UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET

Dr Gradimir Vojvodić

PREDAVANJA IZ ALGEBRE

Novi Sad, 2007.

Naziv Udžbenika ”PREDAVANJA IZ ALGEBRE”(II deo ”Predavanja iz matematičke logike i algebre”)

Autor: Dr Gradimir Vojvodić, redovni profesor Prirodno-matematičkog fakulteta u Novom Sadu

Recenzenti: Dr Miodrag Rašković, redovni profesor Prirodno-matematičkog fakulteta u Kragujevcu
Dr Milan Grulović, redovni profesor Prirodno-matematičkog fakulteta u Novom Sadu

Izdavači: Univerzitet u Novom Sadu
Prirodno-matematički fakultet u Novom Sadu

Glavni i odgovorni urednik pojedinačnog izdanja: Dr Mirosla Vesković, dekan Prirodno-matematičkog fakulteta u Novom Sadu

Štampano u 300 primeraka, III dopunjeno i izmenjeno izdanje
(I izdanje, Edicija Univerzitetski udžbenik, broj 68)

Sadržaj

Predgovor

Ovaj tekst obuhvata predavanja iz predmeta Algebra za informatičare. Namenjen je pre svega studentima matematike, smer Diplomirani informatičar Prirodno-matematičkog fakulteta u Novom Sadu. Nastao je iz moje knjige ”Predavanja iz Matematičke logike i algebre”, Univerzitet u Novom Sadu, PMF Novi Sad, 1998.

Knjiga sadrži 8 poglavlja. Tekst sadrži i brojne primere i urađene zadatke. Sve to treba da omogući brže i lakše usvajanje gradiva. Deo gradiva obrađen je u knjizi G. Vojvodić, B. Šobot: Zbirka zadataka iz matematičke logike i algebre, Univerzitet u Novom Sadu, PMF Novi Sad , 2003. Takođe, i okviri u kojima su izloženi pojedini delovi teksta, uslovljeni su fondom časova, pa čitaoce koji ih žele proširiti upućujem na literaturu navedenu na kraju knjige. Iz tih knjiga preuzeti su neki zadaci, tvrđenja, kao i neki primeri. Gradivo poslednja četiri poglavlja proučava se i proširuje u više redovnih kurseva za studente informatike.

Posebnu zahvalnost dugujem Viktoru Kunčaku, iz čijih beležaka sa mojih predavanja je nastao ovaj tekst. Viktor Kunčak je tehnički obradio tekst, dao brojne korisne sugestije i pažljivo proverio rešenja zadataka.

Zahvaljujem se recenzentima prof. dr Miodragu Raškoviću sa PMF iz Kragujevca i prof. dr Milanu Gruloviću sa PMF iz Novog Sada na korisnim komentarima i primedbama koje su mi ukazali nakon pažljivog čitanja rukopisa.

U Novom Sadu, novembra 2007. Gradimir Vojvodić

Glava 1

Grupoidi

1.1 Operacije i algebarske strukture

Ako je A proizvoljan skup, preslikavanje $\sigma : A \times A \to A$ se naziva *binarna operacija* skupa A. Umesto $\sigma((a, b)) = c$ pišemo skraćeno $a\,\sigma\,b = c$. Ako je σ binarna operacija skupa A, tada se uređeni par (A, σ) naziva *grupoid*. Funkcija $f : A^n \to A$ gde $n \in \{0, 1, 2, \ldots\}$ se naziva n-arna operacija skupa A. Za $n = 0$ operacija $c : A^0 \to A$ se identifikuje sa konstantom $c \in A$.

Primer 1.1 Ako je N skup prirodnih brojeva, Z skup celih brojeva, a R_e skup realnih brojeva, onda je su $(N, +)$, $(N, \cdot)$, $(Z, +)$ i $(R_e, \cdot)$ grupoidi. Uređen par $(N, -)$ nije grupoid jer $a - b$ nije definisano za sve vrednosti $a, b \in N$. $\triangle$

Definicija 1.2 Ako je $D \subseteq A^2$ i $A \neq \emptyset$ tada se preslikavanje $p : D \to A$ naziva *parcijalna (binarna) operacija* skupa A.

Definicija 1.3 *Višeznačna (binarna) operacija* skupa A je preslikavanje $v : A^2 \to \mathcal{P}(A)$.

Definicija 1.4 *(Univerzalna) algebra* je struktura

$$(A, f, g, \ldots)$$

gde je A proizvoljan skup koji se naziva *nosač* algebre, a $f, g, \ldots$ operacije skupa A. Ako su arnosti operacija $f, g, \ldots$ redom $n_1, n_2, \ldots$ tada kažemo da se radi o algebri tipa $(n_1, n_2, \ldots)$.

Primer 1.5 Struktura $(R_e, +, \cdot)$ gde je R_e skup realnih brojeva, $+$ sabiranje, a $\cdot$ množenje realnih brojeva, je primer univerzalne algebre tipa $(2, 2)$. $\triangle$

Definicija 1.6 *Algebarski sistem* je struktura

$$\mathcal{A} = (A, f, g, \ldots, R, S, \ldots)$$

gde je A proizvoljan skup, $f, g, \ldots$ operacije skupa A, a $R, S, \ldots$ relacije skupa A.

Primer 1.7 Primer algebarskog sistema je struktura $(R_e, +, \cdot, \leq)$ gde je R_e skup realnih brojeva, $+$ operacija sabiranja realnih brojeva, $\cdot$ operacija množenja realnih brojava, a $\leq$ uobičajena relacija totalnog poretka nad realnim brojevima. $\triangle$

Kada razmatramo algebarski sistem $(A, f, g, \ldots)$ podrazumevamo da je na skupu A definisana i relacija jednakosti $=$, što ne naglašavamo posebno u definiciji algebarskog sistema.

1.2 Grupoidi

Grupoidi su interpretacije predikatskog računa sa jednakošću sa jezikom $\mathcal{J} = \{\sigma, \approx\}$, gde je σ funkcijski simbol arnosti 2, a $\approx$ relacijski simbol arnosti 2. Pri tome se $\approx$ interpretira kao relacija jednakosti i često se izostavlja, pa pišemo samo $\mathcal{J} = \{\sigma\}$. Term nad jezikom koji sadrži neke od primenljivih $x_1, \ldots, x_n$ se označava sa $t(x_1, \ldots, x_n; \sigma)$. Tako je $((x\,\sigma\,y)\,\sigma\,z)\,\sigma(z\,\sigma\,x))$ jedan term nad jezikom $\{\sigma\}$.

Definicija 1.8 Identiteti su formule oblika

$$(\forall x_1), \ldots, (\forall x_n)\, t(x_1, \ldots, x_n; \sigma) \approx v(x_1, \ldots, x_n; \sigma),$$

gde su t i v termi, a kvantifikatori deluju na sve promenljive.

Ubuduće umesto simbola $\approx$ koristimo simbol $=$.

Primer 1.9 Posmatrajmo identitet $(\forall x)(\forall y)\, x\,\sigma\, y = y\,\sigma\, x$. Ukoliko formulu interpretiramo u skupu prirodnih brojeva i $+$ kao operaciju sabiranja prirodnih brojeva, zaključujemo da je identitet tačan nad $(N, +)$.

Interpretirajmo sada formulu u strukturi $(A, \cdot)$ gde je $A = \{a, b\}$, a operacijskom slovu σ pridružujemo operaciju $\cdot$ definisanu tablicom:

$\cdot$	a	b
a	a	b
b	a	b

Tada formula $(\forall x)(\forall y)\, xy = yx$ nije tačna jer $a \cdot b \neq b \cdot a$. Zato $(A, \cdot)$ nije model za navedenu formulu. Kažemo da $\cdot$ *nije komutativna* operacija na skupu A. $\triangle$

Definicija 1.10 *Trivijalni grupoid* je grupoid oblika $(\{a\}, \cdot)$.

U trivijalnom grupoidu operacija $\cdot$ može biti definisana jedino tako da važi $a \cdot a = a$. U ovom grupoidu je vrednost svakog terma a, pa su svi identiteti zadovoljeni. Zato trivijalne grupoide ne razmatramo. Ovaj pojam se može i uopštiti.

Definicija 1.11 *Trivijalna algebra* je algebra oblika $(\{a\}, f, g, \ldots)$.

U nastavku ćemo opisati neke postupke konstrukcije novih algebarskih struktura na osnovu postojećih, kao i osobine koje imaju konstruisani objekti. Zbog jednostavnosti, sve konstrukcije opisujemo na grupoidima.

1.3 Podgrupoid grupoida

Definicija 1.12 Neka je $(A, \circ)$ grupoid. Ako je $B \subseteq A$ proizvoljan podskup i važi $(\forall x, y \in B)\, x \circ y \in B$, tada se grupoid $(B, \circ_B)$, gde je $\circ_B = \circ|_{B^2}$, naziva *podgrupoid* grupoida $(A, \circ)$, što označavamo sa $(B, \circ_B) \prec (A, \circ)$.

Napomena 1.13 I prazan skup možemo smatrati za nosač grupoida tj. i prazan skup možemo smatrati podgrupoidom. Ako imamo i nularne operacije, onda je podalgebra uvek neprazna. $\diamond$

Kako je iz konteksta obično jasno na kojem skupu se primenjuje operacija, umesto $\circ_B$ pišemo često samo $\circ$.

Primer 1.14 Grupoid $(N, \cdot)$ je podgrupoid grupoida $(Z, \cdot)$ jer je proizvod dva pozitivna cela broja opet pozitivan ceo broj. $\triangle$

Tvrđenje 1.15 *Neka je $\{\mathcal{A}_i \mid i \in I\}$ familija podgrupoida grupoida $\mathcal{A} = (A, \circ)$, pri čemu je $\mathcal{A}_i = (A_i, \circ)$. Tada je*

$$\mathcal{B} = \left(\bigcap_{i \in I} A_i, \circ \right)$$

podgrupoid grupoida $\mathcal{A}$.

Dokaz. Neka su a, b proizvoljni. Tada

$$\begin{aligned} a, b \in \bigcap_{i \in I} A_i &\Leftrightarrow (\forall i \in I)\, a, b \in A_i \\ &\Rightarrow (\forall i \in I)\, a \circ b \in A_i \\ &\Leftrightarrow a \circ b \in \bigcap_{i \in I} A_i, \end{aligned}$$

što znači da je $(\bigcap_{i \in I} A_i, \circ) \prec (A, \circ)$. ∎

Tvrđenje 1.16 (Prvo tvrđenje o stabilnosti) *Ako identitet $t = v$ važi u grupoidu $(A, \circ)$, onda on važi i u svakom njegovom podgrupoidu $(B, \circ)$.*

Dokaz. Neka je $t = v$ proizvoljan identitet, $(A, \circ)$ proizvoljan grupoid i $(B, \circ)$ njegov proizvoljan podgrupoid. Neka je a proizvoljna valuacija grupoida $(B, \circ)$. a dodeljuje svakoj promenljivoj element skupa $B \subseteq A$, pa je a istovremeno i valuacija grupoida $(A, \circ)$. Kako $t = v$ važi na grupoidu $(A, \circ)$, on je tačan i za valuaciju a. Dakle $t = v$ je tačan za sve valuacije na grupoidu $(B, \circ)$, pa važi na grupoidu $(B, \circ)$. ∎

Videli smo da je presek podgrupoida podgrupoid. Sledeći primer pokazuje da unija podgrupoida ne mora biti podgrupoid.

Primer 1.17 Neka je $\mathbf{Z} = (Z, +)$ grupoid, gde je Z skup celih brojeva, a $+$ sabiranje celih brojeva. Posmatrajmo skupove

$$Z_2 = \{2n \mid n \in Z\}$$

i

$$Z_3 = \{3n \mid n \in Z\}.$$

Tada su $(Z_2, +)$ i $(Z_3, +)$ podgrupoidi grupoida $(Z, +)$, ali $(Z_2 \cup Z_3, +)$ nije grupoid, pa ni podgrupoid grupoida $(Z, +)$, jer $2, 3 \in Z_2 \cup Z_3$, a $2 + 3 = 5 \notin Z_2 \cup Z_3$. △

1.4 Neke osobine grupoida

1.4.1 Neutralni element

Definicija 1.18 Element $e \in A$ je *neutralni element* grupoida $(A, \circ)$ akko važi $(\forall x \in A)\, x \circ e = e \circ x = x$.

Primer 1.19 Broj 0 je neutralni element grupoida $(Z, +)$, jer za proizvoljan ceo broj x važi $x + 0 = 0 + x = x$. △

Za grupoid $(A, \circ)$ kažemo da ima neutralni element akko postoji element e koji je neutralni element za $\circ$ tj. akko važi sledeća univerzalno egzistencijalna formula:

$$(\exists y)(\forall x)\, x \circ y = y \circ x = x.$$

Primer 1.20 Neka je $N = \{1, 2, \ldots\}$ skup prirodnih brojeva, $N_0 = N \cup \{0\}$, a $+$ operacija sabiranja. Kako je zbir dva pozitivna broja pozitivan, važi $(N, +) \prec (N_0, +)$. Pri tome $(N_0, +)$ ima neutralni element 0, a $(N, +)$ nema. $\triangle$

Prethodni primer pokazuje da se svojstvo "imati neutralni element" ne prenosi na podgrupoid grupoida. Može se pokazati da se važenje univerzalno kvantifikovanih formula na grupoidu prenosi na svaki njegov podgrupoid.

Tvrđenje 1.21 *Neka je $(A, \circ)$ grupoid i e neutralni element operacije $\circ$. Tada je e jedinstven.*

Dokaz. Neka su e_1 i e_2 proizvoljni neutralni elementi grupoida $(A, \circ)$. Pošto je e_1 neutralni element, važi $e_1 \circ x = x$ za svaki element $x \in A$, pa i za $x = e_2$ važi $e_1 \circ e_2 = e_2$. Pošto je e_2 neutralni elemnt, važi $y \circ e_2 = y$ za svako $y \in A$, pa i za $y = e_1$ važi $e_1 \circ e_2 = e_1$. Dakle važi

$$e_1 = e_1 \circ e_2 = e_2.$$

Kako su e_1 i e_2 bila dva proizvoljna neutralna elemnta grupoida $(A, \circ)$ sledi da su svaka dva neutralna elementa jednaka, pa postoji samo jedan neutralni element. ∎

1.4.2 Idempotentni element

Definicija 1.22 Neka je $(G, *)$ grupoid. Element $x \in G$ se naziva *idempotentan element* (*idempotent*) akko važi $x * x = x$. Ako su svi elementi grupoida idempotentni, tada je grupoid idempotentan.

Primer 1.23 Ako je e neutralni element grupoida $(G, *)$, tada je $e * e = e$, pa je e idempotent. Ako je A proizvoljan skup, a $\cap$ presek skupova, tada je grupoid $(\mathcal{P}(A), \cap)$ idempotentan. $\triangle$

1.4.3 Inverzni element. Asocijativnost

Definicija 1.24 Neka je $(A, \circ)$ grupoid sa neutralnim elementom e i neka $x \in A$. Element $y \in A$ je *inverzni element* elementa x akko važi

$$x \circ y = y \circ x = e.$$

Definicija 1.25 Operacija $\circ$ grupoida $(A, \circ)$ je *asocijativna* akko na grupoidu važi

$$(\forall x)(\forall y)(\forall z)\, x \circ (y \circ z) = (x \circ y) \circ z.$$

Tvrđenje 1.26 *Neka je $(A, \circ)$ grupoid sa neutralnim elementom i neka je operacija $\circ$ asocijativna. Tada svaki elemnt $x \in A$ može imati najviše jedan inverzni element.*

Dokaz. Neka su y_1 i y_2 inverzni elementi elementa $x \in A$. Tada prema definiciji inverznog elementa primenom asocijativnosti dobijamo:

$$y_1 = y_1 \circ e = y_1 \circ (x \circ y_2) = (y_1 \circ x) \circ y_2 = e \circ y_2 = y_2.$$

Dakle svaka dva inverzna elementa su jednaka, pa postoji u stvari samo jedan inverzni element. Njega označavamo sa $-x$ ako operaciju grupoida označavamo sa $+$, a sa x^{-1} inače. ∎

1.4.4 Distributivnost

Definicija 1.27 Neka je $(A, \circ, *)$ algebra tipa $(2, 2)$. Kažemo da je operacija $*$ *levo distributivna* prema operaciji $\circ$ akko važi

$$(\forall x)(\forall y)(\forall z)\, x * (y \circ z) = (x * y) \circ (x * z).$$

Analogno se definiše i desna distributivnost. Ako je $*$ i levo i desno distributivna prema operaciji $\circ$, kažemo da je $*$ distributivna prema operaciji $\circ$.

Primer 1.28 U algebri $(Z, +, \cdot)$ gde je Z skup celih brojeva, $+$ sabiranje, a $\cdot$ množenje celih brojeva operacija $\cdot$ je distributivna prema operaciji $+$. U algebri $(\mathcal{P}(S), \cup, \cap)$ gde je $\mathcal{P}(S)$ partitivni skup skupa S, $\cup$ unija, a $\cap$ presek skupova, operacija $\cup$ je distributivna prema $\cap$, a operacija $\cap$ je distributivna prema operaciji $\cup$. △

1.4.5 Uslov skraćivanja

Definicija 1.29 Grupoid $(A, \circ)$ zadovoljava uslov skraćivanja sleva akko važi kvazi-identitet

$$(\forall x)(\forall y)(\forall z)(x \circ y = x \circ z \Rightarrow y = z).$$

Analogno se definiše skraćivanje zdesna.

Primer 1.30 Skup $(N, +)$ gde je $N = \{0, 1, \ldots\}$ zadovoljava zakon skraćivanja, jer iz $k + m = k + n$ sledi $m = n$ za $m, n, k \in N$. △

1.4.6 Kvazigrupe

Definicija 1.31 Kvazigrupa je grupoid koji zadovoljava jednačine:

$$(\forall u, v \in Q)(\exists_1 x, y \in Q)(u * x = v \wedge y * u = v)$$

Primer 1.32 Ako je $Q = \{a, b, c\}$ i $*$ data sa

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

onda je $(Q, *)$ kvazigrupa. $\triangle$

Definicija 1.33 Neka je data kvazigrupa $(Q, *)$. Definišemo binarnu operaciju $\backslash$ na Q na sledeći način:

$$x \backslash y = z \text{ akko } x * z = y, \quad \text{za sve } x, y \in Q$$

Neposredno se proverava da važi:

Tvrđenje 1.34 *Grupoid $(Q, \backslash)$ je kvazigrupa.*

Tako za prethodni primer tablica za $\backslash$ je:

$\backslash$	a	b	c
a	c	a	b
b	b	c	a
c	a	b	c

Definicija 1.35 Za operaciju $\backslash$ reći ćemo da je *dualna* operaciji $*$, a za $(Q, \backslash)$ da je *dualna kvazigrupa* za $(Q, *)$. Algebru $(Q, *, \backslash)$ zvaćemo *kvazigrupno proširenje* od $(Q, *)$.

Lema 1.36 *Kvazigrupno proširenje $(Q, *, \backslash)$ zadovoljava sledeće identitete:*

1. $x \backslash (x * y) = y$
2. $x * (x \backslash y) = y$

Dokaz.

1. Prema definiciji operacije $\backslash$ je

$$x\backslash(x * y) = y \text{ akko } x * y = x * y$$

2. Ako definiciju za $\backslash$ primenimo u suprotnom smeru, dobijamo

$$x * (x\backslash y) = y \text{ akko } x\backslash y = x\backslash y$$

■

Neka je $A = \{a_1, \ldots, a_n\}$, $n \geq 1$ azbuka i neka je $(A, *, \backslash)$ kvazigrupno proširenje. Označimo sa A^+ skup svih nepraznih reči nad azbukom A. Definišemo dve unarne operacije f_* i $f_\backslash$ na A^+ sa:

Definicija 1.37 Neka je $u_i \in A$, $k \geq 1$ i neka je $a_1 \in A$ izabrani fiksni elemenat iz A. Tada

$$\begin{aligned} f_*(u_1u_2\ldots u_k) = v_1v_2\ldots v_k \text{ akko } & v_1 = a_1 * u_1, \\ & v_{i+1} = v_i * u_{i+1},\ i = 1, 2, \ldots, k-1 \\ f_\backslash(u_1u_2\ldots u_k) = v_1v_2\ldots v_k \text{ akko } & v_1 = a_1\backslash u_1, \\ & v_{i+1} = u_i\backslash u_{i+1},\ i = 1, 2, \ldots, k-1 \end{aligned}$$

Uređenu šestorku $(A, *, \backslash, a_1, f_*, f_\backslash)$ nazivamo *kvazigrupskom šifrom* nad azbukom A.

Tvrđenje 1.38 *Neka je $(A, *, \backslash, a_1, f_*, f_\backslash)$ kvazigrupska šifra nad azbukom $A = \{a_1, \ldots, a_n\}$. Tada važi $f_\backslash \circ f_* = 1_A$ gde je 1_A identičko preslikavanje.*

Dokaz. Neka je $u_i \in A$, $k \geq 1$ i $f_*(u_1u_2\ldots u_k) = v_1v_2\ldots v_k$. Tada $f_\backslash \circ f_*(u_1u_2\ldots u_k) = f_\backslash(v_1v_2\ldots v_k) = w_1w_2\ldots w_k$. Tada iz $v_1 = a_1 * u_1$, $v_{i+1} = v_i * u_{i+1}$, $w_1 = a_1\backslash v_1$, $w_{i+1} = v_i\backslash v_{i+1}$ za $i = 1, 2, \ldots, k-1$, koristeći lemu 1.36, direktno dobijamo $w_1 = a_1\backslash(a_1 * u_1) = u_1$, $w_{i+1} = v_i\backslash(v_i * u_{i+1}) = u_{i+1}$, za $i = 1, 2, \ldots, k-1$.
■

Sada je jasno, na osnovu tvrđenja 1.34, da f_* možemo koristiti kao funkciju za šifrovanje, dok $f_\backslash$ koristimo kao funkciju za dešifrovanje nad azbukom A. Naime, ako je $u \in A^+$ polazni tekst, $f_*(u)$ je odgovarajući šifrovani tekst, i važi $f_\backslash(f_*(u)) = u$.

Primer 1.39 Neka je data azbuka $Q = \{a, b, c\}$ i neka dato kvazigrupno proširenje $(Q, *, \backslash)$ gde su $*$ i $\backslash$ definisani kao u prethodnom primeru. Neka je dalje $a_1 = a$ i $u = bcaaabbca$. Tada je šifrovani tekst $v = f_*(u) = ccabcbaab$. Primenom funkcije $f_\backslash$ dobija se $f_\backslash(ccabcbaab) = bcaaabbca = u$, tj. polazni tekst. △

1.5 Faktor-grupoid grupoida

Sada ćemo govoriti o tzv. *faktor-strukturama*. Neka je dat grupoid $(A, \circ)$ i neka je $\sim$ relacija ekvivalencije skupa A. Tada važi da ako je $A/_\sim = \{a/_\sim \mid a \in A\}$ količnički skup skupa A, tada za $a, b \in A$ važi $a/_\sim = b/_\sim$ ili $a/_\sim \cap b/_\sim = \emptyset$, kao i

$$\cup_{a\in A} a/_\sim = A.$$

Prirodno se postavlja pitanje da li se pomoću operacije $\circ$ na A može definisati binarna operacija $\odot$ na $A/_\sim$.

