle\delta,\tau,\delta^n=1,\tau=1,\tau\delta=\delta^3\tau\rangle$, *gde* $\delta: c\to ic$, $\tau: i\to -i$.

2.16. Ako polje F sadrži primitivne n-te korene jedinice, korensko polje K polinoma $p(x)=(x^n-a_1)(x^n-a_2)\ldots(x^n-a_k)$, $a_1,\ldots,a_k\in F$, naziva se *Kummer-ovim raščirenjem* polja F.

Dokazati da je za svako Kumerovo rašširenje K polja F, Galoisova grupa G=G(K/F) Abelova.

Rešenje: Dokaz je sličan rešenju z.2.14 . Naime, dovoljno je primetiti da ako je w koren jednačine $x^n-a_i=0$ *i* $\delta \in G$, *tada je* $\delta(w)$ *koren iste jednačine. Dalje, ako su* $d_1,\ldots,d_k$ *koreni redom jednačina* $x^n=a_1,\ldots,x^n=a_k$, *tada* $K=F(d_1,\ldots,d_k)$. *Slično kao u z.2.14. dokazuje se da za* $\varphi,\psi \in G$ *važi*

$$(\varphi\circ\psi)(d_i) = (\psi\circ\varphi)(d_i), \quad i=1,\ldots,k$$

pa otuda $\varphi\circ\psi=\psi\circ\varphi$.

Proširenje K polja F je *radikalsko* ukoliko je $K=F(a_1,\ldots,a_n)$ gde je a_i koren neke jednačine $x^n=b$ za neki $n \in N$ i $b \in F(a_1,\ldots,a_{i-1})$, $i=1,\ldots,n$.

Primetimo da je svako radikalsko rašširenje konačno rašširenje. Dalje, može se pretpostaviti da prost stepen elementa a_i pripada $F(a_1,..,a_{i-1})$; ako to nije slučaj tada se može prost koren od a_i dodati skupu $F(a_1,..,a_{i-1})$, pritom pretpostavljajući da je $F(a_1,..,a_{i-1})$ sadržan u algebarskom zatvorenju od F.

Unija konačnog broja radikalskih rašširenja je radikalsko rašširenje; ako je $L=F(a_1,..,a_n)$, $K=F(b_1,..,b_m)$ tada $<L \cup K=F(a_1,..,a_n, b_1,..,b_m)$.

Najzad, bilo koje radikalsko rašširenje K polja F sadržano je u nekom normalnom radikalskom rašširenju. Zaista, možemo uzeti da je $K\subseteq\bar{F}$ gde je $\bar{F}$ algebarsko zatvorenje polja F. Ako je $K=F(a_1,..,a_k)$ neka je $p_1(x)=x^{n_1}-b_1$, gde je $a^{n_1}=b_1$ i $b_1 \in F$. Neka je $L_1 \subseteq \bar{F}$ korensko polje polinoma p_1 nad F. Dalje, neka je $p_2(x)=x^{n_2}-b_2$ gde je $b_2 \in F(a_1)$ i $L_2 \subseteq \bar{F}$ korensko polje polinoma p_2 nad L_1. Nastavljajući ovaj postupak dolazimo do normalnog rašširenja L_K tako da $F(a_1,\ldots,a_k)\subseteq L_K$. Tada je L_K takodje i radikalsko rašširenje polja K.

Algebarska jednačina $p(x)=0$ je rešiva radikalima akko je korensko polje polinoma p podpolje nekog radikalskog rašširenja polja F, $p \in F[x]$.

<u>Teorema</u> (E. Galois) Algebarska jednačina $p(x)=0$, $p \in F[x]$, *je rešiva u radikalima akko je Galoisova grupa polinoma p rešiva.*

Ovde dajemo dokaz samo dela ($\Rightarrow$).

Neka je $p(x)=0$ rešiva u radikalima. Dalje, neka je K normalno radikalsko rašširenje polja F koje sadrži korensko polje L polinoma p. Ako je $K=F(a_1,\ldots,a_k)$ neka su $L_0=F$, $L_i=L_{i-1}(a_i)$,

$i=1,\ldots,k$. Prema prethodnim napomenama možemo uzeti da je L_i Kummer-ovo rašširenje polja L_{i-1}, dakle grupe $G_i=G(L_i/L_{i-1})$, $i=1,\ldots,k$ su Abelove.

