Univerzitet u Beogradu
PRIRODNO-MATEMATIČKI FAKULTET U BEOGRADU
Institut za matematiku

Daniel A. Romano:

KONSTRUKTIVNA ALGEBRA - ALGEBARSKE STRUKTURE I PRSTEN ENDOMORFIZAMA

(doktorska disertacija)

Bihać 1985.

kandidat: Daniel A. Romano;

naziv teme: Konstruktivna algebra - algebarske strukture i prsten endomorfizama;

AMS Subjekt Classification (1985): Primary 03 F 65; Secondary 03 E 15, 04 A 05, 12 E 99, 13 A 99, 13 C 99, 13 E 99, 20 A 99, 20 L 99, 16 A 65 ;

Ključne riječi i fraze: Konstruktivna matematika, konstruktivna, algebra, klasa, jednakost, različitost, relacija ekvivalencije, relacija koekvivalencije, relacija kongruencije, relacija kokongruencije, podgrupa i kopodgrupa, ideal i koideal, podmodul i kopodmodul, diskretnost, odlučivost;

fakultet: Prirodno-matematički fakultet Univerziteta u Beogradu; OOUR Instituti za matematiku, mehaniku i astronomiju; Institut za matematiku;

voditelj: dr Milan Božić, docent PMF-a u Beogradu.

Zahvalnica

U toku postdiplomskog studija na Odsjeku za matematiku Prirodno-matematičkog fakulteta u Sarajevu, imao sam sreću da slušam predavanja dr-a Vladimira Devide'a iz matematičke logike, gdje sam prvi put upoznao ideje intuicionističke matematike holandske škole, s posebnim osvrtom na Brouwera i Heytinga.

U periodu od 1980. do sredine 1984. posjećivao sam Seminar za osnove matematike i matematičku logiku Odjeljenja za matematiku Prirododlovno-matematičkog fakulteta u Zagrebu. Dugujem zahvalnost članovima Seminara što su pokazali strpljivost pri mojoj težnji da im izložim probleme zasnivanja konstruktivne algebre bishopovske orijentacije, koja je bila predmet moje preokupacije. Posebnu zahvalnost dugujem dr-u Kajetanu Šeperu za podršku koju mi je tom prilikom pružio.

U tom smislu zahvalan sam dr-u Đuri Kurepi koji me je uputio na čovjeka u Jugoslaviji koga zanima ta oblast i za koga je kazao da će se sasvim uspješno nositi sa problemima konstruktivne algebre. Posebnu zahvalnost dugujem voditelju ove disertacije, dr-u Milanu Božiću, docentu Prirodno-matematičkog fakulteta u Beogradu, za pokazanu dobru volju, za strpljenje, za časove koje smo proveli zajedno, a naročito za sugestiju da je richmanovska relacija različitosti simetrična relacija relaciji bishopovske jednakosti. U ovom mom pionirskom radu na zasnivanju teorije konstruktivne algebre u okviru konstruktivne matematike bishopovske orijentacije - oblasti koja još nije stekla legitimnost u matematičkom smislu, od koristi mi je bila podrška i razumjevanje dr-a Koste Došena, naučnog saradnika Matematičkog instituta u Beogradu.

Zahvalnost dugujem i dr-u Dirkku van Dalenu sa univetziteta u Utrechtu, koji mi je poslao rukopis rada za knjigu "Constructivism in Mathematics, An introduction", koju

radi zajedno sa A.S.Troelstrom.

Od posebne važnosti u mom radu na ovoj disertaciji bila je saradnja sa dr-om Fredom Richmanom, profesorom State University Las Cruces, New Mexico, USA. Zahvaljujem mu se za brojne separate svojih radova koje mi je poslao, za ukazivanje na probleme u teoriji grupa konstruktivne algebre kao i za rukopis knjige koju priprema u saradnji sa W.B.G.Ruitenburgom. U toku rada na konstruktivnoj algebri bila mi je od velike koristi i Ruitenburgova doktorska disertacija "Intuitionistic Algebra" koju mi je sam autor poslao.

U toku rada na ovoj disertaciji kontaktirao sam sa većim brojem ljudi i kojima na ovaj način iskazujem zahvalnost. Na prvom mjestu to su D.S.Scott, P.T.Johnstone, D.C.McCarty.

Moram priznati, da najveću zahvalnost dugujem svojoj supruzi Ani, koja me je hrabrila u trenutcima malodušnosti u toku šestogodišnjeg rada na ovoj disertaciji.

S A D R Ž A J

DIO 0

Uvod

I

Intuicionističko shvatanje matematike razvio je holandski matematičar Luitzen Egbertus Jan Brouwer. Kao početak ovog pravca u matematici uzima se Brouwerova doktorska disertacija "Over de Groundeslagen der Wiskunde", 1907. godine. Polazni je Brouwerov zahtijev da matematička nauka bude dovoljno pouzdana. Njegovo neslaganje s "tadašnjom" matematikom bilo je u kriteriju pouzdanosti, kao i u izboru sredstava za osiguravanje te pouzdanosti. Brouwer je odbacio kao nepouzdan pojam akutelne beskonačnosti, tj. pojam beskonačnog skupa, do kraja izgrađenog i postojećeg istovremeno sa svim svojim elementima. Sem toga, proglasio je da primjena aristotelovske logike, što uključuje i princip isključenja trećeg, na beskonačnosti nije mjerodavna. Prema Brouweru, matematika nije sistem formula i pravila već osnovni oblik ljudske djelatnosti. Preobrazba logike, što ju je poduzeo Brouwer, je potaknuta konstruktivnim shvatanjem tvrdnji o postojanju matematičkih objekata. Postavka "postojati - znači biti konsruisan" je ishodište Brouwerove reformatorske djelatnosti. To insistiranje na identifikaciji egzistencije s mogućnošću konstruisanja potiće od Leopolda Kroneckera, a precizno formulisanje principa intuicionističke logike izvršio je 1930. Brouwerov učenik Arend Heyting. Intuicionizam je ponikao iz poricanja matematičkog platonizma, ali se fundamentalnosti nije odrekao. Sačuvao je priznavanje apsolutne istinitosti matematičkih tvrdnji, ali nije ih tretirao kao korespodenciju s nečim što postoji neovisno o nama, nego kao dosljedno i korektno razvijanje struktura datih nam u našoj intuiciji. S tog je stanovišta razumljivo zašto je Heyting govorio da je intuicionistička matematika "proučavanje određenih funkcija ljudskog uma". Prihvatajući neka svojstva ljudske psihe i gledajući na matematičko stvaralaštvo kao na "čisto" ispoljavanje tih svojstava, intuicionisti poistovjećuju matematiku s konstruktivnom djelatnošću mišljenja što se oslanja na mehanizam svjesne konstrukcije neograničeno produživog niza prirodnih brojeva, koji se uvijek sastoji od konač-

nog broja elementarnih koraka. O odnosu intuicionističke matematike prema klasičnoj sa aspekta intuicionističke matematike vidi se iz Heytingovih riječi: "Predmet intuicionizma - - konstruktivna matematička misao - jednoznačno određuje njegove premise i smiješta ga ne unutar klasične matematike, nego pored nje. Klasična matematika proučava posve drugi predmet, štogod bio taj predmet."

Principijelno-filozofske tendencije i konkretno-naučni rezultati intuicionističke matematike bili su preduslovi postanka konstruktivnih matematičkih škola. Konstruktivisti se kritički odnose prema pojmu aktuelno-beskonačnih skupova, a njihovo poricanje univerzalnosti principa isključenja trećeg preuzeto je neposredno od Brouwerovog intuicionizma. Fundamentalni pojam u konstruktivnoj matematici je pojam postupka. Pod tim izrazom se podrazumjeva tačan propis koji određuje postupke što vode od promjenjivih polaznih podataka prema traženom rezultatu. Upotreba tog pojma omogućila je konstruktivistima da se ne ograniče na poricanje nekih klasičnih metoda nego da razrade i pozitivni radni program mnogo jasniji od programa intuicionista:

1) Postojanje matematičkog objekta tumači se kao postojanje postupka koji opisuje konstrukciju tog objekta od nekog već ranije konstruisanog objekta.

2) U skladu s tim odbacuju se klasični dokazi postojenja indirektnim metodama i modificiraju se pravila logike, tj. primjenjuje se posebna "konstruktivna" logika.

3) Dopušta se apstrakcija potencijalne ostvarljivosti koliko god dugog postupka, tj. priznaje se apstrakcija potencijalne beskonačnosti. Istovremeno se kategorički odbacuje apstrakcija aktuelne beskonačnosti.

(U ruskom konstruktivizmu pored gore navedenih crta prihvata se i tzv. Markovljev princip.)

1967. godine američki matematičar Erett Bishop publikovao je knjigu "Foundations of constructive analysis", Mc Grow-Hill Book Company, New York 1967. koja se odnosi na tzv. američki pragmatički konstruktivizam u kojem su fundamentalni pojmovi, klase, prirodni brojevi i postupci (intuitivni pojam algoritma).

II

Neka je X klasa u bishopovskom smislu. Za njenu egzistenciju potrebno je i dovoljno da znamo postupak konstruisanja njenih elemenata na bazi neke, već ranije konstruisane klase. (U principu, u konstruktivnoj matematici bishopovske orijentacije sve su klase konstruisane na bazi klase prirodnih brojeva.) Ako taj postupak označimo sa K_{YX}, gdje je sa Y označena bazna klasa za konstrisanje klase X, tada možemo pisati

$$x \in X \longleftrightarrow K_{YX}(x)x,$$

pri čemu desnu stranu gornje ekvivalencije shvatamo u slijedećem smislu: element x je konstruisan postupkom K_{YX} onako kako se konstruiše element x. Intuitivno je jasno da vrijedi

$$K_{YX}(x)y \wedge K_{YX}(y)z \Longrightarrow K_{YX}(x)z$$

i

$$x \equiv y \Longleftrightarrow K_{YX}(x)y \wedge K_{YX}(y)x .$$

Na klasi X definišu se jednakost "$=_X$", u bishopovskom smislu, i različitost "$\neq_X$", u richmanskom smislu, i tako formira skup $(X,=_X,\neq_X)$. Razumljivo je, da se na klasi može definisati više jednakosti i više različitosti. Ovo je zahtijevalo da se uvede poredak između jednakosti i poredak između različitosti.

Jednakost na klasi X definiše se kao relacija ekvivalencije na klasi X sa

$$(1)\ (\forall x \in X)(x =_X x),$$

$$(2)\ (\forall xy \in X)(x =_X y \Longrightarrow y =_X x),$$

$$(3)\ (\forall xyz \in X)(x =_X y \wedge y =_X z \Longrightarrow x =_X z),$$

a različitost se definiše na X sa

$$(4)\ (\forall xy \in X)\neg(x =_X y \wedge x \neq_X y),$$

$$(5)\ (\forall xy \in X)(x \neq_X y \Longrightarrow y \neq_X x),$$

$$(6)\ (\forall xyz \in X)(x \neq_X y \wedge y =_X z \Longrightarrow x \neq_X z).$$

Za relaciju različitosti, u richmanskovom smislu, u opštem slučaju, ne vrijedi aksiom tranzitivnosti

$$(7)\ (\forall xyz \in X)(x \neq_X z \Longrightarrow x \neq_X y \vee y \neq_X z).$$

Relaciji ekvivalencije na klasi X definisanoj aksiomama (1), (2) i (3) možemo definisati simetričnu relaciju na klasi X. Za klasu Y kaže se da je <u>podklasa</u> klase X akko vrijedi

$$(\forall x)(x \in Y \longrightarrow x \in X)$$

i to obilježavamo sa $Y \subseteq X$. Za podklasu Y kaže se da je <u>podskup</u> skupa $(X,=_X,\neq_X)$ akko nasleđuje relacije jednakosti i različitosti. Sada imamo

$$x \in Y \Longleftrightarrow (\exists y \in Y)(x =_X y).$$

Simetrično definišemo: za element x skupa $(X,=_X,\neq_X)$ kaže se da je <u>oddjeljiv</u> od podskupa $(Y,=_X,\neq_X)$ akko vrijedi

$$(\forall y \in Y)(y \neq_X x),$$

i to obilježavamo sa $x \# Y$. Relacija $C \subset X \times X$ naziva se <u>relacija koekvivalencije</u> na klasi X akko vrijedi

$$(4') \quad (\forall x \in X)((x,x) \# C),$$

$$(5') \quad (\forall xy \in X)((x,y) \in C \longrightarrow (y,x)),$$

$$(6') \quad (\forall xyz \in X)((x,y) \in C \wedge y =_X z \longrightarrow (x,z) \in C),$$

$$(7') \quad (\forall xyz \in X)((x,z) \in C \longrightarrow (x,y) \in C \vee (y,z) \in C).$$

Relacija koekvivalencije C je relacija različitosti u richmanskovom smislu, ali obrnuto ne mora biti. To se lako vidi na primjeru klase P_X svih podskupova skupa X, gdje su relacije jednakosti i različitosti definisane sa

$$Y =_{P_X} Z \Longleftrightarrow Y \subseteq Z \wedge Z \subseteq Y,$$

$$Y \neq_{P_X} Z \Longleftrightarrow (\exists y \in Y)(y \# Z) \vee (\exists z \in Z)(z \# Y).$$

Da bi relacije ekvivalencije i koekvivalencije izgradivale strukturu skupa na klasi potrebno je i dovoljno da je negacija relacije koekvivalencije relacija ekvivalencije nižeg reda od relacije ekvivalencije.

III

Neka su $(X,=_X,\neq_X)$ i $(Y,=_Y,\neq_Y)$ skupovi a $f:X \longrightarrow Y$ preslikavanje skupa X u skup Y. Preslikavanje f je <u>funkcija</u> akko vrijedi

$$x =_X x' \longrightarrow f(x) =_Y f(x'),$$

$$f(x) \neq_Y f(x') \longrightarrow x =_X x'.$$

relacija koekvivalencije na klasi X; preciznije

Specifičnost ove definicije je u simetriji relacija koje vrijede za jednakost i relacija koje vrijede za različitost. Tako, pored klasičnog pojma injektivnosti funkcije imamo i simetričan pojam <u>utapanja</u> preuzet od Ruitenburga,

$$x \neq_X x' \Longrightarrow f(x) \neq_Y f(x') \quad .$$

Gornja definicija funkcije daje posebnu specifičnost pri definisanju unutrašnje binarne operacije: Neka je $(X,=,\neq)$ skup. Totalna funkcija $f: X \times X \ni (x,y) \longmapsto f(x,y) \in X$ naziva se <u>unutrašnja binarna operacija</u> u skupu X. Zato vrijedi

$$x = x' \wedge y = y' \longrightarrow f(x,y) = f(x',y'),$$

$$f(x,y) \neq f(x',y') \Longrightarrow x \neq x' \vee y \neq y'.$$

Ova specifičnost konstruktivne algebre ima za posljedicu da, ponekad, aksiome algebarskih struktura izgledaju drugačije nego je to u klasičnoj algebri. Na primjer, definicija modula nad prstenom data je sa:

Neka je $(A,=_A,\neq_A,+,.)$ prsten a $(M,=_M,\neq_M,+)$ abelova grupa. Za grupu M kaže se da je <u>A-modul</u> akko postoji vanjska operacija u M nad A, tj. totalne funkcije

$$A \times M \ni (a,x) \longmapsto ax \in M$$

takva da vrijedi

(i) $(\forall ab \in A)(\forall x \in M)((a+b)x =_M ax+bx)$,

(ii) $(\forall a \in A)(\forall xy \in M)(a(x+y) =_M ax+ay)$,

(iii) $(\forall ab \in A)(\forall x \in M)((ab)x =_M a(bx))$,

(iv) $(\forall x \in M)(1.x =_M x)$,

(v) $(\forall a \in A)(\forall x \in M)(ax \neq_M o \Longrightarrow a \neq_A o \wedge x \neq_M o)$.

Sem ove specifičnosti, konstruktivna algebra ima još jednu specifičnost, koja će biti prezentovana na primjeru modula.

(a) Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,.)$ sa jedinicom 1 $(\neq_A o)$, a $(S,=_M,\neq_M)$ neka je podskup A-modula M. Za S se kaže da je <u>A-podmodul</u> A-modula M akko

$o \in S$,

$x \in S \wedge y \in S \Longrightarrow x+y \in S$,

$a \in A \wedge x \in S \longrightarrow ax \in S$.

(b) Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,.)$ sa jedinicom $1(\neq_A 0)$, a $(C,=_M,\neq_M)$ neka je podskup A-modula M. Za C se kaže da je <u>A-kopodmodul</u> A-modula M akko

$$0 \notin C,$$
$$x+y \in C \longrightarrow x \in C \vee y \in C,$$
$$ax \in C \longrightarrow x \in C \wedge a \neq_A 0 .$$

(c) Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,.)$ sa jedinicom $1(\neq_A 0)$, i neka je R relacija ekvivalencije na M, a F relacija koekvivalencije na M. Za R se kaže da je <u>relacija kongruencije</u> na M akko

$$(x,y)\in R \wedge (x',y')\in R \longrightarrow (x+x',y+y')\in R,$$
$$(\forall a\in A)(\forall xy\in M)((x,y)\in R \Longrightarrow (ax,ay)\in R).$$

Za relaciju F se kaže da je <u>relacija kokongruencije</u> na M akko

$$(x+x',y+y')\in F \Longrightarrow (x,y)\in F \vee (x',y')\in F,$$
$$(\forall a\in A)(\forall x\in M)((ax,o)\in F \longrightarrow a \neq_A o \wedge (x,o)\in F).$$

(d) Neka je M A-modul a R relacija ekvivalencije na M. Tada je relacija R relacija kongruencije na M akko je skup $\{x\in M:(x,o)\in R\}$ A-podmodul A-modula M.

(e) Neka je M A-modul a F relacija koekvivalencije na M. Tada je F relacija kokongruencije na M akko je skup $\{x\in M:(x,o)\in F\}$ A-Kopodmodul A-modula M.

(f) Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,.)$, a R relacija kongruencije na M sa $R \propto =_M$, i C relacija kokongruencije na M sa $\neq_M \propto C$, takve da je $\neg C \propto R$.

Tada je $(M,=,\neq,+')$ modul nad prstenom A sa relacijama jednakosti i različitosti definisanim sa

$$x = y \iff (x,y) \in R,$$

$$x \neq y \iff (x,y) \in C$$

i operacijama sabiranja i vanjskog množenja

$$x +' y = x+y,$$

$$a \cdot' x = ax.$$

A-modul $(M,=,\neq,+')$ naziva se <u>faktorski modul</u> i obilježava se sa $M/(R,C)$. Ako su P i S odgovarajući A-podmodul i A-kopodmodul A-modula M koji odgovaraju relacijama kongruencije R i kokongruencije C takvi da je $P \subseteq \neg S$, tada se faktorski modul $(M,=,\neq,+')$ obilježava sa $M/(P,S)$. U njemu imamo

$$x+P = y+P \iff x-y \in P,$$

$$x+P \neq y+P \iff x-y \in S,$$

$$(x+P)+'(y+P) = x+y+P,$$

$$a \cdot'(x+P) = ax+P.$$

(g) Neka je $(A,=_A,\neq_A,+,\cdot)$ prsten, a $(M,=_M,\neq_M,+)$ i $(P,=_P,\neq_P,+)$ A-moduli. Totalna funkcija $f:M \longrightarrow P$ naziva se <u>homomorfizam</u> A-modula akko

$$(\forall xy \in M)(f(x+y) =_P f(x)+f(y)),$$

$$(\forall a \in A)(\forall x \in M)(f(ax) =_P af(x)).$$

Homomorfizam f je <u>bijektivan</u> akko je injektivan i sirjektivan. Homomorfizam f je <u>izomorfizam</u> akko je bijektivno utapanje.

(h) Neka je $f:M \longrightarrow P$ homomorfizam A-modula. Tada:

1. Skup $Ker(f) = \{x \in M : f(x) =_P o\}$ je A-podmodul A-modula M, i vrijedi $(o) \subseteq Ker(f)$.
2. Skup $C_f = \{x \in M : f(x) \neq_P o\}$ je A-kopodmodul A-modula M, i vrijedi $C_f \subseteq C_o$.

3. $\mathrm{Ker}(f) \subseteq \neg C_f$.

4. Skup $\mathrm{Im}(f)$ je A-podmodul A-modula P.

5. Postoji jedinstveni izomorfizam

$$h: M/(\mathrm{Ker}(f), C_f) \longrightarrow \mathrm{Im}(f)$$

za koji vrijedi $f =_{\mathrm{Hom}(M,P)} h.p$, gdje je $p: M \longrightarrow M/(\mathrm{Ker}(f), C_f)$ prirodni epimorfizam.

(i) Neka je $(M, =_M, \neq_M, +)$ modul nad prstenom A i neka su (H_1, C_1) i (H_2, C_2) dva para koji se sastoje od A-podmodula i A-kopodmodula A-modula M takvih da je $H_1 \subseteq \neg C_1$, $H_2 \subseteq \neg C_2$ i $H_1 \cap C_2 \neq_{P_M} \emptyset$ i neka je H_2 podmodul A-modula H_1. Tada postoji jedinstveni izomorfizam

$$f: M/(H_1, C_1) \longrightarrow (M/(H_2, C_2))/(H_1/(H_2, H_1 \cap C_2), C_1/(H_2, H_1 \cap C_2)).$$

Iz ovih nekoliko primjera koji se odnose na module nad prstenom, vidi se specifičnost konstruktivne algebre u konstruktivnoj matematici bishopovske orijentacije, ali i problemi koji se pri razvijanju ove algebre pojavljuju.

IV

Kandidat je mišljenja da originalni doprinosi jesu:

1. Definicija pojma oddjeljivosti.

2. Definicija različitosti u klasi P_X .

3. Definicija relacije poredka među relacijama jednakosti.

4. Definicija relacije poredka među relacijama različitosti.

5. Veći dio materijala izložen u dijelovima II i III.

1.1. PRIMITIVNI POJMOVI KONSTRUKTIVNE MATEMATIKE

Primitivni pojmovi bishopovske matematike su slijedeća tri primitivna pojma: prirodni brojevi, klase i postupci (Bridges, st.2.).

1.1.1. Prirodni brojevi. Uzima se da su prirodni brojevi: 0,1,2,... , i njihove bazne osobine slijedbeništva i indukcije, razumljivi svakom inteligentnom ljudskom biću.

1.1.2. Klase. Klasa objekata je determinisana kada se može opisati postupak konstruisanja njenih članova od ranije konstruisanih objekata. Prirodni brojevi formiraju klasu koju ćemo označavati sa $\hat{N}$; podklasu klase $\hat{N}$, koja se sastoji od 1,2,... , označavaćemo sa N. Pisaćemo $x \in A$ ako je objekt x član (ili element) klase A.

Pojam "postupak konstruisanja" je fundamentalan u konstruktivnoj matematici. Pod ovim podrazumjevamo konačan, konkretan objekat koji je dat spiskom instrukcija. Ove instrukcije moraju biti eksplicitno date i moraju biti takve da se efektivno mogu provoditi. Više detalja o shvatanju pojma postupaka u konstruktivnoj matematici može se naći u Beesonovom članku (Beeson,[3]) i u Goodmanovom članku (Goodman,[10]). Dalje, mi uvodimo novu osobinu matematičkih objekata. Za postupak konstruisanja uvodimo oznaku K_{YX}, ili kratko K_Y u slijedećem smislu: K_{YX} je postupak kojim konstruišemo klasu X od objekata već ranije konstruisane klase Y. Dakle, $x \in X$ ako i samo ako $K_{YX}(x)x$, gdje $K_{YX}(x)x$ ima smisao: element x je konstruisan na bazi objekata klase Y onako kako se konstruiše objekat x. Intuitivno je jasno da vrijedi

$$K_{YX}(x)y \wedge K_{YX}(y)z \Longrightarrow K_{YX}(x)z.$$

Ako su X i Y klase, pisaćemo $X \subseteq Y$ ako i samo ako, za svako x, ako $K_{ZX}(x)x$, tada $K_{ZY}(x)x$, i govoriti da je X podklasa klase Y.

1.1.3. Preslikavanja. Ako su X i Y klase, preslikavanje iz X u Y je postupak ili metod kojim se transformišu neki elementi klase X u neke elemente klase Y konačnim postupkom. Ako $x \in X$ i ako preslikavanje f djeluje na element x, pisaćemo f(x) kao konačan rezultat djelovanja preslikavanja f. Sa preslikavanjem f imamo asocirane slijedeće klase:

- domena preslikavanja f
  $D(f) \equiv \{ x \in X : K_Y(f(x))f(x) \}$;
- slika preslikavanja f
  $Im(f) \equiv \{ f(x) \in Y : K_{D(f)Y}(f(x))f(x) \}$,
- graf preslikavanja f
  $G(f) \equiv \{ (x,f(x)) : x \in D(f) \}$

gdje je (x,y) jedna od osnovnih operacija, nazvana sparivanje, u smislu da dva objekta x i y kombinujemo u jedan ovjekat.

1.2. LOGIKA KONSTRUKTIVNE MATEMATIKE

Prema konstruktivnim shvatanjima, matematička tvrdnja je data ako se može dati njen dokaz.

1.2.1. Logika. U terminologiji dokaza logičke funkcije imaju slijedeće značenje:

- dokaz p od $A \wedge B$ je par dokaza p_1, p_2 takvih da p_1 dokazuje A i p_2 dokazuje B;
- dokaz p od $A \vee B$ je dokaz p_1 kojim se dokazuje A ili p_2 kojim se dokazuje B;
- dokaz p od $A \longrightarrow B$ je konstrukcija koja se sastoji od dokaza q za A i dokaza p(q) za B plus verifikacija da p zadovoljava dati uslov;
- $A \Longleftrightarrow B$ ako i samo ako $(A \Longrightarrow B) \wedge (B \Longrightarrow A)$;
- dokaz p od $\neg A$ je dokaz za $A \longrightarrow \perp$, gdje je $\perp$ neka kontradikcija.

1.2.2. Klase i propozicije. Pod propozicijom ćemo podrazumjevati klasu čiji su elementi dokazi: konstruisati propoziciju A znači imati njen dokaz. Ovim je dat opis šta sve može biti propozicija, tj. kako se konstruiše klasa Ω svih propozicija.

1.2.3. Kvantifikatori. Kvantifikatore shvatamo u slijedećem smislu:

- dokaz za $\exists x\, A$ sastoji se od izbora specifičnog x i dokaza za A(x):

p je dokaz za $\exists x\, A(x)$ ako i samo ako je p par (q,x) gdje je q dokaz za A(x).

- formulu $\forall x A$ shvatamo u smislu da se propozicija A može, bar u primcipu, efektivno provjeriti za po volji izabran element klase X.

1.3. JEDNAKOSTI I SKUPOVI

U klasičnoj matematici relacija jednakosti je potpuno neutralna, što nije slučaj sa konstruktivnom matematikom. Ovaj problem je istraživao D.S.Scott u svom radu "Identity and existence in Intuitionistic Logic", Springer LNM 753(1979),660--696., zatim Dirk van Dalen i R.Statman u radu "Equality in the presence of apartness". Situacija je kompletno različita u bishopovskoj matematici. U konstruktivnoj matematici, ako je X klasa i $x,y \in X$, imamo

$$x \equiv y \iff K_X(x)y \wedge K_X(y)x\ ,$$

pri čemu na lijevoj strani podrazumjevamo identitet.

1.3.1. Jednakosti. Relacija jednakosti "=" na klasi X zadovoljava

(1) $\quad (\forall x \in X)(x = x)$,

(2) $\quad (\forall xy \in X)(x = y \Longrightarrow y = x)$,

(3) $\quad (\forall xyz \in X)(x = y \wedge y = z \Longrightarrow x = z)$.

Kako treba shvatiti jednakost x = y? Imamo dvije mogućnosti: (i) objekti x i y postoje i jednaki su; i (ii) ako postoji jedan od objekata x ili y, tada postoji i drugi i jednaki su.

Neka je X klasa, tj. neka je dat postupak konstruisanja klase X, K_{YX}. Na klasi se definiše relacija jednakosti kao relacija ekvivalencije. Pri ovome se intuitivno nameće prirodno definisanje relacije ekvivalencije. Međutim, ponekad ovo prirodno definisanje uključuje izvjesnu neodređenost, koja se često očituje u našoj nemogućnosti da utvrdimo da li su dva elementa međusobno jenaka ili različita. Ovaj problem sugeriše da se "posmatra" postupak konstruisanja elemenata date klase i utvrdi "momenat" kada više nismo u mogućnosti da upore ujemo elemente u odnosu na prirodnu jed st. Zato se predlaže uspostavljanje hijerarhije relacije jednkasti, čime se omogućuje utvrđivanje "jednakosti do određenog reda" između dva elementa. Definišimo <u>relaciju poredka</u> $\prec$ između relacija jednakosti $=_1$ i $=_2$ na slijedeći način:

$$(\forall xy \in X)(x =_1 y \Longrightarrow x =_2 y) \Longleftrightarrow =_2 \prec =_1 .$$

<u>1.3.2. Skupovi.</u> U klasičnoj matematici postavlja se pitanje: Šta je to skup? i uzima se kao kolekcija objekata nekog preegzistirajućeg univerzuma. U konstruktivnoj matematici to pitanje glasi: šta treba učiniti da bi se konstruisao skup? Bishop (Bishop, [4] , a takođe Bridges [5] i Greenleaf [12]) je opisao konstrukciju skupa X posredstvom slijedeća tri postupka: prvi, mora biti opisano kako se konstruiše proizvoljan element od X, tj. mora biti dato K_X; drugi, mora biti opisano kada će dva proizvoljna elementa od X biti međusobno jednaka; treći, relacija jednakosti "=" mora zadovoljavati (1),(2) i (3). Dakle, u konstruktivnoj matematici skup je uređeni par (X,R_X) koji se sastoji od klase X nekih elemenata, izgrađenih na bazi već ranije konstruisanih objekata, i relacije ekvivalencije R_X na X. To znači da (X,R) i (X,P) treba shvatati kao dva skupa, gdje su R i P dvije relacije ekvivalencije. Vidi se da je od posebnog interesa u konstruktivnoj matematici način determinisanja relacije jednakosti, koju ćemo ubuduće, na klasi X, pisati sa $x =_X y$, umjesto $(x,y) \in R_X$. O ovome se nešto više može vidjeti u autorovom članku (Romano, [36]).