Definicija 1.40 Za relaciju $\sim \subseteq A^2$ kažemo da je *kongruencija* grupoida $(A, \circ)$ akko je $\sim$ relacija ekvivalencije i za svaka četiri elementa $x, y, u, v \in A$ važi

$$x \sim y \wedge u \sim v \Rightarrow (x \circ u) \sim (y \circ v).$$

Poslednja osobina se naziva *saglasnost* relacije $\sim$ sa operacijom $\circ$.

Definišimo $\odot$ na $A/_\sim$ sa

$$x/_\sim \odot y/_\sim \stackrel{\text{def}}{=} (x \circ y)/_\sim \tag{1.1}$$

za sve $x, y \in A$.

Tvrđenje 1.41 *$\odot$ definisana sa 1.1 jeste operacija na $A/_\sim$ akko je*

$$x \sim u, y \sim v \quad \Rightarrow \quad (x \circ y) \sim (u \circ v) \tag{1.2}$$

tj. $\sim$ je kongruencija na A.

Dokaz. Pretpostavimo da je 1.2 tačno. Tada, ako je $x/_\sim = u/_\sim$ i $y/_\sim = v/_\sim$ imamo $x \sim u$ i $y \sim v$, pa iz 1.2 dobijamo $(x \circ y) \sim (u \circ v)$, odnosno $(x \circ y)/_\sim = (u \circ v)/_\sim$. Time smo pokazali da desna strana formule 1.1 zavisi samo od klasa $x/_\sim$ i $y/_\sim$, a ne i od njihovih predstavnika tj. formulom 1.1 je definisana operacija na $A/_\sim$.

Pretpostavimo da je formulom 1.1 definisana operacija $A/_\sim$. Ako je

$$x \sim u \qquad \text{i} \qquad y \sim v,$$

imamo $x/_\sim = y/_\sim$ i $y/_\sim = v/_\sim$, pa je po formuli 1.1

$$(x \circ y)/_\sim = x/_\sim \odot y/_\sim = u/_\sim \odot v/_\sim = (u \circ v)/_\sim$$

odnosno dobijamo $(x \circ y) \sim (u \sim v)$, pa važi formula 1.2. ∎

Za dobijeni grupoid $(A/_\sim, \odot)$ kažemo da je *faktor-grupoid* na A u odnosu na $\sim$.

Primer 1.42 Neka je $A = \{e, a, b, c\}$ i neka je operacija $\circ$ definisana sa:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Neka je relacija $\sim$ data particijom $\{e, a\}, \{b, c\}$ skupa A. Tada je $A/_\sim = \{\{e, a\}, \{b, c\}\}$. Lako se proverava da je relacija $\sim$ kongruencija. Grupoid $(A/_\sim, \odot)$ ima tablicu operacije datu sa:

$\odot$	$e/_\sim$	$b/_\sim$
$e/_\sim$	$e/_\sim$	$b/_\sim$
$b/_\sim$	$b/_\sim$	$e/_\sim$

Na A postoje i relacije koje nisu kongruencije. Na primer, neka je $A/_\beta = \{\{e, a\}, \{b\}, \{c\}\}$. Tada je $e\,\beta\,a$ i $b\,\beta\,b$ ali nije $(e \circ b)\,\beta(a \circ b)$, tj. nije $b\,\beta\,c$. $\triangle$

Sledeće tvrđenje govori o vezi između grupoida $(A, \circ)$ i $(A/_\sim, \odot)$.

Tvrđenje 1.43 (Drugo tvrđenje o stabilnosti) *Ako identitet važi na grupoidu* $(A, \circ)$ *onda on važi i na svakom njegovom faktor-grupoidu.*

Ovo tvrđenje je posledica opštijeg tvrđenja 1.51 koje će biti dokazano kasnije. Sledeći primer pokazuje da se na faktor-grupoid ne prenose sva svojstva polaznog grupoida.

Primer 1.44 U grupoidu $(N, \cdot)$ gde je N skup prirodnih brojeva, a $\cdot$ operacija množenja, važi zakon skraćivanja:

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

Relacija data sa

$$x \sim y \overset{\text{def}}{\iff} (x = 1 \wedge y = 1) \vee (x \neq 1 \wedge y \neq 1)$$

je relacija ekvivalencije i njene klase su $C_1 = \{1\}$ i $C_2 = \{2, 3, 4, \ldots\}$. Pošto je množenje neopadajuća funkcija, proizvod dva broja veća od jedan je broj veći od jedan. Zato je $\sim$ kongruencija. Kako je

$$C_2 \odot C_2 = C_{2\cdot 2} = C_4 = C_2 = C_{2\cdot 1} = C_2 \odot C_1,$$

ali ne važi $C_2 = C_1$, sledi da u faktor-grupoidu $(A/_\sim, \odot)$ *ne važi* zakon skraćivanja. $\triangle$

Sledeće tvrđenje pokazuje da se još neke osobine prenose na faktor-grupoid grupoida.

Tvrđenje 1.45 *Neka je $\mathcal{A} = (A, \circ)$ grupoid i $\mathcal{A}/_\sim = (A/_\sim, \odot)$ njegov faktor-grupoid po kongruenciji $\sim$. Tada važe sledeća tvrđenja.*

1. *Ako je $\mathcal{A}$ komutativan, onda je i $\mathcal{A}/_\sim$ komutativan.*
2. *Ako je $\mathcal{A}$ asocijativan, onda je i $\mathcal{A}/_\sim$ asocijativan.*
3. *Ako $\mathcal{A}$ ima neutralni element e, onda $\mathcal{A}/_\sim$ ima neutralni element $e/_\sim$.*
4. *Ako element $x \in A$ ima inverzni element y, tada element $x/_\sim$ ima inverzni element $y/_\sim$.*

Dokaz. Primetimo da su tvrđenja pod 1 i 2 specijalni slučajevi tvrđenja 1.43, a tvrđenja pod 3 i 4 specijalni slučajevi tvrđenja 1.53.

1. Neka je $\mathcal{A}$ komutativan i neka su $x/_\sim, y/_\sim \in A/_\sim$ proizvoljni. Tada je $x \circ y = y \circ x$, pa važi
$$x/_\sim \odot y/_\sim = (x \circ y)/_\sim = (y \circ x)/_\sim = y/_\sim \odot x/_\sim,$$
pa je $\mathcal{A}/_\sim$ komutativan.
2. Dokazuje se analogno prvom tvrđenju.
3. Neka je $e \in A$ neutralni element grupoida $\mathcal{A}$. Neka je $x/_\sim \in A/_\sim$ proizvoljan. Tada važi
$$x/_\sim \odot e/_\sim = (x \circ e)/_\sim = x/_\sim,$$
a takođe
$$e/_\sim \odot x/_\sim = (e \circ x)/_\sim = x/_\sim,$$
pa je $e/_\sim$ neutralni element u $\mathcal{A}/_\sim$.
4. Neka element $x \in A$ ima inverzni element y. Tada važi
$$x/_\sim \odot y/_\sim = (x \circ y)/_\sim = e/_\sim$$
i analogno
$$y/_\sim \odot x/_\sim = (y \circ x)/_\sim = e/_\sim,$$
pa je $y/_\sim$ inverzni element elementa $x/_\sim$.

■

Napomena 1.46 Često operaciju nad klasama $\odot$ obeležavamo isto kao i operaciju nad samim elementima $\circ$; značenje operacije je vidljivo iz argumenata na koje se primenjuje. $\diamond$

Primer 1.47 Neka je Z skup celih brojeva, $+$ sabiranje, a $\cdot$ množenje celih brojeva. Algebarska struktura $(Z, +, \cdot)$ je prsten celih brojeva (o prstenima ćemo više govoriti kasnije). Primetimo da su $(Z, +)$ i $(Z, \cdot)$ grupoidi. Definišimo relaciju kongruencije po modulu $m \in Z$:

$$x \equiv y \pmod{m} \overset{\text{def}}{\iff} (\exists k \in Z)\, x - y = k \cdot m.$$

Pokazaćemo da je $\equiv$ kongruencija grupoida $(Z, +)$ i grupoida $(Z, \cdot)$.

Refleksivnost Neka je $x \in Z$ proizvoljno. Kako je $x - x = 0 = 0 \cdot m$, važi $x \equiv x \pmod{m}$.

Simetričnost Neka je $x \equiv y \pmod{m}$. Za neko $k \in Z$ važi $x - y = k \cdot m$. Tada je $y - x = (-k) \cdot m$. Kako $-k \in Z$, sledi $y \equiv x \pmod{m}$.

Tranzitivnost Neka $x \equiv y \pmod{m}$ i $y \equiv z \pmod{m}$. Tada postoje $k, l \in Z$ tako da

$$x - y = k \cdot m \qquad \text{i} \qquad y - z = l \cdot m.$$

Sabiranjem ovih jednačina dobijamo $x - z = (k + l) \cdot m$, a kako $k + l \in Z$, sledi $x \equiv z \pmod{m}$.

Saglasnost sa $+$ Neka je $x \equiv y \pmod{m}$ i $u \equiv v \pmod{m}$. Tada za neke $k, l \in Z$ važi

$$x - y = k \cdot m \qquad \text{i} \qquad u - v = l \cdot m.$$

Sabiranjem ovih jednakosti dobijamo $(x+u)-(y+v) = (k+l)\cdot m$ pa $x+u \equiv y+v \pmod{m}$.

Saglasnost sa $\cdot$ Neka je $x \equiv y \pmod{m}$ i $u \equiv v \pmod{m}$. Tada za neke $k, l \in Z$ važi

$$x = y + k \cdot m \qquad \text{i} \qquad u = v + l \cdot m.$$

Odatle sledi

$$x \cdot u = y \cdot v + m \cdot (y \cdot l + k \cdot v + k \cdot l \cdot m)$$

pa $x \cdot u - y \cdot v = p \cdot m$ za $p = y \cdot l + k \cdot v + k \cdot l \cdot m$ što znači da $x \cdot u \equiv y \cdot v \pmod{m}$.

Tako smo dobili faktor-grupoide $(Z/_{\equiv}, +)$ i $(Z/_{\equiv}, \cdot)$, pa možemo posmatrati faktor-algebru $(Z/_{\equiv}, +, \cdot)$. Na sličan način se konstruišu faktor-strukture i za druge algebre. $\triangle$

1.6 Homomorfizmi

Definicija 1.48 Preslikavanje $f : A \to B$ je *homomorfizam* grupoida $(A, \circ)$ u grupoid $(B, *)$ akko važi

$$(\forall x, y \in A)\, f(x \circ y) = f(x) * f(y).$$

Ako je homomorfizam 1-1 preslikavanje, naziva se *monomorfizam* ili potapanje. Ako je homomorfizam na, onda se naziva *epimorfizam*, a za grupoid $(B, *)$ kažemo da je *homomorfna slika* grupoida $(A, \circ)$. Ako je homomorfizam bijekcija naziva se *izomorfizam*. Homomorfizam f grupoida $(A, \circ)$ u isti grupoid $(A, \circ)$ naziva se *endomorfizam*, a ako je endomorfizam istovremeno i izomorfizam, onda se on naziva *automorfizam*.

Ako postoji izomorfizam grupoida $(A, \circ)$ u grupoid $(B, *)$ kažemo da su grupoidi $(A, \circ)$ i $(B, *)$ izomorfni i pišemo $(A, \circ) \cong (B, *)$.

Primer 1.49 Neka je R_e skup realnih brojeva, a R_e^+ skup pozitivnih realnih brojeva. Tada je funkcija $\ln$ (prirodni logaritam realnog broja) izomorfizam grupoida $(R_e^+, \cdot)$ u grupoid $(R_e, +)$, jer je $\ln$ bijekcija skupa R_e^+ u skup R_e i važi

$$\ln(x \cdot y) = \ln x + \ln y.$$

$\triangle$

Tvrđenje 1.50 (Osnovno tvrđenje o homomorfizmu)

1. *Neka je $\sim$ kongruencija grupoida $(G, \cdot)$. Tada je $(G/_\sim, \odot)$ homomorfna slika grupoida $(G, \cdot)$ za prirodno preslikavanje Φ dato sa $\Phi(x) = x/_\sim$.*

2. *Ako je $(G', *)$ homomorfna slika grupoida $(G, \cdot)$, tada grupoid $(G, \cdot)$ ima bar jednu kongruenciju $\sim$ takvu da $(G', *) \cong (G/_\sim, \odot)$. Ako je f homomorfizam grupoida $(G, \cdot)$ na grupoid $(G', *)$, tada je izomorfizam $\bar{\Phi}$ grupoida $(G', *)$ i $(G/_\sim, \odot)$ jedinstven i važi*

   $$\bar{\Phi} \circ \Phi = f$$

   tj. sledeći dijagram komutira:

$$\begin{array}{ccc} & G & \xrightarrow{f} & G' \\ \Phi & \downarrow & \bar{\Phi}\nearrow & \\ & G/_\sim & & \end{array}$$

Dokaz.

1. Treba dokazati da je prirodno preslikavanje dato sa $\Phi(x) = x/_\sim$ na i homomorfizam.

na Neka je $C \in G/_\sim$ klasa ekvivalencije. Ona je neprazna, pa postoji neko $x \in C$. Tada važi $C = x/_\sim$, pa je $\Phi(x) = C$.

Homomorfizam Neka su $x, y \in G$ proizvoljni. Tada je, po definiciji funkcije Φ i definiciji operacije $\odot$ na klasama:

$$\Phi(x \cdot y) = (x \cdot y)/_\sim = x/_\sim \odot y/_\sim = \Phi(x) \odot \Phi(y).$$

2. Neka je $f : G \to G'$ epimorfizam, tj. neka važi

$$f(x \cdot y) = f(x) * f(y)$$

za sve $x, y \in G$ i f je na. Pokazaćemo da je tražena kongruencija $\sim$ *jezgro preslikavanja* f, koje se definiše sa

$$x \sim y \overset{\text{def}}{\iff} f(x) = f(y).$$

Direktno iz definicije sledi da je $\sim$ relacija ekvivalencije.

Refleksivnost Kako je $f(x) = f(x)$, sledi $x \sim x$.

Simetričnost Neka je $x \sim y$. Tada je $f(x) = f(y)$, pa i $f(y) = f(x)$, što znači da je $y \sim x$.

Tranzitivnost Neka je $x \sim y$ i $y \sim z$. Tada je $f(x) = f(y)$ i $f(y) = f(z)$, pa je $f(x) = f(z)$, pa je $x \sim z$.

Sada ćemo pokazati da je $\sim$ saglasna sa operacijom $\cdot$. Neka je $x \sim y$ i $u \sim v$. Tada je $f(x) = f(y)$ i $f(u) = f(v)$. Zato je

$$f(x \cdot u) = f(x) * f(u) = f(y) * f(v) = f(y \cdot v),$$

a to po definiciji znači da je $x \cdot u \sim y \cdot v$. Dakle $\sim$ je kongruencija, pa postoji $(G/_\sim, \odot)$. Pokazaćemo da je funkcija $\bar{\Phi} : G/_\sim \to G'$ definisana sa

$$\bar{\Phi}(x/_\sim) = f(x)$$

dobro definisana i predstavlja izomorfizam grupoida $(G/_\sim, \odot)$ na grupoid $(G', *)$.

Definisanost Pošto je vrednost funkcije za datu klasu definisana preko predstavnika klase, treba dokazati da rezultat ne zavisi od izbora predstavnika. Neka su $x/_\sim, y/_\sim \in G/_\sim$ dve proizvoljne klase takve da je $x/_\sim = y/_\sim$. Tada je $x \sim y$, pa po definiciji $\sim$ važi $f(x) = f(y)$. Zato je

$$\bar{\Phi}(x/_\sim) = f(x) = f(y) = \bar{\Phi}(y/_\sim).$$

Dakle, $\bar{\Phi}$ je dobro definisana.

na Neka je sada $x' \in G'$ proizvoljan. Kako je f na, postoji $x \in G$ tako da je $f(x) = x'$. Tada je $\bar{\Phi}(x/_\sim) = f(x) = x'$. Dakle $\bar{\Phi}$ je na.

1-1 Neka je $\bar{\Phi}(x/_\sim) = \bar{\Phi}(y/_\sim)$. Tada je $f(x) = f(y)$, pa je $x \sim y$. Odatle sledi $x/_\sim = y/_\sim$, pa je $\bar{\Phi}$ 1-1.

Homomorfizam Neka su $x/_\sim, y/_\sim \in G/_\sim$ proizvoljni. Tada je

$$\begin{aligned} \bar{\Phi}(x/_\sim \odot y/_\sim) &= \bar{\Phi}((x \cdot y)/_\sim) \\ &= f(x \cdot y) \\ &= f(x) * f(y) \\ &= \bar{\Phi}(x/_\sim) * \bar{\Phi}(y/_\sim) \end{aligned}$$

Dakle $\bar{\Phi}$ je izomorfizam grupoida $(G/_\sim)$ i $(G', *)$. Kako je po definiciji $\bar{\Phi}(x/_\sim) = f(x)$, za svako $x \in G$ važi $(\bar{\Phi} \circ \Phi)(x) = f(x)$, pa je $\bar{\Phi} \circ \Phi = f$. Ako je Ψ proizvoljno preslikavanje $G/_\sim \to G'$ takvo da je $\Psi \circ \Phi = f$, tada za proizvoljno $x/_\sim \in G/_\sim$ važi

$$\begin{aligned} \Psi(x/_\sim) &= \Psi(\Phi(x)) \\ &= (\Psi \circ \Phi)(x) \\ &= f(x) \\ &= \bar{\Phi}(x/_\sim) \end{aligned}$$

pa je $\Psi = \bar{\Phi}$, što znači da je $\bar{\Phi}$ jedinstveno.

■

Tvrđenje 1.51 *Neka grupoid $(G_1, *_1)$ zadovoljava identitet $u = v$ nad jezikom $\{*\}$ i neka je $(G_2, *_2)$ homomorfna slika grupoida $(G_1, *_1)$. Tada i $(G_2, *_2)$ zadovoljava identitet $u = v$.*

Dokaz. Podsetimo se da terme nad jezikom $\{*\}$ označavamo sa $t(x_1, \ldots, x_n; *)$. Interpretacijom terma u grupoidu $(G_1, *_1)$ za date vrednosti $a_1, \ldots, a_n \in G_1$ dobijamo vrednost terma $t(a_1, \ldots, a_n; *_1)$, a interpretacijom terma u grupoidu $(G_2, *_2)$ za vrednosti $b_1, \ldots, b_n$ dobijamo vrednost $t(b_1, \ldots, b_n; *_2)$.

Neka je f homomorfizam. Pokazaćemo prvo sledeću lemu.

Lema 1.52 *Za svaki term $t(x_1, \ldots, x_n; \sigma)$ i za sve $a_1, \ldots, a_n \in G_1$ važi*

$$f(t(a_1, \ldots, a_n; *_1)) = t(f(a_1), \ldots, f(a_n); *_2).$$

Dokaz. Dokaz leme sprovodimo indukcijom po broju k operacija u termu t.

Neka je $k = 1$.Tada je $t \equiv x * y$. Po definiciji homomorfizma za svaka dva elementa $a_1, a_2 \in G_1$ važi $f(a_1 *_1 a_2) = f(a_1) *_2 f(a_2)$. Zato za proizvoljne $a_1, a_2 \in G_1$ važi

$$f(t(a_1, a_2; *_1)) = f(a_1 *_1 a_2) = f(a_1) *_2 f(a_2) = t(f(a_1), f(a_2), *_2).$$

Pretpostavimo da tvrđenje važi za sve prirodne brojeve manje od $k > 1$. Neka je t term sa k operacija. Tada je $t \equiv t' \sigma t''$ gde su t' i t'' termi sa manje od k operacija. Prema induktivnoj hipotezi tada za sve $a_1, \ldots, a_n \in G_1$ važi

$$\begin{aligned} f(t'(a_1, \ldots, a_n; *_1)) &= t'(f(a_1), \ldots, f(a_n); *_2) \\ f(t''(a_1, \ldots, a_n; *_1)) &= t''(f(a_1), \ldots, f(a_n); *_2) \end{aligned}$$

Po definiciji vrednosti terma, pošto je f homomorfizam, za proizvoljne $a_1, \ldots, a_n$ važi

$$\begin{aligned} f(t(a_1, \ldots, a_n; *_1) &= f(t'(a_1, \ldots, a_n; *_1) *_1 t''(a_1, \ldots, a_n; *_1)) \\ &= f(t'(a_1, \ldots, a_n; *_1)) *_2 f(t''(a_1, \ldots, a_n; *_1)) \\ &= t'(f(a_1), \ldots, f(a_n); *_2) *_2 t''(f(a_1), \ldots, f(a_n); *_2) \\ &= t(f(a_1), \ldots, f(a_n); *_2). \end{aligned}$$

Time je dokaz leme završen. ∎

Neka identitet $u = v$ važi na grupoidu $(G_1, *_1)$. Tada za sve vrednosti $a_1, \ldots, a_n \in G_1$ važi

$$u(a_1, \ldots, a_n; *_1) = v(a_1, \ldots, a_n; *_1).$$

Neka su $b_1, \ldots, b_n \in G_2$ proizvoljni. Pošto je f na, postoje elementi $a_1, \ldots, a_n$ tako da za $i \in \{1, \ldots, n\}$ važi $b_i = f(a_i)$. Tada prema prethodnoj lemi važi

$$\begin{aligned} u(b_1, \ldots, b_n; *_2) &= u(f(a_1), \ldots, f(a_n); *_2) \\ &= f(u(a_1, \ldots, a_n; *_1)) \\ &= f(v(a_1, \ldots, a_n; *_1)) \\ &= v(f(a_1), \ldots, f(a_n); *_2) \\ &= v(b_1, \ldots, b_n; *_2). \end{aligned}$$

Dakle identitet $u = v$ važi i na grupoidu $(G_2, *_2)$. ∎

Tvrđenja o prenošenju osobina grupoida na njegov faktor-grupoid (odeljak 1.5) specijalni su slučajevi ogovarajućih tvrđenja o homomorfizmima, jer je prirodno preslikavanje (dato sa $\Phi(x) = x/_\sim$) epimorfizam, pa je faktor-grupoid homomorfna slika polaznog grupoida.

Tvrđenje 1.53 *Neka je $(G_1, *_1)$ grupoid i $(G_2, *_2)$ homomorfna slika grupoida $(G_1, *_1)$. Tada važe sledeća tvrđenja.*

1. *Ako je* $(G_1, *_1)$ *komutativan, onda je i* $(G_2, *_2)$ *komutativan.*
2. *Ako je* $(G_1, *_1)$ *asocijativan, onda je i* $(G_2, *_2)$ *asocijativan.*
3. *Ako* $(G_1, *_1)$ *ima neutralni element* e*, onda je* $f(e)$ *neutralni element grupoida* $(G_2, *_2)$.
4. *Ako element* $x \in G_1$ *ima inverzni element* y*, onda i* $f(x)$ *ima inverzni element* $f(y)$.