Kako je $L_0\subseteq L_1\subseteq\ldots\subseteq L_k$ to $G=L_0^*>L_1^*,>\ldots>L_k^*=<1>$ (setimo se da je $L^*_i=G(K/L_i)$). Kumerovo rašširenje je normalno jer je korensko polje polinoma, pa prema osnovnoj teoremi Teorije Galoisa važi $L_0^*>L_1^*>\ldots>L_k^*$ i $L_{i-1}^*/L_i^* = G(L_i/L_{i-1})$. Ali, grupa $G_i=G(L_i/L_{i-1})$ je Abelova, pa je $G=G(K/F)$ rešiva grupa. Dalje, polje L kao korensko polje je normalno rašširenje polja F, dakle, prema Osnovnoj teoremi grupa $L^*=G(K/L)$ je normalna podgrupa grupe $G=G(K/F)$, i $G/L^* = G(L/F)$, tj. G/L^* je Galoisova grupa polinoma p. S druge strane, G/L^* je homomorfna slika rešive grupe G, pa je i sama grupa G/L^* rešiva (v. poglavlje 9.).

2.17. Neka je $K=Q(x_1,\ldots,x_n)$ polje racionalnih izraza od promenljivih $x_1,\ldots,x_n$ nad poljem racionalnih izraza. Dokazati da je $G(K/Q) = S_n$.

Rešenje: Prema prethodnim napomenama $G(K/Q)$ je izomorfna nekoj podgrupi grupe S_n. S druge strane, za svaku permutaciju $\alpha\in Sym\{x_1,\ldots,x_n\}$ postoji $\delta_\alpha\in G(K/Q)$ koji produžuje α. Zaista, δ_α je odredjeno na sledeći način: ako je $p\in K$, tada $\delta_\alpha(p)\ (x_1,\ldots,x_n)=p(\alpha(x_1),\ldots,\alpha(x_n))$. Očigledno, preslikavanje $\alpha\to\delta_\alpha$ je 1-1, dakle $G(K/Q)\cong S_n$.

2.18. Neka je p prost broj >3 i f nesvodljiv polinom stepena p nad Q. Pretpostavimo da f ima tačno dva realna korena. Dokazati da je Galois-ova grupa G polinoma f izomorfna grupi S_p.

Rešenje: Neka je K korensko polje polinoma f, $a\in K$ koren polinoma f u polju K i neka je $G=G(K/Q)$ Galoisova grupa polinoma f. Možemo pretpostaviti da je $K\subseteq\underline{C}$, gde je $\underline{C}$ polje kompleksnih brojeva. Tada je K Galois-ovo rašširenje polja Q, pa prema Osnovnoj teoremi $|G|=|K:Q|$. S druge strane, $|K:Q|=|K:Q(a)|\cdot|Q(a):Q|$ pa kako je $|Q(a):Q|=p$ jer je R nesvodljiv nad Q, to $p\mid|G|$. Prema Cauchy-evoj lemi (v. poglavlje 10), G ima element reda 2, neka je to δ.

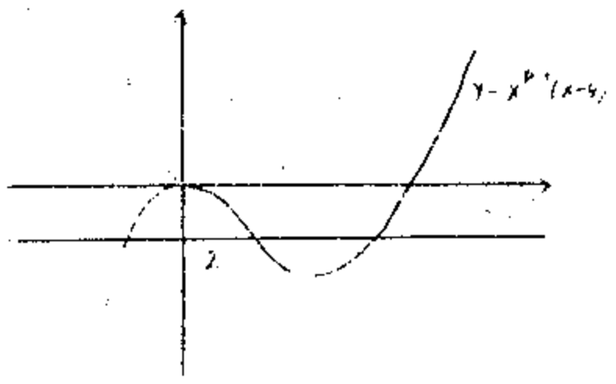
Dalje, ako je $\varphi: E\mapsto E$, tada je φ automorfizam

polja kompleksnih brojeva i $\varphi \in G(\underline{C}/\underline{R})$, i za svaki realan polinom g važi $g(x)=0 \Rightarrow g(\bar{x})=0$ $(x \in C)$. Polinom g ima bar jedan nerealan koren, pa $\tau = \varphi / K$ pripada G i jeste reda 2. (Primetimo da odavde sledi da je $p \geq 5$).