Neka je $(A,=_A)$ skup a X i Y podklase klase A za koje ćemo predpostavljati da nasleduju relaciju jednakosti $=_A$. Za X se kaže da je <u>podskup</u> od Y i piše $X \subseteq Y$ ako i samo ako

$$(\forall x \in X)(\exists y \in Y)(x =_A y).$$

<u>1.3.3. Scottov predikat egzistencije.</u> Neka je $(X,=_X)$ skup. <u>Scottov predikat egzistencije</u> E, u terminima kvantifikatora (vidjeti Scott [43] i Ruitenburg [41]), definiše se ovako

$$Ey \iff (\exists x \in X)(x =_X y).$$

Ovaj predikat egzistencije je veoma koristan. Neka je $(=_i)_i$ rastući niz relacija jednakosti na klasi X sa $(\forall i)(=_i \prec =_X)$. Tada možemo da definišemo niz predikata egzistencije, u smislu

$$E_i y \iff \exists x(x =_i y).$$

Prema tome, za klasu X i za njen element $y \in X$ sa osobinom A možemo konstruisati nepraznu podklasu

$$A_i \equiv \{x \in X : x =_i y\} \quad (i \in I)$$

koja se sastoji od elemenata klase X koji zadovoljavaju osobinu A. Jasno je da, u opštem slučaju, pod $E_i y$ ne podrazumjevamo i $E_j y$, odnosno , u opštem sluačju, ne vrijedi da je A_i isto što i A_j.

Za relaciju jednakosti "$=_X$" na klasi X imamo

$$x =_X x \iff Ex,$$

tj. mi smo se oprijedjelili za prvo značenje od dva moguća relacija jednakosti o kojima je bilo riječi u 1.3.1., tj. imamo

$$x =_X y \longrightarrow Ex \wedge Ey.$$

1.4. RAZLIČITOST I FUNKCIJE

<u>1.4.1. Nejednakost, različitost i odvojenost.</u> Neka je $(X,=)$ skup i neka je $x,y \in X$. Imamo

$$x \neq y \longrightarrow \neg\neg(x = y))$$

ali obrnuto, u opštem slučaju, ne vrijedi. Ako u skupu $(X,=)$ imamo

$$(\forall xy \in X)(\neg\neg(x = y) \Longrightarrow x = y)$$

kada za relaciju jednakosti $=$ kažemo da je stabilna. Nejednakost na skupu $(X,=)$ se definiše sa $\neg(x = y)$ i

$$(x = y) \Longrightarrow Ex \wedge Ey.$$

Relacija nejednakosti na skupu $(X,=)$ zadovoljava

$$(\forall x \in X)\neg\neg(x = x),$$

$$(\forall xy \in X)(\neg(x = y) \Longrightarrow \neg(y = x)),$$

$$(\forall xyz \in X)(\neg(x = z) \wedge Ey \Longrightarrow \neg(x = y \wedge y = z)).$$

U konstruktivnoj matematici postoji "pozitivna" teorija različitosti. U konstruktivnoj matematici na skupovima relacija različitosti, u richmanskom smislu (Richman, [14]) definiše se na slijedeći način:

(i) $(\forall xy \in X)(x \neq y \Longrightarrow y \neq x)$,

(ii) $(\forall xyz \in X)(x = y \wedge y \neq z \Longrightarrow x \neq z)$,

(iii) $(\forall xy \in X)\neg(x = y \wedge x \neq y)$.

Jasno je da vrijedi

$$(\forall xy \in X)(x \neq y \Longrightarrow \neg(x = y)),$$

ali, obrnuto, u opštem slučaju nije tačno. Za relaciju različitosti u richmanskom smislu, nemamo

(iv) $(\forall xy \in X)(\neg(x \neq y) \Longrightarrow x = y)$

(što je aksiom za relaciju odvojenosti u Heytingovom smislu). Koje značenje imaju gornji aksiomi? Prvi možemo shvatiti kao simetriju, drugi - kao tranzitivnost (preciznije, tranzitivnost za relaciju odvojenosti u Heytingovom smislu, u Scottovim oznakama, ima formu

$$(\forall xyz \in X)(x \neq y \Longrightarrow x \neq z \vee z \neq y)$$

koju zadovoljava svaka aditivna abelova grupa, kako će to biti pokazano kasnije), a treći - kao irefleksivnost, jer iz njega, za $x = y$ imamo

$$(\forall x \in X)\neg(x \neq x).$$

U shvatanju ovih aksioma treba relacijsku oznaku "$\neq$" shvatiti kao posebnu i $x \neq y$ ne treba shvatati kao kraticu za $\neg(x = y)$. U Skottovim oznakama značenje različitosti možemo dopuniti sa

$$x \neq y \Longrightarrow Ex \wedge Ey.$$

Dalje, definišimo relaciju poredka između relacija različitosti $\neq_1 \propto \neq_2$ na slijedeći način:

$$(\forall xy \in X)(x \neq_2 y \Longrightarrow x \neq_1 y) \Longleftrightarrow \neq_2 \propto \neq_1 .$$

Relacija odvojenosti u Heytingovom smislu definiše se na skupu $(X,=)$ kao relacija $\neq\!\!\neq$ sa osobinama

$$(\forall x \in X)\neg(x \neq\!\!\neq y),$$
$$(\forall xy \in X)(x \neq\!\!\neq y \Longrightarrow y \neq\!\!\neq x),$$
$$(\forall xyz \in X)(x \neq\!\!\neq z \Longrightarrow x \neq\!\!\neq y \vee y \neq\!\!\neq z),$$
$$(\forall xy \in X)(\neg(x \neq\!\!\neq y) \Longrightarrow x = y).$$

Relaciju "$\neq\!\!\neq$" shvatamo ovim aksiomama sa dodatkom

$$x \neq\!\!\neq y \Longrightarrow Ex \wedge Ey.$$

1.4.2. Funkcije. Neka su $(X,=_X,\neq_X)$ i $(Y,=_Y,\neq_Y)$ skupovi. Preslikavanje $f:X \longrightarrow Y$ je funkcija ako i samo ako

(f) $\quad (\forall xx' \in D(f))(x =_X x' \Longrightarrow f(x) =_Y f(x')),$

(swf) $\quad (\forall xx' \in D(f))(f(x) \neq_Y f(x') \Longrightarrow x \neq_X x').$

Oznaka slabe funkcije je data sa

(wf) $\quad (\forall xx' \in D(f))(\neg(f(x) =_Y f(x')) \Longrightarrow \neg(x =_X x'))$

Ako je domen funkcije f takav da je na njemu relacija jednakosti stabilna tada je uslov (wf) ekvivalentan uslovu (f). U opštem slučaju, uslov (swf) nije ekvivalentan uslovu (f).

Ako je $(X,=_X)$ skup, predikat na X shvatamo kao funkciju iz X u skup $(\Omega, \Longleftrightarrow)$. Tako za svaki element $x \in X$ $A(x)$ je propozicija i imamo

$$x =_X x' \Longrightarrow A(x) \Longleftrightarrow A(x').$$

Neka je $(X,=_X,\neq_X)$ skup a A predikat na klasi X. Predikatu A može se korenspondirati podskup $S \equiv \{x \in X : A(x)\}$. Za konstrukciju elemenata od S potrebno je prvo konstruisati elemente od X, tj imati konstrukciju K_X, a onda je potrebno da imamo dokaz za $A(x)$, tj. potrebno je da imamo konstrukciju $K_{XS}(x)x$. Naravno, podrazumjevamo da podskup S nasleđuje relaciju jednakosti skupa $(X,=_X,\neq_X)$. Međutim, nije sasvim korektno govoriti sa je element od S i element od X:, sem toga što objekat x mora zadovoljavati konstrukciju $K_X(x)x$ on mora zadovoljavati i konstrukciju $K_{XS}(x)x$, tj. mora se znati dokaz za $A(x)$. Ovim opisom podskupa opisali smo konstrukciju klase P_X koja se sastoji od svih podskupova skupa $(X,=_X,\neq_X)$. Ako su Y i Z podskupovi skupa X definiše se

$$Y =_{P_X} Z \Longleftrightarrow Y \subseteq Z \wedge Z \subseteq Y$$

odnosno

$$Y =_{P_X} Z \iff (\forall y \in Y)(\exists z \in Z)(y =_X z) \wedge$$
$$\wedge (\forall z \in Z)(\exists y \in Y)(z =_X y),$$

gdje je P_X partitivni skup skupa $(X, =_X, \neq_X)$. Relaciju slabog razlikovanja u skupu P_X definišemo sa

$$Y \neq'_{P_X} Z \iff (\exists y \in Y)\neg(y \in Z) \vee (\exists z \in Z)\neg(z \in Y).$$

Uvođenjem slijedećeg pojma u konstruktivnu matematiku: za element $x \in X$ pišemo

$$x \notin Y \iff (\forall y \in Y)(y \neq_X x)$$

možemo determinisati pojam stroge razlikovanja u skupu P_X

$$Y \neq_{P_X} Z \iff (\exists y \in Y)(y \notin Z) \vee (\exists z \in Z)(z \notin Y).$$

Opis konstruisanja funkcija $f:X \longrightarrow Y$ omogućava nam da determinišemo klasu $F(X,Y)$ svih funkcija iz X u Y. U klasi $F(X,Y)$ definišemo: ako su $f, g \in F(X,Y)$, tada

$$f =_F g \iff D(f) =_{P_X} D(g) \wedge Im(f) =_{P_Y} Im(g) \wedge$$
$$\wedge (\forall x \in D(f))(f(x) =_Y g(x)).$$

Ako su f i g totalne funkcije iz $F(X,Y)$ tada definišemo

$$f \neq_F g \iff (\exists x \in X)(f(x) \neq_Y g(x)).$$

Napomena. P_X je upravo $F(X, \Omega)$. Napomenimo, takođe, da je partitivni skup singla upravo Ω.

1.4.3. Bazne definicije. Neka su $(X, =_X, \neq_X)$ i $(Y, =_Y, \neq_Y)$ skupovi i neka je $f:X \longrightarrow Y$ funkcija. Za funkciju f se kaže da je

- totalna ako i samo ako
  $(\forall x \in X)(Ef(x) \wedge f(x) \in Y)$;
- injektivna ako i samo ako
  $(\forall xx' \in D(f))(f(x) =_Y f(x') \Longrightarrow x =_X x')$;
- ulaganje (engleski termin: embedding, Rutherburg) ako i samo ako
  $(\forall xx' \in D(f))(x \neq_X x' \Longrightarrow f(x) \neq_Y f(x'))$;
- sirjektivna ako i samo ako
  $(\forall y \in Y)(Ex \wedge x \in D(f) \wedge y =_Y f(x))$;

- slabo injektivna ako i samo ako
$(\forall x x' \in D(f))(\neg(f(x) =_Y f(x')) \Longrightarrow \neg(x =_X x'))$;
- bijekcija ako i samo ako je funkcija f totalna, injektivna i sirjektivna.

Neka je $(X,=)$ skup. Za element x skupa $(X,=)$ se kaže da je diskretan ako i samo ako
$$(\forall y \in X)(y = x \vee \neg(y = x)).$$
Za skup $(X,=)$ se kaže da je diskretan skup ako i samo ako je svaki element skupa $(X,=)$ diskretan, tj. ako i samo ako vrijedi
(d) $$(\forall xy \in X)(x = y \vee \neg(x = y)).$$

Neka je X klasa i Y njena podklasa. Za Y se kaže da je odlučiva u X ako i samo ako vrijedi
(D) $$(\forall x \in X)(x \in Y \vee \neg(x \in Y)).$$

Napomena. Ovaj termin ima i slabiju verziju: Za podklasu Y se kaže da je slabo odlučiva u X ako i samo ako je
$$(\forall x \in X)(\neg(x \in Y) \vee \neg\neg(x \in Y)).$$
Međutim, ako je Y slabo odlučivo u X i X slabo odlučivo u Z, tada ne možemo dokazati, u općem slučaju, da je Y slabo odlučivo u Z; prema tome, ovaj termin nije od velike koristi.

1.4.4. Osnovne osobine.

1. (Romano,) Neka je $(X,=)$ skup. Tada su slijedeći uslovi ekvivalentni:

(i) Skup $(X,=)$ je diskretan.

(ii) Dijagonala skupa $(X\times X,=_{X\times X})$ je odlučiv podskup u X X.

(iii) Svaki singl skupa $(X,=)$ je odlučiv podskup u X.

(iv) Za svaki skup $(Y,=)$ i svaku totalnu funkciju f: Y X, njen graf G(f) je odlučiv u $Y\times X$.

2. (Romano, [38]) Neka su $(X,=_X,\neq_X)$ i $(Y,=_Y,\neq_Y)$ skupovi i neka je $f:X \longrightarrow Y$ totalna funkcija. $f^{-1}:Y \longrightarrow X$ je funkcija ako i samo ako je f injektivno utapanje, i vrijedi
$$f^{-1}.f =_{F(X,X)} Id_X \quad \text{i} \quad f.f^{-1} =_{(Im(f),Im(f))} Id_{Im}$$

3.(Romano, [38]) Neka su $(X,=_X,\neq_X)$ i $(Y,=_Y,\neq_Y)$ skupovi i neka za fukkciju $f:X \longrightarrow Y$ postoji totalna funkcija $f'':Y \to X$ takva da je $f.f'' =_{F(Y,Y)} Id_Y$. Tada je f sirjektivna funkcija.

Napomena: Neka je $f:X \longrightarrow Y$ totalna sirjektivna funkcija. Tada relacija

$$f^{-1} = \{(y,x) \in Y \times X : (x,y) \in f\}$$

jeste injektivna relacija ali nije funkcija.

Za funkciju f se kaže da je na (engleski: onto) ako i samo ako postoji funkcija g koja je desni inverz funkcije f.

1.4.5. Primjeri. U ovom dijelu imamo namjeru da kroz primjere ilustrujemo problematiku u vezi sa jednakošću i različitošću bishopovske konstruktivne matematike koja se, inače, ne pojavljuje u klasičnoj matematici.

1° a) U klasi $\hat{N}$ definišemo

(a_1) $\quad a =_N b \iff a \equiv b$,

(a_2) $\quad a =^m b \iff (|a - b| \text{ je djeljivo sa } m)$.

Tada razlikujemo radi ilustracije, $(\hat{N},=_N)$ od $(\hat{N},=^5)$, jer je, na primejr

$$7 =^5 2 \quad \text{i} \quad \neg(7 =_N 2).$$

Skup $(\hat{N},=_N)$ nazivamo skupom prirodnih brojeva.

b) U klasi $N \times N$ definišemo

$$(m,n) =_Z (u,v) \iff m+v =_N u+n.$$

Skup $(N \times N,=_Z)$ nazivamo skupom cijelih brojeva i obilježavamo ga sa Z. U skupu Z definišemo vanjsko množenje elementima skupa $(\hat{N},=_N)$ sa

$$(m,n).v =_Z (m.v,n.v).$$

c) U klasi $Z \times N$ definišemo

$$((m,n),p) =_Q ((u,v),s) \iff (m,n).s =_Z (u,v).p .$$

Skup $(Z \times N,=_Q)$ nazivamo skupom racionalnih brojeva i obilježavamo ga sa Q.

d) Neka je Q^{∞} klasa nizova $(x_n)_n$ racionalnih brojeva za koje vrijedi

$$\forall m \geq 1 \; \forall n \geq 1 (|x_m - x_n| \leq m^{-1} + n^{-1}).$$

U Q^{∞} definišemo

(d_1) $\quad (x_n)_n =_p (y_n)_n \iff \forall i \leq p(|x_i - y_i| \leq 2i^{-1})$,

(d_2) $\quad (x_n)_n =_R (y_n)_n \iff \forall n \leq 1(|x_n - y_n| \leq 2n^{-1})$.

Skup $(Q^{\infty}, =_R)$ nazivamo skupom Cauchyevih realnih brojeva.

e) Neka je Q_1^{∞} klasa nizova $(x_n)_n$ racionalnih brojeva za koje vrijedi

(1) $\quad \forall k \geq 1^{\nabla} \exists n \; \forall m \geq 1 \; \forall m' \geq 1 (|x_{n+m} - x_{n+m'}| < 2^{-k})$.

Skup $(Q_1^{\infty}, =_{R_1})$, u kojem je jednakost definisana sa

(2) $\quad (x_n)_n =_{R_1} (y_n)_n \iff \forall k \geq 1^{\nabla} \exists n \; \forall m \geq n (|x_m - y_m| \leq 2^{-k})$,

nazivamo skupom slabih Cauchyevih realnih brojeva, ili skupom neoscilatornih Cauchyevih realnih brojeva (Heyting, [13]; Troelstra, [54]).

f) Neka je Q_2^{∞} klasa nizova $(x_n)_n$ racionalnih brojeva koji osim uslova (1), zadovoljavaju i uslov uniformne ograničenosti

$$\exists m \; \forall n \geq 1 (|x_n| \leq m).$$

Skup $(Q_2^{\infty}, =_{R_1})$, u kojem je jednakost definisana sa (2), naziva se skupom ograničenih slabih Cauchyevih realnih brojeva, (Heyting, [13]; Troelstra [54]).

g) Ashvinikumar ([2],[54]) je uveo nizove ograničene varijacije kao nizove $(x_n)_n$ racionalnih brojeva za koje vrijedi

$$\exists m \; \forall k \geq 1 (|x_0| + \sum_{i=0}^{k} |x_{i+1} - x_i| < m).$$

Skup $(Q_3^{\infty}, =_{R_1})$, nazivamo skupom Cauchyevih kvazi-brojeva.

Koristeći se rezultatima radova [2], [4], [5], [13], [58], [54] može se zaključiti da vrijedi

$$\hat{N} \subset Z \subset Q \subset (Q^{\infty}, =_R) \subset (Q_1^{\infty}, =_{R_1}) \subset (Q_2^{\infty}, =_{R_1}) \subset (Q_3^{\infty}, =_{R_1}).$$

2° Neka je R^{∞} klasa objekata $(x_n)_n$, gdje su članovi nizova realni brojevi. U R^{∞} definišemo

i) $(x_n)_n =_o (y_n)_n \iff \forall n(x_n =_R y_n)$,

ii) $(x_n)_n =_p (y_n)_n \iff \forall i \leq p(x_i =_R y_i)$.

Neka je niz $(a_n)_n$ formiran na slijedeći način:

$$a_n \equiv \begin{cases} 0 & \text{Ako je } a_m =_N 1, \text{ za neko } m < n, \text{ ili se ne} \\ & \text{može naći niz od sedam uzastopnih sedmica} \\ & \text{među prvih } n \text{ decimala dekadskog razvoja} \\ & \text{broja } \overline{1}, \\ 1 & \text{u ostalim slučajevima .} \end{cases}$$

Ne može se dokazati da vrijedi $(a_n)_n =_o (o)_n$, ali sigurno, za svako unaprijd izabrano, p vrijedi $(a_n)_n =_p (o)_n$.

3° Neka je $(X,=)$ skup a Y i Z njegovi podskupovi. Podsjetimo se da je

$$Y =_{P_X} Z \iff Y \subseteq Z \wedge Z \subseteq Y.$$

a)(Johnstone, [16]) Dedekind-Trierneyov presjek u skupu $(Q,=_Q)$ racionalnih brojeva je par (L,U) podklasa skupa $(Q,=_Q)$ za koje vrijedi

$$\exists\, q \in L \wedge \exists\, r \in U,$$
$$q \in L \iff \exists\, q' > q(q' \in L),$$
$$r \in U \iff \exists\, r' < r(r' \in U),$$
$$q \in L \wedge q' \in U \Longrightarrow q < q',$$
$$q < q' \Longrightarrow q \in L \vee q' \in U.$$

Ako je R_t klasa svih takvih presjeka, tada se skup $(R_t,=_{P_Q})$ naziva skupom Dedekind-Tierneyevih realnih brojeva.

b)(Johnstone, [16]) Dedekind-McNiellеov presjek u skupu $(Q,=_Q)$ je par (L,U) podklasa skupa $(Q,=_Q)$ koji zadovoljava:

$$\exists\, q \in L \wedge \exists r \in U,$$
$$L \equiv \{q \in Q:(\exists\, q' < q)(\forall q'' \in U)(q'' > q')\},$$
$$U \equiv \{r \in Q:(\exists r' > r)(\forall r'' \in L)(r'' < r')\} .$$

Ako je R_m klasa svih ovakvih presjeka, tada se skup $(R_m,=_{P_Q})$ naziva skupom Dedekind-McNiellеovih realnih brojeva. Prema , svaki Dedekind-Tierneyev realan broj je i Dedekind-McNiellеov realan broj, ali u općem slučaju ne vrijedi obrnuto.

c)(Staples, [47]) Dedekind-Staplesov presjek u skupu $(Q,=_Q)$ racionalnih brojeva je par (S,T) podklasa skupa $(Q,=_Q)$

za koji vrijedi:

$$\exists s \in S \wedge \exists t \in T,$$
$$(\forall s \in S)(\forall t \in T)(s \leqslant t),$$
$$(\forall r \in Q)((\forall s \in S)(s < r) \Rightarrow (s > r \Rightarrow t \in T)),$$
$$(\forall r \in Q)((\forall t \in T)(t > r) \Rightarrow (s < r \Rightarrow s \in S)).$$

Ako je R_Q klasa svih ovakvih presjeka, tada se [illegible] $(R_Q, =_{R_Q})$ naziva skupom Dedekind-Stapleovih realnih brojeva.

d)(i) Podklasa S skupa $(Q, =_Q)$ naziva se lijevim presjekom u skupu $(Q, =_Q)$ ako:

(a) $\exists s \in S \wedge (\exists t)\neg(t \in S)$,

(b) $\forall sr((s < r \wedge \neg\neg(r \in S)) \Rightarrow s \in S)$,

(c) $(\forall s \in S)(\exists s' \in S)(s < s')$,

(d) $\forall rr'((r < r') \Rightarrow (r \in S \vee \neg(r' \in S)))$.

(ii) Podklasa S skupa $(Q, =_Q)$ naziva se slabim lijevim presjekom u skupu $(Q, =_Q)$ ako zadovoljava (a), (b) i (c).

(iii) Podklasa S skupa $(Q, =_Q)$ naziva se slabim lijevim slabo ograničenim presjekom u skupu $(Q, =_Q)$ ako vrijedi (b), (c) i

(a') $\neg\neg(\exists s \in S) \wedge \neg\neg(\exists t)\neg(t \in S)$.

Neka su R, R_e, R_{oe} klasa svih presjeka, slabih presjeka i slabih slabo ograničenih presjeka respektivno. Tada se skup $(R, =_{P_Q})$, $(R_e, =_{P_Q})$ i $(R_{oe}, =_{P_Q})$ respektivno naziva Dedekind-Troelstraovim skupom realnih brojeva, proširenim skupom realnih brojeva i jako proširenim skupom realnih brojeva. U je pokazano da vrijedi

$$(Q, =_Q) \subset (R, =_{P_Q}) \subset (R_e, =_{P_Q}) \subset (R_{oe}, =_{P_Q}).$$

Napomena: Ako uvedemo poredak za jednakosti kako je to pokazano ranije tada za jednakosti $=_p$ i $=_R$ na klasi Q, iz primjera 1°d), imamo

$$=_p \prec =_R .$$

Sličnu, ali jače izraženu, situaciju imamo u primjeru 2°:

$$=_1 \prec =_2 \prec =_3 \prec \ldots \prec =_p \prec \ldots \prec =_0 .$$

Dakle, ako imamo dva elementa i hoćemo da utvrdimo odnos između njih, možemo samo utvrditi "koliko" su jednaki. Ako ovo razmišljanje uopštimo, onda imamo potpuno prirodan postupak koji se primjenjuje u prirodnim naukama.

Neka je M neki objekat (klasa) elemenata, a $(P_i)_i$

(striktno)izbrojiv niz dvovalentnih predikata na M sa svojstvima:

(1) $(\forall a \in M)(\forall i)(P_i(a) \vee \neg P_i(a))$,

(2) $(\forall ab \in M)(\forall i)(P_i(a)b \wedge P_i(b)a \wedge P_i(a)c \Rightarrow P_i(a)c)$.

Na klasi M definišemo jednakosti "$=_i$" ovako

$$a =_i b \longleftrightarrow \bigwedge_{s=1}^{i} (P_s(a) \leftrightarrow P_s(b)).$$

Tada je $(=_i)_i$ uzlazni niz relacija jednakosti na klasi M. Neka je X nama nepoznat objekat elemenata (tzv. konstruktivna klasa) a $(f_i)_i$ (striktno) izbrojiv niz postupaka pri ispitivanju objekata (t.j. $f_i : X \longrightarrow (M, =_i)$ su totalna preslikavanja). Za par elemenata x i x' iz klase X, primjenom postupka f_i ovako

$$x =^{ij} x' \Longleftrightarrow f_j(x) =_i f_j(x'),$$

imamo mogućnost da ispitamo "koliko" su elementi x i x' jednaki kao članovi klase X (tada su f_i injektivne funkcije i mogu se shvatiti kao ulaganja u M).

4° a) U skupovima $(\hat{\Omega}, =_\Omega)$, Z i Q relacija različitosti $\neq$ zadovoljava uslov $x \neq y \longleftrightarrow \neg(x = y)$.

b) U skupu $(\mathcal{C}^\infty, =_R)$ Cauchyevih realnih brojeva relacija različitosti se definiše na slijedeći način ([4],[5],[13],[41])

$$(x_n)_n \neq_R (y_n)_n \longleftrightarrow (\forall k \geq 1)(\exists p \geq 1)(\forall i \geq 1)(|x_{p+i} - y_{p+i}| \geq 2^{-k}).$$

Za ovu relaciju, kako je to pokazano u [4], [5], [13], [41], [53] i [54], vrijedi i aksiom (iv), što znači da je ovo relacija odvojenosti u heytingovom smislu.

1.4.6. Konačnost i beskonačnost. Oprijedjeljivanjem za principe intuicionističke logike (Heyting,[18]) odustaje se od nekih klasičnih logičkih tautologija, kao na primjer, principa tertuim non datur (ili TND), $F \vee \neg F$, za proizvoljnu formulu F koja može sadržavati slobodne parametre; što povlači razlikovanje nekih rezultata konstruktivne matematike od rezultata klasične matematike. U ovom dijelu pokušaćemo prezentirati varijante konačnosti, izbrojivosti i beskonačnosti koje su uveli Brouwer (Brouwer,[6]) i Heyting (Heyting,[18]). Posebno značajan doprinos u konsolidaciji shvatanja ideja Brouwera i Heyting, dali su Troelstra ([55]), Dummett ([11]) i

McCarty ([18]).

Neka su $(X,=_X,\neq_X)$ i $(Y,=_Y,\neq_Y)$ skupovi i neka je $f:X \longrightarrow Y$ funkcija. Pišaćemo

(1)([18]) $f:X \longrightarrow Y$ akko je f funkcija iz X u Y.

(2) $f:X \rightarrowtail Y$ akko je f injektivna funkcija iz X u Y.

(3)([18]) $f:X \twoheadrightarrow Y$ akko je f funkcija iz X na Y.

(4) $f:X \twoheadrightarrow Y$ akko je f injektivna funkcija iz X na Y.

(5)([18]) $f:X \rightarrowtail Y$ akko je f bijekcija iz X u Y.

(6)([18]) $f:X \rightarrowtail\!\!\!\!\twoheadrightarrow Y$ akko je f bijekcija iz X na Y.

Napomena: ([55]) Uvedimo predikat $P^k_n(m);k,n,m \in N$. $P^k_n(m) \Longleftrightarrow$ m je broj posljednje decimale n-tog niza od deset uzastopnih sedmica u dekadnom razvoju broja π^k.

Definicija a) Neka je $(N,=_N)$ skup prirodnih brojeva. Za skup $(X,=_X,\neq_X)$ se kaže da je:

(1)([18],[55]) striktno konačan akko
$$En \in N\ Ef\ (f:\bar{n} \rightarrowtail\!\!\!\!\twoheadrightarrow X).$$

(2)([55]) injektivno konačan akko
$$En \in N\ Ef\ (f:\bar{n} \rightarrowtail X).$$

(3)([18],[55]) konačan akko
$$En \in N\ Ef\ (f:\bar{n} \twoheadrightarrow X).$$

(4)([55]) injektivno subkonačan akko
$$En \in N\ EA \subset \bar{n}\ Ef\ (f:A \rightarrowtail X).$$

(5)([18],[55]) subkonačan akko
$$En \in N\ EA \subset \bar{n}\ Ef\ (f:A \twoheadrightarrow X).$$

Primjeri I:

1.([18]) Klasa $\{\{o\},\{o:F \vee \neg F\}\}$ je konačna, ali nije striktno konačna.

2.([18]) Klasa $\{o:F \vee \neg F\}$ je subkonačna, ali nije konačna.

3.([55]) Neka je $X \equiv \{s:(s = 2) \vee (s = 1 \wedge P^1_1(s))\}$. Tada je X injektivno subkonačna klasa jer $n = 2$, $A \equiv \{x:(x = 2 \vee (x = 1 \quad ExP^1_1(x))$ a f neka je
$$f(2) = 2,\ f(1) = s \text{ ako } P^1_1(s).$$

Tvrdnja a1)([18])

(1) $\forall X$(X je konačan $\longrightarrow$ X je striktno konačan) $\Longrightarrow$ TND,

(2) $\forall X$(X je subkonačan $\longrightarrow$ X je konačan) $\Longrightarrow$ TND.

Tvrdnja a2)([11]) (1) Podskup subkonačnog skupa jeste subkonačan skup.

(2) Subkonačna unija subkonačnih skupova jeste subkonačan skup.

(3) Svaki podskup singla jeste subkonačan skup.

Tvrdnja a3)([18]) Skup je subkonačan akko je podskup konačnog skupa.