Dokaz. Tvrđenja 1 i 2 su specijalni slučajevi tvrđenja 1.51, jer je grupoid komutativan akko važi identitet $x*y = y*x$, a asocijativan akko važi identitet $x*(y*z) = (x*y)*z$. Dokažimo tvrđenja 3 i 4.

3. Neka je e neutralni element grupoida $(G_1, *_1)$ i neka je $y \in G_2$ proizvoljan. Pošto je f na, postoji $x \in G_1$ tako da $f(x) = y$. Tada važi

$$f(x) *_2 f(e) = f(x *_1 e) = f(x),$$

kao i

$$f(e) *_2 f(x) = f(e *_1 x) = f(x),$$

pa je $f(e)$ neutralni element grupoida $(G_2, *_2)$.

4. Neka $(G_1, *_1)$ ima neutralni element e i neka je $y \in G_1$ inverzni element elementa $x \in G_1$ u grupoidu $(G_1, *_1)$. Tada važi

$$f(x) *_2 f(y) = f(x *_1 y) = f(e),$$

i analogno

$$f(y) *_2 f(x) = f(y *_1 x) = f(e).$$

Kako je $f(e)$ prema prethodnom tvrđenju neutralni element u grupoidu $(G_2, *_2)$, sledi da je $f(y)$ inverzni element za $f(x)$ u grupoidu $(G_2, *_2)$.

■

Kao što je pokazano pri razmatranju faktor-grupoida, postoje osobine koje se ne prenose homomorfizmom.

Tvrđenje 1.54 *Neka su dati grupoidi* $(G_1, *_1)$, $(G_2, *_2)$ *i* $(G_3, *_3)$ *i neka su* $f : G_1 \to G_2$ *i* $g : G_2 \to G_3$ *homomorfizmi. Tada je* $g \circ f : G_1 \to G_3$ *homomorfizam.*

Dokaz. Neka su $x, y \in G_1$ proizvoljni. Tada važi

$$\begin{aligned}(g \circ f)(x *_1 y) &= g(f(x *_1 y)) \\ &= g(f(x) *_2 f(y)) \\ &= g(f(x)) *_3 g(f(y)) \\ &= (g \circ f)(x) *_3 (g \circ f)(x),\end{aligned}$$

što znači da je $g \circ f$ homomorfizam. ∎

Tvrđenje 1.55 *Neka su $(G, *_G)$, $(H, *_H)$ i $(S, *_S)$ proizvoljni grupoidi. Tada važi*

1. $G \cong G$;
2. $G \cong H \Rightarrow H \cong G$;
3. $G \cong H \wedge H \cong S \Rightarrow G \cong S$.

Dokaz.

1. Identičko preslikavanje $1_G : G \to G$ je 1-1 i na, a kako je

$$1_G(x *_G y) = x *_G y = 1_G(x) *_G 1_G(y),$$

preslikavanje 1_G je i homomorfizam. Dakle 1_G je izomorfizam.

2. Neka je $G \cong H$. Tada postoji bijekcija $f : G \to H$ koja je homomorfizam. Inverzno preslikavanje f^{-1} je takođe bijekcija. Neka je $x, y \in H$. Tada je

$$\begin{aligned}f^{-1}(x *_H y) &= f^{-1}(f(f^{-1}(x)) *_H f(f^{-1}(y)) \\ &= f^{-1}(f(f^{-1}(x) *_G f^{-1}(y))) \\ &= f^{-1}(x) *_G f^{-1}(y),\end{aligned}$$

pa je f^{-1} homomorfizam. Dakle f^{-1} je izomorfizam grupoida $(H, *_H)$ u grupoid $(G, *_G)$, pa je $H \cong G$.

3. Neka je $G \cong H$ i $H \cong S$. Tada postoji izomorfizam $f : G \to H$ i izomorfizam $g : H \to S$. Kako su f i g bijekcije, i $g \circ f : G \to S$ je bijekcija. Kako su f i g homomorfizmi, prema tvrđenju 1.54 i $g \circ f$ je homomorfizam. Zato je $g \circ f$ izomorfizam grupoida $(G, *_G)$ u grupoid $(S, *_S)$, pa $G \cong S$.

∎

Napomena 1.56 Pojam homomorfizma se definiše za proizvoljne dve univerzalne algebre istog tipa. Ako su $\mathcal{A} = (A, f_1, f_2, \ldots)$ i $\mathcal{B} = (B, g_1, g_2, \ldots)$ algebre tipa $(n_1, n_2, \ldots)$, tada za funkciju $h : A \to B$ kažemo da je homomorfizam algebre $\mathcal{A}$ u algebru $\mathcal{B}$ akko za svako i i za sve $x_1, \ldots, x_{n_i}$ važi

$$h(f_i(x_1, \ldots, x_{n_i})) = g_i(h(x_1), \ldots, h(x_{n_i})).$$

Tako se tvrđenja o homomorfizmu koja smo ovde dokazali za grupoide mogu uopštiti na univerzalne algebre. $\diamond$

1.7 Direktan proizvod

Definišimo prvo pojam direktnog proizvoda za skupove.

Definicija 1.57 *Direktan proizvod* konačnog broja skupova $A_1, \ldots, A_n$ je skup

$$A_1 \times A_2 \times \cdots A_n = \{\, (a_1, \ldots, a_n) \mid a_k \in A_k, k \in \{1, \ldots, n\}\,\}.$$

Prethodni pojam se može uopštiti na sledeći način.

Definicija 1.58 Direktan proizvod *familije skupova* $\mathcal{F} = \{A_i \mid i \in I\}$ je skup

$$\prod_{i \in I} A_i = \{f \mid f : I \to \bigcup_{i \in I} A_i, (\forall i \in I)\, f(i) \in A_i\}.$$

Primer 1.59 Neka je $I = \{1, 2\}$ i neka je $\mathcal{F} = \{A_1, A_2\}$. Tada je

$$\begin{aligned} \prod_{i \in \{1,2\}} A_i &= \{f \mid f : \{1, 2\} \to A_1 \cup A_2, f(1) \in A_1, f(2) \in A_2\} \\ &= \left\{ \begin{pmatrix} 1 & 2 \\ a_1 & a_2 \end{pmatrix} \mid a_1 \in A_1, a_2 \in A_2 \right\}. \end{aligned}$$

Postoji bijekcija između skupa $A_1 \times A_2$ i skupa $\prod_{i \in \{1,2\}} A_i$ koja elementu (a_1, a_2) dodeljuje funkciju $\left(\begin{smallmatrix} 1 & 2 \\ a_1 & a_2 \end{smallmatrix}\right)$. Primećujemo da je proizvod familije skupova uopštenje Dekartovog proizvoda skupova. $\triangle$

Definicija 1.60 Neka je dat direktan proizvod familije skupova $\prod_{i \in I} A_i$ i neka je $i \in I$ proizvoljno. Funkcija $\pi_i : \prod_{i \in I} A_i \to A_i$, definisana sa

$$\pi_i(f) = f(i)$$

se naziva *projekcija*.

Za svaki proizvod $\prod_{i\in I} A_i$ postoji familija projekcija $\{\pi_i \mid i \in I\}$.

Tvrđenje 1.61 *Ako je $A = \prod_{i\in I} A_i \neq \emptyset$, tada je svaka projekcija π_i* na *preslikavanje.*

Dokaz. Ukoliko bi za neko $i \in I$ važilo $A_i = \emptyset$ tada bi važilo i $\prod_{i\in I} A_i = \emptyset$, jer ne postoji preslikavanje $f : I \to \cup_{j\in I} A_j$ takvo da $f(i) \in A_i$. Dakle skupovi A_i, $i \in I$ su neprazni. Neka je dato proizvoljno $i \in I$ i neka je $x \in A_i$ proizvoljan element. Pošto su skupovi A_j, $j \in I$ neprazni, postoji funkcija f za koju važi $f(i) = x$ (definišemo $f(i) = x$, a egzistencija ostalih vrednosti za funkciju f sledi iz aksiome izbora). Tada važi $\pi_i(f) = f(i) = x$. Kako je $x \in A_i$ bilo proizvoljno, π_i je na. ∎

Definicija 1.62 Neka je $\mathcal{F} = \{\mathcal{G}_i \mid i \in I\}$ familija grupoida, gde je $\mathcal{G}_i = (G_i, *_i)$. Direktni proizvod familije $\mathcal{F}$ je grupoid $\prod_{i\in I} \mathcal{G}_i = (\prod_{i\in I} G_i, *)$ gde je za $f, g \in \prod_{i\in I} G_i$ vrednost $f * g \in \prod_{i\in I} G_i$ definisana sa

$$(f * g)(i) = f(i) *_i g(i).$$

Ukoliko je familija grupoida konačna, $\mathcal{F} = \{G_1, \ldots, G_n\}$, tada funkcije $f, g \in \prod_{i\in I} G_i$ posmatramo kao uređene n-torke $(a_1, \ldots, a_n)$ i $(b_1, \ldots, b_n)$, i za njih se prethodna definicija svodi na

$$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 *_1 b_1, \ldots, a_n *_n b_n).$$

Tvrđenje 1.63 *Neka je $\{(G_i, *_i) \mid i \in I\}$ familija grupoida i neka je $(G, *) = \prod_{i\in I}(G_i, *_i)$. Tada je za svako $i \in I$ projekcija $\pi_i : G \to G_i$ epimorfizam.*

Dokaz. Prema tvrđenju 1.61, funkcija π_i je na. Treba još pokazati da je homomorfizam. Neka su $f, g \in G$. Tada po definiciji projekcije i operacije $*$ na skupu G važi

$$\pi_i(f * g) = (f * g)(i) = f(i) *_i g(i) = \pi_i(f) *_i \pi_i(g),$$

što znači da je π_i homomorfizam. ∎

Tvrđenje 1.64 *Neka je $(G, *)$ direktan proizvod familije grupoida $(G_i, *_i)$. Tada važe sledeća tvrđenja.*

1. **(Treće tvrđenje o stabilnosti)** *Identitet $u = v$ važi na grupoidu $(G, *)$ akko taj identitet važi na svakom od grupoida $(G_i, *_i)$.*
2. *$e \in G$ je neutralni element grupoida $(G, *)$ akko je za svako $i \in I$ element $e(i)$ neutralni element grupoida $(G_i, *_i)$.*

3. *Element $y \in G$ je inverzni element elementa $x \in G$ akko je za svako $i \in I$ element $y(i)$ inverzan element elementa $x(i)$ u grupoidu $(G_i, *_i)$.*

Dokaz. Jedan smer ovih tvrđenja sledi direktno iz tvrđenja 1.51, a drugi smer se dobija primenom analognog postupka kao u dokazu tog tvrđenja.

1. Ukoliko identitet $u = v$ važi na grupoidu $(G, *)$, tada prema tvrđenju 1.51, identitet $u = v$ važi i na grupoidu $(G_i, *_i)$ za proizvoljno $i \in I$, jer je $(G_i, *_i)$ homomorfna slika grupoida $(G, *)$. Obrnuto, neka za svako $i \in I$ identitet $u = v$ važi na grupoidu $(G_i, *_i)$. Neka je $i \in I$ proizvoljno. Tada za proizvoljne $f_1, \ldots, f_n \in G$ važi

$$\begin{aligned} &u(f_1, \ldots, f_n; *)(i) = \\ &\quad = \pi_i(u(f_1, \ldots, f_n; *)) \\ &\quad = u(\pi_i(f_1), \ldots, \pi_i(f_n); *_i) \quad \text{jer je } \pi_i \text{ homomorfizam} \\ &\quad = v(\pi_i(f_1), \ldots, \pi_i(f_n); *_i) \quad \text{jer } u = v \text{ važi u } (G_i, *_i) \\ &\quad = \pi_i(f_1, \ldots, f_n; *) \quad \text{jer je } \pi_i \text{ homomorfizam} \\ &\quad = v(f_1, \ldots, f_n)(i). \end{aligned}$$

   Kako se funkcije $u(f_1, \ldots, f_n; *)$ i $v(f_1, \ldots, f_n; *)$ poklapaju za sve vrednosti $i \in I$, sledi

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

   Dakle $u = v$ važi na grupoidu $(G, *)$.

2. Ako je e neutralni element u grupoidu $(G, *)$, tada je za svako $i \in I$ element $e(i) \in G_i$ neutralni element u $(G_i, *_i)$ jer je $(G_i, *_i)$ homorfna slika grupoida $(G, *)$. Obrnuto, neka je za svako $i \in I$ element $e(i) \in G_i$ neutralni element za $(G_i, *_i)$. Tada za proizvoljno $x \in G$ za svako $i \in I$ važi

$$(e * x)(i) = e(i) *_i x(i) = x(i),$$

   i analogno

$$(x * e)(i) = x(i) *_i e(i) = x(i).$$

   Kako je $i \in I$ bilo proizvoljno, važi $e * x = x$ i $x * e = x$, pa je e neutralni element u $(G, *)$.

3. Ako je $y \in G$ inverzni element elementa $x \in G$ u $(G, *)$, tada je za svako $i \in I$ element $y(i) = \pi_i(y)$ inverzni element elementa $x(i) = \pi_i(x)$ jer je $(G_i, *_i)$ homomorfna slika grupoida $(G, *)$. Obrnuto, neka za je sve $i \in I$ element $y(i)$ inverzni element elementa $x(i)$ u grupoidu $(G_i, *_i)$. Tada je za svako $i \in I$

$$(x * y)(i) = x(i) *_i y(i) = e(i),$$

i

$$(y * x)(i) = y(i) *_i x(i) = e(i),$$

pa je $x * y = e$ i $y * x = e$, što znači da je y inverzni element elementa x.

■

Primetimo da kao specijalni slučaj prethodnog tvrđenja važi: direktan proizvod grupoida je komutativan akko je svaki od grupoida komutativan, a asocijativan akko je svaki od grupoida asocijativan. Napomenimo da ne moraju sva svojstva sa familije grupoida da se prenesu na direktan proizvod grupoida.

Zadatak 1.65 Pokazati da svaki grupoid $(G, \circ)$ sa dva elementa zadovoljava identitet:

$$((x \circ x) \circ x) \circ x = x \circ x. \tag{1.3}$$

Da li postoji grupoid sa tri elementa koji ne zadovoljava taj identitet?

Rešenje. Neka je $(G, \circ)$ proizvoljan grupoid takav da $|G| = 2$. Neka je $x \in G$ proizvoljan element i $y \in G \setminus \{x\}$. Pokazaćemo da za x važi identitet 1.3. Razlikujemo sledeće slučajeve u zavisnosti od definicije operacije $\circ : G^2 \to G$.

1. $x \circ x = x$. Tada su vrednosti obe strane jednakosti jednake x.

2. $x \circ x = y$. Tada se identitet svodi na

$$(y \circ x) \circ x = y.$$

Ako je $y \circ x = y$, tada se identitet svodi na $y \circ x = y$, a ako je $y \circ x = x$, tada se svodi na $x \circ x = y$. Dakle u oba slučaja identitet važi.

Prema tome, bez obzira na definiciju operacije $\circ$, identitet 1.3 važi za element x, a kako je $x \in G$ bio proizvoljan, sledi da 1.3 važi na svakom grupoidu $(G, \circ)$ za koji je $|G| = 2$.

Sa druge strane, posmatrajmo grupoid $G = (G, \circ)$ gde je $G = \{a, b, c\}$, a operacija $\circ$ je data sledećom tablicom:

$\circ$	a	b	c
a	b	a	a
b	c	a	a
c	a	a	a

Tada je za $x = a$ vrednost leve strane u 1.3 jednaka a, a desne b. Prema tome, identitet $(*)$ ne važi na ovom grupoidu. ■

Glava 2

Klasične algebarske strukture

2.1 Polugrupa

Definicija 2.1 *Polugrupa (semigrupa)* je grupoid $(G, *)$ koji zadovoljava zakon asocijativnosti:

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

Primer 2.2 Sabiranje prirodnih brojeva je asocijativna operacija, pa je $(N, +)$ polugrupa. $\triangle$

Definicija 2.3 *Monoid* je polugrupa $(G, *)$ koja ima neutralni element e:

$$(\exists e \in G)(\forall x \in G)\, x * e = e * x = x.$$

Napomena 2.4 Monoid možemo definisati i kao algebru $(G, *, e)$ na jeziku $\{\sigma, a\}$, gde je σ operacijski simbol arnosti 2 koji se interpretira kao binarna operacija $*$, a a simbol konstante koja se interpretira kao konstanta e. Tada zahtevamo da važi identitet:

$$(\forall x)(x\, \sigma\, a = a \wedge a\, \sigma\, x = x).$$

Egzistencija neutralnog elementa je tako obezbeđena interpretacijom u algebri odgovarajućeg tipa, pa je dovoljno navesti osobinu neutralnog elementa. Time je monoid definisan isključivo univerzalno kvantifikovanim formulama, što omogućava prenošenje većeg broja tvrđenja pri konstrukacijama kao što su podalgebra, homomorfizam i direktni proizvod. Slično se i druge univerzalne algebre mogu definisati na različitim jezicima. Ovaj postupak ogovara skolemizaciji i njime se eliminišu egzistencijalni kvantifikatori, ali se proširuje jezik. Mi nećemo posebno voditi računa o razlici između ova dva oblika i koristićemo onaj koji nam je u datom trenutku pogodniji. $\diamond$

Primer 2.5 Ako je $N_0 = \{0, 1, 2, \dots, \}$ i $+$ sabiranje prirodnih brojeva, tada je struktura $(N_0, +)$ monoid. Ako i konstantu 0 uključimo u jezik, dobijamo strukturu $(N, +, 0)$. $\triangle$

Pokazaćemo da u polugrupi vrednost terma ne zavisi od rasporeda zagrada oko promenljivih koje term sačinjavaju. Označimo sa $\pi(x_1, \dots, x_n)$ proizvoljan term u kome se, redom, pojavljuju promenljive $x_1, \dots, x_n$, a raspored zagrada oko njih je proizvoljan.

Tvrđenje 2.6 *Neka je $(G, *)$ polugrupa. Neka su $\pi(x_1, \dots, x_n)$ i $\pi'(x_1, \dots, x_n)$ proizvoljni termi sastavljeni od promenljivih $x_1, \dots, x_n$ u istom redosledu $x_1, \dots, x_n$. Tada za sve vrednosti $a_1, \dots, a_n \in G$ važi $\pi(a_1, \dots, a_n) = \pi'(a_1, \dots, a_n)$.*

Dokaz. Neka $(a_1, \dots, a_n)$ označava $(\dots((a_1 * a_2) * a_3) \cdots * a_n)$, što možemo definisati na sledeći način:

$$\begin{aligned} (a_1) &= a_1 \\ (a_1 a_2 \cdots a_n) &= (a_1 a_2 \cdots a_{n-1}) * a_n, \quad n > 1. \end{aligned}$$

Prvo ćemo pokazati sledeću lemu.

Lema 2.7 $(a_1 a_2 \cdots a_n) * (b_1 b_2 \cdots b_m) = (a_1 a_2 \cdots a_n b_1 b_2 \cdots b_m)$

Dokaz. Dokaz leme sprovodimo indukcijom po m. Ako je $m = 1$, tada je $(a_1 a_2 \cdots a_n) * (b_1) = (a_1 a_2 \cdots a_n) * b_1 = (a_1 a_2 \cdots a_n b_1)$. Pretpostavimo da tvrđenje važi za m. Tada primenom asocijativnosti i induktivne hipoteze dobijamo:

$$\begin{aligned} (a_1 a_2 \cdots a_n) * (b_1 b_2 \cdots b_m b_{m+1}) &= (a_1 a_2 \cdots a_n) * ((b_1 b_2 \cdots b_m) * b_{m+1}) \\ &= ((a_1 a_2 \cdots a_n) * (b_1 b_2 \cdots b_m)) * b_{m+1} \\ &= (a_1 a_2 \cdots a_n b_1 b_2 \cdots b_m) * b_{m+1} \\ &= (a_1 a_2 \cdots a_n b_1 b_2 \cdots b_m b_{m+1}), \end{aligned}$$

što znači da lema važi i za $m + 1$. ∎

Sada ćemo pokazati da za svaki term $\pi(x_1, \dots, x_n; \sigma)$ važi

$$\pi(a_1, \dots, a_n; *) = (a_1, \dots, a_n).$$

Dokaz sprovodimo indukcijom po n gde je n broj operacija σ u termu $\pi(x_1, \dots, x_n; \sigma)$. Ako je $n = 0$ tada je $\pi = x_1$, pa je $\pi(a_1) = a_1 = (a_1)$. Pretpostavimo da tvrđenje važi za svako $k < n$ za $n > 1$. Neka je $\pi(x_1, \dots, x_n; \sigma)$ term sa n operacija. Tada je $\pi \equiv \pi' \, \sigma \, \pi''$, pa je

$$\pi(a_1, \dots, a_n; *) = \pi'(a_1, \dots, a_m; *) * \pi''(a_{m+1}, \dots, a_n)$$

$$\begin{aligned} & \text{prema definiciji interpretacije} \\ = \quad & (a_1 a_2 \cdots a_m) * (a_{m+1} a_{m+2} \cdots a_n) \\ & \text{prema induktivnoj hipotezi} \\ = \quad & (a_1 a_2 \cdots a_m a_{m+1} a_{m+2} \cdots a_n) \\ & \text{prema lemi.} \end{aligned}$$

Neka su sada $\pi(x_1, \ldots, x_n)$ i $\pi'(x_1, \ldots, x_n)$ proizvoljni. Tada za proizvoljne $a_1, \ldots, a_n$ važi

$$\pi(a_1, \ldots, a_n; *) = (a_1 a_2 \cdots a_n) = \pi'(a_1, \ldots, a_n; *).$$

■

Ubuduće nećemo pisati zagrade tamo gde zbog asocijativnosti one ne utiču na vrednost terma.

Definicija 2.8 Neka je $(G, *)$ polugrupa. Tada za proizvoljno $a \in G$ vrednost $(\underbrace{aa \cdots a}_{n})$ označavamo sa a^n. Ako je $(G, *, e)$ monoid, tada definišemo i $a^0 = e$.

Prema prethodnoj lemi 2.7, u polugrupi važi

$$a^n * a^m = (\underbrace{aa \cdots a}_{n}) * (\underbrace{aa \cdots a}_{m}) = (\underbrace{aa \cdots a}_{n+m}) = a^{n+m}.$$

Lako se proverava da u monoidu ovo tvrđenje važi i za $n = 0$ ili $m = 0$.

2.1.1 Polugrupa reči

Neka je X neki skup. *Reč* nad X je svaki niz simbola (slova) $a_1 a_2 \ldots a_n$ gde $a_1, \ldots a_n \in X$. Ako neka reč ima n slova, onda kažemo da je n dužina te reči. Reč koja nema ni jedno slovo zovemo prazna reč i njena dužina je 0. Skup svih nepraznih reči nad X obeležavamo sa X^+.