Kako je G izomorfna podgrupi grupe S_n, to možemo za trenutak pretpostaviti da je $G < S_n$. Kako je red $(\delta)=p$, i p prost broj, to je onda δ ciklus dužine p, recimo $\delta=(1\ 2\ \ldots\ p)$. Dalje, kako je red$(\tau)=2$, onda je τ transpozicija, recimo $\tau=(p/p)$. Tada je prema z. 4.1.20. $G \cong S_p$.

2.19. Navesti primer polinoma f prostog stepena p koji ispunjava uslove prethodnog zadatka.

Rešenje: $f(x)=x^p-4x^{p-1}+2$. *Polinom je nesvodljiv nad Q prema Eisenstein-ovom kriterijumu (za $p \geq 5$). $f(x)$ ima tačno dva realna korena, v. sliku.*



Dakle, Galois-ova grupa ovog polinoma je S_p

Za $p \geq 5$ njegova grupa nije rešiva (z.9.1.9), pa prema Galois-ovoj teoremi jednačina $x^p-4x^{p-1}=2$ ne može se rešiti u radikalima.

I N D E K S

SPISAK SIMBOLA

$\underline{A} = (A, \Omega, C)$	algebarska struktura (A je domen, Ω skup operacija, C skup konstanti iz A), 220
$\underline{A} = (A, F_i, a_j)_{i\in I, j\in J}$	NAPOMENA: U slučaju grupa, pored oznake $\underline{G}=(G,*,^{-1},e)$, korišćene su često i kraće oznake: $(G,*,^{-1})$, $(G,*,e)$, $(G,*)$. Takodje smo često grupu i njen domen označavali istim znakom, G (ako je iz konteksta jasno na šta se simbol odnosi).
$A = \prod_{i\in I} A_i$	Dekartov proizvod skupova A_i, VIII
$\underline{A} = \prod_{i\in I} \underline{A}_i$	direktan proizvod algebri $\underline{A}_i$, 221
$\underline{A}_1 \times \underline{A}_2 \times \ldots \times \underline{A}_n$	direktan proizvod konačnog broja algebri $\underline{A}_1, \ldots, \underline{A}_n$, 221
$\underline{A} \times_\sigma \underline{B}$	semi-direktni proizvod algebri $\underline{A}$ i $\underline{B}$, 167
$\underline{A}^I$	stepen algebre $\underline{A}$ ($\prod_{i\in I} \underline{A}$), 221
$(\underline{A}, b_i)_{i\in I}$	slobodan proizvod algebri $\underline{A}_i$ ($i\in I$), 233
$A_1 * A_2 * \ldots * A_n$	slobodan proizvod konačnog broja algebri $\underline{A}_1, \ldots, \underline{A}_n$, 233
$\underline{A}_1 \overset{*}{_H} \underline{A}_2$	slobodan proizvod grupa sa zajedničkom podgrupom H; koristi se još i oznaka (A_1, A_2, H_1, H_2, f) gde su $H_1 < A_1$, $H_2 < A_2$, $f: H_1 \rightarrow H_2$, kao i $A_1 \overset{*}{_f} A_2$, 284
A_n	alternirajuća grupa, 93
ar(F)	dužina, arnost operacije F, 220
Aut $\underline{A}$	skup automorfizama algebra $\underline{A}$, 221
Aut $\underline{A}$	grupa automorfizama algebre $\underline{A}$, 221
$\underline{A}/\sim$	količnik algebra, 237
$\underline{A}_\Pi$	algebra odredjena prezentacijom Π, 256
C	skup kompleksnih brojeva
$C(a)_G$, C(a)	centralizator elementa a u grupi G, 46
$C(A)_G$, C(A)	centralizator skupa A u grupi G, 46
C_n	ciklična grupa reda n, 129
Char(G)	skup svih karakterističnih podgrupa grupe G, 80
$Const_L$	skup konstanti jezika L, 220
Cx, $X/\sim$, x/ϱ	klasa ekvivalencije elementa X, XI
Def(f), Dom(f)	oblast definisanosti funkcije f; domen funkcije f, VIII