Tvrdnja a4)([18]) Ako je X konačna i diskretna skup, tada je X striktno konačan skup.

Tvrdnja a5)([11]) (1) Konačna unija konačnih klasa jeste konačna klasa.

(2) Svaki singl je konačan.

Definicija b) Za skup $(X,=_X,\neq_X)$ je kaže da je:

(1)([18],[55]) striktno izbrojiv akko

$$Ef\ (f:N \rightarrowtail\!\!\!\!\!\rightarrow X).$$

(2)([55]) injektivno izbrojiv akko

$$Ef\ (f:N \rightarrowtail\!\!\!\!\!\twoheadrightarrow X).$$

(3)([18],[55]) izbrojiv akko

$$Ef\ (f:N \longrightarrow\!\!\!\!\!\rightarrow X).$$

(4)([55]) injektivno subizbrojiv akko

$$EA \subset N\ Ef\ (f:A \rightarrowtail\!\!\!\!\!\twoheadrightarrow X).$$

(5)([18],[55]) subizbrojiv akko

$$EA \subset N\ Ef\ (f:A \longrightarrow\!\!\!\!\!\rightarrow X).$$

Primjeri II:

1. Klasa $X = \{n: (EmP_1^n(m))\}$ je injektivno subizbrojiva ali nije izbrojiva ([55]).

2.([55]) Klasa $X \equiv \{n+r_n : EnP_m^1(n)\}$, gdje je

$$r_k = \sum_{i=1}^{\infty} a_{ik} 10^{-i} \quad \text{sa} \quad a_{ik} = \begin{cases} 1 & \text{ako } P_1^k(i) \\ 0 & \text{inače,} \end{cases}$$

je subizbrojiva jer za A možemo uzeti $A = \{n : EmP_1^n(m)\}$ i $f:A \longrightarrow X$ definisano ovako

$$2n \in A \Longrightarrow f(2n) = n + r_{2n},$$

$$2n+1 \in A \Longrightarrow f(2n+1) = n + r_{2n+1}.$$

Tvrdnja b1)([11])

(1) Konačna unija izbrojivih skupova jeste izbrojiv skup.

(2) Svaki konačan skup jeste izbrojiv.

Tvrdnja b2)([11])

(1) Podskup subizbrojivog skupa jeste subizbrojiv skup.

(2) Subkonačna unija subkonačnih skupova jeste subizbrojiv skup.

(3) Svaki subkonačan skup jeste subizbrojiv.

Definicija c) Za skup $(X,=_X,\neq_X)$ se kaže da je:

(1)([55]) injektivno beskonačan akko

$$Ef\ (f:X \rightarrowtail\!\!\!\!\!\rightarrow N).$$

(2)([18] ,[55]) beskonačan akko

$$Ef\ (f:X \longrightarrow\!\!\!\!\!\rightarrow N).$$

(3)([55]) injektivno subbeskonačan akko

$$EY \subset X\ Ef\ (f:Y \rightarrowtail\!\!\!\!\!\rightarrow N).$$

(4)([55]) injektivno odlučivo subbeskonačan akko

$$EY \subset X\ Ef\ (f:Y \rightarrowtail\!\!\!\!\!\rightarrow N)$$

i podskup Y je odlučiv u X.

(5)([18] ,[55]) subbeskonačan akko

$$EY \subset X\ Ef\ (f:Y \longrightarrow\!\!\!\!\!\rightarrow N).$$

(6)([18]) beskonačan u klasičnom smislu akko

$$Ef(f:N \rightarrowtail X).$$

Primjeri III:

1.([55]) Klasa $V \equiv \bigcup_{n=1}^{\infty}[n,n+1/n]$ jeste beskonačna klasa jer se može preslikati na N, uzimajući $f(x) = n$ za $x \in [n,n+1/n]$, ali nije injektivno odlučivo beskonačna.

2. Segment $[0,1]$ nije beskonačan jer se ne može preslikati na N. U [55] je pokazano, u intuicionističkoj matematici, da je segment $[0,1]$ injektivno subbeskonačan.

Komentari.

1. U [11] je uveden termin slabe konačnosti za skup X ovako

$$\forall f \in X^N\ \exists i,j \in N\ (i < j \rightarrow f(i) = f(j)).$$

2. Prema A.S.Troelstri ([55]), J.J.Jonge je održao predavanje na univerzitetu u Amsterdamu decembra 1976. godine

koje se, između ostalog, odnosilo i na pojam konačnosti u intuicionističkoj matematici.

Koristeći se Brouwerovim definicijama ograničenosti (Heyting,[16], 3.4.4.) de Iongh je, prema Troelstri, uveo pojam "determined in number (by n)", ako je skup ograničen sa brojem n i sadrži konačan podskup od n elemenata.

3. A.S.Troelstra je u svom radu [55] uveo i neke druge oznake odnosa između skupa $(N,=_N)$ sa drugim skupovima.

2.0. OSNOVNE ALGEBARSKE STRUKTURE

2.0.1. Definicije.

Lema 1. Neka su $(X,=_X,\neq_X)$ i $(Y,=_Y,\neq_Y)$ skupovi. U klasi X Y imamo kanonske relacije jednakosti i različitosti date sa

$$(x,y) = (u,v) \iff x =_X u \wedge y =_Y v ,$$

$$(x,y) \neq (u,v) \iff x \neq_X u \vee y \neq_Y v .$$

Dokaz: Provjeravanjem.

Definicija 0. Neka je $(X,=_X,\neq_X)$ skup. Za totalnu funkciju

$$\phi: X \times X \ni (a,b) \longmapsto \phi(a,b) \in X$$

se kaže da je unutrašnja binarna operacija u X.

Napomena I:

$$x =_X x' \wedge y =_X y' \Longrightarrow \phi(x,y) =_X \phi(x',y'),$$

$$\phi(x,y) =_X \phi(x',y') \Longrightarrow x \neq_X x' \vee y \neq_X y'.$$

Definicija 1. Neka je $(X,=_X,\neq_X)$ skup koji sadrži bar jedan element o (nula).

(a) Monoid je skup X sa jednom unutrašnjom binarnom operacijom "+" za koju vrijedi

$$(\forall abc \in X)(a+(b+c) =_X (a+b)+c),$$

$$(\forall a \in X)(a+o =_X a).$$

(b) Grupa je skup X sa jednom unutrašnjom binarnom operacijom "+" za koju vrijedi

$$(\forall abc \in X)(a+(b+c) =_X (a+b)+c),$$

$$(\forall a \in X)(a+o =_X a)$$

$$(\forall a \in X)(\exists b \in X)(a+b =_X o),$$

Za grupu $(X,=_X,\neq_X,+)$ se kaže da je abelova ako

$$(\forall ab \in X)(a+b =_X b+a).$$

Napomene II:

1. $a =_X a' \wedge b =_X b' \Longrightarrow a+b =_X a'+b'$,
2. $a+b \neq_X a'+b' \Longrightarrow a \neq_X a' \vee b \neq_X b'$,
3. $a+b \neq_X o \Longrightarrow a \neq_X o \vee b \neq_X o$,
4. $-a \neq_X -a' \Longleftrightarrow a \neq_X a'$,
5. $a+b \neq_X a'+b \Longleftrightarrow a \neq_X a'$.

<u>Definicija 2.</u> <u>Prsten</u> je skup $(A,=_A,\neq_A)$ koji sadrži element o (nula) i dvije unutrašnje binarne operacije "+" i "." (totalne funkcije iz $A \times A$ u A) koje zadovoljavaju slijedeće osobine (pisaćemo ab umjesto a.b):

$$(\forall abc \in A)(a+(b+c) =_A (a+b)+c),$$

$$(\forall a \in A)(a+o =_A a),$$

$$(\forall a \in A)(\exists a' \in A)(a+a' =_A o),$$

$$(\forall ab \in A)(a+b =_A b+a),$$

$$(\forall abc \in A)(a(bc) =_A (ab)c),$$

$$(\forall abc \in A)(a(b+c) =_A ab+ac),$$

$$(\forall ab \in A)(ab =_A ba).$$

Napomene III:

6. $a =_A a' \wedge b =_A b' \Longrightarrow ab =_A a'b'$,
7. $ab \neq_A a'b' \Longrightarrow a \neq_A a' \vee b \neq_A b'$,
8. Ako prsten $(A,=_A,\neq_A,+,.)$ ima jedinicu 1 , tada vrijedi:

(i) $o =_A 1 \vee o \neq_A 1$,

(ii) Ako je $o =_A 1$, tada je $A \equiv \{o\}$.

(iii) Ako je $o \neq_A 1$, tada vrijedi

$$(\forall a \in A)(a.1 =_A a).$$

Definicija 3. Neka je $(A,=_A,\neq_A,+,.)$ prsten.

(a) Richmanovo polje je prsten A sa jedinicom $1(\neq_A 0)$ za koji vrijedi

(F_1) $\quad (\forall a \in A)(a \neq_A 0 \Longrightarrow (\exists a' \in A)(aa' =_A 1))$.

(b) Ruitenburgovo polje je prsten A sa jedinicom $1(\neq_A 0)$ za koji vrijedi

(F_2) $\quad (\forall a \in A)(a =_A 0 \vee (\exists a' \in A)(aa' =_A 1))$.

Definicija 4. Neka je $(A,\neq_A,\neq_A,+,.)$ prsten a $(G,=_G,\neq_G,+)$ abelova grupa. Za grupu G se kaže da je A-modul akko postoji vanjska operacija u G nad A, tj. totalna funkcija

$$A \times G \ni (a,x) \longmapsto ax \in G$$

takva da vrijedi

$$(\forall ab \in A)(\forall x \in G)((ab)x =_G a(bx)),$$

$$(\forall x \in G)(1.x =_G x),$$

$$(\forall ab \in A)(\forall x \in G)((a+b)x =_G ax+bx),$$

$$(\forall a \in A)(\forall xy \in G)(a(x+y) =_G ax+ay).$$

$$(\forall a \in A)(\forall x \in G)(ax \neq_G o \Rightarrow a \neq_A o \wedge x \neq_G o).$$

Ako je prsten A polje, tada se A-modul naziva vektorski prostor.

Napomene IV:

1. $a =_A b \wedge x =_G y \Longrightarrow ax =_G by$,
2. $ax \neq_G by \Longrightarrow a \neq_A b \vee x \neq_G y$.

2.0.2. Grupe.

Tvrdnja 2.([32], Lemma 2.1.) Ako je bar jedan element abelove grupe $(G,=_G,\neq_G,+)$ diskretan, tada je grupa G diskretna.

Dokaz: Neka je x diskretan element grupe G, tj. neka vrijedi

$$(\forall y \in G)(y = x \vee \neg(y = x)).$$

Ako umjesto elementa y uzmemo y+x-z $(z \in G)$, tada imamo

$$(\forall xyz \in G)(y+x-z = x \vee \neg(y+x-z = x)),$$

odnosno

$$(\forall yz \in G)(y = z \vee \neg(y = z)).$$

Tvrdnja 3.([30], Lemma 2.2.) Neka je $(G,=,\neq,+)$ grupa. Tada vrijedi

$$(\forall abc \in G)(a \neq b \Longrightarrow a \neq c \vee c \neq b).$$

Dokaz:

$a \neq b \Longleftrightarrow a-b \neq o \Longleftrightarrow (a-c)+(c-b) \neq o \Longrightarrow a-c \neq o \vee c-b \neq o \Longleftrightarrow a \neq c \vee c \neq b.$

Definicija 5.([34]) Neka je $(G,=_G,\neq_G,+)$ grupa. Relacija ekvivalencije R_G na G naziva se relacija kongruencije na G akko vrijedi

$$(a,b)\in R_G \wedge (a',b')\in R_G \Longrightarrow (a+a',b+b')\in R_G .$$

Relacija C_G na G koja zadovoljava slijedeće uslove

$$(a,a) \notin C_G ,$$

$$(a,b) \in C_G \Longrightarrow (b,a) \in C_G ,$$

$$(a,b) \in C_G \Longrightarrow (a,c) \in C_G \vee (c,b) \in C_G ,$$

$$(a+a',b+b') \in C_G \Longrightarrow (a,b) \in C_G \vee (a',b') \in C_G$$

za svako $a,b,a',b' \in G$ naziva se relacija kokongruencije na G.

Definicija 6. Neka je $(G,=_G,\neq_G,+)$ grupa a $(H,=_G,\neq_G)$ njen podskup. Za skup H se kaže da je podgrupa grupe G akko vrijedi

$$o \in H,$$

$$a \in H \wedge b \in H \Longrightarrow a+b \in H,$$

$$a \in H \Longrightarrow -a \in H.$$

Tvrdnja 4. Ako je $(G,=_G,\neq_G,+)$ grupa a R_G relacija ekvivalencije na G, tada je R_G relacija kongruencije na G akko je $H = \{a \in G:(a,o) \in R_G\}$ podgrupa grupe G i

$$(a,b) \in R_G \Longleftrightarrow a-b \in H.$$

Dokaz: Kao u klasičnoj algebri.

Definicija 7.([41]) Neka je $(G,=_G,\neq_G,+)$ grupa a $(C,=_G,\neq_G)$ njen podskup. Za C se kaže da je kopodgrupa grupe G akko

$$o \notin C ,$$

$$a+b \in C \Longrightarrow a \in C \vee b \in C,$$

$$-a \in C \Longrightarrow a \in C.$$

Napomena V: Neka je $(G,=,\neq,+)$ grupa. Tada je relacija "$=$" jednaksoti na G relacija kongruencije na G a skup $(o) \equiv \{a \in G : a =_G o\}$ je podgrupa grupe G. Dalje, relacija različitosti "$\neq$" na G je relacija kokongruencije na G a skup $\{a \in G : a \neq_G o\}$ je kopodgrupa grupe G.

Tvrdnja 5.([34], Proposition 4.) Ako je $(G,=_G,\neq_G,+)$ grupa a C_G relacija na G, tada je C_G relacija kokongruencije na G takva da je $\neq_G \asymp C_G$ akko je skup $C \equiv \{a \in G : (a,o) \in C_G\}$ kopodgrupa grupe G i vrijedi

$$(a,b) \in C_G \iff a-b \in C.$$

Dokaz:

(1) Neka je C_G relacija kokongruencije na grupi G. Tada

(i) $o \notin C$, jer $\neg\,(o,o) \notin C_G$.

(ii) $-a \in C \iff (-a,o) \in C_G \iff (o-a,a-a) \in C_G \Longrightarrow$

$\Longrightarrow (a-a,o-a) \in C_G \Longrightarrow (a,o) \in C_G \vee (-a,-a) \in C_G$.

(iii) $a+b \in C \Longrightarrow (a+b,o) \in C_G \Longrightarrow (a,o) \in C_G \vee (b,o) \in C_G \iff$

$\iff a \in C \vee b \in C$.

(2) Neka je C kopodgrupa grupe G. Definišimo relaciju C_G na slijedeći način

$$(\forall ab \in G)((a,b) \in C_G \iff a-b \in C).$$

Provjerima da li je C_G relacija kokongruencije. Imamo

a) $(\forall a \in G)\ ((a,a) \notin C_G)$ jer $\neg\,(C \ni o =_G a-a)$.

b) $(\forall ab \in G)((a,b) \in C_G \iff a-b \in C \Longrightarrow b-a \in C \iff (b,a) \in C_G)$.

c) $(\forall abc \in G)((a,b) \in C_G \iff a-b \in C \iff (a-c)+(c-b) \in C \Longrightarrow$

$\Longrightarrow a-c \in C \vee c-b \in C \iff (a,c) \in C_G \vee (c,b) \in C_G$).

d) $(\forall aa'bb' \in G)((a+a',b+b') \in C_G \iff a+a'-b-b' \in C \Longrightarrow$

$\Longrightarrow a-b \in C \vee a'-b' \in C \iff (a,b) \in C_G \vee (a',b') \in C_G)$.

Lema 6. Neka je $(G,=_G,\neq_G,+)$ grupa a C_G relacija kokongruencije na G. Tada je relacija $\neg C_G$ definisana ovako

$$(a,b) \in \neg C_G \iff \neg((a,b) \in C_G)$$

relacija kongruencije na G takva da je $\neg C_G \asymp =_G$.

Dokaz: (i) $(a,a) \in \neg C_G$.

(ii) $(a,b) \in \neg C_G \wedge (b,c) \in \neg C_G \iff \neg((a,b) \in C_G) \wedge \neg((b,c) \in C_G)$
$\longrightarrow \neg((a,b) \in C_G \vee (b,c) \in C_G) \longrightarrow \neg((a,c) \in C_G) \longleftrightarrow$
$\longleftrightarrow (a,c) \in \neg C_G$.

(iii) $(a,b) \in \neg C_G \longleftrightarrow \neg((a,b) \in C_G) \longrightarrow \neg((b,a) \in C_G) \longleftrightarrow$
$\longleftrightarrow (b,a) \in \neg C_G$.

(iV) $(a,b) \in \neg C_G \wedge (c,d) \in \neg C_G \iff \neg((a,b) \in C_G) \wedge \neg((c,d) \in C_G)$
$\longrightarrow \neg((a,b) \in C_G \vee (c,d) \in C_G) \longrightarrow \neg((a+c,b+d) \in C_G) \longleftrightarrow$
$\longleftrightarrow (a+c,b+d) \in \neg C_G$.

Posljedica 6.1. ([41], pp 24.) Neka je $(G,=_G,\neq_G,+)$ grupa i neka je $(C,=_G,\neq_G,+)$ njena kopodgruapa. Tada je skup $\neg C \equiv \{a \in G : \neg(a \in C)\}$ podgrupa grupa G.

Posljedica 6.2. Neka je $(G,=_G,\neq_G,+)$ grupa. Tada je relacija "$=_s$" na G definisana ovako

$$(\forall ab \in G)(a =_s b \iff \neg(a \neq_G b))$$

relacija kongruencije na grupi G takva da je $=_s \prec\!\!\prec =_G$.

Napomena VI: Neka je $(G,=_G,\neq_G,+)$ grupa. Tada je skup $T \equiv \{a \in G : a =_s o\}$ podgrupa grupe G i vrijedi $(o) \subseteq T$.

Teorem 7. Neka je $(G,=_G,\neq_G,+)$ grupa a R_G relacija kongruencije na G sa $R_G \prec\!\!\prec =_G$, i C_G relacija kokongruencije na G sa $\neq_G \prec\!\!\prec C_G$, takvi da je $\neg C_G \prec\!\!\prec R_G$. Tada je $(G,=,\neq,+')$ grupa sa relacijom jednakosti i različitosti definisanom sa

$$a = b \longleftrightarrow (a,b) \in R_G,$$

$$a \neq b \longleftrightarrow (a,b) \in C_G$$

i operacijom adicije definisanom sa

$$a +' b = a+b.$$

Dokaz: Prema Propoziciji 4. i Propoziciji 5. relacije kongruencije i kokongruencije = i $\neq$ na G definisane su sa

$$a = b \longleftrightarrow a-b \in H$$

$$a \neq b \longleftrightarrow a-b \in C$$

gdje su H i C odgovarajuća podgrupa koja odgovara kongruenciji R_G, i kopodgrupa koja odgovara kokongruenciji C_G. Jednostavno

se provjerava da je pri ovako shvaćenoj jednakosti zapravo elementi ove grupe podskupovi oblika $a+H$ ($a \in$).

Napomene VII: Grupa $(G,=,\neq,+')$ definisana u prethodnoj teoremi naziva se faktorska grupa i obilježava sa $G/(R_G,C_G)$. Ako su H i C odgovarajuća podgrupa i kopodgrupa koje odgovaraju relacijama kongruencije R_G i C_G takve da je $H \subseteq \neg C$, tada se grupa $(G,=,\neq,+')$ obilježava sa $G/(H,C)$. U njoj imamo

$$x+H = y+H \iff x-y \in H$$
$$x+H \neq y+H \iff x-y \in C$$
$$(x+H)+'(y+H) = x+y+H.$$

Definicija 8. Neka su $(G,=_G,\neq_G,+)$ i $(F,=_F,\neq_F,+')$ grupe. Totalno funkcija $f:G \longrightarrow F$ naziva se homomorfizam grupa akko $(\forall ab \in G)(f(a+b) =_F f(a)+'f(b))$. Homomorfizam f je bijektivan akko je injektivan i sirjektivan. Homomorfizam f je izomorfizam akko je bijektivno ulaganje na.

Tvrdnja 8. Neka je $f:G \longrightarrow F$ homomorfizam grupa. Tada je skup $Ker(f) = \{a \in G: f(a) =_F o\}$ podgrupa grupe G, a skup Im(f) podgrupa grupe F.

Dokaz: Kao u klasičnom slučaju.

Tvrdnja 9. Neka je $f:G \longrightarrow F$ homomorfizam grupa. Tada je podgrupa Ker(f) odlučiva u G akko je Im(f) diskretan skup.

Dokaz: $(\forall a \in G)(f(a) =_F o \vee \neg(f(a) =_F o)) \iff$

$$\iff (\forall a \in G)(a \in Ker(f) \vee \neg(a \in Ker(f))).$$

Posljedica 9.1. Neka je G grupa a H njena podgrupa. Tada je grupa G/H diskretna grupa akko je podgrupa H odlučiva u G.

Dokaz: Kanonski epimorfizam $p:G \longrightarrow G/H$ definisan sa $G \ni a \longmapsto a+H \in G/H$ ima jezgru upravo H.

Posljedica 9.2. Grupa G je diskretna akko je podgrupa (o) odlučiva u G.

Napomena VIII: Neka je $f:G \to F$ homomorfizam grupa. Tada vrijedi

$$f(a) \neq_F o \iff (\forall x \in Ker(f))(a \neq_G x).$$

Ako je f utapanje tada imamo

$$f(a) \neq_F o \iff a \notin Ker(f).$$

Teorem 10. Neka je $f:G \to F$ homomorfizam grupa. Tada postoji jedinstveni izomorfizam $h:G/Ker(f) \to Im(f)$ za koji vrijedi $f =_{Hom(G,F)} h \cdot p$.

Dokaz: (1) Dokažimo da je skup $C_f \equiv \{a \in G: f(a) \neq_F o\}$ kopodgrupa grupe G. Imamo

(i) $o \notin C_f$.

(ii) $a+b \in C_f \iff f(a+b) \neq_F o \iff f(a)+'f(b) \neq_F o \implies$

$\implies f(a) \neq_F o \vee f(b) \neq_F o \iff a \in C_f \vee b \in C_f$.

(iii) $-a \in C_f \iff f(-a) \neq_F o \iff f(a) \neq_F o \iff a \in C_f$.

(2) Neka je $H \equiv Ker(f)$. Definirajmo preslikavanje $h:G/H \to Im(f)$ na slijedeći način:

$$(\forall a+H \in G/H)(h(a+H) =_F f(a)).$$

Tada imamo

(iv) $a+H =_{G/H} b+H \iff a-b \in H \iff f(a-b) =_F o \iff f(a) =_F f(b)$

$\iff h(a+H) =_F h(b+H)$.

(v) $h(a+H) \neq_F h(b+H) \iff f(a) \neq_F f(b) \iff f(a-b) \neq_F o \iff$

$\iff a-b \in C_f \iff a+H \neq_{G/H} b+H$.

Teorem 11. Neka je $f:G \to F$ homomorfizam grupa i neka su H podgrupa grupe Im(f) i C kopodgrupa grupe Im(f) takve da je $H \subseteq \neg C$. Tada

(1) Skup $f^{-1}(H) \equiv \{a \in G: f(a) \in H\}$ je podgrupa grupe G takva da je $Ker(f) \subseteq f^{-1}(H)$.

(2) Skup $f^{-1}(C) \equiv \{a \in G: f(a) \in C\}$ je kopodgrupa grupe G takva da je $f^{-1}(C) \subseteq \{a \in G: f(a) \neq_F o\} \equiv C_f$.

(3) $f^{-1}(H) \subseteq \neg f^{-1}(C)$.

(4) Postoji jedinstveni izomorfizam

$G/(f^{-1}(H),f^{-1}(C)) \longrightarrow \mathrm{Im}(f)/(H,C)$.

Dokaz:

(1) Jednostavno.

(2) $a \# C \Longrightarrow f(a) =_F a \# C \Longrightarrow b \# f^{-1}(C)$.

$a+b \in f^{-1}(C) \Longleftrightarrow f(a+b) \in C \Longleftrightarrow f(a) \in C \vee f(b) \in C \Longleftrightarrow$

$\Longleftrightarrow a \in f^{-1}(C) \vee b \in f^{-1}(C)$.

$-a \in f^{-1}(C) \Longleftrightarrow f(-a) \in C \Longrightarrow f(a) \in C \Longleftrightarrow a \in f^{-1}(C)$.

(3) $a \in f^{-1}(H) \Longleftrightarrow f(a) \in H \Longrightarrow f(a) \in \neg C \Longleftrightarrow$

$\Longleftrightarrow \neg(f(a) \in C) \Longleftrightarrow \neg(a \in f^{-1}(C)) \Longleftrightarrow a \in \neg f^{-1}(C)$.

(4) Homomorfizam h se definira sa

$G/(f^{-1}(H),f^{-1}(C)) \ni a+f^{-1}(H) \longmapsto f(a)+H \in \mathrm{Im}(f)/(H,C)$.

Tada imamo

$a+f^{-1}(H) =_{G/f^{-1}(H)} b+f^{-1}(H) \Longleftrightarrow a-b \in f^{-1}(H) \Longleftrightarrow$

$\Longleftrightarrow f(a-b) \in H \Longleftrightarrow f(a)+H =_{\mathrm{Im}(f)/H} f(b)+H$.

$f(a)+H \neq_{\mathrm{Im}(f)/H} f(b)+H \Longleftrightarrow f(a)-f(b) \notin C \Longleftrightarrow$

$\Longleftrightarrow f(a-b) \notin C \Longleftrightarrow a-b \in f^{-1}(C) \Longleftrightarrow a+f^{-1}(H) \neq_{G/f^{-1}(H)} b+f^{-1}(H)$.

<u>Posljedica 11.1.</u> Neka je $(G,=_G,\neq_G,+)$ grupa i neka je (H,C) par podgrupa-kopodgrupa grupe G takve da je $H \subseteq \neg C$. Tada postoji bijektivna korespodencija između podgrupa grupe G koje sadrže podgrupu H i podgrupa grupe $G/(H,C)$ i postoji bijektivna korespodencija između kopodgrupa grupe G koje su sadržane u kopodgrupi C i kopodgrupa grupe $G/(H,C)$.

Dokaz:

(1) Neka je $\hat{S}$ podgrupa grupe $G/(H,C)$ i neka je $\hat{C}_1$ kopodgrupa grupe $G/(H,C)$ takve da je $\hat{S} \subseteq \neg\hat{C}_1$. Tada je (lako se provjerava)

(a) skup $S \equiv \{a \in G : a+H \in \hat{S}\}$ podgrupa grupe G takva da $H \subseteq S$;

(b) skup $C_1 \equiv \{a \in G : a+H \in \hat{C}_1\}$ kopodgrupa grupe G takva da vrijedi $C_1 \subseteq C$;

(c) $S \subseteq \neg C_1$.

(2) Neka je S podgrupa grupe G sa $S \supseteq H$ i neka je C_1 kopodgrupa grupe G sa $C_1 \subseteq C$ takve da je $S \subseteq \neg C_1$. Tada

(i) skup $\hat{S} \equiv \{a+H \in G/(H,C) : a \in S\}$ je podgrupa grupe

$G/(H,C)$.

(ii) Skup $\hat{C}_1 \doteq \{a+H \in G/(H,C) : a \in C_1\}$ je kopodgrupa grupe $G/(H,C)$.

(iii) $\hat{S} \subseteq \neg\hat{C}_1$.

Lema 12. Neka je $(G,=_G,\neq_G,+)$ grupa i neka su (H_1,C_1) i (H_2,C_2) dva para podgrupa - kopodgrupa grupa G takve da je $H_1 \subseteq \neg C_1$ i $H_2 \subseteq \neg C_2$ i $C_2 \cap H_1 \neq_{P_G} \emptyset$. Ako je H_2 podgrupa grupe H_1 , tada je $C_2 \cap H_1$ kopodgrupa grupe H_1 takva da je $H_2 \subseteq \neg(C_2 \cap H_1)$ (u odnosu na H_1).

Dokaz: Očigledno.

Teorem 13. Neka je $(G,=_G,\neq_G,+)$ grupa i neka su (H_1,C_1) i (H_2,C_2) dva para podgrupa - kopodgrupa grupe G takve da je $H_1 \subseteq \neg C_1$ i $H_2 \subseteq \neg C_2$ i $C_2 \cap H_1 \neq_{P_G} \emptyset$, i neka je H_2 podgrupa grupe H_1. Tada postoji jedinstveni izomorfizam

$$f: G/(H_1,C_1) \longrightarrow (G/(H_2,C_2))/(H_1/(H_2,H_1\cap C_2), C_1/(H_2,H_1\cap C_2)).$$

Dokaz:

(1) Prvo je potrebno definisati $C_1/(H_2,H_1\cap C_2)$ i pokazati da je to kopodgrupa grupe $G/(H_2,C_2)$ i da vrijedi

$$H_1/(H_2,H_1\cap C_2) \subseteq \neg(C_1/(H_2,H_1\cap C_2)).$$

Definišimo

$$C_1/(H_2,H_1\cap C_2) \doteq \{a+H_2 \in G/(H_2,C_2) : a \in C_1\}.$$

Lako se provjerava da je to kopodgrupa grupe $G/(H_2,C_2)$ i da ima traženu osobinu.