Ako su w_1 i w_2 dve reči, onda je *konkatenacija* te dve reči nova reč $w_1 w_2$ koja se dobija ako se na w_1 dopiše w_2. Dakle definisali smo binarnu operaciju, konkatenaciju, na skupu X^+ sa $w_1 \cdot w_2 = w_1 w_2$. Kako važi

$$(w_1 \cdot w_2) \cdot w_3 = w_1 w_2 w_3 = w_1 \cdot (w_2 \cdot w_3)$$

sledi da je konkatenacija asocijativna operacija nad X^+, pa smo tako došli do grupoida $(X^+, \cdot)$ koji se naziva *polugrupa nepraznih reči nad* X.

Neka je K neka klasa polugrupa i neka je $\mathcal{F}$ polugrupa takva da $X \subseteq F$. Za $\mathcal{F}$ kažemo da je *slobodna nad* X *za klasu* K ako za svaku $\mathcal{A} \in K$ i svako preslikavanje $f : X \to A$ postoji *homomorfno proširenje* $\bar{f} : F \to A$ tj. homomorfizam polugrupe F u polugrupu A takav da je $\bar{f}|_X = f$.

Tvrđenje 2.9 *Neka je X neprazan skup. Tada je polugrupa svih nepraznih reči nad X slobodna polugrupa nad X u klasi svih polugrupa.*

Dokaz. Neka je $(S, *)$ proizvoljna polugrupa i neka je $f : X \to S$. Ovo preslikavanje proširujemo do homomorfizma

$$\bar{f} : X^+ \to S$$

na sledeći način. Neka je $w \in X^+$ tj. $w = a_1 \dots a_n$ gde $a_1, \dots, a_n \in X$. Tada stavljamo

$$\bar{f}(w) \stackrel{\text{def}}{=} f(a_1) * f(a_2) * \cdots * f(a_n).$$

Primetimo prvo da je $\bar{f}$ proširenje od f. Naime, $\bar{f}(a_k) = f(a_k)$ za $a_k \in X$. Pokažimo sada da je $\bar{f}$ homomorfizam grupoida $(X^+, \cdot)$ u grupoid $(S, *)$. Za $w_1 = a_1 \dots a_n$ i $w_2 = b_1 \dots b_m$ imamo

$$\begin{aligned} \bar{f}(w_1 \cdot w_2) &= \bar{f}(a_1 \dots a_n\, b_1 \dots b_m) \\ &= \bar{f}(a_1) * \cdots * \bar{f}(a_n) * \bar{f}(b_1) * \cdots * \bar{f}(b_m) \\ &= (\bar{f}(a_1) * \cdots * \bar{f}(a_n)) * (\bar{f}(b_1) * \cdots * \bar{f}(b_m)) \\ &= \bar{f}(w_1) * \bar{f}(w_2). \end{aligned}$$

■

2.2 Grupa

Definicija 2.10 Grupoid $(G, *)$ je grupa akko važi

1. $(\forall x, y, z \in G)\, x * (y * z) = (x * y) * z$
2. $(\exists e \in G)(\forall x \in G)(x * e = e * x = x \wedge (\exists y \in G)\, x * y = y * x = e)$

Dakle grupa je monoid u kome svaki element ima inverzni. Sledeća definicija je ekvivalentna prethodnoj i iz nje se dobija skolemizacijom.

Definicija 2.11 Grupa je algebarska struktura $(G, *, ^{-1}, e)$ tipa $(2, 1, 0)$ u kojoj važe sledeći identiteti:

1. $(\forall x, y, z)\, x * (y * z) = (x * y) * z$
2. $(\forall x)\, x * e = e * x = x$
3. $(\forall x)\, x * x^{-1} = x^{-1} * x = e.$

Primer 2.12 Ako je Z skup celih brojeva, $+$ sabiranje celih brojeva, a $-$ unarna operacija promene znaka, tada je struktura $(Z, +, -, 0)$ grupa. Strukture $(N, +)$ i $(N_0, +)$ nisu grupe. $\triangle$

Primer 2.13 Neka je $A = \{1, 2, 3\}$ i neka je G skup svih permutacija skupa A. Tada je

$$G = \left\{ \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix} \right\}.$$

Kompozicija dve permutacije je permutacija, pa je $(G, \circ)$ grupoid. Operacija $\circ$ je asocijativna, a preslikavanje 1_A je permutacija i važi $1_A \circ f = f \circ 1_A = f$ za svaku permutaciju $f \in G$. Svaka permutacija ima inverznu, pa važi $f \circ f^{-1} = f^{-1} \circ f = 1_A$. Dakle $(G, \circ, ^{-1}, 1_A)$ je grupa. Neposrednom proverom utvrđujemo da je $\binom{1\,2\,3}{1\,3\,2} \circ \binom{1\,2\,3}{2\,1\,3} = \binom{1\,2\,3}{3\,1\,2}$, a $\binom{1\,2\,3}{2\,1\,3} \circ \binom{1\,2\,3}{1\,3\,2} = \binom{1\,2\,3}{2\,3\,1}$, pa operacija $\circ$ nije komutativna operacija na skupu G. $\triangle$

Definicija 2.14 Grupa $(G, *)$ je komutativna (Abelova (N. Abel)) akko je $*$ komutativna operacija tj. važi

$$(\forall x, y)\, x * y = y * x.$$

Primer 2.15 Grupa $(Z, +)$ je komutativna, a grupa permutacija $(G, \circ)$ iz prethodnog primera nije komutativna. $\triangle$

Tvrđenje 2.16 *Neka je $(G, *)$ grupa. Tada su tačne sledeće formule:*

1. $x * a = y * a \Rightarrow x = y$
2. $a * x = a * y \Rightarrow x = y$
3. $(a^{-1})^{-1} = a$
4. $(a * b)^{-1} = b^{-1} * a^{-1}$.

Dokaz.

1. Neka je $x * a = y * a$. Ako jednakost pomnožimo sa desne strane sa a^{-1} dobijamo $x * a * a^{-1} = y * a * a^{-1}$, tj. $x * e = y * e$, pa važi $x = y$.
2. Dokazuje se analogno kao prethodno tvrđenje, samo što množimo sa leve strane.
3. $(a^{-1})^{-1} = (a^{-1})^{-1} * e = (a^{-1})^{-1} * a^{-1} * a = e * a = a$.
4. $(a * b)^{-1} = (a * b)^{-1} * e = (a * b)^{-1} * a * a^{-1} = (a * b)^{-1} * a * e * a^{-1} = (a * b)^{-1} * a * b * b^{-1} * a^{-1} = e * b^{-1} * a^{-1} = b^{-1} * a^{-1}$.

■

Lema 2.17 *Neka je $(G, *)$ grupa sa neutralnim elementom e. Tada je e jedinstven idempotentni element.*

Dokaz. Kako je $e * e = e$, sledi da e jeste idempotentni element. Neka je x idempotentan element. Tada je $x * x = x$. Množenjem obe strane sa x^{-1} dobijamo $x * x * x^{-1} = x * x^{-1}$ tj. $x * e = e$, pa je $x = e$. ∎

2.2.1 Podgrupa

Definicija 2.18 Neka je $(G, *_G)$ grupa, $\emptyset \neq H \subseteq G$ i neka je $*_H = *_G|_H$. Ako je struktura $(H, *_H)$ grupa, tada se ona naziva *podgrupa* grupe $(G, *_G)$ i pišemo $(H, *_H) \prec (G, *_G)$.

Primer 2.19 Trivijalna grupa $(\{e\}, *)$ je podgrupa svake grupe. Takođe je svaka grupa sama sebi podgrupa. Ove dve podgrupe se nazivaju *trivijalne podgrupe*. Podgrupa je *prava* akko je njen nosač pravi podskup nosača grupe. Ako je Z skup celih brojeva, a $+$ sabiranje, struktura $(Z, +)$ je grupa. Ako je $2Z$ skup parnih celih brojeva, tada je struktura $(2Z, +)$ prava podgrupa grupe $(Z, +)$. △

Tvrđenje 2.20 *Neka je $(G, *)$ grupa. Tada su sledeći uslovi ekvivalentni.*

1. $(H, *_H) \prec (G, *)$
2. $H \neq \emptyset$, $H \subseteq G$, $(\forall a, b \in H)(a * b \in H \wedge a^{-1} \in H)$
3. $H \neq \emptyset$, $H \subseteq G$, $(\forall a, b \in H)\, a * b^{-1} \in H$.

Dokaz.

(1) ⇒(2) Neka je $(H, *_H) \prec (G, *)$. Tada je $\emptyset \neq H \subseteq G$. Neka su $a, b \in H$ proizvoljni. Pošto je $(H, *_H)$ grupoid, sledi $a *_G b = a *_H b \in H$. Grupa $(H, *_H)$ ima neutralni element e. On je idempotentni element grupe $(G, *_G)$, pa je prema lemi 2.17 element e istovremeno i neutralni element grupe $(G, *_G)$. Element $x \in H$ ima inverzni element $y \in H$ u grupi $(H, *_H)$. Za njega važi $x *_G y = e$, odakle množenjem sa x^{-1} sa leve strane sledi $y = x^{-1}$. Dakle $x^{-1} \in H$.

(2) ⇒(3) Neka je $\emptyset \neq H \subseteq G$ i neka važi $(\forall a, b \in H)(a * b \in H \wedge a^{-1} \in H)$. Neka su $a, b \in H$ proizvoljni. Tada po pretpostavci $b^{-1} \in H$, a stoga i $a * b^{-1} \in H$.

(3) ⇒(1) Neka je $\emptyset \neq H \subseteq G$ i neka važi $(\forall a, b \in H)\, a * b^{-1} \in H$. Treba još da pokažemo da je $(H, *_H)$ grupa. Kako je $H \neq \emptyset$, postoji $x \in H$. Tada po pretpostavci $e = x * x^{-1} \in H$. Neka je $a \in H$ proizvoljan. Kako $e \in H$, sledi $a^{-1} = e * a^{-1} \in H$. Dakle u H postoji neutralni element i postoje inverzni

elementi. Neka su $a, b \in H$ proizvoljni. Tada $b^{-1} \in H$, pa $a * (b^{-1})^{-1} \in H$, tj. $a * b \in H$. Dakle $(H, *)$ je i grupoid, pa je podgrupoid grupoida $(G, *)$. Kako je $(G, *)$ grupa, $(G, *)$ je asocijativan grupoid, a identiteti se prenose na podgrupoide, te je i $(H, *_H)$ asocijativan grupoid. Dakle $(H, *_H)$ je grupa.

■

Napomena 2.21 S obzirom da se radi o operaciji i njenoj restrikciji ubuduće nećemo praviti razliku između operacije $*$ grupe $(G, *)$ i operacije $*_H$ njene podgrupe $(H, *_H)$. ◇

Tvrđenje 2.22 *Neka je* $\{H_i \mid i \in I\}$ *familija podgrupa grupe* $(G, *)$. *Tada je* $(H, *)$ *gde je* $H = \bigcap_{i \in I} H_i$ *podgrupa grupe* $(G, *)$.

Dokaz. H je neprazan skup jer bar $e \in H$. Neka su $a, b \in H$ proizvoljni. Tada za svako $i \in I$ važi $a, b \in H_i$, pa prema tvrđenju 2.20 važi $a * b^{-1} \in H_i$. Odatle sledi $a * b^{-1} \in H$, pa opet prema tvrđenju 2.20 sledi $(H, *) \prec (G, *)$. ■

Napomena 2.23 Radi kraćeg zapisa često izostavljamo binarnu operaciju $*$ $(G, *)$ grupe, pa pišemo xy umesto $x * y$. ◇

Definicija 2.24 Neka je $(H, *) \prec (G, *)$. *Leva klasa* elementa $g \in G$ s obzirom na podgrupu H je skup

$$gH = \{gh \mid h \in H\}.$$

Desna klasa elementa $g \in G$ s obzirom na podgrupu H je skup

$$Hg = \{hg \mid h \in H\}.$$

Tako za podgrupu

$$(H, \circ) = \left(\left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix} \right\}, \circ \right)$$

grupe $(G, \circ)$ date u primeru 2.13 za $g = \binom{123}{321}$ je $gH \neq Hg$, što se neposredno proverava.

Definicija 2.25 Ako je $(H, *) \prec (G, *)$ tada definišemo binarne relacije $\equiv (\mathrm{mod}_{\mathrm{L}}\, H)$ i $\equiv (\mathrm{mod}_{\mathrm{D}}\, H)$.

$$x \equiv y \,(\mathrm{mod}_{\mathrm{L}}\, H) \overset{\mathrm{def}}{\iff} x^{-1}y \in H$$
$$x \equiv y \,(\mathrm{mod}_{\mathrm{D}}\, H) \overset{\mathrm{def}}{\iff} xy^{-1} \in H$$

Lema 2.26 *Neka je* $(H,*) \prec (G,*)$. *Tada su*

$$\equiv (\mathrm{mod}_{\mathrm{L}}\, H)$$

i

$$\equiv (\mathrm{mod}_{\mathrm{D}}\, H)$$

relacije ekvivalencije na skupu G. *Pri tome za* $g \in G$ *važi* $g/_{\equiv(\mathrm{mod}_{\mathrm{L}}\, H)} = gH$ *i* $g/_{\equiv(\mathrm{mod}_{\mathrm{D}}\, H)} = Hg$.

Dokaz. Tvrđenje ćemo pokazati za $\equiv\ (\mathrm{mod}_{\mathrm{L}}\, H)$, analogno se pokazuje i za $\equiv (\mathrm{mod}_{\mathrm{D}}\, H)$.

Refleksivnost Neka je $x \in G$. Kako je $x^{-1}x = e \in H$, sledi $x \equiv x\ (\mathrm{mod}_{\mathrm{L}}\, H)$.

Simetričnost Neka je $x \equiv y\ (\mathrm{mod}_{\mathrm{L}}\, H)$. Tada je $x^{-1}y \in H$, a kako je H podgrupa, sledi

$$(x^{-1}y)^{-1} = y^{-1}(x^{-1})^{-1} = y^{-1}x \in H,$$

što znači $y \equiv x\ (\mathrm{mod}_{\mathrm{L}}\, H)$.

Tranzitivnost Neka je $x \equiv y\ (\mathrm{mod}_{\mathrm{L}}\, H)$ i $y \equiv z\ (\mathrm{mod}_{\mathrm{L}}\, H)$. Tada je $x^{-1}y \in H$ i $y^{-1}z \in H$. Kako je $(H,*)$ grupoid važi $x^{-1}yy^{-1}z \in H$ tj. $x^{-1}z \in H$, što znači $x \equiv z\ (\mathrm{mod}_{\mathrm{L}}\, H)$.

Treba još pokazati $x/_{\equiv\,(\mathrm{mod}_{\mathrm{L}}\, H)} = xH$. Neka je $a \in G$ proizvoljan element. Tada važi:

$$\begin{aligned} a \in xH &\Leftrightarrow (\exists h \in H)\, a = xh \\ &\Leftrightarrow (\exists h \in H)\, x^{-1}a = h \\ &\Leftrightarrow x^{-1}a \in H \\ &\Leftrightarrow x \equiv a\ (\mathrm{mod}_{\mathrm{L}}\, H) \\ &\Leftrightarrow a \in x/_{\equiv\,(\mathrm{mod}_{\mathrm{L}}\, H)}, \end{aligned}$$

što znači $xH = x/_{\equiv\,(\mathrm{mod}_{\mathrm{L}}\, H)}$. ∎

Lema 2.27 *Neka je* $(H,*) \prec (G,*)$. *Tada za svako* $x \in G$ *važi* $|H| = |xH|$ *i* $|H| = |Hx|$.

Dokaz. Neka je $(H,*) \prec (G,*)$ i neka je $x \in G$ proizvoljno. Dokazaćemo da je $|H| = |xH|$, analogno se dokazuje $|H| = |Hx|$. Definišimo preslikavanje $f : H \to xH$ sa $f(h) = xh$. Pokazaćemo da je f bijekcija.

1-1 Neka je $f(h_1) = f(h_2)$. Tada je $xh_1 = xh_2$. Kako u grupi važi zakon skraćivanja (tvrđenje 2.16), sledi $h_1 = h_2$.

na Neka je $xh \in xH$ proizvoljan. Tada je $f(h) = xh$.

Dakle f je 1-1 i na, pa je bijekcija; odatle sledi $|H| = |xH|$. ∎

U opštem slučaju ne mora važiti $xH = Hx$. Ukoliko je grupa $(G, *)$ komutativna, onda to važi, ali može važiti $xH = Hx$ i kada $(G, *)$ nije komutativna. Tako podgrupa

$$(H, \circ) = \left(\left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix} \right\}, \circ \right)$$

grupe $(G, \circ)$ date u primeru 2.13 zadovoljava uslov $xH = Hx$ za sve $x \in G$, a grupa $(G, \circ)$ nije komutativna. To nas dovodi do pojma normalne podgrupe.

Definicija 2.28 Podgrupa $(H, *)$ je *normalna podgrupa* grupe $(G, *)$, u oznaci $(H, *) \lhd (G, *)$, akko za svako $x \in G$ važi $xH = Hx$.

Tvrđenje 2.29 *Neka je* $(H, *) \prec (G, *)$. *Tada je* $(H, *) \lhd (G, *)$ *akko važi* $\equiv (\mathrm{mod_L}\, H) = \equiv (\mathrm{mod_D}\, H)$.

Dokaz. Prema lemi 2.26 treba dokazati da je podgrupa $(H, *)$ normalna akko za svako $x \in G$ važi $x/_{\equiv (\mathrm{mod_L}\, H)} = x/_{\equiv (\mathrm{mod_D}\, H)}$. Jedan smer trivijalno važi, jer ako su relacije $\equiv (\mathrm{mod_L}\, H)$ i $\equiv (\mathrm{mod_D}\, H)$ jednake, onda su i klase svih elemenata jednake. Obrnuto, neka za svako $x \in G$ važi $x/_{\equiv \mathrm{mod_L}\, H} = x/_{\equiv \mathrm{mod_D}\, H}$. Tada

$$\begin{aligned} x \equiv y\ (\mathrm{mod_L}\, H) &\Leftrightarrow x/_{\equiv (\mathrm{mod_L}\, H)} = y/_{\equiv (\mathrm{mod_L}\, H)} \\ &\Leftrightarrow x/_{\equiv (\mathrm{mod_D}\, H)} = y/_{\equiv (\mathrm{mod_D}\, H)} \\ &\Leftrightarrow x \equiv y\ (\mathrm{mod_D}\, H), \end{aligned}$$

a to znači $\equiv (\mathrm{mod_L}\, H) = \equiv (\mathrm{mod_D}\, H)$. ∎

Ukoliko je $\equiv (\mathrm{mod_L}\, H) = \equiv (\mathrm{mod_D}\, H)$ tada koristimo oznaku $\equiv (\mathrm{mod}\, H)$.

Tvrđenje 2.30 (O kongruencijama grupe)

1. *Ako je* $(H, *) \lhd (G, *)$, *onda je* $\equiv (\mathrm{mod}\, H)$ *kongruencija grupe* $(G, *)$.
2. *Ako je* $\sim$ *kongruencija grupe* $(G, *)$, *onda postoji* $(H, *) \lhd (G, *)$ *tako da je* $\sim = \equiv (\mathrm{mod}\, H)$.

Dokaz.

1. Neka je $(H,*) \lhd (G,*)$. Prema lemi 2.26 tada je $\equiv (\mathrm{mod}\, H)$ relacija ekvivalencije. Treba još pokazati saglasnost sa operacijom $*$. Neka je $x \equiv y$ i $u \equiv v\ (\mathrm{mod}\, H)$. Tada je $xy^{-1} \in H$ i $uv^{-1} \in H$, pa postoje $h', h'' \in H$ tako da $xy^{-1} = h'$ i $uv^{-1} = h''$, pa $x = h'y$ i $u = h''v$. Odatle je $xu = h'yh''v$. Kako $yh'' \in yH = Hy$, postoji $h \in H$ tako da je $yh'' = hy$. Tada je $xu = h'hyv$, što znači da $xu(yv)^{-1} = h'h \in H$, pa $xy \equiv yv\ (\mathrm{mod}\, H)$, što je i trebalo dokazati.
2. Neka je $\sim$ kongruencija u grupi $(G,*)$. Neka je $H = e/_\sim$ tj.

$$H = \{x \mid x \sim e\}.$$

Kako je $\sim$ refleksivna, važi $e \sim e$, pa $e \in H$. Zato je $H \neq \emptyset$. Neka $x, y \in H$. Tada je $x \sim e$ i $y \sim e$. Kako je $\sim$ refleksivna, važi $y^{-1} \sim y^{-1}$, a pošto je kongruencija, sledi $yy^{-1} \sim ey^{-1}$ tj. $e \sim y^{-1}$. Iz simetričnosti sledi $y^{-1} \sim e$, a množenjem dobijene formule sa $x \sim e$ dobijamo $xy^{-1} \sim ee$ tj. $xy^{-1} \sim e$, što znači $xy^{-1} \in H$. Dakle $(H,*) \prec (G,*)$.

Pokažimo da za svako $x \in G$ važi $xH = Hx$. Neka je $a \in G$ proizvoljan. Tada primenom saglasnosti $\sim$ sa $*$ dobijamo sledeći niz ekvivalencija:

$$\begin{aligned} a \in xH &\Leftrightarrow x^{-1}a \in H \\ &\Leftrightarrow x^{-1}a \sim e \\ &\Leftrightarrow a \sim x \\ &\Leftrightarrow ax^{-1} \sim e \\ &\Leftrightarrow ax^{-1} \in H \\ &\Leftrightarrow a \in Hx. \end{aligned}$$

To znači da je $xH = Hx$. Kako je x bilo proizvoljno, sledi $(H,*) \lhd (G,*)$. Preostaje još da se pokaže da je $\sim\, = \equiv$. Za $x, y \in G$ je

$$\begin{aligned} x \sim y &\Leftrightarrow xy^{-1} \sim e \\ &\Leftrightarrow xy^{-1} \in H \\ &\Leftrightarrow x \equiv y (\mathrm{mod}\, H). \end{aligned}$$

■

Na osnovu prethodnog tvrđenja i tvrđenja 1.41, ako je $H \lhd G$, onda možemo formirati grupu $G/_\equiv$ koju označavamo sa $G/_H$ i nazivamo *faktor-grupa*.

Neka je $\emptyset \neq A \subseteq G$. Neka je

$$S = \{H \mid (H,*) \prec (G,*), A \subseteq H\}.$$

Kako je $(G,*) \prec (G,*)$ sledi $G \in S$, pa je $S \neq \emptyset$. Zato postoji $\cap S$. Kako je presek proizvoljne familije podgrupa grupe opet podgrupa, sledi $(\cap S,*) \prec (G,*)$. Grupa

$(\cap S, *)$ se naziva *podgrupa generisana skupom* A i obeležava se sa $[A]$ (često se koristi i oznaka $\langle A \rangle$). Ako je $[A] = G$, skup A se naziva *generatorni skup* grupe G, a njegovi elementi *generatori*.