det(A)	determinanta matrice A, 359
dim (V)	dimenzija vektorskog prostora V; takodje, dim V
Dn	dijedarska grupa, 35
e, 0, 1	jedinični element grupe, semigrupe, 1
E	jedinična matrica
End A	skup endomorfizama algebre $\underline{A}$, 221
End $\underline{A}$	monoid endomorfizama algebre $\underline{A}$, 221
F	algebarsko zatvorenje polja F, 367
G_a	stabilizator elementa a u grupi G, 105,167
$G = \langle A \rangle$	grupa G generisana skupom A, 1, 129
$G = \langle A \rangle_S$	grupa G, slobodno generisana skupom A,242,262
$G^{(i)}$	i-ta izvedena grupa grupe G, 46, 209
G/N	količnička grupa, 63
$G/\mathcal{S}$	količnička grupa grupe G, po kongruenciji $\mathcal{S}$, 63
G'	komutant grupe G, 46
G(F/K)	Galois-ova grupa polja F nad poljem K, 369
Hom (G_1, G_2)	skup svih homomorfizama grupe G_1 u grupu G_2, 56, 71
I, I_S	identičko preslikavanje skupa S, VIII
Im(f)	oblast vrednosti funkcije f i takodje, Im f, VIII
Inn(G)	skup svih unutrašnjih automorfizama grupe G, 56
Inv(G)	skup svih potpuno invarijantnih podgrupa grupe G, 80
J	jednakosna logika, 6, 241
K	grupa kvaterniona, 38
ker f	kernel, jezgro preslikavanja, 3, 57, 236
[k,h]	komutator elemenata k i h u grupi, 46
[K,H]	komutant podgrupa K i H u grupi; [K,K] se označava se K', 46
L	algebarski jezik, 220
N	skup {1,2,3,...}
$N(a)_G$, N(a)	normalizator elementa a u grupi G; 46
$N(A)_G$, N(A)	normalizator skupa A u grupi G, 46
N(G)	skup svih normalnih podgrupa grupe G, 56
p	prost broj
Pr	skup promenljivih

R	skup realnih brojeva
r(a)	red elementa a u grupi, 53
r(G)	red grupe G, 45
Sn	simetrična grupa reda n, 84
S_X, Sym(X)	simetrična grupa skupa X, 84
T	transverzala podgrupe, 264
Term(L)	skup svih terma jezika L, 1, 227
$t(x_1,\ldots,x_n)$	term čije su sve promenljive neke od promenljivih $x_1,\ldots,x_n$, 227
V	Klein-ova četvorna grupa, 35, 38
Z	skup celih brojeva
Z(G)	centar grupe G, 46
	skup racionalnih brojeva
$\subseteq$	podskup, podalgebra, VIII, 221
$\subset$	pravi podskup, VIII
$<$	podgrupa, 45
$\lneq$	prava podgrupa, 45
$\lhd$	normalna podgrupa, 56
$\lhd\!\!\lneq$	prava normalna podgrupa, 56
|G:H|	indeks podgrupe H u grupi G, 45
|K:F|	stepen polja K nad poljem F, 366
$[H]^G$, [H]	normalno zatvorenje skupa H u grupi G, 56
$\Pi = \langle A;R\rangle$	prezentacija algebre, grupe, 256, 293
o, ·	operacija proizvoda preslikavanja VIII
$\simeq$	relacija izomorfizma, 3,56,221 NAPOMENA: U tekstu se često, umesto $G_1 \simeq G_2$, sreće $G_1 = G_2$.
$\xrightarrow{\simeq}$	izomorfno preslikavanje, IX
$\xrightarrow{\text{na}}$	preslikavanje koje je na , IX
$\xrightarrow{1\text{-}1}$	preslikavanje koje je 1-1, IX
$\longmapsto$	oznaka za preslikavanje, IX
$f\restriction S$	restrikcija preslikavanja, VIII
$\langle f(i) \mid i\in I\rangle$	funkcija $f:I\to X$, VIII
$\sim_c$	relacija konjugovanosti u grupi, 57
|	relacija deljivosti, 341
$\equiv(\text{mod } n), =_n, =^n$	kongruencija po modulu n u ω ($n\in N$), 341
$\equiv(\text{mod } H), =_H$	kongruencija po modulu podgrupe H u grupi, 63,71