(2) Provjerimo da li su faktorske grupe dobro definisane.

i) U grupi $G/(H_1,C_1)$ imamo

$$a+H_1 =_1 b+H_1 \Longleftrightarrow a-b \in H_1,$$

$$a+H_1 \neq_1 b+H_1 \Longleftrightarrow a-b \in C_1,$$

$$(a+H_1)+_1(b+H_1) \doteq a+b+H_1 ;$$

ii) U grupi $G/(H_2,C_2)$ imamo

$$a+H_2 =_2 b+H_2 \Longleftrightarrow a-b \in H_2,$$

$$a+H_2 \neq_2 b+H_2 \Longleftrightarrow a-b \in C_2,$$

$$(a+H_2)+_2(b+H_2) \doteq a+b+H_2;$$

U grupi $(G/(H_2,C_2)/(H_1/(H_2,H_1\cap C_2),C_1/(H_2,H_1\cap C_2))$ imamo

$(a+H_2)+H_1/H_2 =_3 (b+H_2)+H_1/H_2 \iff (a+H_2)-(b+H_2)\in H_1/H_2$

$(a+H_2)+H_1/H_2 \neq_3 (b+H_2)+H_1/H_2 \iff (a+H_2)-(b+H_2)\in C_1/H_2,$

$(a+H_2)+H_1/H_2 +_3 (b+H_2)+H_1/H_2 \equiv (a+b+H_2)+H_1/H_2$.

(3) Preslikavanje f se definise sa

$$a+H_1 \longmapsto (a+H_2)+H_1/(H_2,H_1\cap C_2).$$

Imamo

$$a+H_1 =_1 b+H_1 \iff a-b\in H_1 \iff a-b+H_2\in H_1/H_2 \iff$$

$$\iff (a+H_2)-(b+H_2)\in H_1/H_2 \iff (a+H_2)+H_1/H_2 =_3 (b+H_2)+H_1/H_2,$$

$$(a+H_2)+H_1/H_2 \neq_3 (b+H_2)+H_1/H_2 \iff (a+H_2)-(b+H_2)\in C_1/H_2$$

$$\iff a-b+H_2\in C_1/H_2 \iff a-b\in C_1 \iff a+H_1 \neq_1 b+H_1 .$$

Lemma 14. Neka je $(G,=_G,\neq_G,+)$ grupa i neka su (H_1,C_1) i (H_2,C_2) dva para podgrupa - kopodgrupa grupe G takve da je $H_1\subseteq \neg C_1$ i $H_2\subseteq \neg C_2$. Tada je $H_1\cap H_2$ podgrupa a $C_1\cup C_2$ kopodgrupa grupe G takve da je $H_1\cap H_2\subseteq \neg(C_1\cup C_2)$.

Dokaz: (1) Jasno je da je $H_1\cap H_2$ podgrupa grupe G.

(2) $\neg(o\in C_1\cup C_2) \iff \neg(o\in C_1 \vee o\in C_2) \Longleftarrow$

$\Longleftarrow \neg(o\in C_1)\wedge\neg(o\in C_2)$;

$a+b\in C_1\cup C_2 \iff a+b\in C_1 \vee a+b\in C_2 \Longrightarrow$

$\Longrightarrow a\in C_1 \vee b\in C_1 \vee a\in C_2 \vee b\in C_2 \iff$

$\iff a\in C_1\cup C_2 \vee b\in C_1\cup C_2$;

$-a\in C_1\cup C_2 \iff -a\in C_1 \vee -a\in C_2 \longrightarrow a\in C_1 \vee a\in C_2$

$\iff a\in C_1\cup C_2$.

Teorem 15. Neka je $(G,=_G,\neq_G,+)$ grupa i neka su (H_1,C_1) i (H_2,C_2) dva para podgrupa - kopodgrupa grupe G takve da je $H_1\subseteq \neg C_1$ i $H_2\subseteq \neg C_2$. Tada postoji jedinstveni izomorfizam

$$f: H_1/(H_1\cap H_2, H_1\cap (C_1\cup C_2)) \longrightarrow (H_1+H_2)/(H_2,C_2\cap \neg(H_1+H_2)).$$

Dokaz:

(1) U grupi $H_1/(H_1\cap H_2, H_1\cap(C_1\cup C_2))$ imamo

i) $H_1\cap(C_1\cup C_2) =_{P_G} (H_1\cap C_1)\cup(H_1\cap C_2) =_{P_G}$

$$=_{P_G} H_1\cap C_2 ;$$

ii) Prema lemi 14. $C_1\cup C_2$ je kopodgrupa grupe G takva da $H_1\cap H_2\subseteq \mathcal{N}(C_1\cup C_2)$, a prema lemi 12. $H_1\cap(C_1\cup C_2)$ je kopodgrupa grupe H_1 takva da je $H_1\cap H_2\subseteq \mathcal{N}((C_1\cup C_2)\cap H_1)$ u H_1 .

iii) $a+H_1\cap H_2 =_1 b+H_1\cap H_2 \iff a-b\in H_1\cap H_2$;

$a+H_1\cap H_2 \neq_1 b+H_1\cap H_2 \iff a-b\in H_1\cap(C_1\cup C_2) =_{P_G}$

$$=_{P_G} H_1\cap C_2 ;$$

$(a+H_1)+_1(b+H_1) \equiv a+b+H_1$.

(2) U grupi $(H_1+H_2)/(H_2, C_2\cap(H_1+H_2))$ imamo $(a\in H_1, b\in H_2)$

$a+b+H_2 =_2 a'+b'+H_2 \iff (a+b+H_2)-(a'+b'+H_2)\in H_2 \iff$

$\iff a-a'+b-b'\in H_2 \iff a-a'\in H_2$;

$a+b+H_2 \neq_2 a'+b'+H_2 \iff (a+b+H_2)-(a'+b'+H_2)\notin C_2\cap H_1$

$\iff a-a'\in C_2\cap H_1$;

$(a+b+H_2)+_2(a'+b'+H_2) \equiv a+a'+b+b'+H_2 =_2 a+a'+H_2$.

(3) Preslikavanje f se definiše sa

$f: H_1/(H_1\cap H_2, H_1\cap(C_1\cup C_2)) \ni a+H_1\cap H_2 \longmapsto$

$\longmapsto a+x+H_2\in (H_1+H_2)/(H_2, C_2\cap(H_1+H_2))$,

gdje je x proizvoljno izabran element iz H_2. Imamo

$a+H_1\cap H_2 =_1 b+H_1\cap H_2 \longrightarrow a-b\in H_1\cap H_2\subseteq H_2 \iff$

$\iff a+H_2 =_2 b+H_2 \iff a+x+H_2 =_2 b+y+H_2$,

gdje su x i x proizvoljno izabrani elementi podgrupe H_2;

$a+b+H_2 \neq_2 a'+b'+H_2 \longrightarrow a+H_2 \neq_2 a'+H_2 \iff a-a'\in C_2\cap H_1$

$\iff a+H_1\cap H_2 \neq_1 a'+H_1\cap H_2$;

Dakle, preslikavanje f je funkcija. Ostaje da se provjeri da je izomorfizam:

a) f je injektivno: Izaberimo $a,a' \in H_1$ i $b,b' \in H_2$ po volji,

$a+b+H_2 =_2 a'+b'+H_2 \longrightarrow a+H_2 =_2 a'+H_2 \longrightarrow a-a' \in H_2 \wedge a-a' \in H_1 \Longrightarrow$

$\longrightarrow a-a' \in H_1 \cap H_2 \Longleftrightarrow a+H_1 \cap H_2 =_1 a'+H_1 \cap H_2$;

b) f je utapanje:

$a+H_1 \cap H_2 \neq_2 b+H_1 \cap H_2 \Longleftrightarrow a-b \in H_1 \cap C_2 =_G H_1 \cap (C_1 \cup C_2) \Longrightarrow$

$\longrightarrow a+H_2 \neq_2 b+H_2 \Longleftrightarrow a+x+H_2 \neq_2 b+y+H_2$,

gdje su x i y po volji izabrani elementi u podgrupi H_2.

c) f je sirjektivno: Za po volji izabran element $a+b+H_2 \in (H_1+H_2)/(H_2, C_2 \cap (H_1+H_2))$ možemo odrediti element $a+H_1 \cap H_2$ iz $H_1/(H_1 \cap H_2, H_1 \cap (C_1 \cup C_2))$ koji je original prvog elementa pri preslikavanju f. Sem toga ovo posljednje pridruživanje je funkcija jer je f funkcija i utapanje.

2.0.3. Prstenovi.

Definicija 9. Neka je $(A,=,\neq,+,.)$ prsten. Relacija ekvivalencije R_A na A naziva se relacija kongruencije na A akko vrijedi

$$(a,b) \in R_A \wedge (a',b') \in R_A \Longrightarrow (a+a',b+b') \in R_A,$$
$$(a,b) \in R_A \wedge (a',b') \in R_A \Longrightarrow (aa',bb') \in R_A$$

za svako $a,a',b,b' \in A$. Za relaciju C_A na A koja zadovoljava slijedeće uslove

$$(a,a) \notin C_A,$$
$$(a,b) \in C_A \Longrightarrow (b,a) \in C_A,$$
$$(a,c) \in C_A \Longrightarrow (a,b) \in C_A \vee (b,c) \in C_A,$$
$$(a+a',b+b') \in C_A \Longrightarrow (a,b) \in C_A \vee (a',b') \in C_A,$$
$$(aa',bb') \in C_A \Longrightarrow (a,b) \in C_A \vee (a',b') \in C_A,$$
$$(ab,o) \in C_A \Longrightarrow (a,o) \in C_A \wedge (b,o) \in C_A$$

za proizvoljno $a,a',b,b' \in A$ naziva se relacija kongruencije na A.

Definicija 10. Neka je $(A,=,\neq,+,\cdot)$ prsten a $(J,-,\neq,$ njegov podskup. Za J se kaže da je ideal prstena A akko vrijedi

$$0 \in J,$$
$$a \in J \wedge b \in J \Rightarrow a+b \in J,$$
$$a \in J \rightarrow -a \in J,$$
$$a \in J \vee b \in J \Rightarrow ab \in J.$$

Tvrdnja 16. Neka je $(A,=,\neq,+,\cdot)$ prsten a R_A relacija ekvivalencije na A. Tada je R_A relacija kongruencije na A tehva da je $R_A[0] =$ akko je skup $J \equiv \{a \in A:(a,0) \in R_A\}$ ideal prstena A i

$$(a,b) \in R_A \Leftrightarrow a-b \in J.$$

Dokaz: Provjeravanje se vrši kao u klasičnoj algebri.

Definicija 11. ([41]) Neka je $(A,=,\neq,+,\cdot)$ prsten i neka je $(C,=,\neq)$ njegov podskup. Za C se kaže da je koideal u A akko vrijedi

$$0 \notin C,$$
$$(\forall ab \in A)(a+b \in C \rightarrow a \in C \vee b \in C),$$
$$(\forall a \in A)(-a \in C \Leftrightarrow a \in C),$$
$$(\forall ab \in A)(ab \in C \Rightarrow a \in C \wedge b \in C).$$

Koideal C je slabo netrivijalan akko $\neg\neg(1 \in C)$. Koideal C je netrivijalan akko $1 \in C$. Koideal C se naziva prostim akko

$$1 \in C,$$
$$(P_3) \quad (\forall ab \in A)(a \in C \wedge b \in C \Rightarrow ab \in C).$$

Koideal C se naziva minimalnim u A akko

$$(\forall a \in A)(a \in C \rightarrow (\exists b \in A)\neg(ab-1 \in C)).$$

Lemma 17. Neka je $(A,=,\neq,+,\cdot)$ prsten. Tada vrijedi

$$(\forall ab \in A)(ab \neq 0 \Rightarrow a \neq 0 \wedge b \neq 0).$$

Dokaz: ([58], Propozicija 8.4.10.)

Napomena IX: Neka je $(A,=,\neq,+,\cdot)$ prsten. Tada je relacija jednakosti u A relacija kongruencije u A a skup $(0) \equiv \{a \in A:a = 0\}$ ideal prstena A. Dalje, relacija različitosti u A je relacija kokongruencije u A a skup $C_0 \equiv \{a \in A: : a \neq 0\}$ koideal u A.

Tvrdnja 18. Neka je $(A,=,\neq,+,.)$ prsten a C_A relacija na A. Tada je C_A relacija kokongruencije na A takva da je $\neq \propto C_A$ akko je $C = \{a \in A:(a,o) \in C_A\}$ koideal prstena A i

$$(a,b) \in C_A \iff a-b \in C.$$

Dokaz: (i) Neka je C_A relacija kokongruencije na A. Tada imamo

(1) $o \notin C$, jer $\neg (o,o) \notin C_A$.

(2) $-a \in C \iff (-a,o) \in C_A \iff (o-a,a-a) \in C_A \implies (a-a,o-a) \in C_A$
$\implies (a,o) \in C_A \vee (-a,-a) \in C_A \implies (a,o) \in C_A \iff a \in C.$

(3) $a+b \in C \iff (a+b,o) \in C_A \iff (a,o) \in C_A \vee (b,o) \in C_A \iff$
$\iff a \in C \vee b \in C.$

(4) $ab \in C \iff (ab,o) \in C_A \implies (a,o) \in C_A \wedge (b,o) \in C_A \iff$
$\iff a \in C \wedge b \in C.$

(ii) Neka je C koideal prstena A. Definišimo relaciju C_A na A na slijedeći način:

$$(\forall ab \in A)((a,b) \in C_A \iff a-b \in C).$$

Tada

(5) $(a,a) \notin C_A$ jer $\neg C \ni o = a-a$.

(6) $(a,b) \in C_A \iff a-b \in C \implies b-a \in C \iff (b,a) \in C_A$.

(7) $(a+a', b+b') \in C_A \iff a+a'-b-b' \in C \iff (a-b)+(a'-b') \in C$
$\implies a-b \in C \vee a'-b' \in C \iff (a,b) \in C_A \vee (a',b') \in C_A.$

(8) $(aa',bb') \in C_A \iff aa'-bb' \in C \iff aa'-ba'+ba'-bb' \in C \iff$
$\iff (a-b)a'+b(a'-b') \in C \implies (a-b)a' \in C \vee b(a'-b') \in C \implies$
$\implies (a-b \in C \wedge a' \in C) \vee (b \in C \wedge a'-b' \in C) \implies a-b \in C \vee a'-b' \in C$
$\iff (a,b) \in C_A \vee (a',b') \in C_A.$

(9) $(ab,o) \in C_A \iff ab \in C \implies a \in C \wedge b \in C \iff$
$\iff (a,o) \in C_A \wedge (b,o) \in C_A.$

Lema 19. Neka je $(A,=,\neq,+,.)$ prsten a C_A relacija kokongruencije na A. Tada je relacija $\neg C_A$ definisana na slijedeći način

$$(a,b) \in \neg C_A \iff \neg((a,b) \in C_A)$$

je relacija kongruencije na A takva da je $C_A = \cdot$.

Dokaz:

(1) $(a,a) \in \neg C_A$.

(2) $(a,b) \in \neg C_A \iff \neg((a,b) \in C_A) \iff \neg((b,a) \in C_A) \iff$
$\iff (b,a) \in \neg C_A$.

(3) $(a,b) \in \neg C_A \wedge (b,c) \in \neg C_A \iff$
$\iff \neg((a,b) \in C_A) \wedge \neg((b,c) \in C_A) \rightarrow \neg((a,b) \in C_A \vee (b,c) \in C_A)$
$\Rightarrow \neg((a,c) \in C_A) \iff (a,c) \in \neg C_A$.

(4) $(a,b) \in \neg C_A \wedge (a',b') \in \neg C_A \iff$
$\iff \neg((a,b) \in C_A) \wedge \neg((a',b') \in C_A) \rightarrow \neg((a,b) \in C_A \vee (a',b') \in C_A)$
$\Rightarrow \neg((a+a',b+b') \in C_A) \iff (a+a',b+b') \in \neg C_A$.

(5) $(a,b) \in \neg C_A \wedge (a',b') \in \neg C_A \iff$
$\iff \neg((a,b) \in C_A) \wedge \neg((a',b') \in C_A) \rightarrow$
$\rightarrow \neg((a,b) \in C_A \vee (a',b') \in C_A) \Rightarrow \neg((aa',bb') \in C_A) \iff$
$\iff (aa',bb') \in \neg C_A$.

Posljedica 19.1.([41], pp.26.) Neka je $(A,=,\neq,+,.)$ prsten i neka je C ko,ideal prstena A. Tada je skup $\neg C \equiv$
$\equiv \{a \in A : \neg(a \in C)\}$ ideal prstena A.

Posljedica 19.2. Neka je $(A,=_A,\neq_A,+,.)$ prsten. Tada je relacija $=_s$ definisana ovako

$$(\forall ab \in A)(a =_s b \iff \neg(a \neq_A b))$$

relacija kongruencije na A takva da je $=_s \propto =_A$.

Napomena X: Neka je $(A,=_A,\neq_A,+,.)$ prsten. Tada je skup $T \equiv \{a \in A : a =_s o\}$ ideal prstena A za koji vrijedi $(o) \subseteq T$.

Teorem 20. Neka je $(A,\neq_A,=_A,+,.)$ prsten a R_A relacija kongruencije na A takva da je $R_A \propto =_A$, a C_A relacija kokongruencije takva da je $\neq \propto C_A$ sa osobinom da je $\neg C_A \propto R_A$. Tada je $(A,=,\neq,+',.')$ prsten u kojem su relacija jednakosti i različitosti definisane sa

$$a = b \iff (a,b) \in R_A ,$$
$$a \neq b \iff (a,b) \in C_A ,$$

a operacija adicije i multiplikacije sa

$$a+'b \equiv a+b ,$$
$$a.'b \equiv ab.$$

Dokaz: Prema Propozicijama 16. i 18. relacijama kongruencije i kokongruencije odgovaraju ideal J i koideal C za koje vrijedi $J \subseteq \neg C$, a relacije jednakosti i različitosti su definisane sa

$$a = b \iff a-b \in J,$$
$$a \neq b \iff a-b \in C.$$

Lako se provjerava da su pri ovako shvaćenim relacijama elementi zapravo oblika $a+x$ $(x \in J)$ pri čemu je x proizvoljan element ideala J. Direktnim provjeravanjem se utvrđuje da je skup $(A,=,\neq)$ prsten u odnosu na operacije $+'$ i $.'$.

Napomena XI: Prsten $(A,=,\neq,+',.')$ definisan u prethodnoj teoremi se naziva faktorski prsten i obilježava se sa $A/(R_A,C_A)$. Ako su odgovarajući ideal i koideal J i C, tada se taktor prsten obilježava sa $A/(J,C)$. U ovom prstenu imamo

$$a+J = b+J \iff a-b \in J,$$
$$a+J \neq b+J \iff a-b \in C,$$
$$(a+J)+'(b+J) \equiv a+b+J,$$
$$(a+J).'(b+J) \equiv ab+J .$$

Definicija 12. Neka su $(A,=_A,\neq_A,+,.)$ i $(B,=_B,\neq_B,+',.')$ prstenovi. Totalna funkcija $f:A \longrightarrow B$ naziva se homomorfizam prstenova akko vrijedi

$$(\forall aa' \in A)(f(a+a') =_B f(a)+'f(a')),$$
$$(\forall aa' \in A)(f(aa') =_B f(a).'f(a')).$$

Homomorfizam $f:A \longrightarrow B$ naziva se bijektivnim akko je injektivan i sirjektivan. Homomorfizan f se naziva izomorfizam akko je bijektivno utapanje na.

Tvrdnja 21. Neka je $f:A \longrightarrow B$ homomorfizam prstenova. Tada je skup $Ker(f) \equiv \{ a \in A : f(a) =_B o \}$ ideal prstena A, a skup Im(f) podprsten prstena B. Ako prsten A ima jedi-

nicu 1 ($\neq_A o$), tada podprsten $Im(f)$ ima jedinicu $f(1)$ ili je $f =_{Hom(A,B)} O$ ili je $B =_{P_B} \{o\}$.

Dokaz:

$o \neq_A 1 \Rightarrow f(1) =_B o \vee f(1) \neq_B o$. Ako je $f(1) \neq_B o$, tada prsten $Im(f)$ ima jedinicu $f(1)$. Ako je $f(1) =_B o$, tada je $f =_{Hom(A,B)} O$ ili $B =_{P_B} \{o\}$.

Tvrdnja 22. Neka je $f:A \longrightarrow B$ homomorfizam prstenova. Tada je ideal $Ker(f)$ odlučiv u A akko je podprsten $Im(f)$ diskretan.

Dokaz: Kao kod propozicije 9.

Posljedica 22.1. Neka je $(A,=,\neq,+,.)$ prsten u J njegov ideal. Tada je prsten A/J diskretan akko je ideal J odlučiv u A.

Dokaz: Kao kod posljedice 9.1.

Posljedica 22.2. Prsten A je diskretan akko je ideal (o) odlučiv u A.

Teorem 23. Neka je $f:A \longrightarrow B$ homomorfizam prstenova. Tada postoji jedinstveni izomorfizam $h:A/Ker(f) \longrightarrow Im(f)$ taka da je $f =_{Hom(A,B)} h \cdot p$.

Dokaz: Dokaz kao u teoremi 10.

Definicija 13. Neka je $(A,=,\neq,+,.)$ prsten. Za prsten A se kaže da je

(1) prsten bez nula-djeljitelja akko

(I_1) $(\forall ab \in A)(ab = o \Longrightarrow a = o \vee b = o)$;

(2) balans (engleski: balanced, Ruitenburg,[36]) akko

(I_2) $(\forall ab \in A)(ab = o \wedge a \neq b \Longrightarrow b = o)$;

(3) slabo balans akko

$(\forall ab \in A)(ab = o \wedge \neg(a = o) \Longrightarrow b = o)$;

(4) integralni domen akko

(I_3) $(\forall ab \in A)(a \neq o \wedge b \neq o \Longrightarrow ab \neq o)$;

(5) slabi integralni domen akko

$(\forall ab \in A)(\neg(a = o) \wedge \neg(b = o) \longrightarrow \neg(ab = o))$.

Tvrdnja 24. Neka je $(A,=,\neq,+,.)$ prsten. Tada imamo

i) (1) $\Longrightarrow$ (2),(3),(5);

ii) (3) $\Longrightarrow$ (2);

iii) Ako je prsten a diskteran, tada su uslovi (1) - (5) međusobno ekvivalentni.

Definicija 14. Neka je $(A,=,\neq,+,.)$ prsten a J njegov ideal, a C koideal prstena A takvi da je $J \subseteq \neg C$. Za ideal J se kaže da je

(1) prost akko $1 \notin J$ i

(P_1) $\quad (\forall ab \in A)(ab \in J \Longrightarrow a \in J \vee b \in J)$;

(2) prost strogo balans ideal akko $1 \notin J$ i

$\quad (\forall ab \in A)(ab \in J \wedge b \notin J \Longrightarrow a \in J)$;

(3) prost balans ideal akko $1 \in C$ i

(P_2) $\quad (\forall ab \in A)(ab \in J \wedge b \in C \Longrightarrow a \in J)$;

(4) prost slabo balans ideal akko $\neg(1 \in J)$ i

$\quad (\forall ab \in A)(ab \in J \wedge \neg(b \in J) \Longrightarrow a \in J)$;

(5) prost strogo cio ideal akko $1 \notin J$ i

$\quad (\forall ab \in A)(a \notin J \wedge b \notin J \Longrightarrow ab \notin J)$;

(6) prost cio ideal akko (P_3);

(7) prost slabo cio ideal akko $\neg(1 \in J)$ i

$\quad (\forall ab \in A)(\neg(a \in J) \wedge \neg(b \in J) \Longrightarrow \neg(ab \in J))$.

Tvrdnja 24. Neka je $(A,=,\neq,+,.)$ prsten a J ideal a C koideal prstena takvi da je $J \subseteq \neg C$. Tada imamo

i) (1) $\Longrightarrow$ (2),(3),(4),(7);

ii) (4) $\Longrightarrow$ (2);

iii) Ako je ideal J odlučov u A tada su uslovi (1)-(7) međusobno ekvivalentni.

Tvrdnja 25. Neka je $(A,=_A,\neq_A,+,.)$ prsten a J i C ideal i koideal prstena A takvi da je $J \subseteq \neg C$. Tada imamo da je prsten $A/(J,C)$ koji zadovoljava uslov (P_i) $(i =_N 1,2,3)$ akko ideal J zadovoljava uslov (I_i) $(i =_N 1,2,3)$ respektivno.

Dokaz: Direktnim provjeravanjem.

Napomena XII: Neka je $(A,=,\neq,+,.)$ prsten a J i C ideal

i koideal prstena A takvi da je $J \subseteq \neg J$. Ovo povlači slijedi

$$(\forall a \in A)(a \in J \Longrightarrow \neg(a \in C)),$$

odakle slijedi da vrijedi

$$(\forall a \in A)(\neg\neg(a \in C) \Longrightarrow \neg(a \in J)),$$

odnosno

$$(\forall a \in A)(\neg\neg(a \in C) \Longrightarrow (\forall x \in J)\neg(a = x)).$$

Kako imamo $a \in C \Longrightarrow \neg\neg(a \in C)$, slijedi da vrijedi

$$(\forall a \in A)(a \in C \Longrightarrow (\forall a \in J)\neg(a = x)).$$

2.3.4. Polja.

Teorem 26. Neka je $(A, =_A, \neq_A, +, .)$ prsten sa jedinicom 1 $(\neq_A 0)$. Tada su slijedeći uslovi međusobno ekvivalentni:

(1) A je Ruitenburgovo polje.

(2) Ideal (o) je odlučiv u A i druga odlučiva ideala, osim ideala (o) i (1), nema u prstenu A.

(3) Svaki homomorfizam $f: A \longrightarrow B$, gdje je B diskretan prsten, je injektivan ili $f =_{Hom(A,B)} 0$ ili $B =_{P_B} \{o\}$.

Dokaz: (1) $\Longrightarrow$ (2). Neka je A Ruitenburgovo polje, tj. neka vrijedi $(\forall a \in A)(a =_A o \vee (\exists a' \in A)(aa' =_A 1))$. Tada je

$$(\forall a \in A)((a) =_{P_A} (o) \vee (a) =_{P_A} (1))$$

i

$$a \in A \Longrightarrow a =_A o \vee (\exists a' \in A)(aa' =_A 1) \to a =_A o \vee a \neq_A o$$

$$\Longrightarrow a \in (o) \vee \neg(a \in (o)).$$ Neka je J proizvoljan odlučiv ideal u A, tj. neka vrijedi $(\forall a \in A)(a \in J \vee \neg(a \in J))$. Ako $a \in J$, tada $a =_A o \vee (\exists a' \in A)(aa' =_A 1)$, tj. $J \subseteq (o)$ ili $1 \in J$.

(2) $\Longrightarrow$ (3). Neka je $f: A \longrightarrow B$ homomorfizam prstenova, gdje je B diskretan prsten. Tada je Ker(f) odlučiv ideal u A i, zato, vrijedi $Ker(f) =_{P_A} (o)$ ili $Ker(f) =_{P_A} (1)$, tj. f je injektivno ili $f =_{Hom(A,B)} 0$ ili $B =_{P_B} \{o\}$.

(3) $\Longrightarrow$ (1). Neka je svaki homomorfizam $f: A \longrightarrow B$ prstenova, gdje je B diskretan prsten, injektivan ili je $f =_{Hom(A,B)} 0$ ili je $B =_{P_B} \{o\}$. Izaberimo po volji izabran element $a \in A$. Tada za prirodni epimorfizam $p: A \longrightarrow A/((a), C_a)$, gdje je C_a koideal prstena A za koji vrijedi $(a) \subseteq \neg C_a$, imamo da je p injektivno ili $(a) =_{P_A} Ker(p) =_{P_A} (o)$ ili $p =_{Hom(A,A/(a))}$

$=_{Hom(A,A/(a))}$ 0 ili $A/(a) =_{P_{A/(a)}}$ (a). Kako je druga mogućnost nemoguća, to imamo $a =_A o$ ili $A =_{P_A}$ (a), tj. $1 \subset (a)$.

Napomena XIII: Napomenimo da je uslov da je prsten A polje ekvivalentan uslovu

$$(\forall a \in A)(a \in (o) \vee 1 \in (a)).$$

Napomena XIV: Ruitenburgovo polje ne treba shvatati kao polje u klasičnoj matematici jer, na primjer, klasična tvrdnja "Prsten A je polje akko nema drugih ideala osim (o) i (1)." ne vrijedi u bishopovskoj matematici jer, na primjer, za ideal $((a_n))$, generisan bježećim nizom $(a_n)_n$ (engleski: fugative sequence; 12) vrijedi $(o) \subseteq ((a_n)) \subseteq (1)$.

Propozicija 27. Neka je $(A,=,\neq,+,.)$ prsten. Tada su slijedeći uslovi ekvivalentni:

(1) A je Ruitenburgovo polje.

(2) A je diskretno Richmanovo polje.

Specijalno,

(a) $(F_1) \Longrightarrow (I_1)$,

(b) $(F_2) \Longrightarrow (I_3)$.

Dokaz: (1) $\Longleftrightarrow$ (2). Očigledno.

(a) $\wedge$ (b). ([15], Lema 2.1.)

Teorem 28. Neka je $(A,=_A,\neq_A,+,.)$ prsten sa jedinicom $1 (\neq_A o)$. Tada su slijedeći uslovi međusobno ekvivalentni:

(1) Prsten A je Richmanovo polje.

(2) $(\forall a \in A)(a \neq_A o \Longrightarrow 1 \in (a))$.

(3) Svaki homomorfizam $f:A \longrightarrow B$ prstenova je utapanje ili $f =_{Hom(A,B)} 0$ ili $B =_{P_B} \{o\}$.