Primer 2.31 Za proizvoljnu grupu važi $G = [G]$. Neka je $G = \{e, a, b, ab\}$ i neka je operacija $*$ data sledećom tablicom.

$*$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Tada je $(G, *)$ grupa koja se naziva *Klajnova četvorna grupa*. Pri tome važi $[\{a, b\}] = G$. $\triangle$

Definicija 2.32 *Ciklična grupa* je grupa generisana jednim elementom.

U monoidu smo definisali vrednost a^k za $k \in \{0, 1, \ldots, \}$. U grupi možemo definisati a^k i za $k < 0$ tako što za $n \in \{1, 2, \ldots, \}$ definišemo $a^{-n} = (a^{-1})^n$. Može se pokazati da i za proizvoljne cele brojeve $m, n \in Z$ u grupi važi

$$a^m a^n = a^{m+n}$$

kao i

$$(a^m)^n = a^{mn}.$$

Nije teško proveriti da je

$$[\{a\}] = \{a^z \mid z \in Z\}.$$

Primer 2.33 Grupa $(Z, +)$ gde je Z skup celih brojeva, a $+$ sabiranje, je ciklična i jedan njen generator je broj 1 (-1 je takođe njen generator i može se pokazati da su ovo jedina dva generatora grupe $(Z, +)$). Grupa $(G, *)$ gde je $G = \{e, a, a^2, a^3, a^4, a^5\}$ u kojoj važi $a^5 a = e$ je takođe ciklična (ona je izomorfna grupi sabiranja po modulu 6). Jedan njen generator je a. $a^5 = a^{-1}$ je takođe generator grupe $(G, *)$. $\triangle$

Definicija 2.34 Neka je $(G, *)$ grupa. Tada se kardinalni broj $|G|$ naziva *red grupe*. Red podgrupe $[a]$ se naziva *red elementa* a u grupi $(G, *)$.

Lako se proverava da je red elementa a jednak najmanjem pozitivnom celom broju k za koji važi $a^k = e$.

Tvrđenje 2.35 (Lagranž (J. Lagrange)) *Neka je* $(G,*)$ *konačna grupa i* $(H,*) \prec (G,*)$. *Tada*

$$|H| \mid |G|.$$

Dokaz. Prema lemi 2.26 relacija $\equiv (\mathrm{mod}_D\, H)$ je relacija ekvivalencije, pa razbija skup G na disjunktne klase čija je unija ceo skup G. Neka su $a_1, \ldots, a_n$ predstavnici klasa (ima ih konačno mnogo jer je G konačna grupa) tako da svaki predstavnik pripada različitoj klasi i za svaku klasu postoji predstavnik a_i. Tada je

$$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_n,$$

a kako su klase disjunktne, sledi

$$|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_n|.$$

Prema lemi 2.27 sve klase imaju isti broj elemenata. Jedna od tih klasa je i $H = He$, pa je

$$|Ha_1| = |Ha_2| = \cdots = |Ha_n| = |H|.$$

Odatle je $|G| = n|H|$. ∎

Posledica 2.36 *Ako je* $(G,*)$ *konačna grupa i* $a \in G$ *proizvoljan, tada je*

$$a^{|G|} = e.$$

Dokaz. Neka je $a \in G$ proizvoljan. Neka je k red elementa a. Tada je prema prethodno tvrđenju $|G| = kn$ za neko $n \in N$. Zato je

$$a^{|G|} = a^{kn} = (a^k)^n = e^n = e.$$

∎

2.2.2 Reprezentacija grupe

Definicija 2.37 Neka je G proizvoljan skup, $S_G = \{f \mid f : G \xrightarrow[\text{na}]{\text{1-1}} G\}$ skup svih permutacija skupa G i $\circ$ kompozicija funkcija. Tada je $(S_G, \circ)$ grupa, pri čemu je 1_G neutralni element, a f^{-1} inverzni element permutacije f. $(S_G, \circ)$ se naziva *grupa permutacija*.

Sledeće tvrđenje govori o značaju grupe permutacija.

Tvrđenje 2.38 (Kejlija (A. Cayley) o reprezentaciji grupe) *Svaka grupa je izomorfna nekoj podgrupi grupe permutacija.*

Dokaz. Neka je $(G, *)$ proizvoljna grupa. Uočimo grupu $(S_G, \circ)$ i posmatrajmo skup

$$H = \{\sigma_a \mid a \in G\}$$

gde je $\sigma_a : G \to G$ definisana sa

$$\sigma_a(x) = ax.$$

Pokazaćemo da je $(H, \circ) \prec (S_G, \circ)$. Prvo ćemo proveriti $H \subseteq S_G$. Neka je $\sigma_a \in H$ proizvoljna funkcija. Ako je $\sigma_a(x) = \sigma_a(y)$ tada je $ax = ay$, pa kako u grupi važi zakon skraćivanja, sledi $x = y$. Dakle σ_a je 1-1. Neka je $x \in G$ proizvoljan. Tada je $a^{-1}x \in G$ i važi

$$\sigma_a(a^{-1}x) = aa^{-1}x = ex = x.$$

Kako je $x \in G$ bilo proizvoljno, sledi da je σ_a na. Dakle σ_a je bijekcija skupa G na skup G, pa $\sigma_a \in S_G$. Time smo pokazali $H \subseteq S_G$. Kako je $1_G = \sigma_e \in H$, sledi $H \neq \emptyset$. Neka su sada $\sigma_a, \sigma_b \in H$. Tada za svako $x \in G$ važi

$$(\sigma_a \circ \sigma_b)(x) = \sigma_a(\sigma_b(x)) = a\sigma_b(x) = abx = \sigma_{ab}(x),$$

pa je $\sigma_a \circ \sigma_b = \sigma_{ab}$. Dakle $(H, \circ)$ je podrupoid grupe $(S_G, \circ)$. Pokazaćemo da je on izomorfan sa grupom $(G, *)$. Neka je $\Phi : G \to H$ definisano sa

$$\Phi(a) = \sigma_a.$$

Pokazaćemo da je Φ izomorfizam, tj. da je 1-1, na i homomorfizam.

1-1 Neka je $\Phi(a) = \Phi(b)$. Tada je $\sigma_a = \sigma_b$, pa je i $\sigma_a(e) = \sigma_b(e)$, odakle sledi $ae = be$, tj. $a = b$.

na Neka je $\sigma_a \in H$ proizvoljan. Tada je $\Phi(a) = \sigma_a$.

Homomorfizam Neka su $a, b \in G$ proizvoljni. Prema prethodom, tada važi

$$\Phi(ab) = \sigma_{ab} = \sigma_a \circ \sigma_b = \Phi(a) \circ \Phi(b),$$

pa je Φ homomorfizam.

Kako je struktura $(H, \circ)$ izomorfna sa $(G, *)$, i $(H, \circ)$ je grupa, pa je podgrupa grupe $(S_G, \circ)$ (inverzni element elementa σ_a je $\sigma_{a^{-1}}$, neutralni element je σ_e). Dakle $(H, \circ)$ je podgrupa grupe $(S_G, \circ)$ koja je izomorfna grupi $(G, *)$. ∎

Lema 2.39 *Neka je $f : G \to G'$ homomorfizam grupe $(G, *)$ u grupu $(G', *')$. Neka je $e \in G$ jedinični element u grupi $(G, *)$ i $e' \in G'$ jedinični element u grupi $(G', *')$. Tada je $f(e) = e'$ i za svako $x \in G$ važi $f(x)^{-1} = f(x^{-1})$.*

Dokaz. Pošto je f homomorfizam, važi

$$f(e) = f(e * e) = f(e) *' f(e),$$

a pošto je e' jedini idempotentni element u grupi $(G', *')$, sledi $f(e) = e'$. Slično, pošto je f homomorfizam, važi

$$f(x) *' f(x^{-1}) = f(x * x^{-1}) = f(e) = e',$$

a odatle se množenjem sa obe strane sa $f(x)^{-1}$ sa leve strane dobija

$$f(x^{-1}) = f(x)^{-1}.$$

■

Napomena 2.40 Ako se grupe posmatraju na jeziku $(G, *, ^{-1}, e)$ tada prethodno tvrđenje sledi direktno po definiciji homomorfizma. ⋄

Definicija 2.41 Neka je $f : G \to G'$ homomorfizam grupe $(G, *)$ u grupu $(G', *')$. *Jezgro homomorfizma* f, u "našoj" oznaci $K(f)$, definisano je sa

$$K(f) = \{x \mid f(x) = e'\},$$

gde je e' neutralni element grupe $(G', *')$.

Lema 2.42 *Neka je* $f : G \to G'$ *homomorfizam grupa* $(G, *)$ *i* $(G', *')$. *Tada* $(K(f), *) \lhd G$.

Dokaz. Pokazali smo da za neutralni element e grupe $(G, *)$ važi $f(e) = e'$. Prema tvrđenju 1.50, homomorfizam f indukuje kongruenciju $\sim$ tako da $x \sim y \Leftrightarrow f(x) = f(y)$. Tada je $K(f) = e/_\sim$. Prema dokazu tvrđenja 2.30 tada je $(K(f), *) \lhd (G, *)$. ■

Lema 2.43 *Neka je* $f : G \to G'$ *homomorfizam grupe* $(G, *)$ *u grupu* $(G', *')$. *Tada je* f *monomorfizam akko je* $K(f) = \{e\}$.

Dokaz. ($\Rightarrow$): Neka je f monomorfizam. Pošto je $f(e) = e'$, sledi $e \in K(f)$. Neka $x \in K(f)$. Tada $f(x) = e' = f(e)$. Kako je f 1-1, sledi $x = e$. Dakle, e je jedini element skupa $K(f)$.

($\Leftarrow$): Neka je $K(f) = \{e\}$ i neka su $x, y \in G$ proizvoljni elementi za koje važi $f(x) = f(y)$. Tada je $f(x)f(y)^{-1} = e'$, pa prema tvrđenju 2.39 važi $f(x)f(y^{-1}) = e'$ tj. $f(xy^{-1}) = e'$. Odatle sledi $xy^{-1} \in K(f)$, pa je $xy^{-1} = e$. Množenjem sa y zdesna dobijamo $x = y$. Dakle, homomorfizam f je 1-1, pa je monomorfizam. ■

Primer 2.44 Neka je $\mathcal{S} = (S, \cdot)$ komutativna polugrupa sa jedinicom 1 u kojoj važe zakoni skraćivanja.

Na $\mathcal{S}^2 = (S \times S, \cdot)$ definišemo relaciju ρ ovako:

$$(a, b)\, \rho (c, d) \qquad \Leftrightarrow \qquad ad = bc.$$

Pokazaćemo da je ρ kongruencija grupoida $\mathcal{S}^2$.

R) $(a, b)\, \rho (a, b)$, jer zbog komutativnosti semigrupe važi $ab = ba$.

S) Iz $(a, b)\, \rho (c, d)$ sledi $ad = bc$. Odatle zbog komutativnosti semigrupe $\mathcal{S}$ sledi $da = cb$, tj. $cb = da$, a to po definiciji relacije ρ znači $(c, d)\, \rho (a, b)$.

T) Neka je $(a, b)\, \rho (c, d)$ i $(c, d)\, \rho (e, f)$. To znači da važi

$$\begin{aligned} ad &= bc \\ cf &= de. \end{aligned}$$

Ako prvu jednakost pomnožimo sa f sa desne strane, a drugu sa b sa leve strane, sledi

$$\begin{aligned} adf = \ & bcf \\ & bcf \ = bde \end{aligned}$$

odakle je $adf = bde$. Primenom komutativnosti i asocijativnosti dobijamo $daf = dbe$, a kako u $\mathcal{S}$ važe zakoni skraćivanja, sledi $af = be$, tj. $(a, b)\, \rho (e, f)$.

Saglasnost. Neka je $(a, b)\, \rho (c, d)$ i $(e, f)\, \rho (g, h)$. To znači da važi $ad = bc$ i $eh = fg$. Množenjem levih i desnih strana jednakosti dobijamo $adeh = bcfg$, odakle primenom asocijativnosti i komutativnosti sledi $aedh = bfcg$, tj. $(ae, bf)\, \rho (cg, dh)$, a to znači

$$(a, b) \odot (e, f) \rho (c, d) \odot (g, h).$$

Time smo pokazali da je ρ kongruencija. Zato postoji $\mathcal{S}^2/_\sim = (S^2/_\sim, \bullet)$ gde je

$$(a, b)/_\sim \bullet (c, d)/_\sim = (ac, bd)/_\sim.$$

Pokazaćemo da je $\mathcal{S}^2/_\sim$ Abelova grupa. Kao direktni proizvod komutativnih semigrupa sa jedinicom, i $\mathcal{S}^2$ je komutativna semigrupa sa jedinicom $(1, 1)$. $\mathcal{S}^2/_\sim$ je homomorfna slika od $\mathcal{S}^2$ (pri prirodnom preslikavanju), pa je i $\mathcal{S}^2/_\sim$ komutativna semigrupa sa jedinicom. Treba još pokazati egzistenciju inverznih elemenata. Neka je $(a, b)/_\sim \in \mathcal{S}^2/_\sim$ proizvoljan element. Pokazaćemo da je $(b, a)/_\sim$ njemu inverzni element. Iz

komutativnosti sledi $ab = ba$, pa $(ab)1 = (ba)1$ odnosno $(ab, ba)\,\rho(1,1)$. Prema tome $(ab, ba)/_\sim = (1,1)/_\sim$, pa važi

$$\begin{aligned}(a,b)/_\sim \bullet (b,a)/_\sim &= (a,b) \odot (b,a)/_\sim \\ &= (ab, ba)/_\sim \\ &= (1,1)/_\sim.\end{aligned}$$

$\triangle$

Napomena 2.45 Ako se radi o skupovima geometrijskog karaktera, kao na primer skup tačaka prave, ravni, prostora itd., onda su od posebnog interesa ona preslikavanja koja čuvaju neko geometrijsko svojstvo (na primer rastojanje tačaka, paralelnost pravih itd.) Izometrijske transformacije (kretanja - izometrije) prostora R^3 su preslikavanja $f : R^3 \to R^3$ koja čuvaju rastojanja $d(A, B)$ tačaka prostora. Rastojanje $d : R^3 \times R^3 \to R$ zadovoljava sledeće osobine: $d(A, B) = 0$ akko $A = B$; $d(A, B) > 0$ akko $A \neq B$; $d(A, B) = d(B, A)$ i $d(A, B) \leq d(A, C) + d(C, B)$ za sve $A, B, C \in R^3$.

Neka je $I(R^3)$ skup izometrija prostora R^3, to jest

$$I(R^3) = \{f | f : R^3 \to R^3,\, d(A, B) = d(f(A), f(B));\, A, B \in R^3\}$$

Tada važi tvrđenje: Skup izometrija u odnosu na kompoziciju preslikavanja čini grupu, tzv. **grupu izometrija** (grupa kretanja). Da je tačno prethodno tvrđenje sledi iz:

Pre svega, izometrijska preslikavanja su bijektivna preslikavanja. Proverimo injektivnost. Iz $f(A) = f(B)$ sledi $d(A, B) = d(f(A), f(B))$, dakle iz $f(A) = f(B)$ i osobine rastojanja imamo $d(A, B) = 0$, odnosno $A = B$. Slično se proverava sirjektivnost.

Dokažimo sada da je proizvod dve izomatije takođe izometrija. Neka je $f, g \in I(R^3)$, tada $d((f \circ g)(A), (f \circ g)(B)) = d(f(g(A)), f(g(B))) = d(g(A), g(B)) = d(A, B)$. Dakle, za ma koje $f, g \in I(R^3)$ sledi $f \circ g \in I(R^3)$. Asocijativnost kompozicije va zi za svako preslikavanje. Identično preslikavanje je izometrija i igra ulogu jediničnog elementa. Dokažimo još da je svaka inverzna izometrija takođe izometrija. Zaista, ako $f \in I(R^3)$, tada $d(f^{-1}(A), f^{-1}(B)) = d(f(f^{-1}(A)), f(f^{-1}(B))) = = f((\circ f^{-1})(A), (f \circ f^{-1})(B)) = d(A, B)$, jer $f \circ f^{-1} = id$, odnosno $f^{-1} \in I(R^3)$. Time smo pokazali tvrđenje

Navedimo na kraju i dva primera:

Prvo, Preslikavanje $t : R^3 \to R^3$ prostora na samog sebe koje tačku $(x, y, z) \in R^3$ preslikava u tačku $(x + m, y + n, z + p)$, nazivamo **translacija prostora**. Skup takvih preslikavanja čine **grupu translacija**. Jasno, da je to podgrupa grupe izometrija.

Drugo, skup rotacija, određenih fiksiranom tačkom, u odnosu na kompoziciju preslikavanja je grupa, tzv. **grupa rotacija**. $\diamond$

2.3 Prsten

Definicija 2.46 *Prsten* je algebarska struktura

$$(A, +, -, 0, \cdot)$$

tipa $(2, 1, 0, 2)$ koja zadovoljava sledeće identitete:

1. $(\forall x, y)\, x + y = y + x$
2. $(\forall x, y, z)\, x + (y + z) = (x + y) + z$
3. $(\forall x)\, x + 0 = x$
4. $(\forall x)\, x + (-x) = 0$
5. $(\forall x, y, z)\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. $(\forall x, y, z)(x \cdot (y + z) = x \cdot y + x \cdot z \wedge (y + z) \cdot x = y \cdot x + z \cdot x)$

Prethodnom definicijom je prsten zadat u skolemiziranom obliku. Možemo posmatrati prsten i na jeziku $(A, +, \cdot)$ i zahtevati da $+$ i $\cdot$ imaju odgovarajuće osobine: $(A, +)$ je Abelova grupa, $(A, \cdot)$ semigrupa, i važi leva i desna distributivnost $\cdot$ prema $+$.

Primer 2.47 Ako je Z skup celih brojeva, $+$ sabiranje, a $\cdot$ množenje celih brojeva, tada je $(Z, +, \cdot)$ prsten. Ako je R_e skup realnih brojeva, $+$ sabiranje, a $\cdot$ množenje realnih brojeva, tada je $(R_e, +, \cdot)$ prsten. Za $n \in \{2, 3, \dots\}$ struktura $(Z_n, +_n, \cdot_n)$ je prsten, gde je $Z_n = \{0, 1, \dots, n-1\}$, $+_n$ sabiranje po modulu n, a $\cdot_n$ množenje po modulu n. $\triangle$

Tvrđenje 2.48 *U svakom prstenu* $(A, +, \cdot)$ *važi:*

1. $x \cdot 0 = 0$
2. $x \cdot (-y) = -(x \cdot y)$
3. $(-x) \cdot y = -(x \cdot y)$
4. $(-x) \cdot (-y) = x \cdot y$

Dokaz.

1. Kako je $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$, a 0 je jedini idempotent u grupi $(A, +)$, sledi $x \cdot 0 = 0$.
2. Kako je $x \cdot (-y) + x \cdot y = x \cdot ((-y) + y) = x \cdot 0 = 0$, sledi $x \cdot (-y) = -(x \cdot y)$.
3. Pokazuje se analogno prethodnom tvrđenju.
4. Primenom prethodna dva tvrđenja dobijamo

$$(-x) \cdot (-y) = -(x \cdot (-y)) = -(-(x \cdot y)) = x \cdot y.$$

■

Napomena 2.49 Prethodno tvrđenje nam daje dobro poznate osobine brojeva Z, R_a, R_e, jer su i oni primer prstena. $\diamond$

Ako je $(P, +, \cdot)$ prsten, tada $x + (-y)$ zapisujemo sa $x - y$.

Definicija 2.50 Prsten $(A, +, \cdot)$ je *komutativan* akko je $\cdot$ komutativna operacija. Prsten sa jedinicom je prsten u kome postoji neutralni element za operaciju $\cdot$.

Definicija 2.51 Za prsten $(A, +, \cdot)$ kažemo da *nema delitelje nule* akko važi

$$(\forall x, y \in A)(x \neq 0 \wedge y \neq 0 \Rightarrow x \cdot y \neq 0).$$

Definicija 2.52 *Integralni domen* je komutativan prsten sa jedinicom bez delitelja nule.

2.4 Polje

Definicija 2.53 Struktura $(A, +, \cdot)$ se naziva *polje* akko važe sledeće formule:

1. U skupu A postoje dva različita elementa 0 i 1.
2. $(\forall x, y \in A)\, x + y = y + x$
3. $(\forall x, y, z \in A)\, x + (y + z) = (x + y) + z$
4. $(\forall x \in A)\, x + 0 = x$
5. $(\forall x \in A)(\exists y \in A)\, x + y = 0$
6. $(\forall x, y \in A)\, x \cdot y = y \cdot x$
7. $(\forall x, y, z \in A)\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
8. $(\forall x \in A)\, x \cdot 1 = x$
9. $(\forall x \in A)(x \neq 0 \Rightarrow (\exists y \in A)(x \cdot y = 1))$
10. $(\forall x, y, z \in A)\, x \cdot (y + z) = x \cdot y + x \cdot z$.

Primer 2.54 Ako je $Z_2 = \{0, 1\}$, $+_2$ sabiranje po modulu 2, a $\cdot_2$ množenje po modulu 2, tada je $(Z_2, +_2, \cdot_2)$ polje. Ako je R_e skup realnih brojeva, $+$ sabiranje, a $\cdot$ množenje realnih brojeva, tada je $(R_e, +, \cdot)$ polje. Prsten celih brojeva $(Z, +, \cdot)$ nije polje, jer ne zadovoljava formulu 9 (npr. element 2 nema inverzni element). $\triangle$

Poređenjem definicije polja i prstena zaključujemo da je svako polje prsten. Zato osobine prstena važe u svakom polju. Polje možemo posmatrati kao komutativni prsten sa jedinicom u kome svaki element različit od nule ima inverzni element u odnosu na operaciju $\cdot$.

Tvrđenje 2.55 *Neka je $(A, +, \cdot)$ polje. Tada je*

1. *$(A, +)$ komutativna grupa i*
2. *$(A \setminus \{0\}, \cdot)$ komutativna grupa.*

Dokaz.

1. Tvrđenja 1–5 u definiciji polja definišu $(A, +)$ kao komutativnu grupu.
2. Operacija $\cdot$ je po definiciji asocijativna i komutativna, a 1 je neutralni element za $\cdot$. Kako je $0 \neq 1$, sledi $1 \in A \setminus \{0\}$. Treba još pokazati da je skup $(A \setminus \{0\})$ zatvoren za $\cdot$, i da inverzni elementi, koji po definiciji polja postoje za sve elemente iz $A \setminus \{0\}$, pripadaju skupu $A \setminus \{0\}$.

   Neka $x, y \in A \setminus \{0\}$. Pretpostavimo da $x \cdot y = 0$. Tada postoji y' tako da $y \cdot y' = 1$, pa $x = x \cdot 1 = x \cdot y \cdot y' = 0 \cdot y' = 0$, što je kontradikcija sa činjenicom da $x \in A \setminus \{0\}$. Dakle pretpostavka $x \cdot y = 0$ je bila pogrešna, pa $x \cdot y \in A \setminus \{0\}$.