$+_n$, $\cdot_n$	sabiranje i množenje po modulu n, 36, 346
$\{1\}$, $\{e\}$, I,0	jedinična podgrupa, 45
C_∞ , Z	beskonačna ciklična grupa, 129
σ_a	unutrašnji automorfizam grupe, 56
φ	Euler-ova funkcija, 135
$\Phi(G)$	Frattini-eva podgrupa grupe G, 80,127
ω	skup $\{0,1,2,\ldots\}$
π_i, P_i	projekcijska preslikavanja skupova, algebri, 110, 221
$Z \vdash_J$ u=v	u=v je posledica skupa zakona Z u jednakosnoj logici J; J se može i izostaviti iz oznake, 6, 241
$\Pi \vdash$ u=v	u=v važi u prezentaciji Π, 256, 293
*	binarna operacija; Galois-ovo preslikavanje, 1, 370

BIBLIOGRAFIJA

1. S.I.Adjan, Problema Bernsaida i toždestva v gruppah, Nauka, Moskva, 1975.
2. E.Artin, Galois Theory, Univ. of Notre Dame Press, (Notre Dame, 1942, 6. izdanje iz 1971.)
3. B.Baumslag, B.Chandler, Group Theory, Shaum's Outline Series, McGraw-Hill Book Co. (New York, 1968)
4. N.Bourbaki, Algebre, ruski prevod, Nauk., (Moskva, 1963)
5. C.C.Chang, J.Keisler, Model Theory, North-Holland, (Amsterdam, 1973)
6. P.M. Cohn, Universal Algebra, D.Reider Publ.Co., (Dordrecht, 1981)
7. J.Dixon, Problems in Group theory, Dover Publ. Co., (New York, 1973)
8. L.Fuchs, Infinite Abelian Groups, Academic Press, (New York, 1973)
9. G.Grätzer, Universal Algebra, D.Van Nostrand Co., (Princeton, 1968)
10. P.Griffith, Infinite Abelian Group Theory, The Univ. of Chicago Press, (Chicago, 1970)
11. I.Kaplansky, Fields and Rings, The Univ. of Chicago Press, (Chicago, 1972)
12. M.Kargapalov, J.Merzljakov, Osnovi Teorii Grupp, Nauka, (Moskva, 1977)
13. Dj. Kurepa, Viša Algebra, Univ. u Beogradu, (Beograd,1969)
14. A.G.Kuroš, Lekcii po Obšćei Algebre, Nauka, (Moskva, 1963)
15. A.G.Kuroš, Teorija Grupp, Nauka, (Moskva, 1967)
16. S.Lang, Algebra, Addison-Wesley Publ.Co., (Reading, Mass., 1965)
17. R.Lyndon, P.Schupp, Combinatorial Group Theory, Springer Verlag, (Berlin, 1977)
18. W.Magnus, A.Karrass, D.Solitar, Combinatorial Group Theory, Interscience Publ., (New York, 1966)
19. Z.Mijajlović, Completions of Models and Galois Theory, Zbornik radova sa 2. Algebarske konferencije, (Novi Sad, 1981), 19-26.
20. H.Neuman, Varieties of Groups, Springer Verlag, (Berlin, 1967)

21. V.Perić, Algebra, Univ. u Sarajevu, (Sarajevo, 1980)
22. S.Prešić, On Quasi-algebras and the Word Problem, Publ. Inst. Math., t.26(40), (1979), 255-268
23. S.Prešić, M.Prešić, Uvod u matematičku logiku (Teorija i zadaci) Matematički institut, Beograd, 1979
24. D.Passman, Permutation Groups, W.A. Benjamin, Inc., (New York, 1968)
25. J.Rotman, The Theory of Groups, an Introduction, Allyn and Bacon, (Boston, 1973)
26. W.R.Scott, Group Theory, Prentice Hall, (Englewood Cliffs, N.J., 1964)
27. Van Der Waerden, Algebra, Springer Verlag, (Berlin, 1967)
28. H.Wielandt, Finite Permutation Groups, Academic Press, (New York, 1964)
29. H.Zassenhaus, The Theory of Groups, Chelsea, (New York,1958).