Dokaz:

(1) $\Longleftrightarrow$ (2). Očigledno je da vrijedi

$$(\forall a \in A)(a \neq_A o \Longrightarrow (\exists a' \in A)(aa' =_A 1)) \Longleftrightarrow$$

$$\Longleftrightarrow (\forall a \in A)(a \neq_A o \Longrightarrow 1 \in (a)).$$

(1) $\Longrightarrow$ (3). Neka je prsten A richmanovo polje i neka

je $f:A \longrightarrow B$ homomorfizam prstenova. Tada

$$0 \neq_A 1 \Rightarrow f(1) =_B 0 \vee f(1) \neq_B 0 .$$

Ako je $f(1) =_B 0$, tada je $f =_{Hom(A,B)} 0$ ili $B =_{P_B} 0$. Ako je $f(1) \neq_B 0$, tada imamo

$$a \neq_A 0 \Rightarrow 0 \neq_B f(1) =_B f(aa') =_B f(a)f(a') \Rightarrow$$
$$\Rightarrow f(a) \neq_B 0.$$

(3) $\Longrightarrow$ (2). Neka je svaki homomorfizam $f:A \longrightarrow B$ prstenova utapanje ili $f =_{Hom(A,B)} 0$ ili $B =_{P_B} 0$. Uzmimo po volji izabran element $a(\neq_A)$ u prstenu A. Tada za prirodni epimorfizam $p:A \longrightarrow A/((a),C_a)$ imamo da je utapanje ili

$$p =_{Hom(A,A/((a),C_a))} 0$$

ili

$$A/((a),C_a) =_{P_{A/((a),C_a)}} (a).$$

Kako $p =_{Hom(A,A/((a),C_a))} 0$ i

$$0 \neq_A a \Rightarrow (\cdot) \neq_{A/((a),C_a)} a+(a)$$

nije moguće, to vrijedi $A =_{1_A} (a)$, odnosno $1 \in (a)$. Dakle,

$$0 \neq_A a \Longrightarrow 1 \in (a).$$

Posljedica 29.1.([41], Teorem 4.7.1.) Neka je $f:A \longrightarrow B$ homomorfizam gdje je A Richmanovo polje a B prsten sa jedinicom. Tada je homomorfizam f utapanje ili $f =_{Hom(A,B)} 0$.

Teorem 30. Neka je A prsten sa jedinicom a C koideal prstena A. Tada je prsten $A/(\neg C,C)$ Richmanovo polje akko je coideal C monimalan.

Dokaz:([56], Propozicija 8.4.14.)

Napomene XV: 1° U prethodnoj teoremi polje $A/(\neg C,C)$ ima jednu karakterističnu osobinu: Neka je $\bar{x}^n = \bar{0}$. Tada $\neg(x^n \in C)$. Predpostavimo da je $x \in C$. Tada bi bilo $x^n \in C$, što nije slučaj. Dakle, $\neg(x \in C)$, tj. $\bar{x} = \bar{0}$.

2° Fred Richman je konstruisao teoriju polja ([14], [10],[27],[30],[31]) na aksiomu (F_2) i aksiomu

(Rf) $\qquad (\forall a \in A)(\forall n \in N)(a^n = 0 \Longrightarrow a = 0)$

koji je posljedica aksiome (I_1). Uslov (..f) je potrebom jer, u opštem slučaju, relacija različitosti $\neq$ nije relacija odvojenosti u hejtingskom smislu. Potrebnost ovog aksioma može se vidjeti u teoremi 3.6. rada [14], a posebnu pažnju njegovoj potrebnosti u definiciji polja kome tarisko je kej Mines u svom članku [22].

Napomena XVI: Kao i u klasičnoj algebri moguće je konstruisati takozvano polje razlomaka na integralnom domenu. Neka je $(A,=_A,\neq_A,+,.)$ integralni domen a $S \equiv \{a \in A : a \neq_A o\}$. Na klasi $A \times S$ definišimo relacije

(x) $\quad (a,s) = (b,t) \iff (\exists u \in S)(u(at-bs) =_A o)$,

(xx) $\quad (a,s) \neq (b,t) \iff at \neq_A bs$.

Teorem 21. Neka je $(A,=_A,\neq_A,+,.)$ proizvoljan sa jedinicom $1(\neq_A o)$ koji je integralni domen. Tada je klasa $A \times S$ Kleinmanovo polje sa relacijom jednakosti i različitosti definisanim sa (x) i (xx) i sa operacijama adicije i multiplikacije definisane sa

$$(a,s)+'(b,t) = (at+bs,st),$$
$$(a,s).'(b,t) = (ab,st).$$

Dokaz: (1) Prvjerimo prvo da su relacije jednakosti i različitosti definisane sa (x) i (xx) korektno definisane. Imamo

(i) Jasno je da je relacija $=$ definisana sa (x) relacija ekvivalencije na klasi $A \times S$ - provjeravanje se vrši kao u klasičnoj algebri.

(ii) $\neg((a,s) \neq (a,s)) \iff \neg(as \neq_A as)$.

$$(a,s) \neq (b,t) \iff at \neq_A bs \implies bs \neq_A at \iff$$
$$\iff (b,t) \neq (a,s).$$

$$(a,s) = (b,t) \wedge (b,t) \neq (c,u) \iff$$
$$\iff (\exists w \in S)(w(at-bs) =_A o) \wedge bu \neq_A ct \implies$$
$$\implies atw =_A bsw \wedge bu \neq_A ct \implies atwu =_A bswu \wedge bswu \neq_A ctsw \implies$$
$$\implies atwu \neq_A ctsw \implies au \neq_A cs \iff (a,s) \neq (c,u).$$

(2) Provjerimo da su operacije adicije i multiplikacije definisane na gore opisani način korektno definisane.

$$(a,s)+'(b,t) \neq (a',s')+'(b',t') \Longleftrightarrow$$

$$\Longleftrightarrow (at+bs,st) \neq (a't'+b's',s't') \Longleftrightarrow$$

$$\Longleftrightarrow (at+bs)s't' \neq_A (a't'+b's')st \Longleftrightarrow$$

$$\Longleftrightarrow ats't'+bss't' \neq_A a't'st+b's'st \Longrightarrow$$

$$\Longrightarrow ats't' \neq_A a't'st \vee bss't' \neq_A b's'st \Longrightarrow$$

$$\Longrightarrow as' \neq_A a's \vee bt' \neq_A b't \Longleftrightarrow$$

$$\Longleftrightarrow (a,s) \neq_A (a',s') \vee (b,t) \neq (b',t');$$

$$(a,s).(b,t) \neq (a',s').'(b',t') \Longleftrightarrow$$

$$\Longleftrightarrow (ab,st) \neq (a'b',s't') \Longleftrightarrow abs't' \neq_A a'b'st \Longrightarrow$$

$$\Longrightarrow as' \neq_A a's \vee bs' \neq b's \Longleftrightarrow$$

$$\Longleftrightarrow (a,s) \neq (a',s') \vee (b,t) \neq (b',t').$$

$$(a,s).'(b,t) \neq (o,1) \Longrightarrow (ab,st) \neq (o,1) \Longleftrightarrow$$

$$\Longleftrightarrow ab \neq_A o \Longrightarrow a \neq_A o \wedge b \neq_A o \Longleftrightarrow a.1 \neq_A o.s \wedge s.1 \neq_A o.t$$

$$\Longleftrightarrow (a,s) \neq (o,1) \wedge (b,t) \neq (o,1).$$

(3) Direktnim provjeravanjem se utvrđuje da je $(A \times S,=,\neq,+',.')$ prsten sa jedinicom $(1,1)$ i nulom $(o,1)$. dalje, imamo

$$(a,s) \neq (o,1) \Longleftrightarrow a.1 \neq_A s.o \Longleftrightarrow a \neq_A o \Longleftrightarrow a \in S.$$

Dakle,

$$(\forall (a,s) \in A \times S)((a,s) \neq (o,1) \Longrightarrow (\exists (s,a))(s,s).'(s,a) = (1,1)).$$

Napomena XVII: U klasičnoj algebri imamo tvrdnju da je konačan integralni domen polje. U konstruktivnoj algebri imamo tvrdnju nešto strožiju od klasične:

Teorem 32. Neka je $(A,=,\neq,+,.)$ slabo konačan integralni domen. Tada je $(A,=_S,+,.)$ Ruitenburgovo polje.

Dokaz: ([41], Teorem 2.5.3.)

2.0.5. Moduli i vektorski prostori

Definicija 15. Neka su $(M,=_M,\neq_M,+)$ i $(S,=_S,\neq_S,+)$ moduli nad istim prstenom $(A,=_A,\neq_A,+,\cdot)$. Totalna funkcija $f:M \longrightarrow S$ naziva se <u>homomorfizam modula</u> akko vrijedi

$$(\forall mm' \in M)(f(m+m') =_S f(m)+f(m')),$$

$$(\forall a \in A)(\forall m \in M)(f(am) =_S af(m)).$$

Klasu svih homomorfizama modula M u modul S označavamo sa $\mathrm{Hom}(M,S)$, a u slučaju $M \equiv S$, pišemo $\mathrm{Hom}(M,S) \equiv \mathrm{End}(M)$. Elementi klase $\mathrm{End}(M)$ zovu se <u>endomorfizmi</u> modula M.

U slučaju kada su M i S vektorski prostori nad poljem A, homomorfizmi se nazivaju <u>linearni operatori</u> a endomorfizmi <u>linearne transformacije</u>.

Lema 33. Neka je $(M,=_M,\neq_M,+)$ vektorski prostor nad poljem $(A,=_A,\neq_A,+,\cdot)$. Tada vrijedi

(1) $(\forall a \in A)(\forall x \in M)(a \neq_A o \wedge x \neq_M o \Rightarrow ax \neq_M o)$,

(2) $(\forall a \in A)(\forall xy \in M)(a \neq_A o \wedge x \neq_M y \Rightarrow ax \neq_M ay)$,

(3) $(\forall ab \in A)(\forall x \in M)(a \neq_A b \wedge x \neq_M o \Rightarrow ax \neq_M bx)$.

Dokaz: ([56], Propozicija 8.4.3.)

Definicija 16. Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,\cdot)$ sa jedinicom $1(\neq_A o)$, a $(S,=_M,\neq_M)$ podskup A-modula M. Za S se kaže da je <u>A-podmodul</u> A-modula M akko

$$o \in S,$$
$$x \in S \wedge y \in S \Rightarrow x+y \in S,$$
$$a \in A \wedge x \in S \Rightarrow ax \in S.$$

U slučaju vektorskog prostora A-podmodul S se naziva vektorski <u>podprostor</u>.

Definicija 17. ([41], Definicija 2.7.1.) Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,\cdot)$, a $(C,=_M,\neq_M)$ neka je podskup A-modula M. Za C se kaže da je <u>A-kopodmodul</u> A-modula akko

$$o \notin C,$$
$$x+y \in C \Rightarrow x \in C \vee y \in C,$$
$$ax \in C \Rightarrow x \in C \wedge a \neq_A o.$$

Definicija 18. Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,\cdot)$.

a) Za relaciju kongruencije R_M na grupi M kaže se da je relacija kongruencije na A-modulu M akko vrijedi

$$(\forall a \in A)(\forall xy \in M)((x,y) \in R_M \Longrightarrow (ax,ay) \in R_M).$$

b) Za relaciju kokongruencije C_M na grupi M kaže se da je relacija kokongruencije na A-modulu M akko vrijedi

$$(\forall a \in A)(\forall x \in M)((ax,o) \in C_M \Longrightarrow a \neq_A o \vee (x,o) \in C_M).$$

Napomena XVIII: Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,\cdot)$. Tada je relacija "=" jednakosti na M relacija kongruencije na M a skup $(o) \equiv \{x \in M: x =_M o\}$ A-podmodul A-modula M. Dalje, relacija različitosti "$\neq$" na M je relacija kokongruencije na M a skup $C_o \equiv \{x \in M: x \neq_M o\}$ je kopodmodul A-modula M.

Tvrdnja 34. Neka je M A-modul a R_M relacija ekvivalencije na M. Tada je relacija R_M relacija kongruencije na A-modulu M akko je skup $S \equiv \{x \in M:(x,o) \in R_M\}$ A-podmodul A-modula M.

Dokaz: Direktnim provjeravanjem.

Tvrdnja 35. Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,\cdot)$, a C_M neka je relacija kokongruencije na grupi M. Tada je relacija C_M relacija kokongruencije na A-modulu M akko je skup $S \equiv \{x \in M:(x,o) \in C_M\}$ A-kopodmodul A-modula M i

$$(x,y) \in C_M \Longleftrightarrow x-y \in C.$$

Dokaz:(1) Neka je C A-kopodmodul A-modula M. Definirajmo relaciju C_M na M na slijedeći način:

$$(x,y) \in C_M \Longleftrightarrow x-y \in C.$$

Jasno je da je C_M relacija kokongruencije na M, prema propoziciji 5. Dalje, imamo

$$(ax,o) \in C_M \Longleftrightarrow ax \in C \Longrightarrow a \neq_A o \wedge x \in C \Longleftrightarrow$$

$$\Longleftrightarrow a \neq_A o \wedge (x,o) \in C_M .$$

(2) Neka je C_M relacija kokongruencije na A-modulu M.

Prema propoziciji 5. skup $C \equiv \{x \in M:(x,o) \in C_M\}$ je podgrupa grupe M. Dalje, imamo

$$ax \in C \iff (ax,o) \in C_M \Rightarrow a \neq_A o \wedge (x,o) \in C_M \iff$$

$$\iff a \neq_A o \wedge x \in C.$$

Napomena XIX: Relacija C_M ima još i sljedeću osobinu:

$$(ax,by) \in C_M \iff (ax-by,o) \in C_M \iff (ax-ay+ay-by,o) \in C_M$$

$$\Rightarrow (a(x-y),o) \in C_M \vee ((a-b)y,o) \in C_M \Rightarrow$$

$$\Rightarrow (a \neq_A o \wedge (x-y,o) \in C_M) \vee (a-b \neq_A o \wedge (y,o) \in C_M) \Rightarrow$$

$$\Rightarrow (x,y) \in C_M \vee a \neq_A b.$$

Lema 36. Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,.)$, a C_M neka je relacija kongruencije na M. Tada je relacija $\neg C_M$ definisana ovako

$$(x,y) \in \neg C_M \iff \neg((x,y) \in C_M)$$

relacija kongruencije na M takva da je $\neg C_M \prec =_M$.

Dokaz: Prema Lemi 6. relacija $\neg C_M$ je relacija kongruencijo na grupi M.

$$a \in A \wedge (x,y) \in \neg C_M \iff a \in A \wedge \neg((x,y) \in C_M) \Rightarrow$$

$$\Rightarrow \neg((ax,ay) \in C_M) \iff (ax,ay) \in \neg C_M.$$

Posljedica 36.1.([41], pp 35.) Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,.)$ a C A-kopodmodul A-modula M. Tada je skup $\neg C \equiv \{x \in M:\neg(x \in C)\}$ A-podmodul A-modula M.

Posljedica 36.2. Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq,+,.)$. Tada je relacija "$=_s$" na M definisana ovako

$$(\forall xy \in M)(x =_s y \iff \neg(x \neq_M y))$$

relacija kongruencije na A-modulu M takva da je $=_s \prec =_M$.

Napomena XX: Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq,+,.)$. Tada je skup $T \equiv \{x \in M:x =_s o\}$ A-podmodul A-modula M za koji vrijedi $(o) \subseteq T$.

Definicija 19. ([41],[56]) Neka je $(\ ,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,.)$ i neka $y,y_1,\ldots,y_m,x_1,\ldots,x_n \in M$ i $a_1,\ldots,a_n \in A$.

(1) $y_1,\ldots,y_m$ je zavisno od $x_1,\ldots,x_n$ akko za svako y_i $(1 \leq i \leq m)$ vrijedi

$$(\exists (a_{ij}) \in A^n)(y_i =_M \sum a_{ij}x_j);$$

(2) $y_1,\ldots,y_m$ i $x_1,\ldots,x_n$ su ekvivalentni akko su ta dva niza zavisna jedan od drugog;

(3) y je nezavisno od $x_1,\ldots,x_n$ akko vrijedi

$$(\forall (a_j)_j \in A^n)\ (y \neq_M \sum a_j x_j).$$

(4) y je slobodno od $x_1,\ldots,x_n$ akko

$$(\forall (a_j)_j \in A^n)(y \neq_M \sum a_j x_j);$$

(5) $x_1,\ldots,x_n$ su međusobno zavisni akko vrijedi

$$(\exists (a_j)_j \in A^n)((a_j)_j \neq (o)_j)(\sum a_j x_j =_M o);$$

(6) $x_1,\ldots,x_n$ su slabo međusobno zavisni akko vrijedi

$$(\exists (a_j)_j \in A^n)(\neg((a_j)_j = (o)_j))(\sum a_j x_j =_M o);$$

(7) $x_1,\ldots,x_n$ su međusobno nezavisni akko vrijedi

$$(\forall (a_j)_j \in A^n)(\sum a_j x_j =_M o \Longrightarrow (a_j)_j = (o)_j).$$

(8) $x_1,\ldots,x_n$ su međusobno slobodni akko vrijedi

$$(\forall (a_j)_j \in A^n)((a_j)_j \neq (o)_j)(\sum a_j x_j \neq_M o).$$

Napomena XXI: Tvrdnje koje se odnose na vektorske prostore nad poljem, a kojima ćemo se u daljem koristiti, mogu se naći u [14],[31],[41],[56].

Definicija 20.( ) Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,.)$ i neka su S i P [illegible] modula M.

(1) $M \equiv S \oplus P$ akko

i) $(\forall x \in M)(\exists y \in S)(\exists z \in P)(x =_M y+z)$,

ii) $(\forall y \in S)(\forall z \in S)(y \neq_M o \vee z \neq_M o \Longrightarrow y+z \neq_M o)$,

iii) $(\forall y \in S)(\forall z \in S)(y+z =_M o \Longrightarrow y =_M o \wedge z =_M o)$.

Napomene XXII:

1. Uslov (i) označava da se svaki element $a \in M$ može napisati u obliku sume $x =_M y+z$ $(y \in S \wedge z \in P)$, a uslov (ii) da je taj zapis jedinstven. Uslov (iii) znači

$$y \neq_M y' \wedge z \neq_M z' \Longrightarrow y+z \neq_M y'+z'.$$

2. Neka je $A = S \oplus P$, gdje su S i P A- podmoduli A-modula M. Tada se, na primjer, može uzeti da je

$$C_S = \{ x \in M : x \in P \wedge x \neq_M o \}.$$

Tada je C_S A-kopodmodul A-podmodula S takav da je $S \subseteq \neg C_S$:

$$o \notin C_S,$$

$$x+y \in C_S \Longleftrightarrow x+y \in P \wedge x+y \neq_M o \Longrightarrow x \neq_M o \vee y \neq_M o$$

$$\Longleftrightarrow x \in C_S \vee y \in C_S,$$

$$-x \in C_S \Longleftrightarrow -x \in P \wedge -x \neq_M o \Longrightarrow x \neq_M o \Longleftrightarrow x \in C_S,$$

$$ax \in C_S \Longleftrightarrow ax \in P \wedge ax \neq_M o \Longrightarrow x \in P \wedge x \neq o \wedge a \neq_A o$$

$$\Longrightarrow x \in C_S \wedge a \neq_A o,$$

$$y \in S \Longrightarrow \neg(y \in \ldots) \Longrightarrow \neg(y \in P \wedge y \neq_M o) \Longleftrightarrow y \in \neg C_S.$$

3. Neka je $M = S \oplus P$. Tada je $M/(S,\ldots)$ $\cong P$ pri čemu je za $x+S \equiv y+z+S$ $(y \in S \wedge z \in P)$ i $x'+S \equiv y'+z'+S$ $(y' \in S \wedge z' \in P)$

$$x+S =_{M/S} x'+S \Longleftrightarrow y+z+S =_{M/S} y'+z'+S \Longleftrightarrow$$

$$\Longleftrightarrow z =_M z',$$

$$x+S \neq_{M/S} x'+S \Longleftrightarrow y+z+S \neq_{M/S} y'+z'+S \Longleftrightarrow$$

$$\Longleftrightarrow z \neq_M z'.$$

[illegible]

[illegible]

Napomena XVIII: Neka je $(G,=_G,\neq_G)$ [illegible] $(G,=_G,\neq_G,+)$. Stavimo $H^* \equiv \{-a : a \in H\}$. Označimo sa $H^{\#}$ skup svih strikтno konačnih, konačnih i subkonačnih nizova iz elemenata skupa $H \cup H^*$:

$$x^{\#} \in H^{\#} \iff (\exists n_x \in \mathbb{N})(\exists f_x)(f_x : \overline{n}_x \rightarrowtail H \cup H^*),$$

$$x^{\#} \in H^{\#} \iff (\exists n_x \in \mathbb{N})(\exists f_x)(f_x : \overline{n}_x \rightarrow H \cup H^*),$$

$$x^{\#} \in H^{\#} \iff (\exists a \in H)(\exists \ldots)(\exists f_x)(f_x : \ldots \rightarrow H \cup H^*)$$

takvih da je

$$(\forall i)(f_x(i) \in H \cup H^*).$$

U skupu $H^{\#}$ definišimo [illegible] nastavljanje o kao nastavljanje nizova: ako su $x^{\#}$ i $y^{\#}$ [illegible] niza, tada je $x^{\#} \circ y^{\#}$ niz nastao nastavljanjem elemenata niza $y^{\#}$ počev iza elemenata niza $x^{\#}$. Jasno je:

(i) ako su oba niza strikтno konačna, tada je i niz nastao njihovim nastavljanjem takođe strikтno konačan;

(ii) ako je jedan niz strikтno konačan a drugi konačan ili subkonačan, tada je niz nastao njihovim nastavljanjem konačan ili subkonačan, respektivno;

(iii) ako su oba niza konačna tada je niz nastao njihovim nastavljanjem takođe konačan;

(iv) ako je jedan niz konačan a drugi subkonačan, tada je niz nastao njihovim nastavljanjem subkonačan;

(v) ako su oba niza subkonačan, tada je niz nastao njihovim nastavljanjem takođe subkonačan niz.

Tvrdnja 37. Neka je $(G,=_G,\neq_G,+)$ [illegible] $(G,=_G,\neq_G)$ njen podskup. Tada je klasa

$$[H] \equiv \{ \sum f_x(i) : x^{\#} \in H^{\#} \}$$

podgrupa grupe G.

Definicija 23. Neka je $(G,=_G,\neq_G,\ldots)$ [illegible] $(H,=_G,\neq_G)$ njen podskup.

(a) Ako je H striktno konačan skup, $H \neq \emptyset$ [illegible] konačan skup, i ako H^* sadrži samo [illegible] tada se za podgrupu $[H]$ kaže da je striktno konačno generisana podgrupa grupe G;

(b) Ako je H konačan skup a H^* [illegible] kaže da je konačno generisana podgrupa grupe G;

(c) Ako je H subkonačan skup, tada se za podgrupu $[H]$ kaže da je subkonačno generisana podgrupa grupe G.

U svakom od prethodna tri slučaja [illegible] da je generator podgrupe $[H]$.

Definicija 23. Neka je $(G,=_G,\neq_G,\cdot)$ [illegible]. U tom slučaju za podgrupu $[e] = \{e\}$ [illegible] podgrupa grupe G.

Tvrdnja 3. Neka je $(G,=_G,\neq_G,\cdot)$ [illegible] $a \in G$ i neka $[a]^*$ sadrži samo [illegible] grupu $[a]$ vrijedi

$$[a] = \{\ldots,-2a,-a,o,a,2a,\ldots\}$$

Za striktno konačnu grupu $[a]$ vrijedi

$$(\exists n \in N)([a] = \{o,a,2a,\ldots,(n-1)a\}\ .$$

Dokaz: Kao u klasičnoj matematici.

Definicija 25. Neka je $(G,=_G,\neq_G,\cdot)$ grupa. Za element a grupe G se kaže da ima konačan red ako

$$(\exists n \in N)(na =_G o).$$

Napomena XXIV: U klasičnoj algebri [illegible] podgrupa cikličke grupe je i sama ciklička grupa. [illegible] vrijedi u konstruktivnoj algebri.

Definicija 24. Neka su $(H,=_G,\neq_G,\ldots)$ i $(G,=_G,\neq_G,+)$ grupe grupe $(G,=_G,\neq_G,+)$ za koje vrijedi

$$(\forall a \in G)(\exists b \in H)(\exists c \in H)(a =_G [illegible]).$$

$$(\forall b \in L)(\forall c \in L)(b+c =_G o \Rightarrow b =_L \dots = o_G)$$

$$(\forall b \in H)(\forall c \in H)(b \neq_G o \vee c \neq_G o \Rightarrow b +_G c \neq_G o).$$

U tom slučaju za grupu G kažemo da je [illegible] podgrupe L i H i to pišemo u obliku $G = L \dots H$.

2.1.2. Slobodne abelove grupe.

Definicija 25.([56], pp 3.3.2.) Grupa $(G,=_G,\neq_G,+)$ naziva se slobodnom abelovom grupom ako postoji takav preslikavanje iz skupa generatora S u grupu G takvo da za svako preslikavanje f iz S u grupu $(G,=_G,\neq_G,+)$ postoji jedinstveni homomorfizam $g:F \longrightarrow G$ takav da je dijagram

komutativan.

Napomena XXV: Neka je $(G,=_G,\neq_G)$ [illegible] formirajmo klasu svih striktno konačnih nizova elemenata iz S:

$$x^* \in S^* \longleftrightarrow (\exists n_x \in N)(\exists f_x)(f_x:\bar{n}_x \longrightarrow x).$$

U klasu S^* uključićemo i prazan niz v. (U slučaju da je S prazan skup, ovaj niz je jedini član klase S^*) Ako su

$$x^* = (f_x(o),f_x(1),\dots,f_x(n_x)),$$

$$y^* = (f_y(o),f_y(1),\dots,f_y(n_y))$$

dva niza iz klase S^* definisaćemo

$$n_{xy} = n_x + n_y$$

i

$$i \in \bar{n}_x \Rightarrow f_{xy}(i) =_S f_x(i),$$

$$i =_N n_x+j \ (j \in \bar{n}_y) \Rightarrow f_{xy}(i) =_S f_y(j),$$

tj.

$$x^* \circ y^* = (f_x(o),\dots,f_x(n_x),f_y(o),f_y(1),\dots,f_y(n_y)).$$

Lema 39. Neka je $(S,=_S,\neq_S)$ skup. Relacija $=_1$ definisana na klasi s^* ovako

$$x^* =_1 y^* \iff n_x =_N n_y \wedge$$
$$\wedge (\forall i \in \bar{n}_x)(\exists j_i \in \bar{n}_y)(f_x(i) =_S f_y(j_i)) \wedge$$
$$\wedge (\forall j \in \bar{n}_y)(\exists i_j \in \bar{n}_x)(f_y(j) =_S f_x(i_j))$$

je relacija ekvivalencije i, prema tome, $(S^*, =_1)$ je skup.

Dokaz: Jasno je da vrijedi

$$x^* =_1 x^*$$

i

$$x^* =_1 y^* \Longrightarrow y^* =_1 x^* .$$

$$x^* =_1 y^* \wedge y^* =_1 z^* \iff n_x =_N n_y =_N n_z \ (=n) \wedge$$
$$\wedge (\forall i \in \bar{n})(\exists j_i \in \bar{n})(f_x(i) =_S f_y(j_i)) \wedge$$
$$\wedge (\forall j \in \bar{n})(\exists i_j \in \bar{n})(f_y(j) =_S f_x(i_j)) \wedge$$
$$\wedge (\forall j \in \bar{n})(\exists k_j \in \bar{n})(f_y(j) =_S f_z(k_j)) \wedge$$
$$\wedge (\forall k \in \bar{n})(\exists j_k \in \bar{n})(f_z(k) =_S f_y(j_k)) \Longrightarrow$$
$$\Longrightarrow n_x =_N n_z \wedge (\forall i \in \bar{n})(\exists k_{j_i} \in \bar{n})(f_x(i) =_S f_z(k_{j_i})) \wedge$$
$$\wedge (\forall k \in \bar{n})(\exists i_{j_k} \in \bar{n})(f_z(k) =_S f_x(i_{j_k})) \iff$$
$$\iff x^* =_1 z^* .$$

Lema 40. Relacija $\neq_1$ definisana u skupu $(S^*, =_1)$ na slijedeći način

$$x^* \neq_1 y^* \iff \neg(n_x =_N n_y) \vee ((n_x =_N n_y =_N n) \wedge$$
$$\wedge((\exists i \in \bar{n})(\forall j \in \bar{n})(f_x(i) \neq_S f_y(j)) \vee$$
$$\vee (\exists j \in \bar{n})(\forall i \in \bar{n})(f_y(j) \neq_S f_x(i)))$$

je relacija različitosti (u richmanskom smislu).

Dokaz: Jasno je da $\neg(x^* \neq_1 x^*)$, i

$$x^* \neq_1 y^* \Longrightarrow y^* \neq_1 x^* .$$

$$x^* =_1 y^* \wedge y^* \neq_1 z^* \iff$$
$$\iff (n_x =_N n_y \wedge (\forall i \in \bar{n}_x)(\exists j_i \in \bar{n}_y)(f_x(i) =_S f_y(j_i)) \wedge$$
$$\wedge (\forall j \in \bar{n}_y)(\exists i_j \in n_x)(f_y(j) =_S f_x(i_j))) \wedge$$

$$\wedge(\neg(n_y =_N n_z)\vee((n_y =_N n_z)\wedge((\exists j\in\bar{n})(\forall k\in\bar{n})(f_y(j)\neq_S f_z(k))\vee$$
$$\vee(\exists k\in\bar{n})(\forall j\in\bar{n})(f_z(k)\neq_S f_y(j)))))$$
$$\Longrightarrow \neg(n_n =_N n_z)\vee$$
$$\vee((n_x =_N n_z)\wedge(\exists i_j\in\bar{n}_z)(f_x(i_j)\neq_S f_z(k)) \Longrightarrow$$
$$\Longrightarrow x^* \neq_1 z^* .$$

Lema 41. Preslikavanje

$$S^*\times S^* \ni (x^*,y^*) \longmapsto x^*\circ y^*\in S^*$$

je unutrašnja binarna operacija.