   Neka je $x \in A \setminus \{0\}$. Tada postoji $x' \in A$ tako da $x \cdot x' = 1$. Ukoliko bi bilo $x' = 0$, tada bi bilo $1 = x \cdot 0 = 0$, što je u suprotnosti sa definicijom elemenata 0 i 1. Dakle $x' \in A \setminus \{0\}$.

■

Posledica 2.56 *Svako polje je integralni domen.*

Dokaz. Neka je $(A, +, \cdot)$ polje. Polje je komutativni prsten sa jedinicom. Prema prethodnom tvrđenju struktura $(A \setminus \{0\}, \cdot)$ je grupa. Ako za $x, y \in A$ važi $x \neq 0$ i $y \neq 0$, tada $x, y \in A \setminus \{0\}$, pa zbog zatvorenosti grupe $(A \setminus \{0\})$ za $\cdot$ važi $x \cdot y \in A \setminus \{0\}$, a to povlači $x \cdot y \neq 0$. Dakle polje je komutativni prsten sa jedinocom bez delitelja nula, tj. integralni domen. ■

Da obrat prethodnog tvrđenja ne važi pokazuje primer prstena celih brojeva $(Z, +, \cdot)$. Ovaj prsten je komutativan, ima jedinicu 1 i nema delitelje nule, ali postoje elementi koji nemaju inverzni element.

Tvrđenje 2.57 *Svaki konačan integralni domen je polje.*

Dokaz. Neka je $(A, +, \cdot)$ integralni domen i neka je skup A konačan. Treba samo da pokažemo egzistenciju inverznih elemenata za elemente različite od 0. Neka je $a \in A \setminus \{0\}$. Kako je $\cdot$ asocijativna operacija i postoji neutralni element 1, postoje elementi a^n za $n \in \{0, 1, 2, \ldots\}$. U nizu

$$a^0, a^1, a^2, \ldots$$

javljaju se neki od elemenata skupa A, a kako je taj skup konačan, u nizu postoji samo konačan broj različitih elemenata. Zato postoje brojevi $r, s \in \{0, 1, \ldots\}$ takvi da $r < s$ i $a^r = a^s$. Odatle dobijamo $a^r - a^s = 0$, pa $a^r(1 - a^{s-r}) = 0$. Kako je $(A, +, \cdot)$ integralni domen i $a \neq 0$, svi elementi niza su različiti od nule, pa je i $a^r \neq 0$. Zato mora biti $1 - a^{s-r} = 0$, odakle sledi $a^{s-r} = 1$. Kako je $r < s$ važi $s - r - 1 \geq 0$, pa je $a \cdot a^{s-r-1} = 1$, što znači da je a^{s-r-1} inverzni element elementa a. ∎

Odsustvo delitelja nule je bitna osobina koja omogućava rešavanje jednačina. Neka je, naime, $(A, +, \cdot)$ integralni domen i neka je $x \cdot y = 0$. Ukoliko bi bilo $x \neq 0$ i $y \neq 0$, tada bi zbog odsustva delitelja nule važilo $x \cdot y \neq 0$. Dakle mora biti $x = 0$ ili $y = 0$. Obrnuto, ako je $x = 0$ ili $y = 0$, tada je $x \cdot y = 0$. Zato u integralnom domenu važi:

$$x \cdot y = 0 \Leftrightarrow x = 0 \vee y = 0.$$

Tako se rešavanje jednačina u integralnom domenu svodi na faktorizaciju.

Lema 2.58 $(A, +, \cdot)$ *je polje akko*

1. $(A, +)$ *je komutativna grupa;*
2. $(A \setminus \{0\}, \cdot)$ *je komutativna grupa i*
3. *važi distributivnost* $\cdot$ *prema* $+$.

Dokaz. Ako je $(A, +, \cdot)$ tada prema definiciji polja i tvrđenju 2.55 važe sva tri tvrđenja. Obrnuto, neka važi 1, 2 i 3. Tada su zadovoljene osobine 1–5 polja i osobine 9 i 10. Osobine 6–8 tada važe za sve elemente različite od nule. Neposrednom proverom se uveravamo da te osobine važe i ako je neki od elemenata $x, y, z \in A$ baš jednak 0. Tako za osobinu 6 ako je $x = 0$ dobijamo $0 \cdot y = 0 = y \cdot 0$, a ako je $y = 0$ dobijamo $x \cdot 0 = 0 = 0 \cdot x$. Slično se pokazuje da važe i osobine 7 i 8. ∎

Definicija 2.59 Neka u polju $(A, +, \cdot)$ važi $y \in A \setminus \{0\}$. Tada postoji y^{-1}, pa i $x \cdot y^{-1}$. Element $x \cdot y^{-1}$ nazivamo *količnik* elemenata x i y, i označavamo sa $\frac{x}{y}$, $x : y$ ili x/y.

Tvrđenje 2.60 *Neka je* $(A, +, \cdot)$ *polje i* $x, y, u, v \in A$. *Tada važi:*

$$\begin{aligned}
y, v \neq 0 \quad &\Rightarrow \quad \left(\frac{x}{y} = \frac{u}{v} \Leftrightarrow x \cdot v = u \cdot y\right) \\
y, v \neq 0 \quad &\Rightarrow \quad \frac{x}{y} \pm \frac{u}{v} = \frac{x \cdot v \pm u \cdot y}{y \cdot v} \\
y, v \neq 0 \quad &\Rightarrow \quad \frac{x}{y} \cdot \frac{u}{v} = \frac{x \cdot u}{y \cdot v} \\
y, u, v \neq 0 \quad &\Rightarrow \quad \frac{x}{y} : \frac{u}{v} = \frac{x \cdot v}{y \cdot u}
\end{aligned}$$

Dokaz. Dokaz dajemo samo za prvu formulu. Ostale osobine se dokazuju slično.

$$\begin{aligned}\frac{x}{y}=\frac{u}{v} &\Rightarrow x\cdot y^{-1}=u\cdot v^{-1} && \text{(po definiciji)}\\ &\Rightarrow x\cdot y^{-1}\cdot y\cdot v=u\cdot v^{-1}\cdot y\cdot v && \text{(množenjem sa } y\cdot v)\\ &\Rightarrow x\cdot 1\cdot v=u\cdot y\cdot 1\\ &\Rightarrow x\cdot v=y\cdot u.\end{aligned}$$

Implikacija u drugom smeru se dokazuje analogno. ∎

Definicija 2.61 Neka je $(A,+,\cdot)$ polje i e neutralni element za operaciju $\cdot$. Neka je za $n\in N$ definisano $na=\underbrace{a+a+\cdots+a}_{n}$. Neka je $S=\{n\mid ne=0\}$. Ako je $S\neq\emptyset$ tada broj $p=\min S$ nazivamo *karakteristika polja* $(A,+,\cdot)$. Ako je $S=\emptyset$, tada za polje kažemo da ima karakterisiku 0 (ili beskonačno).

Drugim rečima, karakteristika polja je red neutralnog elementa operacije $\cdot$ u grupi $(A,+)$.

Primer 2.62 U polju $(Z_2,+_2,\cdot_2)$ je $p=2$ jer je $2\ 1=1+_2 1=0$, a $1\neq 0$, pa je p najmanji prirodan broj sa tim svojstvom. Sa druge strane, polje realnih brojeva $(R_e,+,\cdot)$ ima karakteristiku 0. △

Lema 2.63 *Ako je polje konačne karakteristike $p\neq 0$, onda je karakteristika prost broj.*

Dokaz. Neka je $p\neq 0$ karakteristika polja $(A,+,\cdot)$. Pretpostavimo suprotno: p je složen broj. Tada je $p=nm$ gde $2\leq m,n<p$. Po definiciji karakteristike je $pe=0$ tj. $(mn)e=0$, što znači

$$\begin{aligned}0 &= \underbrace{\underbrace{e+\cdots+e}_{n}+\cdots+\underbrace{e+\cdots+e}_{n}}_{m}\\ &= \underbrace{e(\underbrace{e+\cdots+e}_{n})+\cdots+e(\underbrace{e+\cdots+e}_{n})}_{m}\\ &= (\underbrace{e+\cdots+e}_{m})\cdot(\underbrace{e+\cdots+e}_{n})\\ &= (me)\cdot(ne).\end{aligned}$$

Odatle sledi $me=0$ ili $ne=0$, što je kontradikcija sa pretpostavkom da je p najmanji prirodan broj sa svojstvom $pe=0$. ∎

Neka u prstenu za elemente a i b važi $a \cdot b = b \cdot a$. Tada je

$$(a+b)\cdot(a+b) = a^2 + a\cdot b + b\cdot a + b^2 = a^2 + a\cdot b + a\cdot b + b^2 = a^2 + 2(a\cdot b) + b^2.$$

Ovaj rezultat se može uopštiti primenom matematičke indukcije: ako za elemente a i b prstena $(A, +, \cdot)$ važi $a \cdot b = b \cdot a$, tada za njih važi binomna formula:

$$(a+b)^n = a^n + \sum_{k=1}^{n-1} \binom{n}{k} a^{n-k} b^k + b^n$$

Lema 2.64 *Neka je $(A, +, \cdot)$ polje karakteristike 0. Tada*

$$(\forall a \in A)(\forall n \in N)(\exists_1 x \in A)\, nx = a,$$

tj. jednačina $nx = a$ ima jedinstveno rešenje po x.

Dokaz. Neka je $a \in A$ proizvoljno i $n \in N$. Primetimo da važi

$$\begin{aligned} nx = a &\Leftrightarrow \underbrace{x + \cdots + x}_{n} = a \\ &\Leftrightarrow \underbrace{e\cdot x + \cdots + e\cdot x}_{n} = a \\ &\Leftrightarrow (\underbrace{e + \cdots + e}_{n})\cdot x = a \\ &\Leftrightarrow (ne)\cdot x = a. \end{aligned}$$

Kako je polje karakteristike 0, sledi $ne \neq 0$, pa postoji $(ne)^{-1}$. Tada množenjem poslednje jednačine sa $(ne)^{-1}$ dobijamo $x = (ne)^{-1} \cdot a$. Dakle svako rešenje jednačine je jednako $(ne)^{-1} \cdot a$. Kako je $(ne) \cdot (ne)^{-1} \cdot a = a$, sledi da $(ne)^{-1} \cdot a$ jeste rešenje. Dakle to je jedinstveno rešenje jednačine. ∎

2.5 Ideal prstena

Ako je $(G, *)$ grupoid i $A, B \subseteq G$, tada koristimo oznaku

$$AB = \{a * b \mid a \in A, b \in B\}.$$

Definicija 2.65 Neka je $(P, +, \cdot)$ prsten. Struktura $(I, +, \cdot)$ je *ideal prstena* P akko $I \subseteq P$ i važi:

1. $(I, +)$ je komutativna grupa;

2. $IP \subseteq I$, $PI \subseteq I$.

Lema 2.66 *Ako je $I \neq \emptyset$, tada je $(I, +, \cdot)$ ideal prstena $(P, +, \cdot)$ akko*

1. $(\forall a_1, a_2 \in I)\, a_1 - a_2 \in I$
2. $(\forall a \in I)(\forall r \in P)(r \cdot a \in I \wedge a \cdot r \in I)$

Dokaz. Prema tvrđenju 2.20 $(I, +)$ će biti podgrupa grupe $(P, +)$ akko važi prvi uslov. Komutativnost se, kao identitet, prenosi sa $(P, +)$ na $(I, +)$. Drugi uslov je ekvivalentan konjukciji uslova $IP \subseteq I$ i $PI \subseteq I$. ∎

Svaki prsten $(P, +, \cdot)$ ima bar dva ideala: trivijalan prsten $(\{0\}, +, \cdot)$ i ceo prsten $(P, +, \cdot)$. Ova dva ideala se nazivaju trivijalni.

Primer 2.67 Neka je $(Z, +, \cdot)$ prsten celih brojeva i $n \in N$ prirodan broj. Pokazaćemo da je $(nZ, +, \cdot)$ ideal, gde je

$$nZ = \{nz \mid z \in Z\}.$$

Kako $0 = n \cdot 0$, sledi $nZ \neq \emptyset$. Proverićemo da važe oba uslova leme 2.66.

1. Neka $nx, ny \in nZ$. Tada $nx - ny = n(x - y) \in nZ$.
2. Neka je $nx \in nZ$ i $r \in Z$. Tada $(nx)r = n(xr) \in nZ$ i $r(nx) = (rn)x = (nr)x = n(rx) \in nZ$.

△

Lema 2.68 *Neka su I_1 i I_2 ideali prstena P. Tada je i $I_1 \cap I_2$ ideal prstena P.*

Dokaz. Kako $0 \in I_1$ i $0 \in I_2$, sledi $0 \in I_1 \cap I_2$, pa je $I_1 \cap I_2 \neq \emptyset$. Proveravamo uslove leme 2.66.

1. Neka $a, b \in I_1 \cap I_2$. Tada $a, b \in I_1$, pa $a - b \in I_1$. Takođe $a, b \in I_2$, pa $a - b \in I_2$. Stoga $a - b \in I_1 \cap I_2$.
2. Neka $a \in I_1 \cap I_2$ i $r \in P$. Tada $a \in I_1$ i $r \in P$, pa kako je I_1 ideal, onda $ar \in I_1$ i $ra \in I_1$. Pošto je $a \in I_2$ i $r \in P$, a I_2 je ideal, sledi $ar \in I_2$ i $ra \in I_2$. Odatle dobijamo $ar \in I_1 \cap I_2$ i $ra \in I_1 \cap I_2$.

∎

Neka je $(I,+,\cdot)$ ideal prstena $(P,+,\cdot)$. Tada na skupu P definišemo relaciju $\sim$:

$$x \sim y \overset{\text{def}}{\Longleftrightarrow} x - y \in I.$$

Pošto je grupa $(P,+)$ komutativna, a $(I,+) \prec (P,+)$, sledi $(I,+) \lhd (P,+)$. Zato je prema tvrđenju 2.30 relacija $\sim$ kongruencija grupe $(P,+)$.

Lema 2.69 *Relacija $\sim$ je saglasna sa operacijom $\cdot$.*

Dokaz. Neka je $x \sim y$ i $u \sim v$. Tada $x - y \in I$ i $u - v \in I$. Neka je $x - y = i$ i $u - v = j$. Tada je $x = y + i$ i $u = v + j$, pa je

$$x \cdot u = (y + i) \cdot (v + j) = y \cdot v + y \cdot j + i \cdot v + i \cdot j.$$

Kako $j \in I$ i $i \in I$, a I je ideal, sledi $y \cdot j, i \cdot v, i \cdot j \in I$. Neka je $i_1 = y \cdot j + i \cdot v + i \cdot j$. Pošto je $(I,+)$ grupoid, sledi $i_1 \in I$. Zato $x \cdot u - y \cdot v = i_1 \in I$, što znači $x \cdot u \sim y \cdot v$, pa je $\sim$ saglasna sa $\cdot$. ∎

Kako je $\sim$ kongruencija u odnosu na obe operacije $+$ i $\cdot$, iz tvrđenja 1.50 sledi da se mogu definisati operacije na klasama tako da važi

$$\begin{aligned}(x + I) \oplus (y + I) &= (x + y) + I \\ (x + I) \odot (y + I) &= (x \cdot y) + I.\end{aligned}$$

Kako je prirodno preslikavanje epimorfizam, a identiteti se prenose epimorfizmom, lako se pokazuje da je struktura $(P/_\sim, \oplus, \odot)$ takođe prsten. Tako dobijen prsten se naziva faktor-prsten prstena $(P,+,\cdot)$ i označava se sa $(P/_I, +, \cdot)$.

Primer 2.70 Pokazali smo da je svaki od skupova nZ za $n \in Z$ ideal prstena $(Z,+,\cdot)$. Zato postoji faktor-prsten $(Z/_{nZ}, +, \cdot)$. Odgovarajuća kongruencija je kongruencija celih brojeva po modulu n. △

Primer 2.71 Neka su $\mathbf{I}$, $\mathbf{J}$ i $\mathbf{K}$ ideali prstena $(P,+,\cdot)$. Dokazaćemo da važi

$$\mathbf{I} \subseteq \mathbf{J} \Rightarrow \mathbf{I} + (\mathbf{J} \cap \mathbf{K}) = \mathbf{J} \cap (\mathbf{I} + \mathbf{K}).$$

gde je $\mathbf{I} + \mathbf{J} = \{i + j \mid i \in \mathbf{I}, j \in \mathbf{J}\}$.

$\subseteq$) Iz $\mathbf{I} \subseteq \mathbf{J}$ i $\mathbf{I} \subseteq \mathbf{I} + \mathbf{K}$ sledi

$$I \subseteq \mathbf{J} \cap (\mathbf{I} + \mathbf{K}). \qquad (*)$$

Iz $\mathbf{J} \cap \mathbf{K} \subseteq \mathbf{J}$ i $\mathbf{J} \cap \mathbf{K} \subseteq \mathbf{I} + \mathbf{K}$ sledi

$$\mathbf{J} \cap \mathbf{K} \subseteq \mathbf{J} \cap (\mathbf{I} + \mathbf{K}). \qquad (**)$$

Iz $(*)$ i $(**)$ sledi $\mathbf{I} + (\mathbf{J} \cap \mathbf{K}) \subseteq \mathbf{J} \cap (\mathbf{I} + \mathbf{K})$.

$\supseteq$) Neka $x \in \mathbf{J} \cap (\mathbf{I} + \mathbf{K})$. Tada $x \in \mathbf{J}$ i $x = i + k$ za neke $i \in \mathbf{I}$ i $k \in \mathbf{K}$. Kako $i \in \mathbf{I}$, sledi $i \in \mathbf{J}$. Iz $x \in \mathbf{J}$ i $i \in \mathbf{J}$ sledi $x - i \in \mathbf{J}$, tj. $k \in \mathbf{J}$. Dakle, $i \in \mathbf{I}$ i $k \in \mathbf{J} \cap \mathbf{K}$, pa $x = i + k \in \mathbf{I} + (\mathbf{J} \cap \mathbf{K})$.

$\triangle$

Glava 3

Mreže i Bulove algebre

3.1 Mreže

3.1.1 S-mreža i A-mreža

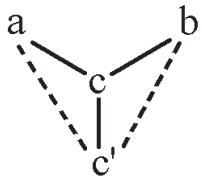
Ako je S proizvoljan skup, a $\leq$ relacija poretka (refleksivna, antisimetrična i tranzitivna) na skupu S, tada $(S, \leq)$ nazivamo parcijalno uređenje. Relaciju strogog poretka $<$ definišemo sa

$$a < b \overset{\text{def}}{\iff} a \leq b \wedge a \neq b.$$

Za element c kažemo da je *između* a i b akko $a < c < b$. Ako je $a < b$ i ne postoji element između elemenata a i b, tada kažemo da b *pokriva* a, što pišemo $a \prec b$.

Definicija 3.1 Parcijalno uređenje $(S, \leq)$ se naziva *S-mreža* akko zadovoljava:

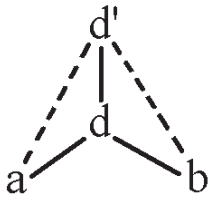
I_1: $(\forall a, b \in S)(\exists c \in S)(c \leq a, c \leq b, (\forall c' \in S)(c' \leq a, c' \leq b \Rightarrow c' \leq c))$



Slika 3.1:

Ako su c_1 i c_2 dva elementa za koje važi osobina iz I_1, tada mora biti $c_1 \leq c_2$ i $c_2 \leq c_1$, pa je $c_1 = c_2$. To znači da je element c jedinstven. Označavamo ga sa sa $\inf\{a, b\}$ ili $a \wedge b$.

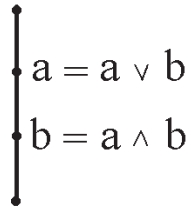
I_2: $(\forall a, b \in S)(\exists d \in S)(a \leq d, b \leq d, (\forall d' \in S)(a \leq d', b \leq d' \Rightarrow d \leq d'))$



Slika 3.2:

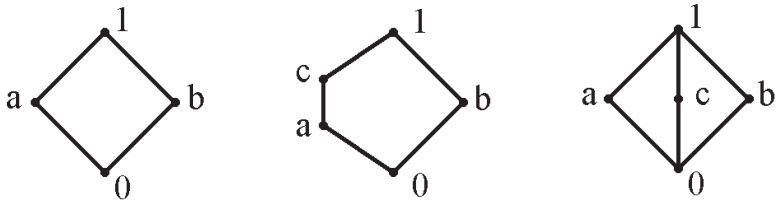
Ako su dati elementi a i b, tada odgovarajući jedinstven element d označavamo sa $\sup\{a, b\}$ ili $a \vee b$.

Primer 3.2 Svaki lanac je mreža, pri čemu je $a \wedge b = \min\{a, b\}$, a $a \vee b = \max\{a, b\}$.



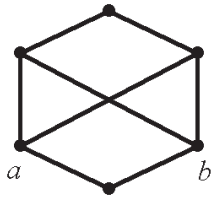
Slika 3.3:

Mreže su i strukture predstavljene sledećim Haseovim prikazima.

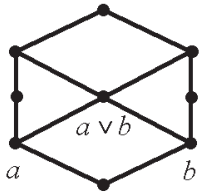


Slika 3.4:

Sledeća struktura nije mreža, jer ne postoji $a \vee b$,



ali se može dopuniti do mreže uvođenjem tri dodatna elementa.



$\triangle$

Osobine I_1 i I_2 u definiciji mreže obezbeđuju egzistenciju operacija $\wedge$ i $\vee$. Posmatraćemo sada strukturu $(S, \wedge, \vee)$.

Lema 3.3 *Neka su $a, b \in S$ proizvoljni. Tada su sledeće formule ekvivalentne:*

1. $a \leq b$
2. $a \wedge b = a$
3. $a \vee b = b$.

Dokaz.

$(1 \Rightarrow 2)$: Neka je $a \leq b$. Tada važi $a \leq a$ i $a \leq b$, pa i $a \leq a \wedge b$. Kako je $a \wedge b \leq a$, to je $a \wedge b = a$.

$(2 \Rightarrow 3)$: Neka je $a \wedge b = a$. Tada $a \leq b$. Dakle važi $a \leq b$ i $b \leq b$, pa i $a \vee b \leq b$. Kako $b \leq a \vee b$, to je $a \vee b = b$.

$(3 \Rightarrow 1)$: Neka je $a \vee b = b$. Tada je po definiciji $a \leq b$. ∎

Uočimo nekoliko jednostavnih osobina koje se često koriste u radu sa mrežama. Za svaka tri elementa x, y, z važi $x \wedge y \leq y \leq y \vee z$. Dalje, ako važi $x \leq y \wedge z$ tada važi $x \leq y$

i važi $x \leq z$. Obrnuto, ako važi $x \leq y$ i $x \leq z$, tada važi i $x \leq y \wedge z$. Dakle uslov $x \leq y \wedge z$ je ekvivalentan konjunkciji uslovu $x \leq y$ i $x \leq z$. Analogno se pokazuje da je uslov $y \vee z \leq x$ ekvivalentan konjunkciji $y \leq x$ i $z \leq x$. Tako je npr. nejednakost $a \vee b \leq c \wedge d$ ekvivalentna konjunkciji nejednakosti $a \leq c$, $a \leq d$, $b \leq c$ i $b \leq d$. Pored toga, relacija $\leq$ je saglasna sa primenom $\wedge$ i $\vee$ tj. važi

$$x \leq y \Rightarrow x \wedge z \leq y \wedge z,$$

kao i

$$x \leq y \Rightarrow x \vee z \leq y \vee z.$$

Prva saglasnost važi prema prethodnom razmatranju stoga što iz $x \leq y$ sledi $x \wedge z \leq x \leq y$ i $x \wedge z \leq z$, a druga se pokazuje analogno. Kada se u mreži dokazuju jednakosti oblika $A = B$, često se dokazuje $A \leq B$ i $B \leq A$, a odatle sledi $A = B$.

Lema 3.4 *Neka je $(S, \leq)$ S-mreža. Tada su tačne sledeće formule.*

II_1: $(\forall x \in S)\, x \wedge x = x$ ***(idempotentnost)***
$(\forall x \in S)\, x \vee x = x$
II_2: $(\forall x, y \in S)\, x \wedge y = y \wedge x$ ***(komutativnost)***
$(\forall x, y \in S)\, x \vee y = y \vee x$
II_3: $(\forall x, y, z \in S)\, x \wedge (y \wedge z) = (x \wedge y) \wedge z$ ***(asocijativnost)***
$(\forall x, y, z \in S)\, x \vee (y \vee z) = (x \vee y) \vee z$
II_4: $(\forall x, y \in S) x \wedge (x \vee y) = x$ ***(zakon apsorpcije)***
$(\forall x, y \in S) x \vee (x \wedge y) = x$

Dokaz. Dokazaćemo samo prvu polovinu tvrđenja (za operaciju $\wedge$), ostala se pokazuju analogno.

II_1: Neka je $x \in S$ proizvoljno. Kako je $x \leq x$, prema lemi 3.3 važi $x \wedge x = x$.

II_2: Dovoljno je primetiti da zamenom mesta simbolima a i b u formuli I_1 dobijamo ekvivalentnu formulu. Otud za definiciju infimuma nije bitan redosled elemenata a i b (ovo se implicitno koristi u oznaci $\inf\{a, b\}$).

II_3: Pokazaćemo da važi $x \wedge (y \wedge z) \leq (x \wedge y) \wedge z$. Dovoljno je pokazati da važi $x \wedge (y \wedge z) \leq x \wedge y$ i $x \wedge (y \wedge z) \leq z$. Prva nejednakost sledi iz $y \wedge z \leq y$ i $x \leq x$, a druga jednakost sledi iz $x \wedge (y \wedge z) \leq y \wedge z \leq z$. Tako smo pokazali

$$x \wedge (y \wedge z) \leq (x \wedge y) \wedge z.$$

Analogno se pokazuje da važi i suprotna nejednakost, odakle sledi tražena jednakost.

II_4: Kako važi $x \wedge (x \vee y) \leq x$, dovoljno je pokazati $x \leq x \wedge (x \vee y)$. Ova druga jednakost sledi iz $x \leq x$ i $x \leq x \vee y$.

■

Definicija 3.5 Neka je S proizvoljan skup, a operacije $\wedge$ i $\vee$ na skupu S zadovoljavaju osobine II_1–II_4 iz prethodnog tvrđenja. Tada se struktura $(S, \wedge, \vee)$ naziva *A-mreža*.

Posledica 3.6 *Ako je $(S, \leq)$ S-mreža, onda je $(S, \wedge, \vee)$ A-mreža.*

Dakle svaka S-mreža se može posmatrati kao A-mreža. U nastavku ćemo pokazati da važi i obrnuto.

Lema 3.7 *Neka je $(S, \wedge, \vee)$ A-mreža. Tada su za $a, b \in S$ formule $a \wedge b = a$ i $a \vee b = b$ ekvivalentne.*

Dokaz. Neka je $a \wedge b = a$. Tada je

$$a \vee b = (a \wedge b) \vee b = b$$

prema zakonu apsorpcije. Obrnuto, ako je $a \vee b = b$, tada je

$$a \wedge b = a \wedge (a \vee b) = a$$

po drugom zakonu apsorpcije. ∎

Definicija 3.8 Neka je $(S, \wedge, \vee)$ A-mreža. Definišemo relaciju $\leqslant$ sa

$$a \leqslant b \overset{\text{def}}{\iff} a \wedge b = a.$$

Tvrđenje 3.9 *Ako je $(S, \wedge, \vee)$ A-mreža, onda je $(S, \leqslant)$ S-mreža.*

Dokaz. Neka je $(S, \wedge, \vee)$ A-mreža. Treba da pokažemo da je $\leqslant$ refleksivna, antisimetrična i tranzitivna kao i da postoje infimum i supremum za svaka dva elementa iz S.

Refleksivnost Neka je $x \in S$ proizvoljno. Kako je prema zakonu apsorpcije $x \wedge x = x$, sledi $x \leqslant x$.

Antisimetričnost Neka za proizvoljne $x, y \in S$ važi $x \leqslant y$ i $y \leqslant x$. Tada je $x \wedge y = x$ i $y \wedge x = y$, pa iz komutativnosti sledi

$$x = x \wedge y = y \wedge x = y.$$

Tranzitivnost Neka za proizvoljne $x, y, z \in S$ važi $x \leqslant y$ i $y \leqslant z$. Tada je $x \wedge y = x$ i $y \wedge z = y$. Primenom asocijativnosti dobijamo

$$\begin{aligned} x \wedge z &= (x \wedge y) \wedge z \\ &= x \wedge (y \wedge z) \\ &= x \wedge y \\ &= x, \end{aligned}$$

a to po definiciji znači $x \leqslant z$.

Infimum Neka su $a, b \in S$ proizvoljni. Pokazaćemo da je $a \wedge b$ infimum elemanta a i b u odnosu na poredak $\leqslant$. Kako je primenom asocijativnosti, komutativnosti i idempotencije

$$(a \wedge b) \wedge a = (b \wedge a) \wedge a = b \wedge (a \wedge a) = b \wedge a = a \wedge b,$$

sledi $a \wedge b \leqslant a$. Analogno iz

$$(a \wedge b) \wedge b = a \wedge (b \wedge b) = a \wedge b$$

sledi $a \wedge b \leqslant b$. Neka je c' proizvoljan element za koji važi $c' \leqslant a$ i $c' \leqslant b$. Tada je $c' \wedge a = c'$ i $c' \wedge b = c'$, pa je

$$c' \wedge (a \wedge b) = (c' \wedge a) \wedge b = c' \wedge b = c',$$

što po definiciji znači $c' \leqslant a \wedge b$. Dakle $\inf\{a, b\} = a \wedge b$.

Supremum Analogno prethodnom, pokazuje se da je supremum elemenata $a, b \in S$ u odnosu na $\leqslant$ element $a \vee b$.

■

Pokazali smo da za svaku S-mrežu $(S, \leq)$ možemo konstruisati odgovarajuću A-mrežu $(S, \wedge, \vee)$, a za svaku A-mrežu $(S, \wedge, \vee)$ odgovarajuću S mreža $(S, \leqslant)$.

Lema 3.10 *Neka je $(S, \leq)$ S-mreža. Tada za S-mrežu $(S, \leqslant)$ važi $\leq = \leqslant$.*

Dokaz. Prema tvrđenju 3.3 $a \leq b$ akko $a \wedge b = a$, a prema definiciji relacije $\leqslant$ važi $a \wedge b = a$ akko $a \leqslant b$. Dakle $a \leq b$ akko $a \leqslant b$, a kako su relacije definisane nad istim skupom, znači $\leq = \leqslant$. ■

Lema 3.11 *Neka je $(S, \wedge, \vee)$ A-mreža i $(S, \leqslant)$ odgovarajuća S-mreža. Tada za A-mrežu $(S, \owedge, \overee)$ gde je $\owedge$ infimum, a $\overee$ supremum u odnosu na relaciju $\leqslant$ važi $\wedge = \owedge$ i $\vee = \overee$.*

Dokaz. Dokaz ovog tvrđenja je sadržan u dokazu tvrđenja 3.9 gde smo pokazali da je infimum za $\leqslant$ upravo $\wedge$, a supremum $\vee$. ■

Time smo pokazali da su pojmovi S-mreže i A-mreže samo različiti načini definisanja iste strukture. Zato možemo koristiti onaj oblik koji nam u datom trenutku više odgovara.

3.1.2 Podmreže

Definicija 3.12 Neka je $(S, \wedge, \vee)$ A-mreža, $T \subseteq S$ i

$$(\forall x, y \in T)\, x \wedge y, x \vee y \in T.$$

Tada se struktura $(T, \wedge, \vee)$ naziva *podmreža* mreže $(S, \wedge, \vee)$.

Pošto je A-mreža definisana identitetima koji se prenose na podstrukturu, svaka podmreža je mreža. Iz istog razloga se svojstva mreže prenose homomorfizmom i direktnim proizvodom.

Primer 3.13

1. Neka je B proizvoljan skup. Lako se proverava da je tada struktura $(\mathcal{P}(B), \cap, \cup)$ gde je $\cap$ presek, a $\cup$ unija, mreža, pri čemu je odgovarajuća relacija poretka skupovna inkluzija $\subseteq$.
2. Ako u prethodnom primeru posmatramo skup $B \times B$, dobijamo da je i $(\mathcal{P}(B \times B), \cap, \cup)$ mreža.
3. Neka je ε_B skup relacija ekvivalencije na skupu B uređenih relacijom $\subseteq$. Ako su $\alpha, \beta \in \varepsilon_B$ tada je $\alpha \cap \beta$ infimum relacija α i β jer jeste relacija ekvivalencija, važi $\alpha \cap \beta \subseteq \alpha$ i $\alpha \cap \beta \subseteq \beta$, a za proizvoljno γ za koje važi $\gamma \subseteq \alpha$ i $\gamma \subseteq \beta$ važi i $\gamma \subseteq \alpha \cap \beta$. Relacija $\alpha \cup \beta$ međutim ne mora biti relacija ekvivalencije. Najmanja relacija ekvivalencije koja sadrži α i β je tranzitivni proizvod relacija α i β: $\{\alpha, \beta\}^T$. Zato je struktura $(\varepsilon_B, \cap, \vee)$ S-mreža gde je $\alpha \vee \beta = \{\alpha, \beta\}^T$. Ova mreža *nije* podmreža mreže $(\mathcal{P}(B \times B), \cap, \cup)$ iz prethodnog primera, upravo stoga što $\vee \neq \cup$.

$\triangle$

3.1.3 Modularnost i distributivnost

Nije teško proveriti da u mreži $(\mathcal{P}(B), \cap, \cup)$ podskupova skupa B uređenih inkluzijom za svaka tri elementa $x, y, z \subseteq B$ važi

$$x \subseteq z \Rightarrow x \cup (y \cap z) = (x \cup y) \cap z,$$

kao i

$$x \cup (y \cap z) = (x \cup y) \cap (x \cup z).$$

Pokazaćemo da ova svojstva ne važe u svakoj mreži, što ćemo iskoristiti za uvođenje pojma modularne i distributivne mreže.

Lema 3.14 *Neka je $(S, \wedge, \vee)$ mreža. Tada za svaka tri elementa $x, y, z \in S$ važi*

$$x \leq z \Rightarrow x \vee (y \wedge z) \leq (x \vee y) \wedge z.$$

Dokaz. Neka je $x \leq z$. Kako važi $x \leq x \vee y$ i $x \leq z$, sledi

$$x \leq (x \vee y) \wedge z. \qquad (*)$$

Kako je $y \wedge z \leq y \vee x = x \vee y$ i $y \wedge z \leq z$, sledi

$$y \wedge z \leq (x \vee y) \wedge z. \qquad (**)$$

Iz $(*)$ i $(**)$ tada dobijamo

$$x \vee (y \wedge z) \leq (x \vee y) \wedge z.$$

■

Lema 3.15 *U svakoj mreži važi*

1. $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$
2. $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$

Dokaz.

1. Rastavljajući $\wedge$ sa desne strane i $\vee$ sa leve strane, dobijamo da je dovoljno pokazati $x \leq x \vee y$, $x \leq x \vee z$, $y \wedge z \leq x \vee y$ i $y \wedge z \leq x \vee z$, a to trivijalno važi.
2. Postupajući kao u prethodnom slučaju, nejednakost svodimo na $x \wedge y \leq x$, $x \wedge y \leq y \vee z$, $x \wedge z \leq x$ i $x \wedge z \leq y \vee z$.

■

Definicija 3.16 Mreža $(S, \wedge, \vee)$ je *modularna* akko važi

$$(\forall x, y, z \in S)(x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z).$$

Definicija 3.17 Mreža $(S, \wedge, \vee)$ je *distributivna* akko važi

$$(\forall x, y, z \in S)\, x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

Lema 3.18 *U distributivnoj mreži važi i distributivnost $\vee$ prema $\wedge$:*

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

Dokaz. Neka je $(S, \wedge, \vee)$ distributivna mreža. Primenom distributivnosti za $\wedge$ dobijamo

$$\begin{aligned}(x \vee y) \wedge (x \vee z) &= ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) \\ &= x \vee ((x \vee y) \wedge z) \\ &= x \vee (x \wedge z) \vee (y \wedge z) \\ &= x \vee (y \wedge z).\end{aligned}$$

■

Tvrđenje 3.19 *Svaka distributivna mreža je modularna.*

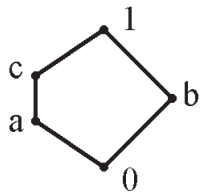
Dokaz. Neka je $(S, \wedge, \vee)$ distributivna mreža i neka su $x, y, z \in S$ proizvoljni elementi takvi da je $x \leq z$. Tada je $x \vee z = z$, pa primenom distributivnosti dobijamo

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) = (x \vee y) \wedge z.$$

■

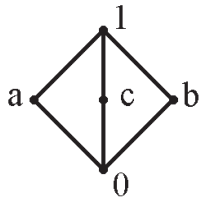
Pokazali smo da su modularne mreže posebne mreže, a distributivne mreže posebne modularne mreže. Navešćemo primere koji pokazuju da je klasa distributivnih mreža prava podklasa modularnih mreža, a ova, pak, prava podklasa klase svih mreža.

Primer 3.20 Posmatrajmo mrežu $(M, \leq)$ gde je $M = \{0, a, b, c, 1\}$, a relacija $\leq$ data sledećim Haseovim dijagramom.



Slika 3.5:

Sa slike vidimo da važi $a \leq c$, ali je $a \vee (b \wedge c) = a \vee 0 = a$ dok je $(a \vee b) \wedge c = 1 \wedge c = c$. Kako je $a \neq c$, ne važi modularni zakon. $\triangle$



Slika 3.6:

Primer 3.21 Neka je data mreža $(M, \leq)$ sa $M = \{0, a, b, c, 1\}$ i relacijom $\leq$ datom Haseovim dijagramom na slici 3.6.

Pokazaćemo da je ova mreža modularna. Neka su $x, y, z \in M$ proizvoljni i neka važi $x \leq z$. Tada mora nastupiti jedan od sledeća tri slučaja.

1. $x = z$. Tada je
$$x \vee (y \wedge z) = x \vee (y \wedge x) = x = (x \vee y) \wedge x = (x \vee y) \wedge z.$$
2. $x = 0$. Tada je
$$x \vee (y \wedge z) = 0 \vee (y \wedge z) = y \wedge z = (0 \vee y) \wedge z = (x \vee y) \wedge z.$$
3. $z = 1$. Tada je
$$x \vee (y \wedge z) = x \vee (y \wedge 1) = x \vee y = (x \vee y) \wedge 1 = (x \vee y) \wedge z.$$

Dakle ova mreža je modularna. Kako je
$$a \wedge (b \vee c) = a \wedge 1 = a,$$
a
$$(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0,$$
i $a \neq 0$, sledi da mreža nije distributivna. $\triangle$

Lema 3.22 *Mreža $(S, \wedge, \vee)$ je modularna akko za svaka tri elementa $x, y, z \in S$ važi*
$$x \wedge ((x \wedge y) \vee z) = (x \wedge y) \vee (x \wedge z). \qquad (*)$$

Dokaz.

($\Rightarrow$): Neka je mreža $(S, \wedge, \vee)$ modularna i neka su $x, y, z \in S$ proizvoljni. Pošto je mreža modularna, a važi $x \wedge y \leq x$, sledi
$$(x \wedge y) \vee (z \wedge x) = ((x \wedge y) \vee z) \wedge x.$$

Odatle se primenom komutativnosti dobija $(*)$.

($\Leftarrow$): Neka u mreži $(S, \wedge, \vee)$ za sve $x, y, z \in S$ važi $(*)$ i neka je $x \leq z$. Tada je $x \wedge z = x$, pa važi

$$\begin{aligned}(x \vee y) \wedge z &= z \wedge (x \vee y) \\ &= z \wedge ((x \wedge z) \vee y) \\ &= (x \wedge z) \vee (z \wedge y) \qquad \text{jer važi } (*) \\ &= x \vee (y \wedge z).\end{aligned}$$

■

Prethodno tvrđenje pokazuje da su i modularne, kao i distributivne mreže, strukture koje se mogu definisati identitetima. Zbog toga su podstruktura, homomorfna slika i direktni proizvod modularnih odnosno distributivih mreža modularne, odnosno distributivne mreže.

3.2 Bulove algebre

Definicija 3.23 *Bulova algebra* je struktura

$$(B, \wedge, \vee, ^-, 0, 1)$$

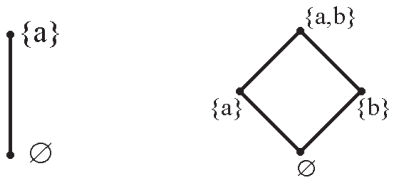
tipa $(2, 2, 1, 0, 0)$ takva da

1. $(\forall x \in B)(x \wedge 0 = 0, x \vee 0 = x \wedge 1 = x, x \vee 1 = 1)$;
2. $(B, \wedge, \vee)$ je distributivna mreža;
3. $(\forall x \in B)(x \wedge \overline{x} = 0, x \vee \overline{x} = 1)$.

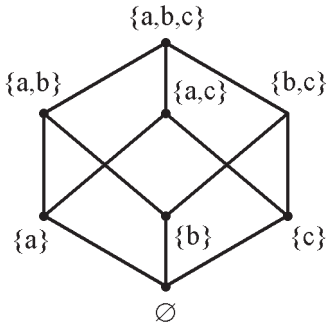
Bulova algebra se može definisati i kao distributivna mreža $(B, \wedge, \vee)$ u kojoj postoje elementi 0 i 1 tako da za svaki element $x \in B$ postoji element $y \in B$ tako da važi $x \wedge y = 0$ i $y \vee x = 1$. Pokazuje se da elementi 0 i 1 tada zadovoljavaju osobinu (1) i da su jedinstveni, a odatle sledi i jedinstvenost elementa y za dato x.

Dakle, kako se Bulova algebra može zadati sa identitetima, sledi da su podstruktura, homomorfna slika i direktni proizvod Bulovih algebri Bulove algebre.

Primer 3.24 Struktura $(\mathcal{P}(A), \cap, \cup)$ za proizvoljan skup A je Bulova algebra. Na slici su dati primeri za jednočlan, dvočlan i tročlan skup A.

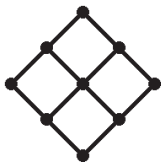


$A = \{a\}$ $A = \{a, b\}$



$A = \{a, b, c\}$

Bulove algebre su specijalne distributivne mreže. Mreža na sledećoj slici je primer distributivne mreže koja nije Bulova algebra.



$\triangle$

Primer 3.25 Neka je $\mathcal{S}$ skup svih iskaznih formula, $\sim$ binarna relacija na $\mathcal{S}$ definisana ovako:

$$\text{za } A, B \in \mathcal{S} \qquad A \sim B \quad \Leftrightarrow \quad \models A \Leftrightarrow B.$$

1. Pokažimo prvo da je $\sim$ relacija ekvivalencije. Prema definiciji $\models A \Leftrightarrow B$ akko za svaku valuaciju α važi $v_\alpha(A) = v_\alpha(B)$. Odatle primenom refleksivnosti,

simetričnosti i tranzitivnosti relacije jednakosti slede odgovarajuća svojstva relacije $\sim$. Dakle $\sim$ je relacija ekvivalencije.

2. Definišimo na skupu $\mathcal{S}/_\sim = \{A/_\sim \mid A \in \mathcal{S}\}$ operacije$\owedge, \owedge, {}^{\oslash}$ ovako:

$$\begin{aligned} A/_\sim \owedge B/_\sim &= (A \wedge B)/_\sim \\ A/_\sim \owedge B/_\sim &= (A \vee B)/_\sim \\ A/_\sim{}^{\oslash} &= (\neg A)/_\sim \\ 0 &= (A \wedge \neg A)/_\sim \\ 1 &= (A \vee \neg A)/_\sim \end{aligned}$$

Pokazaćemo da je $(\mathcal{S}/_\sim, \owedge, \owedge, {}^{\oslash}, 0, 1)$ Bulova algebra.

Prvo treba pokazati da su navedene operacije dobro definisane. Neka je $A/_\sim = A_1/_\sim$ i $B/_\sim = B_1/_\sim$. Tada za svaku valuaciju α važi $v_\alpha(A) = v_\alpha(A_1)$ i $v_\alpha(B) = v_\alpha(B_1)$. Zato za svaku valuaciju α važi $v_\alpha(A) \wedge v_\alpha(B) = v_\alpha(A_1) \wedge v_\alpha(B_1)$, tj.

$$v_\alpha(A \wedge B) = v_\alpha(A_1 \wedge B_1)$$

što znači da $(A \wedge B)/_\sim = (A_1 \wedge B_1)/_\sim$. Dakle$\owedge$ je dobro definisana. Analogno se pokazuje i za$\owedge$ i ${}^{\oslash}$. Za svake dve formule A i B važi $A \wedge \neg A \sim B \wedge \neg B$ kao i $A \vee \neg A \sim B \vee \neg B$, pa su i 0 i 1 dobro definisani. Ostaje da proverimo da važe aksiome Bulove algebre.

komutativnost: $A/_\sim \owedge B/_\sim = B/_\sim \owedge A/_\sim$ jer $\models (A \vee B) \Leftrightarrow (B \vee A)$, a $A/_\sim \owedge B/_\sim = B/_\sim \owedge A/_\sim$ jer $\models (A \vee B) \Leftrightarrow (B \vee A)$.

idempotencija: $A/_\sim \owedge A/_\sim = A/_\sim$ jer $\models (A \wedge A) \Leftrightarrow A$, a

$$A/_\sim \owedge A/_\sim = A/_\sim$$

jer $\models (A \vee A) \Leftrightarrow A$.

asocijativnost: $A/_\sim \owedge (B/_\sim \owedge C/_\sim) = (A/_\sim \owedge B/_\sim) \owedge C/_\sim$ jer

$$\models (A \wedge (B \wedge C)) \Leftrightarrow ((A \wedge B) \wedge C),$$

a $A/_\sim \owedge (B/_\sim \owedge C/_\sim) = (A/_\sim \owedge B/_\sim) \owedge C/_\sim$ jer

$$\models (A \vee (B \vee C)) \Leftrightarrow ((A \vee B) \vee C).$$

apsorpcija: $A/_\sim \owedge (A/_\sim \owedge B/_\sim) = A/_\sim$ jer $\models A \wedge (A \vee B) \Leftrightarrow A$, a $A/_\sim \owedge (A/_\sim \owedge B/_\sim) = A/_\sim$ jer $\models A \vee (A \wedge B) \Leftrightarrow A$.

distributivnost:
$A/_\sim \owedge (B/_\sim \owedge C/_\sim) = (A/_\sim \owedge B/_\sim) \owedge (A/_\sim \owedge C/_\sim)$
jer $\models (A \wedge (B \vee C)) \Leftrightarrow ((A \wedge B) \vee (A \wedge C))$.