Dokaz:

Neka su $(x^*,y^*),(a^*,b^*)\in S^*\times S^*$ proizvoljan par elemenata klase $S^*\times S^*$. Tada

(1) $x^* =_1 a^* \wedge y^* =_1 b^* \Longleftrightarrow$

$$\Longleftrightarrow n_x =_N n_a\ (=_N n)\wedge(\forall i\in\bar{n})(\exists r_i\in\bar{n})(f_x(i)=_S f_a(r_i))\wedge$$
$$\wedge(\forall r\in\bar{n})(\exists i_r\in\bar{n})(f_a(r)=_S f_x(i_r))$$
$$n_y =_N n_b\ (=_N m)\wedge(\forall j\in\bar{m})(\exists s_j\in\bar{m})(f_y(j)=_S f_b(s_j))\wedge$$
$$\wedge(\forall s\in\bar{m})(\exists j_s\in\bar{m})(f_b(s)=_S f_y(j_s))$$

Tada

$$n_x + n_y =_N n_a + n_b .$$

Ako $k\in\bar{n}_{x+y}$, tada $k\in\bar{n}_x \vee k =_N n_x+j\ (j\in\bar{n}_y)$. Ako $k\in\bar{n}_x$, tada $(\exists r_k\in\bar{n}_a)(f_x(k)=_S f_a(r_k))$. Ako $k=_N n_x+j\ (j\in\bar{n}_y)$, tada $(\exists s_j\in\bar{n}_b)(f_y(k)=_S f_b(s_j))$. Dakle,

$$(\forall k\in\bar{n}_{x+y})(\exists t\in\bar{n}_{a+b})(f_{xy}(k)=_S f_{ab}(t)).$$

Drugi dio relacije različitosti dokazuje se slično

$$(\forall t\in\bar{n}_{a+b})(\exists k\in\bar{n}_{x+y})(f_{ab}(t)=_S f_{xy}(k)).$$

Prema tome

$$x^*\circ y^* =_1 a^*\circ b^* .$$

(2) Neka je $x^*\circ y^*\neq_1 a^*\circ b^*$, tj. neka je

$$\neg(n_{xy}=_N n_{ab})\vee((n_{xy}=_N n_{ab})\wedge$$
$$\wedge((\exists k\in\bar{n}_{xy})(\forall t\ \bar{n}_{ab})(f_{xy}(k)\neq_S f_{ab}(t))\vee$$
$$\vee(\exists t\in\bar{n}_{ab})(\forall k\in\bar{n}_{xy})(f_{ab}(t)\neq_S f_{xy}(k)))).$$

(i) Ako je $\neg(n_{xy} =_N n_{ab})$, tj. $\neg(n_x+n_y =_N n_a+n_b)$, tada $\neg(n_x =_N n_a) \vee \neg(n_y =_N n_b)$, tj. $x^* \neq_1 a^*$ $y^* \neq_1 b^*$.

(ii) Neka je $n_{xy} =_N n_{ab}$, tj. $n_x+n_y =_N n_a+n_b$ i

$$(\exists k \in \bar{n}_x+\bar{n}_y)(\forall t \in \bar{n}_a+\bar{n}_b)(f_{xy}(k) \neq_S f_{ab}(t)) \vee$$

$$\vee (\exists t \in \bar{n}_a+\bar{n}_b)(\forall k \in \bar{n}_x+\bar{n}_y)(f_{ab}(t) \neq_S f_{xy}(k)).$$

Ako je $k \in \bar{n}_x$, $t \in \bar{n}_a$ tada $f_{xy}(k) =_S f_x(k)$ i $f_{ab}(t) =_S f_a(t)$ i

$$(\exists k \in \bar{n}_x)(\forall t \in \bar{n}_a)(f_x(k) \neq_S f_a(t)).$$

Ako je $k =_N n_x+j$ $(j \in \bar{n}_y)$, $t =_N n_a+s$ $(s \in \bar{n}_b)$, tada je $f_{xy}(k) =_S f_y(j)$ i $f_{ab}(t) =_S f_b(s)$ i

$$(\exists j \in \bar{n}_y)(\forall s \in \bar{n}_b)(f_y(j) \neq_S f_b(s)).$$

Prema tome,

$$x^* \circ y^* \neq_1 a^* \circ b^* \longrightarrow x^* \neq_1 a^* \vee y^* \neq_1 b^*.$$

<u>Teorem 42.</u> Struktura $(S^* \times S^*, =_2, \neq_2, +)$ je slobodna abelova grupa, gdje je

$$(x^*,y^*) =_2 (a^*,b^*) \Longleftrightarrow x^* \circ b^* =_1 a^* \circ y^*,$$

$$(x^*,y^*) \neq_2 (a^*,b^*) \Longleftrightarrow x^* \circ b^* \neq_1 a^* \circ y^*,$$

$$(x^*,y^*)+(a^*,b^*) =_2 (x^* \circ a^*, y^* \circ b^*).$$

Dokaz:

(1) Skup $(S^*, =_1, \neq_1, \circ)$ je slobodan abelov monoid nad generatorom $(S, =_S, \neq_S)$. Kako je

$$x^* \circ y^* =_1 y^* \circ x^*$$

operacija $\circ$ je komutativna. Nula-element u S^* je prazan niz v. Jednostavno se provjerava da je $(S^*, =_1, \neq_1, \circ)$ abelov monoid. Definišimo ulaganje $e: S \longrightarrow S^*$ sa

$$S \ni a \longmapsto e(a) \equiv (a) \in S^*.$$

Neka je $f: S \longrightarrow G$ funkcija iz skupa S u abelov monoid G. Definišimo preslikavanje $g': S^* \longrightarrow G$ na slijedeći način

$$g': S^* \ni x^* \equiv (f_x(o), \ldots, f_x(n_x)) \longmapsto \sum_{i=o}^{m_x} f(f_x(i))$$

$$v \longmapsto o.$$

Potrebno je dokazati da je preslikavanje g' funkcija. Neka je $x^* =_1 y^*$. Ako je $n_x =_N n_y =_N 1$, tada je sve jasno. Predpostavimo da je tvrdnja tačna za sve nizove sa $n_x =_N n_y =_N k$.

Neka je sada $n_x =_N n_y =_N k+1$ i

$$(\forall i \in \overline{k+1})(\exists j \in \overline{k+1})(f_x(i) =_S f_y(j))$$

$$(\forall j \in \overline{k+1})(\exists i \in \overline{k+1})(f_y(j) =_S f_x(i)),$$

specijalno

$$(\exists j_{k+1} \in \overline{k+1})(f_x(k+1) =_S f_y(j_{k+1}))$$

$$(\exists i_{k+1} \in \overline{k+1})(f_y(k+1) =_S f_x(i_{k+1})).$$

Prema hipotezi indukcije, imamo

$$\sum_{i=0}^{k}(f \cdot f_x)(i) =_G \sum_{j=0 (j \neq j_{k+1})}^{k+1}(f \cdot f_y)(j)$$

odnosno

$$\sum_{j=0}^{k}(f \cdot f_y)(j) =_G \sum_{i=0 (i \neq i_{k+1})}^{k+1}(f \cdot f_x)(i).$$

Dakle

$$\sum_{i=0}^{k+1}(f \cdot f_x)(i) =_G \sum_{j=0}^{k+1}(f \cdot f_y)(j)$$

što znači $g(x^*) =_G g'(y^*)$. Neka je $g'(x^*) \neq_G g'(y^*)$, tj.

$$\sum_{i}(f \cdot f_x)(i) \neq_G \sum_{j}(f \cdot f_y)(j).$$

Ak je $\neg(n_x =_N n_y)$, tada je $x^* \neq_1 y^*$. Neka je $n_x =_N n_y (=_N n)$, tj.

$$\sum_{i=0}^{n}(f \cdot f_x)(i) \neq_G \sum_{j=0}^{n}(f \cdot f_y)(j).$$

Tada

$$(\forall i \in \overline{n})(\bigvee_{j=0}^{n}(f(f_x(i)) \neq_G f(f_y(j))),$$

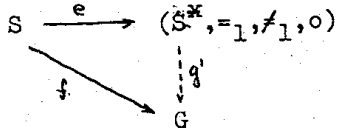
odnosno

$$(\forall i \in \overline{n})(\bigvee_{j=0}^{n}(f_x(i) \neq_S f_y(j)).$$

Dakle

$$x^* \neq_1 y^*.$$

Dijagram



je obavezno komutativan, zapravo g' je jedini homomorfizam monoida takav da je dijagram komutativan:

$$g'(x^* o y^*) =_G g'((f_{xy}(o),\ldots,f_{xy}(n_{xy}))) =_G$$

$$=_G g'((f_x(o),\ldots,f_x(n_x),f_y(o),\ldots,f_y(n_y))) =_G$$

$$=_G (f \cdot f_x)(o)+\ldots+(f \cdot f_x)(n_x) +$$

$$+ (f \cdot f_y)(o)+\ldots+(f \cdot f_y)(n_y) =_G$$

$$=_G g'(x^*) + g'(y^*).$$

(2) Konstruisaćemo grupu od monoida $(S^*,=_1,\neq_1,o)$ standardnim načinom, definišući na klasi $S^* \times S^*$ relaciju jednakosti i različitosti kako je to definisano tvrdnjom teoreme. Jednostavno se provjerava da su to korektne definicije i da je struktura $(S^* \times S^*,=_2,\neq_2,+)$ abelova grupa sa neutralnim elementom (v,v) i sa suprotnim elelemtom definisanim sa

$$-(a^*,b^*) =_2 (b^*,a^*).$$

Uložimo moncid $(S^*,=_1,\neq_1,o)$ u grupu $(S^* \times S^*,=_2,\neq_2,+)$ posredstvom preslikavanja

$$\mu : S^* \ni a^* \longmapsto (a^*,v) \in S^* \times S^* .$$

Neka je $g':(S^*,=_1,\neq_1,o) \longrightarrow (G,=_G,\neq_G,+)$ homomorfizam monoida S^* u abelovu grupu G. Definišimo preslikavanje $g:S^* \times S^* \longrightarrow G$ na slijedeći način

$$g:S^* \times S^* \ni (a^*,b^*) \longmapsto g'(a^*) - g'(b^*) \in G .$$

Provjerimo da je preslikavanje g homomorfizam takav da je dijagram

$$\begin{array}{ccc} (S^*,=_1,\neq_1,o) & \xrightarrow{\mu} & (S^* \times S^*,=_2,\neq_2,+) \\ & \searrow^{g'} & \downarrow g \\ & & G \end{array}$$

komutativan. Imamo

(i) $(a^*,b^*) =_2 (c^*,d^*) \iff a^* \circ d^* =_1 c^* \circ b^* \longrightarrow$

$$\longrightarrow g'(a^* \circ d^*) =_G g'(c^* \circ b^*) \iff$$

$$\iff g'(a^*)+g'(d^*) =_G g'(c^*)+g'(b^*) \iff$$

$$\iff g'(a^*)-g'(b^*) =_G g'(c^*)-g'(d^*) \iff$$

$$\iff g((a^*,b^*)) =_G g((c^*,d^*));$$

(ii) $g((a^*,b^*)) \neq_G g((c^*,d^*)) \iff$

$$\iff g'(a^*)-g'(b^*) \neq_G g'(c^*)-g'(d^*) \iff$$

$$\iff g'(a^*)+g'(d^*) \neq_G g'(c^*)+g'(b^*) \iff$$

$$\longleftarrow g'(a^*\circ d^*) \neq_G g'(b^*\circ c^*) \Longrightarrow$$

$$\Longrightarrow a^*\circ d^* \neq_1 c^*\circ b^* \Longleftrightarrow (a^*,b^*) \neq_2 (c^*,d^*);$$

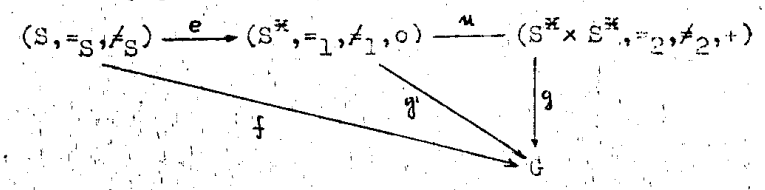
(iii) $g((a^*,b^*)+(c^*,d^*)) =_G g(a^*\circ d^*, c^*\circ b^*)) =_G$

$$=_G g'(a^*\circ d^*)-g'(c^*\circ b^*) =_G$$

$$=_G g'(a^*)+g'(d^*)-g'(c^*)-g'(b^*) =_G$$

$$=_G g((a^*,b^*))+g((c^*,d^*)).$$

Konačno, imamo dijagram



U ovom dijagramu, homomorfizam g' je jedinstveni homomorfizam monoida takav da je lijevi trougao u gornjem dijagramu komutativan. Dalje, homomorfizam g je jedinstveni homomorfizam takav da je desni trougao komutativan. Prema tome, homomorfizam g je jedinstveni homomorfizam takav da je veliki trougao komutativan. Dakle, struktura $(S^*\times S^*,=_2,\neq_2,+)$ je slobodna abelova grupa.

Napomene XXVI: 1. Neka je $S \equiv \{a,b\}$ gdje su a,b realni brojevi za koje nismo u mogućnosti da utvrdimo da li su jednaki ili različiti. Jasno je da se ne može definisati kanonsko preslikavanje $\{a,b\} \longrightarrow Z \oplus Z$, niti preslikavanje $\{a,b\} \longrightarrow Z$ takva da su odgovarajući dijagrami komutativni.

2. U gornjoj teoremi skup S se naziva generator slobodne abelove grupe.

Definicija 26. Neka je $(A_i)_i$ striktno izbrojiva klasa podgrupa grupe $(G,=_G,\neq_G,+)$ koje zadovoljavaju uslove

$$(\forall a \in G)(\exists k_a \in N)(\forall j \in \overline{k})(\exists b_{i_j} \in A_{i_j})(a =_G b_{i_1}+\ldots+b_{i_k}),$$

$$(\forall k \in N)(\ b_{i_1}+b_{i_2}+\ldots+b_{i_k} =_G o \longrightarrow \bigwedge_{j=1,k}(b_{i_j} =_G o)),$$

$$(\forall k \in N)(\bigvee_{j=1,k}(b_{i_j} \neq_G o) \Longrightarrow \sum_{j=1,k} b_{i_j} \neq_G o)$$

Tada se za grupu G kaže da je direktna suma svojih podgrupa i to pišemo na slijedeći način

$$G = \bigoplus_{i=0}^{\infty} A_i .$$

Napomena XXVII: Neka je direktna suma svojih podgrupa, a a i b neka su proizvoljan dva elementa iz grupe G, tj. neka

$$(\exists k_a \in N)(\forall j \in \bar{k}_a)(\exists b_{i_j} \in A_{i_j})(a =_G b_{i_1}+\ldots+b_{i_{k_a}})$$

$$(\exists k_b \in N)(\forall p \in \bar{k}_b)(\exists b_{s_p} \in A_{s_p})(b =_G b_{s_1}+\ldots+b_{s_{k_b}}).$$

Tada je

$$a =_G b \iff (k_a =_N k_b) \wedge (\forall j \in \bar{k}_a)(\exists p \in \bar{k}_b)(b_{i_j} =_G b_{s_p}) \wedge$$

$$\wedge (\forall p \in \bar{k}_b)(\exists j \in \bar{k}_a)(b_{s_p} =_G b_{i_j})$$

i

$$a \neq_G b \iff \neg(k_a =_N k_b) \vee$$

$$\vee ((k_a =_N k_b) \wedge ((\exists j \in \bar{k}_a)(\forall p \in \bar{k}_b)(b_{i_j} \neq_G b_{s_p}) \vee$$

$$\vee (\exists p \in \bar{k}_b)(\forall j \in \bar{k}_a)(b_{s_p} \neq_G b_{i_j}))).$$

Tvrdnja 43. Neka je skup $(S,=_S,\neq_S)$ striktno izbrojiv skup. Tada je slobodna abelova grupa generisana skupom S izomorfna sa direktnom sumom cikličkih grupa [t], $t \in S$.

Dokaz: Prema prethodnoj teoremi, funkcija

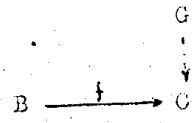
$$(S,=_S,\neq_S) \ni s \longmapsto s \in \bigoplus_{t \in S} [t]$$

može se na jedinstven način produžiti do homomorfizma

$$(S^* \times S^*,=_2,\neq_2,+) \longrightarrow \bigoplus_{t \in S} [t] .$$

Jednostavno se provjerava da je ovaj homomorfizam izomorfizam grupa.

Definicija 27. Grupu $(G,=_G,\neq_G,+)$ nazivamo projektivnom akko se svaki dijagram



gdje je f:B ⟶ C epimorfizam grupa, može nadopuniti do komutativnog dijagrama homomorfizmom h:G ⟶ B .

Tvrdnja 44. Neka je $(S,=_S,\neq_S)$ striktno izbrojiv skup. Tada je slobodna abelova grupa generisana skupom S projektivna.

Dokaz: Kao u klasičnom slučaju.

Napomene XXVIII: Neka je $(a_n)_n$ bježeći niz.

1. Neka je F slobodna abelova grupa generisana sa x i y, i neka je K podgrupa grupe F generisana skupom $(a_n(nx-y))_n$. Podgrupa K, očogledno, nije slobodna abelova grupa.

2. Neka su grupe F i K kao u primjeru 1. Tada je grupa G = F/K diskretna, ali nije slobodna abelova grupa, jer na primjer njena ciklička grupa generisana sa x nije odlučiva u G jer nismo u mogućnosti da odgovorima na pitanje da li je ili ne $y \in [x]$.

3. Neka je F slobodna abelova grupa generisana sa x, y i z, i neka je K njena podgrupa generisana sa $(a_n(nx+ny-z))_n$ Tada je grupa G = F/G je diskretna grupa. Podgrupe [x] i [y] su odlučive podgrupe grupe G, ali podgrupa [x,y] = [x] + [y] nije odlučiva podgrupa grupe G jer nismo u mogućnosti da utvrdimo da li ili ne $z \in [x,y]$.

4.Image homomorfizma diskretne grupe nemora biti odlučiva podgrupa: Neka je F slobodna abelova grupa generisana sa x i y, i neka je K njena podgrupa generisana skupom $(a_n(x-2ny))_n$. Tada je grupa G = F/K diskretna grupa, a multiplikacija brojem 2 je endomorfizam grupe G. Medutim, nismo u mogućnosti da utvrdimo da li je ili ne x slika nekog elementa pri tom homomorfizmu.

Napomene XXVIX: Prethodni primjeri nam govore slijedeće:

1. Drugi dio klasične McLaneove teoreme "Ako je grupa projektivna, tada je ona slobodna abelova grupa." u konstruk-

tivnoj algebri se ne može provesti.

2. Podgrupa slobodne abelove grupe ne mora biti slobodna abelova grupa.

3. U klasičnoj algebri imamo tvrdnju "Konačnogenerisana grupa je direktna suma konačnog broja cikličkih grupa." Kako je to pokazano primjerima u Napomeni XXVIII ova tvrdnja, u općem slučaju, ne vrijedi u konstruktivnoj algebri.

2.1.3. Djeljive grupe.

Definicija 28. Za grupu $(G,=_G,\neq_G,+)$ kazaćemo da je djeljiva akko vrijedi

$$(\forall n \in N)(nG = G).$$

Teorem 45. Neka je $(G,=,+)$ diskretna izbrojiva grupa i neka je D njena odlučiva djeljiva podgrupa. Tada možemo konstruisati izbrojivu podgrupu K grupe G takvu da je $G = K \oplus D$.

Dokaz: Teorem 9, [26].

Napomena XXX: ([26], pp.630) Direktno ili korištenjem teoreme 45. (Theorem 9, u [26]) može se dokazati klasični rezultat da je izbrojiva diskretna djeljiva grupa izomorfna direktnoj sumi grupa $Z(p^\infty)$ i grupa izomorfnih grupi Q.

Definicija 29. Grupu $(G,=_G,\neq_G,+)$ nazivamo injektivnom akko se svaki dijagram

gdje je $f:A \longrightarrow B$ injetivno utapanje, a $g:A \longrightarrow G$ homomorfizam može proširiti do komutativnog nekim homomorfizmom $h:B \longrightarrow G$.

Napomena XXXI: 1. Očigledno je da Baerov teorem u konstruktivnoj algebri nije moguće interpretirati, jer u konst-

ruktivnoj algebri Zornova lema nije legitimna.

2. Za sada se ne može ustanoviti veza između djeljivih grupa i injektivnih grupa.

2.2. PRSTENI I MODULI

2.2.1. Osnovne osobine.

Tvrdnja 46. Neka je $f:A \longrightarrow B$ homomorfizam prstenova i neka su $\bar{J}$ i $\bar{C}$ ideal i coideal podprstena $\mathrm{Im}(f)$ prstena B takvi da je $\bar{J} \subseteq \neg\bar{C}$. Tada

(1) Skup $J \equiv f^{-1}(\bar{J}) \equiv \{a \in A : f(a) \in \bar{J}\}$ je ideal prstena A takav da je $\mathrm{Ker}(f) \subseteq \bar{J}$.

(2) Skup $C \equiv f^{-1}(\bar{C}) \equiv \{a \in A : f(a) \in \bar{C}\}$ je koideal prstena A takav da je $f^{-1}(C) \subseteq C_f$.

(3) $f^{-1}(J) \subseteq \neg f^{-1}(C)$.

(4) Postoji jedinstveni izomorfizam

$$f:A/(f^{-1}(J), f^{-1}(C)) \longrightarrow \mathrm{Im}(f)/(\bar{J},\bar{C}).$$

Dokaz: Dokaz se izvodi ako kod teorema 11.

Posljedica 46.1. Neka je $(A, =_A, \neq_A, +, .)$ prsten i neka je (J,C) par ideal-koideal prstena A takav da je $J \subseteq \neg C$. Tada postoji bijektivna korespodencija između ideala prstena A koji sadrže ideal J i ideala prstena $A/(J,C)$, i postoji bijektivna korespodencija između koideala prstena A koji su sadržani u koidealu C i koideala prstena $A/(J,C)$.

Posljedica 46.2. Neka je $f:A \longrightarrow B$ homomorfizam prstenova i neka su J i C ideal i koideal prstena B takvi da je $J \subseteq \neg C$. Tada

(a) Ako je ideal J prost ideal, tada je ideal $f^{-1}(J)$ prost ideal prstena A;

(b) Ako je ideal J prost balans ideal prstena B, tada je $f^{-1}(J)$ prost balans ideal prstena A;

(c) Ako je J prost cio ideal prstena B, tada je $f^{-1}(J)$ prost cio ideal prstena A;

(d) Ako je f utapanje i J prost strogo balans ideal prstena B, tada je $f^{-1}(J)$ strogo balans ideal prstena A;

(e) Ako je f utapanje i J prost cio ideal prstena B, tada je $f^{-1}(J)$ strogo cio ideal prstena A;

(f) Ako je J prost slabo balans ideal prstena B, tada je $f^{-1}(J)$ prost slabo balans ideal prstena A;

(g) Ako je J prost slabo cio ideal prstena B, tada je $f^{-1}(J)$ prost slabo cio ideal prstena A.

Definicija 30. Neka je $(A,=_A,\neq_A,+,.)$ prsten a $(M,=_M,\neq_M,+)$ i $(P,=_P,\neq_P,+)$ A-moduli. Funkcija $f:M \longrightarrow P$ naziva se A-homomorfizam A-modula akko

$$(\forall xy \in M)(f(x+y) =_P f(x)+f(y)),$$

$$(\forall a \in A)(\forall x \in M)(f(ax) =_P af(x)).$$

Lema 47. Ako su $f:M \longrightarrow P$ i $g:P \longrightarrow S$ homomorfizmi A-modula , tada je i $g \cdot f:M \longrightarrow S$ homomorfizam A-modula.

Teorem 48. Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,.)$ a R_M relacija kongruencije na M sa $R_M \prec =_M$, i C_M relacija kokongruencije na M sa $\neq_M \prec C_M$, takve da je $\neg C_M \prec R_M$. Tada je $(M,=,\neq,+')$ modul nad prstenom A sa relacijom jednakosti i različitosti definisanom sa

$$x = y \iff (x,y) \in R_M,$$

$$x \neq y \iff (x,y) \in C_M$$

i operacijama adicije i vanskog množenja

$$x+'y = x+y,$$

$$a.'x = ax.$$

Dokaz: Jasno.

Napomene XXXII: A-modul $(M,=,\neq,+')$ definisan u prethodnoj teoremi naziva se faktorski modul i obilježava se sa $M/(R_M,C_M)$. Ako su H i C odgovarajući A-podmodul i A-kopodmodul A-modula M koji odgovaraju relacijama kongruencije R_M i kokongruencije C_M takvi da je $H \subseteq \neg C$, tada se grupa

A-modul $(M,=,\neq,+')$ obilježava sa $M/(H,C)$. U njemu imamo

$$x+H = y+H \Longleftrightarrow x-y \in H,$$
$$x+H \neq y+H \Longleftrightarrow x-y \in C,$$
$$(x+H)+'(y+H) \equiv x+y+H,$$
$$a.'(x+H) \equiv ax+H.$$

2. Prirodno preslikavanje $p:M \longrightarrow M/(H,C)$ definisano sa

$$p:M \ni x \longmapsto x+H \in M/(H,C)$$

je epimorfizam A-modula.

3. Ako je S A-podmodul A-modula $M/(H,C)$, tada je $p^{-1}(S)$ A-podmodul A-modula M koji sadrži A-podmodul H. Ako je C_S A--kopodmodul A-modula $M/(H,C)$, tada je $p^{-1}(C_S)$ A-kopodmodul A-modula M sadržan u A-kopodmodulu C. Ako vrijedi $S \subseteq \neg C_S$, tada vrijedi $p^{-1}(S) \subseteq \neg p^{-1}(C_S)$. Pridruživanja

$$S \longmapsto p^{-1}(S) \quad \text{i} \quad C_S \longmapsto p^{-1}(C_S)$$

su bijektivna korespodencije izmedu A-podmodula A-modula M koji sadrže A-podmodul H i A-podmodula A-modula $M/(H,C)$ i izmedu A-kopodmodula A-modula M koji su sadržani u A-kopodmodulu C i A-kopodmodula A-modula $M/(H,C)$.

4. Neka je $f:M \longrightarrow P$ A-homomorfizam A-modula. Tada je $\mathrm{Ker}(f)$ A-podmodul A-modula M, a C_f A-kopodmodul A-modula M. Sem toga, $\mathrm{Im}(f)$ je A-podmodul A-modula P.

Tvrdnja 49. Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,.)$ i neka su (H_1,C_1) i (H_2,C_2) dva para koji sadrže podmodule i kopodmodule A-modula M takvi da je $H_1 \subseteq \neg C_1$ i $H_2 \subseteq \neg C_2$ i $C_2 \cap H_1 \neq_P \emptyset$, i neka je H_2 podmodul od H_1. Tada postoji jedinstveni izomorfizam

$$f:M/(H_1,C_1) \longrightarrow (M/(H_2,C_2))/(H_1/(H_2,H_1 \cap C_2),C_1/(H_2,H_1 \cap C_2)).$$

Dokaz kao dokaz teoreme 13.-

Tvrdnja 50. Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,.)$ i neka su (H_1,C_1) i (H_2,C_2) dva para koji sadrže podmodule i kopodmodule A-modula M takve da je $H_1 \subseteq \neg C_1$ $H_2 \subseteq \neg C_2$. Tada postoji jedinstveni izomorfizam

$f:H_1/(H_1\cap H_2,H_1\cap(C_1\cup C_2)) \longrightarrow (H_1+H_2)/(H_2,C_2\cap(H_1+H_2))$.

Dokaz kao dokaz teorema 15.

Napomene XXXIII: 1. Neka je M A-modul a H_1 i H_2 podmoduli od M. Suma H_1+H_2 se definiše sa

$$H_1+H_2 \equiv \{x+y:x\in H_1 \wedge y\in H_2\}.$$

Jasno je da je H_1+H_2 podmodul od M. Ako su $H_1,\ldots,H_k$ podmoduli A-modula M, tada je skup

$$H_1+\ldots+H_k \equiv \{x_1+\ldots+x_k:x_i\in H_i \wedge i\in\{1,\ldots,k\}\}$$

podmodul A-modula M. Zovemo ga suma podmodula $H_1,\ldots,H_k$.

2. Neka je $(H_i)_{i\in I}$ neprazna klasa podmodula A-modula M. Za svaki striktno konačan skup J od I, skup

$$\sum_{i\in J} H_i$$

je podmodul od M. (U opštem, unija podmodula od M nije podmodul od M.) Skup

$$\bigcup_{J\subseteq I}\sum_{i\in J} H_i$$

je podmodul A-modula M. Nazivamo ga suma familije $(H_i)_{i\in I}$.

3. Neka je M A-modul i neka je $x\in M$. Tada je skup

$$Ax \equiv \{ax:a\in A\}$$

podmodul A-modula M. Pošto je A-modul unitaran, Ax sadrži x.

4. Neka je S neprazan podskup od M. Podmodul modula M generisan skupom S konstruiše se kao podgrupa iz propozicije 37. Jasno je da svijedi

$$[S] \equiv \sum_{x\in S} Ax .$$

Definicija 31. Neka je M A-modul. Ako se može naći striktno konačan podskup $\{x_1,\ldots,x_n\}$ od M takav da je

$$M = Ax_1+\ldots+Ax_n,$$

tada kažemo da je A-modul M striktno konačno generisan.

Tvrdnja 51. Neka je $(M,=_M,\neq_M,+)$ modul nad prstenom $(A,=_A,\neq_A,+,.)$. Ako je A-modul M striktno konačno generisan, tada se može odrediti $n\in N$ i podmodul H i kopodmodul C

takvi da je $H \subseteq \neg C$ i da je M izomorfno sa $A^n/(H,C)$.

Dokaz: Neka je $M = Ax_1+\ldots+Ax_n$, gdje je $S = \{x_1,\ldots,x_n\}$ striktno konačan podskup od M za koji vrijedi

$$(\forall i,j)(\neg(i =_N j))(x_i \neq_M x_j).$$

Definišimo preslikavanje $f:A^n \longrightarrow M$ na slijedeći način

$$A^n \ni (a_1,\ldots,a_n) \longmapsto \sum_{i=1}^{m} a_i x_i \in M.$$

Tada

(i) $(a_1,\ldots,a_n) = (b_1,\ldots,b_n) \Longleftrightarrow (\forall i)(a_i =_A b_i) \Longrightarrow$

$\Longrightarrow (\forall i)(a_i x_i =_M b_i x_i) \qquad \sum_{i=1}^{m} a_i x_i =_M \sum_{i=1}^{m} b_i x_i.$

(ii) $\sum_{i=1}^{m} a_i x_i \neq_M \sum_{i=1}^{m} b_i x_i \Longleftrightarrow \sum_{i=1}^{m} (a_i-b_i)x_i \neq_M o \longrightarrow$

$\longrightarrow \bigvee_{i=1}^{m} ((a_i-b_i)x_i \neq_M o) \Longrightarrow \bigvee_{i=1}^{m} (a_i-b_i \neq_A o \wedge x_i \neq_M o) \longrightarrow$

$\longrightarrow \bigvee_{i=1}^{m} (a_i \neq_A b_i) \Longleftrightarrow (a_1,\ldots,a_n) \neq (b_1,\ldots,b_n).$

(iii) Za proizvoljno $\sum_{i=1}^{m} a_i x_i \in M$ možemo uzeti $(a_1,\ldots,a_n) \in A^n$ pa da bude $f(a_1,\ldots,a_n) =_M \sum_{i=1}^{m} a_i x_i$.

Dakle, ako stavimo

$$\mathrm{Ker}f = \{(a_1,\ldots,a_n) \in A^n : \sum_{i=1}^{m} a_i x_i =_M o\},$$

$$C_f = \{(a_1,\ldots,a_n) \in A^n : \sum_{i=1}^{m} a_i x_i \neq_M o\}$$

imamo

$$M \cong A^n/(\mathrm{Ker}f, C_f).$$

Tvrdnja 52. Neka za A-modul M vrijedi

$$(\exists n \in N)(\exists H,C \subseteq A^n)(h:M \cong A^n/(H,C))$$

gdje je H podmodul a C kopodmodul A-modula A^n sa $H \subseteq \neg C$. Tada je A-modul subkonačno generisan.

Dokaz: Definišimo preslikavanje $f:A^n \longrightarrow M$ slaganjem prirodnog epimorfizma $p:A^n \longrightarrow A^n/(H,C)$ i izomorfizma h. Preslikavanje f je sirjektivni homomorfizam:

(i) $(a_1,\ldots,a_n) = (b_1,\ldots,b_n) \longrightarrow$

$\longrightarrow (a_1,\ldots,a_n)+H =_{A^n/H} (b_1,\ldots,b_n)+H \Longleftrightarrow$

$\Longleftrightarrow h((a_1,\ldots,a_n)+H) =_M h((b_1,\ldots,b_n)+H) \Longleftrightarrow$

$$\Longleftrightarrow f(a_1,\ldots,a_n) =_M f(b_1,\ldots,b_n).$$

(ii) $f(a_1,\ldots,a_n) \neq_M f(b_1,\ldots,b_n) \Longleftrightarrow$

$\Rightarrow (h.p)(a_1,\ldots,a_n) \neq_M (h.p)(b_1,\ldots,b_n) \Longleftrightarrow$

$\Rightarrow h((a_1,\ldots,a_n)+H) \neq_M h((b_1,\ldots,b_n)+H) \Longleftrightarrow$

$\Rightarrow (a_1,\ldots,a_n)+H \neq_{A^n/H} (b_1,\ldots,b_n)+H \Longleftrightarrow$

$\Rightarrow (a_1-b_1,\ldots,a_n-b_n) \in C \not\ni (o,\ldots,o) \Longrightarrow$

$\Rightarrow (a_1,\ldots,a_n) \neq_{A^n} (b_1,\ldots,b_n).$

(iii) Stavimo

$$L \equiv \{i \in \{1,\ldots,n\} : (\delta_{i1},\ldots,\delta_{in}) \in H\}.$$

Izmimo proizvoljno $x \in M$. Zbog izomorfizma h može se pronaći $a_1,\ldots,a_n)+H \in A^n/(H,C)$ takvo da je $h((a_1,\ldots,a_n)+H) =_M x$. Ako uvedemo oznake $(\delta_{i1},\ldots,\delta_{in}) = e_i$ $(i =_N 1,\ldots,n)$, tada

$$h(a_1e_1+\ldots+a_ne_n+H) =_M x,$$

odnosno

$$h(\sum a_ie_i+H) =_M x.$$

Dakle, skup $(f(e_i))_{i \in \overline{n,1}}$ generiše A-modul M.

Napomena XXXIV: Ako bi u prethodnoj propoziciji podmodul H bio odlučiv u odnosu na A^n, tada bi A-modul M bio (diskretan) konačno generisan.

2.2.2. Moduli sa konačnim brojem relacija.

Lema 53. Neka su $(M,=_M,\neq_M,+)$ i $(H,=_H,\neq_H,+)$ moduli nad prstenom $(A,=_A,\neq_A,+,.)$. Neka je $f:M \longrightarrow H$ utapajući homomorfizam i neka postoji utapajući homomorfizam $g:Imf \longrightarrow H$ takav da je $f \cdot g = Id_{Imf}$, tada je

$$M \cong Kerf \oplus Imf.$$

Dokaz: Definišimo preslikavanje $w:M \longrightarrow Kerf \oplus Imf$ na slijedeći način

$$w:M \ni x \longmapsto (x-g(f(x)),f(x)) \in Kerf \oplus Imf.$$

Provjerimo da je w izomorfizam:

a) Iz $f \cdot g = Id_{Imf}$ slijedi

$$(\forall x \in M)((f \cdot g)(f(x)) =_H f(x)),$$

odnosno

$$(\forall x \in M)(f(g(f(x))-x) =_H 0),$$

odakle zaključujemo da vrijedi

$$(\forall x \in M)(x-g(f(x)) \in \mathrm{Kerf}).$$

b) $x =_M x' \longrightarrow f(x) =_H f(x') \longrightarrow g(f(x)) =_M g(f(x')) \longrightarrow$

$\longrightarrow x-g(f(x)) =_M x'-g(f(x')) \longrightarrow$

$\longrightarrow (x-g(f(x)),f(x)) = (x'-g(f(x')),f(x'))$.

c) $(x-g(f(x)),f(x)) \neq (x'-g(f(x')),f(x')) \longrightarrow$

$\longrightarrow x-g(f(x)) \neq_M x'-g(f(x')) \vee f(x) \neq_H f(x') \longrightarrow$

$\longrightarrow x-x'+g(f(x'-x)) \neq_M 0 \vee x \neq_M x' \longrightarrow$

$\longrightarrow x-x' \neq_M 0 \vee g(f(x'-x)) \neq_M 0 \vee x \neq_M x' \longrightarrow x \neq_M x'$.

d) $(x-g(f(x)),f(x)) = (x'-g(f(x')),f(x')) \longrightarrow$

$\longrightarrow x-g(f(x)) =_M x'-g(f(x')) \wedge f(x) =_H f(x') \longrightarrow$

$\longrightarrow x-g(f(x)) =_M x'-g(f(x)) \longrightarrow x =_M x'$.

e) Neka je (x,y) proizvoljan element iz $\mathrm{Kerf} \oplus \mathrm{Imf}$, tj. $x \in \mathrm{Kerf} \wedge y \in \mathrm{Imf}$. Zato $(\exists x' \in M)(y =_H f(x'))$. Zbog jedinstvenosti prikaza elemenata sume je $x =_M x'-g(f(x'))$; dakle, W je sirjektivno.

Definicija 32. Za A-modul M se kaže da je modul sa konačnim brojem relacija akko se može naći utapajući homomorfizam f iz slobodnog A-modula konačnog ranga na M takav da je Kerf striktno konačno generisan.

Tvrdnja 54. Ako je $(M,=_M,\neq_M,+)$ modul sa konačnim brojem relacija nad prstenom $(A,=_A,\neq_A,+,.)$, tada je za svaki utapajući homomorfizam iz slobodnog A-modula konačnog ranga na M jezgro tog homomorfizma striktno konačno generisano.

Dokaz: Prema prethodnoj lemi imamo

$$A^n \cong \mathrm{Kerf} \oplus M,$$

gdje je $f:A^n \longrightarrow M$ utapajući homomorfizam. S druge strane je

$$A^m \cong \mathrm{Kerg} \oplus M,$$

gdje je $g:A^m \longrightarrow M$ utapajući homomorfizam.

a) Predpostavimo da je $n > m$. Tada imamo

$$\mathrm{Ker}f \oplus M \cong A^n \cong A^m \oplus A^{n-m} \cong \mathrm{Ker}g \oplus M \oplus A^{n-m},$$

odakle

$$\mathrm{Ker}f \cong \mathrm{Ker}g \oplus A^{n-m}.$$

Ako je Kerf striktno konačno generiasn A-podmodul A-modula A^n, tada je Kerg striktno konačno generisan A-podmodul A-modula A^m, budući da je direktni sumand u Kerf o A^{n-m} je striktno konačno generisan A-modul.

b) Predpostavimo da je $m > n$. Tada imamo

$$\mathrm{Ker}g \oplus M \cong A^m \cong A^n \oplus A^{m-n} \cong \mathrm{Ker}f \oplus M \oplus A^{m-n},$$

odakle

$$\mathrm{Ker}g \cong \mathrm{Ker}f \oplus A^{m-n}.$$

Ako je Kerf striktno konačno generisan, tada je i Kerg striktno konačno generisan jer je A^{m-n} striktno konačno generisan.

2.2.3. Egzaktni nizovi.

Definicija 33. Za niz

$$(+) \qquad \cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

A-modula M_i i A-homomorfizama f_i kaže se da je egzaktan na mjestu M_i akko je $\mathrm{Im}(f_i) =_{P_{M_i}} \mathrm{Ker}(f_{i+1})$. Za niz (+) se kaže da je egzaktan akko je egzaktan u svakoj svojoj tački M_i.

Lema 55. Neka su M', M i M" A-moduli.

a) Niz $(o) \longrightarrow M' \xrightarrow{f} M$ je egzaktan akko je f injektivno.

b) Niz $M \xrightarrow{g} M'' \longrightarrow (o)$ je egzaktan akko je g sirjektivno.

c) Niz $(o) \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow (o)$ je egzaktan akko je f injektivno a g sirjektivno i postoji izomorfizam

$$M/(\mathrm{Im}(f), C_g) \cong M''.$$

Dokaz: Tvrdnje su očigledne.

Tvrdnja 56. Neka su M', M i M" A-moduli i neka je niz

$$(o) \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow (o)$$

egzaktan. Ako su M' i M" striktno konačno generisani A-moduli, tada je A-modul M konačno generisan.

Dokaz: Neka je $S' \equiv \{x'_1,\dots,x'_n\}$ generator A-modula M', a $S'' \equiv \{x''_1,\dots,x''_m\}$ generator A-modula M". Zbog $\mathrm{Im}\, g = M''$ to

$$(\forall i \in \{1,\dots,m\})(\exists x_i \in M)(x''_i =_{M''} g(x_i)).$$

Sem toga,

$$(\forall ij)(x''_i \neq_{M''} x''_j) \longrightarrow (\forall ij)(g(x_i) \neq_{M''} g(x_j)) \longrightarrow$$

$$\longrightarrow (\forall ij)(x_i \neq_M x_j)$$

i

$$(\forall i)(x''_i \neq_{M''} o \longrightarrow x_i \notin \mathrm{Ker}\, g = \mathrm{Im}\, f).$$

S druge strane imamo

$$(\forall ij)(x'_i =_{M'} x'_j \longrightarrow f(x'_i) =_M f(x'_j))$$

i

$$(\forall ij)(x'_i \neq_{M'} x'_j \longrightarrow \neg(f(x'_i) =_M f(x'_j))).$$

Dakle, skup

$$S \equiv \{f(x'_1),\dots,f(x'_n),x_1,\dots,x_m\}$$

generiše A-modul M ali ne možemo ustanoviti da li je $kS = n+m$.

Posljedica 56.1. Neka je M A-modul a H njegov podmodul. Ako su A-moduli H i M/H striktno konačno generisani , tada je takav i A-modul M.

Dokaz: Imamo egzaktan niz

$$(o) \longrightarrow H \xrightarrow{\iota} M \xrightarrow{p} M/H \longrightarrow (o)$$

gdje je ι ulaganje (dakle, ι je utapanje i injektivno) a p prirodni epimorfizam.

Tvrdnja 57. Za svaki striktno konačno generisan A-modul sa konačnim brojem relacija može se konstruisati egzaktan niz

$$L_1 \longrightarrow L_o \longrightarrow M \longrightarrow (o)$$

A-modula, gdje su L_1 i L_o slobodni A-moduli.

Dokaz: Prema propoziciji 51. imamo

$$(\exists n \in N)(\exists H,C \leq A^n)(M \cong A^n/(H,C)),$$

gdje je H striktno konačno generisan A-modul. Zato

$$(\exists\, n \in \mathbb{N})(\exists H_1, C_1 \subseteq A^n)(H \cong A^n/(H_1, C_1)).$$

Formirajmo epimorfizam $f: A^n \longrightarrow M$ slaganjem prirodnog epimorfizma $A^n \longrightarrow A^n/(H,C)$ i izomorfizma $A^n/(H,C) \cong M$ i homomorfizam $g: A^m \longrightarrow H$ slaganjem prirodnog epimorfizma $A^m \longrightarrow A^m/(H_1, C_1)$ i izomorfizma $A^m/(H_1, C_1) \cong H$. Posljednji homomorfizam možemo shvatiti kao homomorfizam sa A^m u A^n. Prema tome, konstruisali smo niz

$$(++) \qquad A^m \xrightarrow{g} A^n \xrightarrow{f} M \longrightarrow (o)$$

za koji vrijedi

$$\mathrm{Img} \cong A^m/(H_1, C_1) \cong H = \mathrm{Ker}f$$

pri čemu je f sirjektivno. Dakle, niz (++) je egzaktan.

Definicija 34. Reprezentacijom (dužine 1) A-modula M naziva se egzaktni niz

$$(") \qquad L_1 \longrightarrow L_o \longrightarrow M \longrightarrow (o)$$

A-modula u kojem su L_1 i L_o slobodni A-moduli. Za reprezentaciju (") A-modula M se kaže da je striktno konačna akko slobodni moduli L_1 i L_o su striktno konačno generisani.

Napomene XXXV: Prema propoziciji 57. svaki striktno konačno generisan A-modul sa konačnim brojem relacija ima striktno konačnu reprezentaciju.

Neka A-modul M ima striktno konačnu reprezentaciju, tj. neka je niz

$$L_1 \xrightarrow{g} L_o \xrightarrow{f} M \longrightarrow (o)$$

egzaktan gdje su L_1 i L_o striktno konačno generisani slobodni A-moduli. Tada je Kerf subkonačno generisan, a $M \cong L_o/(\mathrm{Ker}f, C_f)$ dakle, prema propoziciji 52, subkonačno generisan.

2.2.4. Slučaj diskretnih modula.

Tvrdnja 58. (Posljedica 51.1. i 52.1.) Neka je M diskretan A-modul. M je konačno generisan akko se može naći $n \in \mathbb{N}$ i podmodul H modula A^n takvi da je M izomorfno sa A^n/H.

Dokaz: U propoziciji 51. podmodul Kerf je odlučiv u

A^n , a u propoziciji 52. u predpostavci tvrdnje mora se predpostaviti da je podmodul H odlučiv u A^n jer je modul M diskretan. Zato je, prema napomeni XXXIV, A-modul M konačno generisan.

Tvrdnja 59. Neka su M i H diskretni moduli nad diskretnim prstenom A i neka je $f:M \longrightarrow H$ homomorfizam takav da postoji homomorfizam $g:Imf \longrightarrow M$ takav da je $f \cdot g = id_{Imf}$. Tada je

$$M \cong Kerf \oplus Imf.$$

Dokaz: ([41], pp. 63 - 64.)

Tvrdnja 60. Neka je M diskretan A-modul. Ako je M modul sa konačnim brojem relacija tada je za svaki homomorfizam iz slobodnog A-modula konačnog ranga na M jezgro tog homomorfizma konačno generisano.

Dokaz: ([27], Lemma 1.)

Tvrdnja 61. Neka su M', M i M" diskretni A-moduli i neka je niz

$$(0) \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow (0)$$

egzaktan. Ako su M'i M" konačno generisani moduli, tada je i M konačno generisan modul.

Dokaz: Prema propoziciji 56. skup generatora S modula M je konačan jer je Kerf odlučiv podmodul A-modula M'.

2.2.5. Uslovi lanaca podmodula.

Definicija 35. Neka je $(A,=_A,\neq_A,+,\cdot)$ prsten a $(M,=_M,\neq_M,+)$ A-modul.

(1) Rastućim nizom podmodula A-modula M nazivamo niz $((H_i,C_i))_i$ podmodula i kopodmodula modula M za koje vrijedi

$$(\forall i)(H_i \subseteq \neg C_i),$$

(+) $$H_1 \subseteq H_2 \subseteq H_3 \subseteq \ldots$$

$$C_1 \supseteq C_2 \supseteq C_3 \supseteq \ldots$$

(2) Opadajućim nizom podmodula A-modula M nazivamo niz $((H_i,C_i))_i$ podmodula i kopodmodula A-modula M za koje vrijedi

$$(\forall j)(H_j \subseteq \neg C_j),$$

$$(2) \qquad H_1 \supseteq H_2 \supseteq H_3 \quad \ldots$$

$$C_1 \subseteq C_2 \subseteq C_3 \quad \ldots$$

(3) Za rastući niz (1) se kaže da je stacionaran akko

$$(\exists n \in \mathbb{N})(\forall i)(H_n = H_{n+i} \wedge C_n = C_{n+i}).$$

(4) Za opadajući niz (2) se kaže da je stacionaran akko

$$(\exists n \in \mathbb{N})(\forall i)(H_n = H_{n+i} \wedge C_n = C_{n+i}).$$

Napomene XXXVI: 1° Uslov stacionarnosti rastućih nizova za podmodula A-modula M nije ekvivalentan uslovu da je svaki podmodul A-modula M konačno generisan (čak ni u slučaju diskretnim A-modula ([27], pp.436.)).

2° J.B.Tennenbaum je u svojoj disertaciji "A constructive version of Hilbert's basic theorem", University of California, San Diego, California 1973. uveo uslov:

"Postoji operator q na A-modulu M koji djeluje na konačne nizove elemenata iz M takav da je $q(x_1,\ldots,x_n)-x_n$, gdje $x_1,\ldots,x_n \in M$, je u podmodulu generisanom sa $x_1,\ldots,x_{n-1}$ i za svaki niz $(x_i)_i$ može da se odredi $n \in \mathbb{N}$ takvo da je $q(x_1,\ldots,x_n) =_M 0$."

koji generalizuje oba slučaja koja, u klasičnoj matematici, definišu Noetherine module.

U slučaju da su u modulu M konačno generisani podmoduli odlučivi u M, tada uslov (T) ima oblik:

"Za svaki niz $(x_i)_i$ elemenata iz modula M može da se odredi $n \in \mathbb{N}$ takav da je x_n u podmodulu generisanom sa $x_1,\ldots,x_{n-1}$. Zapravo klasa $q(x_1,\ldots,x_{n-1})$ je jednako 0 ili x_n u zavisnosti od toga da li je x_n u podmodulu generisanom sa $x_1,\ldots,x_{n-1}$ ili ne.

Lema 62. Neka je $f:L \longrightarrow M$ injektivno utapanje A-modula i neka su H i C podmodul i kopodmodul A-modula L takvi da je $H \subseteq \neg C$. Tada su f(H) i f(C) podmodul i kopodmodul A-modula M takvi da je $f(H) \subseteq \neg f(C)$.

Dokaz: (1) Jasno je da je $f(C)$ podmodul A-modula M.

(2) Dokažimo da je $f(C)$ kopodmodul A-modula M:

(i) $o \# C \longleftrightarrow (\forall c \in C)(o \neq_L c) \Longrightarrow (\forall c \in C)(o \neq_M f(c)) \longleftrightarrow$

$\longleftrightarrow o \# f(C)$.

(ii) $-x \in f(C) \Longleftrightarrow (\exists y \in C)(-x =_M f(y)) \longleftrightarrow$

$\longleftrightarrow (\exists (-(-y)) \in C)(x =_M f(-y)) \longrightarrow (\exists (-y) \in C)(x =_M f(-y)) \longleftrightarrow$

$\longleftrightarrow x \in f(C)$.

(iii) $x'+x'' \in f(C) \longleftrightarrow f^{-1}(x'+x'') \in C \longleftrightarrow f^{-1}(x')+f^{-1}(x'') \in C$

$\Longrightarrow f^{-1}(x') \in C \vee f^{-1}(x'') \in C \longleftrightarrow x' \in f(C) \vee x'' \in f(C)$.

(iv) $ax \in f(C) \Longleftrightarrow f^{-1}(ax) \in C \longleftrightarrow af^{-1}(x) \in C \longrightarrow$

$\Longrightarrow a \neq_A o \wedge f^{-1}(x) \in C \longleftrightarrow a \neq_A o \wedge x \in f(C)$.

(v) $x \in f(H) \Longleftrightarrow (\exists y \in H)(x =_M f(y)) \Longleftrightarrow$

$(\exists y \in H \subseteq \neg C)(x =_M f(y))$.

Predpostavimo da je $x \in f(C)$. Tada bi bilo $(\exists y' \in C)(x =_M f(y'))$. Dakle, $f(y) =_M f(y')$, odakle $y =_L y'$ što je nemoguće. Dakle, $\neg(x \in f(C))$.

<u>Teorem 63.</u> Neka je $(o) \longrightarrow L \xrightarrow{f} M \xrightarrow{g} H \longrightarrow (o)$ egzaktan niz A-modula, gdje je f utapanje a g homomorfizam na. Ako A-modul zadovoljava uslov stacionarnosti za rastuće nizove podmodula, tada su takvi i moduli L i H.

Dokaz:

(1) Neka je $L_1 \subseteq L_2 \subseteq \ldots$ rastući niz podmodula A-modula L i $C_1 \supseteq C_2 \supseteq \ldots$ opadajući niz kopodmodula A-modula L. Tada su $f(L_1) \subseteq f(L_2) \subseteq \ldots$ rastući niz podmodula A-modula M i $f(C_1) \supseteq f(C_2) \supseteq \ldots$ opadajući niz kopodmodula A-modula M. Zato

$$(\exists n \in \mathbb{N})(\forall i)(f(L_n) = f(L_{n+i}) \wedge f(C_n) = f(C_{n+i})).$$

Dokažimo da vrijedi

$$(\forall i)(L_n = L_{n+i} \wedge C_n = C_{n+i}):$$

$$y \in L_{n+i} \rightarrow f(y) \in f(L_{n+i}) = f(L_n) \Longrightarrow$$

$$\Longrightarrow (\exists y' \in L_n)(f(y) =_M f(y')) \Longrightarrow y =_L y' \in L_n.$$

$$y \in C_n \rightarrow f(y) \in f(C_n) = f(C_{n+i}) \Longrightarrow$$

$$\rightarrow (\exists y' \in C_{n+1})(f(y) =_M f(y')) \rightarrow y =_H y' \in C_{n+1}.$$

(2) Neka je $H_1 \subseteq H_2 \subseteq \ldots$ rastući niz podmodula A-modula M a $C_1 \supseteq C_2 \supseteq \ldots$ opadajući niz kopodmodula A-modula M takvi da je $(\forall i)(h_i \subseteq \neg C_i)$. Zbog toga što je g homomorfizam na, postoji homomorfizam $g' : M \rightarrow M$ takav da je $g \cdot g' = 1_M$. Sem toga homomorfizam g' je injektivan i utapanje. Zato je $g'(H_1) \subseteq g'(H_2) \subseteq \ldots$ rastući niz podmodula A-modula M a $g'(C_1) \supseteq g'(C_2) \supseteq \ldots$ opadajući niz kopodmodula A-modula M takvi da je $(\forall i)(g'(H_i) \subseteq \neg g'(C_i))$. Zato

$$(\exists m \in N)(\forall j)(g'(H_m) = g'(H_{m+j}) \wedge g'(C_m) = g'(C_{m+j})).$$

Dokažimo da vrijedi $(\forall j)(H_m = H_{m+j} \wedge C_m = C_{m+j})$.

$$z \in H_{m+j} \rightarrow g'(z) \in g'(H_{m+j}) = g'(H_m) \rightarrow$$

$$\rightarrow (\exists z' \in H_m)(g'(z) =_M g'(z')) \rightarrow z =_H z' \in H_m.$$

$$z \in C_m \rightarrow g'(z) \in g'(C_m) = g'(C_{m+j}) \rightarrow$$

$$\rightarrow (\exists z' \in C_{m+j})(g'(z) =_M g'(z')) \rightarrow z =_H z' \in C_{m+j}.$$

Napomena XXXVII: Dokaz obrnutog dijela odgovarajuće klasične teoreme ne može se provesti kao u klasičnom slučaju jer se ne može pokazati da ako je C kopodmodul A-modula M tada je g(C) kopodmodul A-modula H.

Posljedica 63.1. Neka je M A-modul koji zadovoljava uslov stacionarnosti za rastuće nizove podmodula i neka su H i C podmodul i kopodmodul A-modula M. Tada i moduli H i M/(H,C) su takvi.

Dokaz: Imamo egzaktan niz

$$(o) \rightarrow H \xrightarrow{u} M \xrightarrow{p} M/(H,C) \rightarrow (o)$$

gdje je u ulaganje u H (injektivno utapanje) a p prirodni epimorfizam na.

Posljedica 63.2. Neka je M A-modul koji zadovoljava uslov stacionarnosti za rastuće nizove podmodula i neka je $f : M \rightarrow H$ epimorfizam A-modula. Tada i A-modul H zadovoljava-

uslov stacionarnosti za rastuće nizove podmodula.

Dokaz: Imamo $H = M/(\mathrm{Ker} f, C_f)$, a prema posljednjoj posljedici A-modul an desnoj strani je takav da zadovoljava uslov stacionarnosti za rastuće nizove podmodula.

DIO III

Prsten endomorfizama

3.1. GRUPA HOMOMORFIZAMA

3.1.1. Definicije i osnovne osobine

Neka su f i g homomorfizmi grupe $(A,=_A,\neq_A,+)$ u grupu $(B,=_B,\neq_B,+)$. Definiše se

$$f =_H g \iff (\forall x \in A)(f(x) =_B g(x)),$$

$$f \neq_H g \iff (\exists x \in A)(f(x) \neq_B g(x)),$$

$$(\forall x \in A)((f+g)(x) =_B f(x)+g(x)).$$

Lako se provjerava da je $(\mathrm{Hom}(A,B),=_H,\neq_H,+)$ abelova grupa. Pišemo $\mathrm{End}(A) = \mathrm{Hom}(A,A)$.

Primjeri I:

1° $\mathrm{Hom}(Z,B) \cong B$ za proizvoljnu grupu B. Specijalno $\mathrm{End}(Z) \cong Z$.

2° $\mathrm{End}(Z(p^\infty)) \cong J_p$, gdje je J_p aditivna grupa prstena Q_p cijelih p-adskih brojeva.

3° $\mathrm{End}(Q) \cong Q$.

Lema 1. Dijagram

(1)
$$\begin{array}{ccccc} & & & & G \\ & & & & \downarrow u \\ (o) & \longrightarrow & A & \xrightarrow{f} & B \xrightarrow{g} C \end{array}$$

s egzaktnom vrstom, gdje je f utapanje, može se nadopuniti u komutativni dijagram

(2)
$$\begin{array}{ccccccc} & & & & & & G \\ & & & \swarrow h & & & \downarrow u \\ (o) & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C \end{array}$$

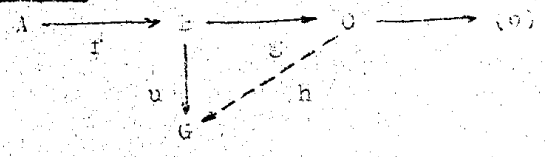
akko je $gu = 0$. Pri tome, homomorfizam h je definisan jednoznačno.

Dokaz: (1) Neka postoji traženi homomorfizam $h:G \longrightarrow A$. Tada iz $u = fh$ slijedi $gu = g(fh) = (gf)h = 0h = 0$.

(2) Obrnuto, neka je u dijagramu (1) $gu = 0$. Tada je $\mathrm{Im}f \subseteq \mathrm{Ker}g = \mathrm{Im}f$, pri čemu je f injektivno utapanje. Definišimo $b = f^{-1}u:G \longrightarrow A$. Tada je $fh = f(f^{-1}u) = (ff^{-1})u = u$. Ako je $h':G \longrightarrow A$ neki drugi homomorfizam za koji je $fh' = u$, imamo

$$fh = fh' \longrightarrow f^{-1}(fh) = f^{-1}(fh') \longleftrightarrow (f^{-1}f)h = (f^{-1}f)h'$$
$$\longrightarrow h = h'.$$

Lemma 2. Dijagram



sa egzaktnom vrstom, gdje je f utapanje, može se nadopuniti homomorfizmom $h:G \longrightarrow B$ do komutativnog dijagrama onda i samo ako je $uf = 0$. Pri tome, homomorfizam h je definisan jednoznačno.

Dokaz: (1) Neka postoji traženo $h:G \longrightarrow B$ za koje $u = hg$. Tada je

$$uf = (ug)f = u(gf) = u0 = 0.$$

(2) Obrnuto, neka je $uf = 0$. Tada $\mathrm{Im}f \subseteq \mathrm{Ker}u$ i zbog egzaktnosti niza $\mathrm{Ker}g \subseteq \mathrm{Ker}u$. Definišimo $h:G \longrightarrow C$ ovako: za proizvoljno $c \in C$ može se naći $b \in B$ takvo da je $g(b) = c$; stavljamo $h(c) = u(b)$. Definicija je korektna:

$$c = c' \longrightarrow (\exists\, bb' \in B)(g(b) = c = c' = g(b')) \longrightarrow$$
$$\longrightarrow b-b' \in \mathrm{Ker}g \subseteq \mathrm{Ker}u \longrightarrow u(b) = u(b'),$$
$$u(b) \neq u(b') \longleftrightarrow b-b' \in C_u \longrightarrow g(b) \neq g(b') \longrightarrow c \neq c'.$$

Napomena I: Razlika između klasično formulisanih lema i ovdje je u zahtijevu da je homomorfizam f utapanje.

Neka su $f:A' \longrightarrow A$ i $h:C \longrightarrow C'$ homomorfizmi grupa. Svaki homomorfizam $g \in \mathrm{Hom}(A,C)$ indukuje homomorfizam $A' \longrightarrow C'$ na sljedeći način

$$A' \xrightarrow{f} A \xrightarrow{g} C \xrightarrow{h} C'.$$

Korespodencija $g \longmapsto hgf$ je homomorfizam grupe $\mathrm{Hom}(A,C)$ u grupu $\mathrm{Hom}(A',C')$.

Tvrdnja 3. Neka je

(3) $$(o) \longrightarrow A \xrightarrow[f]{} B \xrightarrow[g]{} C \longrightarrow (o)$$

egzaktan niz, gdje je f utapanje. Tada su, za proizvoljnu grupu G, inducirani nizovi

(4) $$(0) \longrightarrow Hom(C,G) \xrightarrow{g^*} Hom(B,G) \xrightarrow{f^*} Hom(A,G),$$

(5) $$(0) \longrightarrow Hom(G,A) \xrightarrow{f_*} Hom(G,B) \xrightarrow{g_*} Hom(G,C)$$

egzaktni, pri čemu su g^* i f_* utapanja.

Dokaz:

1^0 Da bi dokazali da je g^* injektivno uzmimo $x:C \longrightarrow G$ takvo da je $0 = g^*x = xg$. Kako je g epimorfizam to je $x = 0$. Da bi dokazali da je g^* utapanje uzmimo $x:C \longrightarrow G$ takvo da je $x \neq 0$, tj. $(\exists c \in C)(x(c) \neq o)$. Zbog injektivnosti homomorfizma g imamo $(\exists b \in B)(g(b) = c)$. Dakle, $x(g(b)) \neq 0$, tj. $g^*x \neq 0$. Iz $f^*g^* = (gf)^* = 0^* = 0$ slijedi $\mathrm{Im}g^* \subseteq \mathrm{Ker}f^*$. Dokažimo obrnutu inkluziju. Neka je $y \in \mathrm{Ker}f^*$, tj. $f^*(y) = 0$, odnosno $yf = 0$. Prema lemi 2, postoji jedinstveni homomorfizam $x \in \mathrm{Hom}(C,G)$ takav da je $y = xg$. Dakle, $y \in \mathrm{Im}g^*$, što znači da je niz (4) egzaktan.

$$\begin{array}{ccccccccc} (o) & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & (o) \\ & & \downarrow & \overset{g^*}{\swarrow} & \downarrow & \overset{f^*}{\swarrow} & \downarrow & & \\ & & G & = & G & = & G & & \end{array}$$

2^0

$$\begin{array}{ccccccccc} & & G & = & G & = & G & & \\ & & \downarrow & \overset{f_*}{\searrow} & \downarrow & \overset{g_*}{\searrow} & \downarrow & & \\ (o) & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & (o) \end{array}$$

Ako je $x \in \mathrm{Ker}f_*$, tj. $0 = f_*(x) = fx$, onda je $x = 0$ jer je f injektivno utapanje. Iz $g_*f_* = (gf)_* = 0_* = 0$ slijedi da je $\mathrm{Im}f_* \subseteq \mathrm{Ker}g_*$. Dokažimo da svaki element $y \in \mathrm{Ker}g_*$ leži u $\mathrm{Im}f_*$. Prema lemi 1, iz jednakosti $0 = g_*y = gy$ slijedi

obratno je jednoznačno homomorfizma $x \in \mathrm{Hom}(A,G)$ za koje je

$nx = y$, tj. $y \in \mathrm{Im} f_x$.

Napomena II: Ako je $(G,=_G,\neq_G,\cdot)$ grupa i $n \in \mathbb{N}$, stavimo

$$nG = \{ab : b \in G\},$$

$$G[n] = \{b \in G : nb =_G o\},$$

$$C_n = \{b \in G : nb \neq_G o\}.$$

Jasno je da su nG i $G[n]$ podgrupe grupe G a C_n je podskup grupe G za koje vrijedi $nG \subseteq C_n$. Štoviše vrijedi

$$G/(G[n],C_n) \cong nG.$$

Tvrdnja 4. Ako $(\exists n \in \mathbb{N})(G[n] = (o))$, tada je $\mathrm{Hom}(A,G)[n] = (0)$ za proizvoljnu grupu G.

Dokaz: Neka je $x \in \mathrm{Hom}(A,G)$ i $nx = 0$. Za proizvoljno $a \in A$ imamo $n(x(a)) =_G (nx)(a) =_G 0(a) =_G o$, odnosno $x(a) \in G[n] = (o)$. Dakle, $x(a) =_G o$, što znači da je $x = 0$.

Definicija 1. Neka je $(G,=_G,\neq_G,+)$ grupa. Za element g grupe G kaže se da je beskonačnog reda ako vrijedi

$$(1) \qquad (\forall n \in \mathbb{N})(ng =_G o \longrightarrow g =_G o),$$

$$(2) \qquad (\forall n \in \mathbb{N})(g \neq_G o \longrightarrow ng \neq_G o).$$

Za grupu G se kaže da je grupa bez torzije ako joj je svaki element beskonačnog reda.

Lema 5. Grupa G je grupa bez torzije akko je za svako $n \in \mathbb{N}$ homomorfizam $f_n : G \ni g \longmapsto ng \in G$ injektivno utapanje.

Dokaz: Očigledno.

Napomena III: Grupa G je djeljiva ako vrijedi

$$(\forall n \in \mathbb{N})(nG = G),$$

tj. ako je za svako $n \in \mathbb{N}$ homomorfizam $f_n : G \longrightarrow G$ injektivan.

Tvrdnja 6. Ako je B grupa bez torzije, tada je grupa $\mathrm{Hom}(A,B)$ grupa bez torzije, za proizvoljnu grupu A.

Neka je B grupa bez torzije. Tada je za svako $n \in \mathbb{N}$ homomorfizam $f_n : B \to b \longmapsto nb \in B$ injektivno preslikavanje. Ako je $f \in \mathrm{Hom}(A,B)$ tada

$$f \neq_H 0 \Longrightarrow f_n f \neq_H 0 \Longleftrightarrow nf \neq_H 0 ,$$

$$nf =_H 0 \Longleftarrow f_n f =_H 0 \Longrightarrow f_n^{-1}(f_n f) =_H 0 \Longleftrightarrow f =_H 0.$$

Tvrdnja 7. Ako je B djeljiva grupa bez torzije, tada je $\mathrm{Hom}(A,B)$ djeljiva grupa bez torzije.

Dokaz: Ako je B djeljiva grupa bez torzije, tada je za svako $n \in \mathbb{N}$ homomorfizam $f_n : B \longrightarrow B$ izomorfizam. Prema prethodnoj propoziciji, $\mathrm{Hom}(A,B)$ je grupa bez torzije. Dokažimo da je $\mathrm{Hom}(A,B)$ djeljiva grupa. Za $f \in \mathrm{Hom}(A,B)$ i za $n \in \mathbb{N}$ uzmimo $g = f_n^{-1} f$. Tada imamo

$$f =_H (f_n f_n^{-1}) f =_H f_n (f_n^{-1} f) =_H f_n g =_H ng.$$

Tvrdnja 8. Ako $(\exists\, n \in \mathbb{N})(nA = A)$, tada $\mathrm{Hom}(A,B)[n] = (0)$ za proizvoljnu grupu B.

Dokaz: Neka je $f \in \mathrm{Hom}(A,B)$ i $nf =_H 0$. Kako

$$(\forall a \in A)(\exists\, b \in A)(a =_A nb)$$

imamo

$$f(a) =_B f(nb) =_B nf(b) = 0(b) =_B 0$$

tj. $f =_H 0$.

Tvrdnja 9. Ako je A djeljiva grupa, tada je $\mathrm{Hom}(A,n)$ grupa bez torzije, za proizvoljnu grupu B.

Dokaz: Neka je $f \in \mathrm{Hom}(A,B)$. Ako je $f \neq_H 0$, tj. $(\exists a \in A)(f(a) \neq_B 0)$, tada, zbog djeljivosti grupe A $(\exists\, a' \in A)(a =_A na')$, imamo

$$(\exists\, a' \in A)((nf)(a') \neq_B 0).$$

Ako je $nf =_H 0$, tada imamo

$$f(a) =_B f(na') =_B nf(a') = 0(a') =_B 0$$

odakle slijedi da je $f =_H 0$.

Tvrdnja 10. Ako je A djeljiva grupa bez torzije, tada je $\mathrm{Hom}(A,B)$ djeljiva grupa bez torzije.

Dokaz: Prema prethodnoj propoziciji, $\mathrm{Hom}(A,B)$ je grupa bez torzije. Za $f \in \mathrm{Hom}(A,B)$ uzmimo $g = f_n^{-1}f$, gdje je f_n^{-1} izomorfizam. Imamo

$$f =_H (f_n f_n^{-1})f =_H f_n(f_n^{-1}f) =_H f_n g =_H 0.$$

3.1.2. Direktni proizvod grupa homomorfizama

Teorem 11. Ako je $\bigoplus_{i=1}^{\infty} A_i$ striktno izbrojiva direktna suma grupa A_i, tada se $\prod_{i=1}^{\infty} \mathrm{Hom}(A_i,B)$ može injektivno utopiti u grupu $\mathrm{Hom}(\bigoplus_{i=1}^{\infty} A_i, B)$.

Dokaz: Uzmimo proizvoljno $(f_i)_i \in \prod_{i=1}^{\infty} \mathrm{Hom}(A_i,B)$, gdje je $f_i \in \mathrm{Hom}(A_i,B)$ $(i = \overline{1,\infty})$. Definišimo preslikavanje $f: \bigoplus A_i \longrightarrow B$ na slijedeći način

$$b_{i_1}+b_{i_2}+\ldots+b_{i_k} \longmapsto f_{i_1}(b_{i_1})+f_{i_2}(b_{i_2})+\ldots+f_{i_k}(b_{i_k}).$$

Dokažimo da je f definisano korektno:

(i) Za $a,b \in \bigoplus_{i=1}^{\infty} A_i$ imamo

$$(\exists k_a \in \mathbb{N})(\forall j \in \overline{k_a})(\exists b_{i_j} \in A_{i_j})(a = b_{i_1}+\ldots+b_{i_{k_a}})$$

$$(\exists k_b \in \mathbb{N})(\forall p \in \overline{k_b})(\exists b_{s_p} \in A_{s_p})(b = b_{s_1}+\ldots+b_{s_{k_b}})$$

$$a = b \iff (k_a =_{\mathbb{N}} k_b) \wedge (\forall j \in \overline{k_a})(\exists p \in \overline{k_b})(b_{i_j} = b_{s_p}) \wedge$$

$$\wedge (\forall p \in \overline{k_b})(\exists j \in \overline{k_a})(b_{s_p} = b_{i_j}) \Longrightarrow$$

$$\Longrightarrow (k_a =_{\mathbb{N}} k_b) \wedge (\forall j \in \overline{k_a})(\exists p \in \overline{k_b})(f_{i_j}(b_{i_j}) =_B f_{s_p}(b_{s_p})) \wedge$$

$$\wedge (\forall p \in \overline{k_b})(\exists j \in \overline{k_a})(f_{s_p}(b_{s_p}) =_B f_{i_j}(b_{i_j})) \Longrightarrow$$

$$\Longrightarrow f_{i_j}(b_{i_j})+\ldots+f_{i_k}(b_{i_k}) =_B f_{s_1}(b_{s_1})+\ldots+f_{s_k}(b_{s_k}).$$

(ii) $f(a) \neq_B f(b)$

$$f_{i_1}(b_{i_1})+\ldots+f_{i_{k_a}}(b_{i_{k_a}}) \neq_B f_{s_1}(b_{s_1})+\ldots+f_{s_{k_b}}(b_{s_{k_b}}) \longrightarrow$$

$$\Longrightarrow \bigvee_{\substack{u=1,k_a \\ v=1,k_b}} (f_{i_u}(b_{i_u}) \neq_B f_{j_v}(b_{j_v})) \Longrightarrow \bigvee_{\substack{u=1,k_a \\ v=1,k_b}} (b_{i_u} \neq b_{j_v}) \Longrightarrow$$

$$\Longrightarrow b_{i_1} + b_{i_2} + \ldots + b_{i_{k_a}} \neq b_{j_1} + b_{j_2} + \ldots + b_{j_{k_b}}.$$

(iii) Dakle, možemo definisati pridruživanje

$$\Psi: \prod_{i=1}^{\infty} \mathrm{Hom}(A_i, B) \ni (f_i)_i \longmapsto f \in \mathrm{Hom}(\oplus_{i=1}^{\infty} A_i, B).$$

$(\forall i)(f_i = 0) \Longrightarrow f = 0$, $f \neq 0 \Longrightarrow (\exists f_{i_j})(f_{i_j} \neq 0) \Longrightarrow (f_i)_i \neq (0)_i$

te zaključujemo da je to pridruživanje funkcija.

(iv) Ψ je utapanje:

$$(f_i)_i \neq (0)_i \Longleftrightarrow (\exists j)(f_j \neq 0) \Longleftrightarrow$$

$$\Longleftrightarrow (\exists j)(\exists b_j \in A_j)(f_j(b_j) \neq_B 0).$$

Za elemenu $a \in \oplus A_i$ dat sa $a = 0+\ldots+b_j+\ldots+0$ imamo

$$f(a) =_B f_j(b_j) \neq_B 0 .$$

(v) Ψ je injektivno:

$$f = 0 \Longleftrightarrow (\forall a \in \oplus A_i)(f(a) =_B 0) \Longrightarrow$$

$$\Longrightarrow (s = b_i \in A_i)(f(s) =_B \ldots + f_i(b_i) + \ldots =_B 0) \Longrightarrow (\forall i)(f_i = 0).$$

<u>Teorem 12.</u>

$$\mathrm{Hom}(A, \prod_{i=1}^{\infty} B_i) \cong \prod_{i=1}^{\infty} \mathrm{Hom}(A, B_i) .$$

Dokaz: Ako sa P_i označimo i-tu projekciju $\prod_{i=1}^{\infty} B_i \longrightarrow B_i$ tada za svako $f \in \mathrm{Hom}(A, \prod_{i=1}^{\infty} B_i)$ možemo definisati homomorfizam $P_i f \in \mathrm{Hom}(A, B_i)$. Ako definišemo

$$\Psi: f \longmapsto (P_i f)_i$$

direktnim provjeravanjem se može ustanoviti da je Ψ izomorfizam.

<u>Napomena IV:</u> Kako u konstruktivnoj matematici može biti govora samo o potencijalnoj beskonačnosti, to su teoreme 11. i 12. preformulisane u tom smislu. U opštem slučaju

obrnuta tvrdnja tvrdnji teorema 11. nije ispunjena.

3.2. PRSTEN ENDOMORFIZAMA

3.2.1. Ideali prstena endomorfizama

Vidjeli smo da je $(End(G),=_E,\neq_E,+)$ grupa. Ako operaciju slaganja homomorfizama uzmemo kao multiplikaviju, tada je End(G) prsten sa jediničnim elementom Id_G koji nije komutativan.

Napomena V: 1^o Za $(J,=,\neq)$ se kaže da je desni ideal prstena $(A,=,\neq,+,.)$ akko vrijedi

$$a \in J \wedge b \in J \Rightarrow a+b \in J,$$
$$a \in J \Rightarrow -a \in J,$$
$$a \in J \wedge b \in A \Rightarrow ab \in J.$$

2^o Za $(J,=,\neq)$ se kaže da je lijevi ideal prstena $(A,=,\neq,+,.)$ akko vrijedi

$$a \in J \wedge b \in J \Rightarrow a+b \in J,$$
$$a \in J \Rightarrow -a \in J,$$
$$a \in A \wedge b \in J \Rightarrow ab \in J.$$

3^o Za $(C,=,\neq)$ se kaže da je lijevi koideal prstena $(A,=,\neq,+,.)$ akko vrijedi

$$a+b \in C \Rightarrow a \in C \vee b \in C,$$
$$0 \notin C,$$
$$-a \in C \Rightarrow a \in C,$$
$$ab \in C \Rightarrow b \in C.$$

4^o Za $(C,=,\neq)$ se kaže da je desni koideal prstena $(A,=,\neq,+,.)$ akko vrijedi

$$0 \notin C,$$
$$a+b \in C \Rightarrow a \in C \vee b \in C,$$
$$-a \in C \Rightarrow a \in C,$$
$$ab \in C \Rightarrow a \in C.$$

Lema 13. Neka je H podgrupa grupe $(G,=_G,\neq_G,+)$. Tada je skup

$$L_H \equiv \{f \in End(G) : f(H) = (o)\}$$

Lijevi ideal prstena $End(G)$, a skup

$$O_H \equiv \{f \in End(G) : f(H) \neq (o)\}$$

Lijevi ideal prstena $End(G)$ za koje vrijedi $\subseteq \neg$).

Dokaz:

i) $f \in O_H \longleftrightarrow f(H) \neq (o) \longleftrightarrow (\exists a \in H)(f(a) \neq_G o = _G O(a))$

$\Longleftrightarrow f \neq_E 0 \longleftrightarrow o \notin O_H$,

ii) $f+g \in O_H \longleftrightarrow (f+g)(H) \neq (o) \longleftrightarrow (\exists a \in H)((f+g)(a) \neq_G o)$

$\longrightarrow (\exists a \in H)(f(a) \neq_G o \vee g(a) \neq_G o) \longleftrightarrow f \in O_H \vee f \in O_H$,

iii) $-f \in O_H \longrightarrow f \in O_H$,

iv) $f_0 \in O_H \longleftrightarrow (f_0)(H) \neq (o) \longleftrightarrow (\exists a \in H)((f_0)(a) \neq_G o)$

$\longleftrightarrow (\exists a \in H)(f(g(a)) \neq_G o) \longrightarrow$

$\longrightarrow (\exists a \in H)(g(a) \neq_G o) \longleftrightarrow g \in O_H$,

v) $f \in L \longleftrightarrow f(H) = (o) \longleftrightarrow (\forall a \in H)(f(a) =_G o) \longrightarrow$

$\longrightarrow (\forall a \in H)(f(a) \neq_G o) \longleftrightarrow \neg(\exists a \in H)(f(a) \neq_G o) \longleftrightarrow$

$\longleftrightarrow \neg(f \in O_H) \longleftrightarrow f \in \neg O_H$.

Posljedica 13.1. Za svaki element grupe $(G, =_G, \neq_G, +)$ skup $L_x \equiv \{f \in End(G) : f(x) =_G o\}$ je lijevi ideal prstena $End(G)$, a skup $O_x \equiv \{f \in End(G) : f(x) \neq_G o\}$ je lijevi kodideal prstena $End(G)$ i vrijedi $L_x \subseteq \neg O_x$. Ideal L_x je odlučiv u $End(G)$ akko je za svako $f \in L_x$ element $f(x)$ dishretan element u G.

Teorem 14. Neka je H podgrupa grupe $(G, =_G, \neq_G, +)$. Tada je skup $D_H \equiv \{f \in End(G) : Imf \subseteq H\}$ desni ideal prstena $End(G)$. Ako je C kopodgrupa grupe G takva da je $H \subseteq \neg C$, tada je skup $S_C \equiv \{f \in End(G) : (\exists x \in G)(f(x) \in C)\}$ desni coideal prstena $End(G)$ za koji vrijedi $D_H \subseteq \neg S_C$.

Dokaz:

$C \notin S_C$,

$f+g \in S_C \longleftrightarrow (\exists x \in G)((f+g)(x) \in C) \longrightarrow$

$\longrightarrow (\exists x \in G)(f(x) \in C \vee g(x) \in C) \longleftrightarrow f \in S_C \vee g \in S_C$,

$-f \in S_C \longleftrightarrow (\exists x \in G)((-f)(x) \in C) \longrightarrow (\exists x \in G)(f(x) \in C)$

$\longleftrightarrow f \in S_C$,

$$\ldots \in \ldots \iff (\exists x \in \ldots)(\ldots \in \ldots \iff \exists \ldots) \ldots \in \ldots$$

$$\longrightarrow (\exists \ldots \in \ldots) f(\ldots(x)) \in \ldots \iff f \in \ldots .$$

$$f \in \ldots \longrightarrow \ldots \subseteq \ldots \subseteq \ldots \iff (\forall x \in \ldots) \ldots \in \ldots \iff \ldots$$

$$\iff (\forall x \in \ldots) \neg f(x) \in \ldots \iff \neg(\exists \ldots \in \ldots) \ldots \iff \ldots \in \ldots .$$

<u>Lemma 15.</u> Neka je $(G,=_G,\neq_G,+)$ grupa. Tada je skup

$$O_x = \{f(x) : f \in End(G)\}$$

(potpuno karakteristična) podgrupa grupe G i postoji bijektivni homomorfizam

$$W : End(G)/(L_x, O_x) \longrightarrow O_x .$$

Dokaz:

(i) Jednostavnim provjeravanjem se utvrđuje da je O_x (potpuno karakteristična) podgrupa grupe G.

(ii) Definišimo

$$W : End(G) \ni f \longmapsto f(x) \in G$$

Tada

$$f =_E g \Longrightarrow f(x) =_G g(x) \iff W(f) =_G W(g),$$

$$W(f) \neq_G W(g) \iff f(x) \neq_G g(x) \longrightarrow f \neq_E g,$$

$$W(f) =_G W(g) \iff f(x) =_G g(x) \longrightarrow f - g \in L_x,$$

$$(\forall f(x) \in O_x)(\exists f \in End(G))(W(f) =_G f(\tau)).$$

<u>Napomena V:</u> U prethodnoj lemi, kažemo da W nije izomorfizam, jer da bi W bilo utapanje, tj. da bi vrijedilo

$$f \neq_E g \longleftarrow (\exists z \in G)(f(z) \neq_G g(z))$$

trebalo bi da bude $z =_G x$, što nismo u mogućnosti da ustanovimo.

Literatura

[1] Acuña,O. - Ortega and F.E.Linton: Finitenes and decidability, I; Springer Lecture Notes in Mathematics, 753(1979),80-100.

[2] Ashvinikumar: On Brouwer-Stieltjes integration; Indag. Math. 32(1970),161-170.

[3] M.J.Beeson: Formalizing Constructive mathematics: Why and How?; Springer Lecture Notes in Mathematics, 873(1981),146-190.

[4] E.Bishop, FOUNDATIONS OF CONSTRUCTIVE ANALYSIS; McGrow-Hill, New York 1967.

[5] D.S.Bridges, CONSTRUCTIVE FUNCTIONAL ANALYSIS; Pitman Published Limited No 28., London 1979.

[6] Brouwer,L.E.J., Zur Bergünder der intuitionischen Mathematic,I; Math.Ann. 93(1924),244-258.

[7] J.C.Dekker, Countable vector spaces with recursive operations, I and II; JSL (34)3(1969),363--387. i (36)3(1971),477-493.

[8] J.P.Deldin, A Constructive Approach to Classical Mathematics; Springer Lecture Notes in Mathematics, 873(1981),105-110.

[9] A.Fröhlich and J.C.Shepherdson, Efective Procedure in Field Theory; Philos. Trans.Roy.Soc.London, Ser.A. 248(1955),407-432.

[10] N.D.Goodman, Reflections on Bishop's Philosophy of Mathematics; Springer Lecture Notes in Mathematics, 873(1981),135-145.

[11] R.J.Grayson, Intuitionistic Set Theory; Ph.D. thesis. Oxford University, Oxford 1978. v+177.

[12] N.Greenleaf, Liberal Constructive Set Theory; Springer Lecture Notes in Mathematics, 873(1981), 213-240.

[13] A.Heyting, INTUITIONISM, An introduction; North-Holland Publishing Company, Amsterdam 1956.

[14] W.Julian, R.Mines and F.Richman, Algebraic Numbers, a Constructive Development; Pacific Journal of the Mathematics,(74)1(1978),91--102.

[15] P.T.Johnstone, Rings, Fields and Spectra; Journal of Algebra, 49(1977),238-260.

[16] ----------, Conditions Related to deMorgan's Law; Applications as Cheaves; Lecture Notes in Mathematics, 753(1979),479-491.

[17] V.Lifschitz, Constructive Assertations in an Extension of Classical Mathematics; JSL (4)2(1982) 359-387.

[18] D.S.McCarty, Realizibity and Recursive Mathematics; Ph.D. thesis, Carnegie-Mellon University, Pittsburg 1984, iii+281 pp.

[19] J.C.Mulvey, Intuitionistic Algebra and Representations of Rings; Mem.Am.Math.Soc. (148)1974, 3-57.

[20] R.Mines and F.Richman, Dedekind Domains; Springer Lectures in Mathematics, 873(1981),16-30.

[21] ----------, Separabitlity and Factoring Polinomials; Rocky Mountanian Journal of Mathematics, (12)1(1982),43-54.

[22] R.Mines, Algebraic Number Theory; The L.E.J. Brouwer Centenary Symposium, North-Holland Publishing Company, Amsterdam 1982, 337-358.

[23] G.Metakides and A.Nerode, Recursion Theory and Logic, Lecture Notes in Mathematics, 450(1975), 209-219.

[24] ----------, Effective content of Fields Theory; Ann. of Math.Logic, 17(1979), 86-92.

[25] M.O.Rabin, Computable Algebra; Trans.Am.Math.Soc. 95 (1960),341-360.

[26] F.Richman, The constructive theory of countable p-groups; Pacific J. of the Math. (45)2(1973),621--637.

[27] ---------, Constructive Aspect of Noetherian Rings; Proc. of the Am.Math.Soc. (44)2(1974),436-441.

[28] ---------, The Constructive Theory of KT-Modules; Pacific J of Math. (61)1(1975),263-274.

[29] ---------, Computing Heights in Thor; Houston J. of the Math. (3)2(1977),267-270.

[30] ---------, Seidenberg's Conditions P; Springer Lecture Notes in Mathematics, 873(1981),1-11.

[31] ---------, Finite Dimensional Theory Algebras over Discrete Fields; The L.E.J.Brouwer Centenary Simposium, North-Holland Publishning Company, Amsterdam 1982, 397-411.

[32] D.A.Romano: Intuicionistička reinterpretacija nekih klasičnih matematičkih struktura; magistarski rad, Prirodno-matematički fakultet u Sarajevu 1978.

[33] ----------, Intuicionistički principi matematike; Matematika,(10)3(1981),31-33.

[34] ----------, Groups, a constructive view; Pojaviće se u časopisu "Radovi matematički", Sarajevo.

[35] ----------, Preliminaries of Algebra of Bishop's Constructive Mathematics; Pojaviće se u časopisu Publikacije matematičkog instituta u Beogradu, Beograd.

[36] ----------, O jednakosti i različitosti u konstruktivnoj matematici; Publikacija Više tehničke škole u Bihaću, Serija A: Matematika, 1(1985),1-14.

[37] ----------, Konačnost i beskonačnost u konstruktivnoj matematici, predavanj; Publikacija Više tehničke škole u Bihaću, Serija A: Matematika, 1(1985), 15-21.

[38] ----------, Relacije, funkcijske relacije u biskupovskoj konstruktivnoj matematici; Publikacija Više tehničke škole u Bihaću, Serija A: Matematika, 2(1985).

[39] ----------, Rings and ideals, a constructive view; Publikacija Više tehničke škole u Bihaću, Serija A: Matematika, 2(1985).

[40] D.A.Romano, M.Božić, Rings and Modules, a Constructive View; Naučnoistraživački projekt u okviru naučnoistraživačkog rada na Višoj tehničkoj školu u Bihaću (Recenzentska Komisija u Sastavu: dr Mirko Mihaljinec, Zagreb; dr Fred Richman New Mexico - Las Cruces, USA; Dirkk van Dalen, Utrecht - Holandija)

[41] W.B.G.Ruitenburg, Intuitionistic Algebra; Ph.D.Thesis. University of Utrecht, Utrecht 1982.

[42] ----------, Field Extensions; Springer Lecture Notes in Mathematics, 873(1981),12-15.

[43] D.S.Scott, Identity and Existence in Intuitionstic Logic; Springer Lecture Notes in Mathematics, 753(1979),660-696.

[44] A-Seidenberg, On the Lenght of a Hilbert Ascending Chain Proc. of the Am.Math.Soc. (29)3(1971), 443-450.

[45] ----------, Constructive Proof of Hilbert's Theorem on Ascending Chain; Trans.Math,Am.Soc. (174)(1972),305-350.

[46] ----------, Constructions in Algebra; Trans.Am.Math. Soc. (197)(1974),273-313.

[47] J.Staples, On constructive Fields; Proc.of the London Math.Soc. (3)23(1971),753-768.

[48] C.Smorinsky, Elemntary Intuitionistic Theory; JSL (38) 1(1973),102-134.

[49] K.Šeper, Konstruktivna matematika,I,II; Matematika (6)3 (1977),69-75 i (6)4(1977),19-24.

[50] -------, Numerička analiza - klasična ili konstruktivna? Matematika, (12)4(1983),37-43.

[51] -------, Some thesis concering the development of Mathematics; Zbornik radova Matematičkog

insituta u Beogradu, Nova serija, 2 (1o),1977, 140-142.

[52] A.S.Troelstra, Aspects of Constructive Mathematics; in Handbook of Mathematical Logic (ed. J.Barwise), North-Holland Publishing Company, 1977.

[53] ----------, PRINCIPLES OF INTUITIONISM; Springer Lecture Notes in Mathematics 95(1969).

[54] ----------, Intuitionistic Extensions of the Reals; Nieuw Archief voor Wiscunde (3)28 (1980),63-113.

[55] ----------, Finite and Infinite in Intuitionistic Mathematics; Comp.Math. 18(1967),94--116.

[56] A.S.Troelstra and D.van Dalen, CONSTRUCTIVISM IN MATHEMATICS, An introduction (preliminary draft of Chapter VIII: Algebra)

[57] V.N.Trostnjikov, Što su konstruktivni procesi u matematici; Školska knjiga, Zagreb 1983.