$A/_\sim \textcircled{\wedge}\, 0 = 0$ jer

$$\begin{aligned} A/_\sim \textcircled{\wedge}\, 0 &= (A \wedge (A \wedge \neg A))/_\sim \\ &= ((A \wedge A) \wedge \neg A)/_\sim \\ &= (A \wedge \neg A)/_\sim = 0. \end{aligned}$$

$A/_\sim \textcircled{\vee}\, 1 = 1$ jer

$$\begin{aligned} A/_\sim \textcircled{\vee}\, 1 &= (A \vee (A \vee \neg A))/_\sim \\ &= ((A \vee A) \vee \neg A)/_\sim \\ &= (A \vee \neg A)/_\sim = 1. \end{aligned}$$

$$A/_\sim \textcircled{\wedge}\, A/_\sim{}^{\oslash} = A/_\sim \textcircled{\wedge}(\neg A)/_\sim = (A \wedge \neg A)/_\sim = 0$$
$$A/_\sim \textcircled{\vee}\, A/_\sim{}^{\oslash} = A/_\sim \textcircled{\vee}(\neg A)/_\sim = (A \vee \neg A)/_\sim = 1$$

Ovim je dokazano da je $(\mathcal{S}/_\sim, \textcircled{\vee}, \textcircled{\wedge}, {}^{\oslash}, 0, 1)$ Bulova algebra.

$\triangle$

3.3 Mreže podalgebri

Ako je $\mathcal{A}$ algebra, tada ćemo njen nosač obeležavati sa A. Posmatraćemo algebru $\mathcal{A}$ i skup svih njenih podalgebri $\mathrm{Sub}(\mathcal{A})$. Jasno je da je svaka podalgebra algebre $\mathcal{A}$ okarakterisana skupom $B \subseteq A$, jer operacije moraju biti restrikcije odgovarajućih operacija algebre $\mathcal{A}$. Zato možemo za algebru $\mathcal{B}$ koristiti oznaku njenog nosača: B.

Neka je $\mathcal{A}$ algebra, a $B_1, B_2 \subseteq A$ dve njene podalgebre. Tada je i $B_1 \cap B_2$ podalgebra algebre $\mathcal{A}$. $B_1 \cup B_2$ u opštem slučaju nije podalgebra, ali je skup

$$S = \{\mathcal{C} \in \mathrm{Sub}\,\mathcal{A} \mid B_1 \cup B_2 \subseteq C\}$$

neprazan pošto $A \in S$, pa postoji podalgebra $\cap S$ koju označavamo sa $[B_1 \cup B_2]$ (podalgebra generisana sa $B_1 \cup B_2$). Ako za podalgebre B_1 i B_2 definišemo $B_1 \wedge B_2 = B_1 \cap B_2$ i $B_1 \vee B_2 = [B_1 \cup B_2]$, tada je struktura $(\mathrm{Sub}(\mathcal{A}), \wedge, \vee)$ mreža. Odgovarajuća relacija poretka je skupovna inkluzija $\subseteq$ nad nosačima podalgebri.

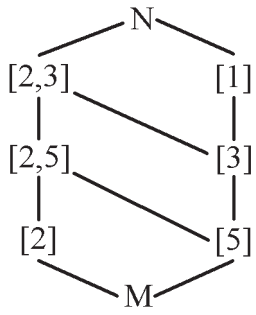
Primer 3.26 [GCBT] Neka je data algebra $(N, \varphi, 4, 7)$ gde je N skup prirodnih brojeva, a $\varphi : N \to N$ definisana sa $\varphi(x) = x + 2$. Ispitaćemo mrežu podalgebri algebre $(N, \varphi, 4, 7)$. Svaka podalgebra $B \subseteq N$ sadrži brojeve 4 i 7, a zbog zatvorenosti za operaciju φ važi

$$k \in B \Rightarrow k + 2 \in B \Rightarrow \cdots \Rightarrow k + 2n \in B, \qquad \text{za } n \in N.$$

Zato sve podalgebre sadrže prirodan broj 4 i sve brojeve 6, 7, 8, ..., pa se međusobno razlikuju samo po prisustvu ili odsustvu elemenata iz skupa $\{1,2,3,5\}$. Najmanja podalgebra je $M = \{4,6,7,\ldots\} = [\emptyset]$, a cela algebra N je generisana skupom $\{1,2\}$. Mreža sadrži sledeće elemente:

$$\begin{aligned} & M \\ [1] &= \{1,3,5\} \cup M \\ [2] &= \{2\} \cup M \\ [3] &= \{3,5\} \cup M \\ [5] &= \{5\} \cup M \\ [2,3] &= \{2,3,5\} \cup M \\ [2,5] &= \{2,5\} \cup M \\ & N \end{aligned}$$

Njihov međusobni odnos prikazan je na slici.



$\triangle$

Ako se zna da su mreže podalgebri za dve algebre međusobno izomorfne, postavlja se pitanje kakav je odnos između samih algebri. Ovo pitanje je proučavano za različite algebarske strukture.

Mreže se takođe javljaju i prilikom poređenja svih kongruencija date univerzalne algebre.

Glava 4

Tri interesantna problema

4.1 Identitet Dudeka

Univerzalne algebre možemo posmatrati kao modele teorija prvog reda. Teorije prvog reda se dobijaju kao ekstenzije predikatskog računa prvog reda sa jednakošću, pri čemu se dodaju funkcijski simboli i zadaju dodatne aksiome koje se nazivaju specijalne aksiome.

Broj operacija algebre koja predstavlja model date teorije i njihova arnost su određeni brojem i arnostima funkcijskih slova jezika teorije, a zakonitosti koje važe u algebri su određene aksiomama teorije. U algebri su od posebnog značaja *identiteti* kao formule oblika

$$(\forall x_1) \dots (\forall x_n)\, u(x_1, \dots, x_n; f_1, \dots, f_k) \approx v(x_1, \dots, x_n; f_1, \dots, f_k)$$

gde su u i v termi izgrađeni pomoću promenljivih $x_1, \dots, x_n$ i operacija $f_1, \dots, f_k$, a $\approx$ relacijski simbol arnosti 2 koji se interpretira kao jednakost. Ako je data teorija prvog reda, jedno od osnovnih pitanja je egzistencija i osobine njenih modela, između ostalog i kardinalnost nosača modela.

Uzmimo za primer zakon komutativnosti koji se izražava identitetom

$$(\forall x)(\forall y)\, x \cdot y = y \cdot x.$$

Struktura $(\{0, 1\}, \wedge)$ gde je $\wedge$ data tablicom

$\wedge$	0	1
0	0	0
1	0	1

zadovoljava ovaj identitet. Struktura $(N, +)$ gde je N skup prirodnih brojeva, a $+$ sabiranje prirordnih brojeva, takođe zadovoljava ovaj identitet. Dakle, zakon komutativnosti

ima i netrivijalne konačne, i beskonačne modele. Ukoliko neki identitet (ili skup identiteta) ima netrivijalan konačan model, tada je i direktni proizvod, pa i direktni stepen tih modela takođe model. Zahvaljujući tome, od svakog konačnog modela možemo doći do beskonačnog modela, pa svaki identitet koji ima konačan netrivijalan model ima i beskonačan model. Pokazaćemo da obrnuto ne važi: postoje identiteti koji imaju samo beskonačne netrivijalne modele.

Tvrđenje 4.1 (J. Dudek, 1988.) *Neka je $'$ funkcijski simbol arnosti 1, a $\cdot$ funkcijski simbol arnosti 2. Tada je svaki netrivijalan model identiteta*

$$(x' \cdot y) \cdot z = y \qquad (*)$$

beskonačan.

Dokaz. Prvo ćemo pokazati da identitet ima beskonačan model. Neka je N skup prirodnih brojeva, $'$ konstantna unarna operacija data sa $x' = 1$, a $\cdot$ binarna operacija definisana sa

$$x \cdot y = \begin{cases} x - 1, & x > 1 \\ y + 1, & x = 1. \end{cases}$$

Tada je $(N, ', \cdot)$ model identiteta $(*)$, jer je $x' = 1$, pa je $x' \cdot y = y+1$, a kako je $y+1 > 1$, sledi $(y + 1) \cdot z = (y + 1) - 1 = y$.

Sada ćemo pokazati da je svaki netrivijalan model identiteta $(*)$ beskonačan. Pretpostavimo da je $(A, \cdot, ')$ model identiteta $(*)$, pri čemu je $|A| > 1$. Neka je funkcija $T_a : A \to A$, gde je $a \in A$, definisana sa

$$T_a(x) = a' \cdot x.$$

Pokazaćemo da je T_a 1-1. Pretpostavimo da za $z_1, z_2 \in A$ važi $T_a(z_1) = T_a(z_2)$. Tada je

$$a' \cdot z_1 = a' \cdot z_2$$

odakle množenjem obe strane sa proizvoljnim $b \in A$ dobijamo

$$(a' \cdot z_1) \cdot b = (a' \cdot z_2) \cdot b$$

što se primenom identiteta $(*)$ svodi na $z_1 = z_2$. Međutim, T_a nije na. Zaista, pretpostavimo suprotno: da je T_a na preslikavanje. Kako je $a' \in A$, tada postoji $b \in A$ tako da važi $T_a(b) = a'$ tj. $a' \cdot b = a'$. Tada za svako $z \in A$ važi

$$(a' \cdot b) \cdot z = a' \cdot z$$

a kako je $(a' \cdot b) \cdot z = b$ i $a' \cdot z = T_a(z)$, sledi

$$b = T_a(z).$$

Pošto je $|A| > 1$, postoje dva različita elementa $x, y \in A$. Tada važi $T_a(x) = b = T_a(y)$, što je u suprotnosti sa činjenicom da je T_a 1-1. Dakle T_a *nije* na. Prema tome, postoji 1-1 preslikavanje skupa A u pravi podskup skupa A, a to znači da je skup A beskonačan.

■

4.2 Grupoid Parka

Sada će nas interesovati sledeći problem. Pretpostavimo da je $\mathcal{A}$ jedna konačna algebra sa konačno mnogo konačnih operacija. Da li postoji konačan skup Σ_0 identiteta koji su tačni na $\mathcal{A}$ tako da iz Σ_0 možemo izvesti (uz primenu aksioma jednakosti i pravila izvođenja predikatskog računa prvog reda) sve identiteta Σ koji važe u $\mathcal{A}$. Ovde izlažemo jedan primer grupoida kod koga je odgovor negativan. Kažemo da taj grupoid nema konačnu bazu identiteta. Pozitivan odgovor je u slučaju kada je $\mathcal{A}$ na primer grupa, prsten, mreža, komutativna polugrupa.

Grupoid Parka, u oznaci $\mathcal{A}_2$, je uređen par $(\{0,1,2,a\},\cdot)$ gde je operacija $\cdot$ data tablicom:

$\cdot$	0	1	2	a
0	0	1	a	a
1	1	1	2	a
2	a	2	2	a
a	a	a	a	a

Tvrđenje 4.2 (P. Park, 1980) *Grupoid $\mathcal{A}_2$ nema konačnu bazu identiteta tj. zadovoljava beskonačno mnogo identiteta koji nisu posledica jedan drugog.*

Dokaz. Primetimo prvo da u grupoidu $\mathcal{A}_2$ važe zakoni komutativnosti i idempotencije, a ne važi asocijativni zakon. Operacija $\cdot$ je slična operaciji maksimuma u lancu, samo što važi $0\cdot 2 = 2\cdot 0 = a$, a ne $0\cdot 2 = 2$. Takođe važi i osobina

$$x\cdot(x\cdot y) = x\cdot y.$$

Ako definišemo relaciju $\leqslant$ sa

$$x \leqslant y \overset{\text{def}}{\iff} x\cdot y = y,$$

tada je $\leqslant$ je refleksivna i antisimetrična, ali nije tranzitivna.

Lema 4.3 *Neka je $\mathcal{A}_n = (\{0,1,\ldots,n,a\},\cdot)$ grupoid gde je operacija $\cdot$ data sledećom tablicom.*

$\cdot$	0	1	2	3	$\cdots$	$n-1$	n	a
0	0	1	a	a	$\cdots$	a	a	a
1	1	1	2	a	$\cdots$	a	a	a
2	a	2	2	3	$\cdots$	a	a	a
3	a	a	3	3	$\cdots$	a	a	a
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$
$n-1$	a	a	a	a	$\cdots$	$n-1$	n	a
n	a	a	a	a	$\cdots$	n	n	a
a	a	a	a	a	$\cdots$	a	a	a

Tada grupoid $\mathcal{A}_2$ zadovoljava tačno one identitete koje zadovoljava grupoid $\mathcal{A}_n$.

Dokaz. Operaciju $\cdot$ možemo opisati na sledeći način.

- za svako $x \in A_n$ važi $x \cdot a = a \cdot x = a$;
- $i \cdot i = i$;
- $i \cdot (i+1) = (i+1) \cdot i = i+1$;
- u ostalim slučajevima je $i \cdot j = a$.

Podgrupoid generisan elementima $0, 1, 2, a$ je upravo grupoid $\mathcal{A}_2$. Kako se identiteti prenose na podstrukture, svaki identitet koji važi na $\mathcal{A}_n$, važi i na $\mathcal{A}_2$. Treba da pokažemo da važi i suprotno: da svi identiteti koji važe na $\mathcal{A}_2$ važe i na $\mathcal{A}_n$. Neka je I proizvoljan identitet koji važi na grupoidu $\mathcal{A}_2$. Kako se identiteti prenose direktnim proizvodom, I važi i na grupoidu

$$\mathcal{A}_2^{n-1} = \underbrace{\mathcal{A}_2 \times \cdots \times \mathcal{A}_2}_{n-1}.$$

Posmatraćemo podgrupoid B grupoida $\mathcal{A}_2^{n-1}$ koji sadrži elemente oblika

$$(0, 0, \ldots, 0, 1, 2, 2, \ldots, 2)$$

i sve elemente koje sadrže a bar na jednoj koordinati. Lako se proverava da je ovaj skup elemenata zatvoren za operaciju $\cdot$ primenjenu po komponentama. Pošto se identiteti prenose na podgrupoid, I važi i na grupoidu B. Definisaćemo preslikavanje h grupoida B na grupoid $\mathcal{A}_n$ na sledeći način:

$$\begin{aligned}
(0,0,0,\ldots,0,0,0,0) &\mapsto 0\\
(0,0,0,\ldots,0,0,0,1) &\mapsto 1\\
(0,0,0,\ldots,0,0,1,2) &\mapsto 2\\
(0,0,0,\ldots,0,1,2,2) &\mapsto 3\\
\cdots \quad &\cdots \quad \cdots\\
(1,2,2,\ldots,2,2,2,2) &\mapsto n-1\\
(2,2,2,\ldots,2,2,2,2) &\mapsto n\\
(n-1)\text{-torke koje sadrže bar jedno } a &\mapsto a
\end{aligned}$$

Treba da pokažemo da je h homomorfizam, tj. da važi:

$$h((x_1,\dots,x_{n-1})\cdot(y_1,\dots,y_{n-1})) = h((x_1,\dots,x_{n-1}))\cdot h((y_1,\dots,y_{n-1})).$$

za sve uređene $(n-1)$-torke $(x_1,\dots,x_{n-1})$ i $(y_1,\dots,y_{n-1})$. Ukoliko ni jedna od $(n-1)$-torki ne sadrži a, tada su one okarakterisane pozicijom jedinice gledano sa desne strane (s tim da uzimamo da se u $(0,\dots,0)$ jedinica nalazi na nultom, a u $(2,\dots,2)$ na n-tom mestu). h slika uređenu $(n-1)$-torku upravo u poziciju jedinice. Ako se položaj jedinice u $(n-1)$-torkama $(x_1,\dots,x_{n-1})$ i $(y_1,\dots,y_{n-1})$ razlikuje za najviše jedno mesto, tada će rezultat biti ona uređena $(n-1)$-torka čija jedinica ima veći redni broj:

$$\begin{array}{r}(0,\dots,0,0,1,2,2,2,\dots,2)\\ \cdot\,(0,\dots,0,0,0,1,2,2,\dots,2)\\ \hline (0,\dots,0,0,1,2,2,2,\dots,2)\end{array}$$

Sa druge strane, rezultat primene operacije $\cdot$ u grupoidu $\mathcal{A}_2$ na homomorfne slike $(n-1)$-torki je tada $\max(h(x_1,\dots,x_{n-1}), h(y_1,\dots,y_{n-1}))$ jer je $|h(x_1,\dots,x_{n-1}) - h(y_1,\dots,y_{n-1})| \leq 1$. Dakle u ovom slučaju je uslov homomorfizma zadovoljen. Ako se položaj jedinice u $(n-1)$-torkama razlikuje za više od jednog mesta, tada je zbog $2\cdot 0 = a$ rezultat $(n-1)$-torka koja sadrži a, pa je

$$h((x_1,\dots,x_{n-1})\cdot(y_1,\dots,y_{n-1})) = a = h(x_1,\dots,x_{n-1})\cdot h(y_1,\dots,y_{n-1}).$$

Ako pak jedna od $(n-1)$-torki sadrži a, tada će na istoj poziciji i proizvod $(n-1)$-torki sadržati a. Neka npr. $(x_1,\dots,x_{n-1})$ sadrži a. Tada je $h(x_1,\dots,x_{n-1}) = a$, a kako i $(x_1,\dots,x_{n-1})\cdot(y_1,\dots,y_{n-1})$ sadrži a, važi $h((x_1,\dots,x_{n-1})\cdot(y_1,\dots,y_{n-1})) = a$, što je u skladu sa operacijom $\cdot$ na grupoidu $\mathcal{A}_n$ jer je

$$a\cdot h((y_1,\dots,y_{n-1})) = a.$$

Dakle h je homomorfizam. Iz definicije se vidi da je h na, pa je epimorfizam. Kako se identiteti prenose epimorfizmom, a I važi na grupoidu B, sledi da I važi i na $\mathcal{A}_n$ koji je njegova homomorfna slika. Dakle, dobili smo da identitet I za koji smo pretpostavili da važi na $\mathcal{A}_2$, važi i na $\mathcal{A}_n$, čime smo pokazali i drugi smer tvrđenja. ∎

Da pokažemo da $\mathcal{A}_2$ nema konačnu bazu identiteta pretpostavićemo suprotno, da $\mathcal{A}_2$ ima konačnu bazu identiteta Σ_0 i da svaki identitet iz Σ_0 ima manje od n promenljivih.

Uvedimo oznaku $x_1x_2\cdots x_k$ za

$$(\cdots((x_1\cdot x_2)\cdot x_3)\cdots)\cdot x_k.$$

Lema 4.4 *Za $n\geq 3$ grupoid $\mathcal{A}_2$ zadovoljava identitet*

$$x_1x_2\cdots x_nx_1x_2\cdots x_n = x_2x_3\cdots x_nx_1\cdots x_nx_1. \qquad (*)$$

Dokaz. Neka je u term sa leve, a v term sa desne strane jednakosti $(*)$. Neka su $c_1, \ldots, c_n$ vrednosti koje uzimaju redom promenljive $x_1, \ldots, x_n$. Razlikujemo dva slučaja.

1. Među vrednostima $c_1, \ldots, c_n$ se ne pojavljuju istovremeno 0 i 2. Tada se vrednosti računaju u podgrupoidu $\{0, 1, a\}$ ili podgrupoidu $\{1, 2, a\}$ datog grupoida. Lako se proverava da su oba ova grupoida lanci, gde se $\cdot$ ponaša kao maksimum dva elementa. Kako je maksimum komutativna, asocijativna i idempotentna operacija, svaka od promenljivih x_i se na obe strane javlja po dva puta, znači da će vrednosti oba terma biti jednake, pa će jednakost biti zadovoljena.
2. Među vrednostima $c_1, \ldots, c_n$ se pojavljuju i 0 i 2. Pokazaćemo da je tada vrednost i terma v i terma u jednaka a. Neka je $c_i = 0$ i $c_j = 2$. Ako stavimo da važi $0 < 1 < 2 < a$, tada se iz tablice za operaciju $\cdot$ vidi da važi $x \cdot y \geq x$ i $x \cdot y \geq y$ tj. operacija $\cdot$ je monotona. Posmatrajmo proces računanja vrednosti terma u. Neka je e_k za $k \in \{1, 2, \ldots, 2n\}$ oznaka za vrednost dobijenu računanjen prvih k članova terma. Kako je $c_j = 2$, iz monotonosti sledi $e_j \geq 2$. Tada je i $e_{n+i-1} \geq 2$. Kako je $c_i = 0$, vrednost $e_{n+i} = e_{n+i-1} \cdot c_i$ je ili $2 \cdot 0 = a$ ili $a \cdot 0 = a$. Dakle $e_{n+i} = a$, pa je zbog monotonosti i vrednost celog terma u jednaka a. Ako analogno razmatranje ponovimo i za term v, zaključujemo da je i vrednost terma v jednaka a (dovoljno je uočiti da prvih n članova predstavlja permutaciju promenljivih $x_1, \ldots, x_n$ i drugih n članova takođe predstavlja permutaciju promenljivih $x_1, \ldots, x_n$).

■

Treba još pokazati da $(*)$ nije posledica ni jednog od identiteta skupa Σ_0. Ako bi $(*)$ bio posledica skupa identiteta Σ_0, tada bi svaki grupoid koji zadovoljava Σ_0 zadovoljavao i $(*)$. Pokazaćemo da to ne važi na primeru grupoida $\mathcal{B}_n = (B_n, \cdot)$ gde je $\cdot$ operacija data sledećom tablicom:

$\cdot$	b_1	b_2	b_3	$\cdots$	b_{n-1}	b_n	a
b_1	b_1	b_2	a	$\cdots$	a	b_1	a
b_2	b_2	b_2	b_3	$\cdots$	a	a	a
b_3	a	b_3	b_3	$\cdots$	a	a	a
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$
b_{n-1}	a	a	a	$\cdots$	b_{n-1}	b_n	a
b_n	b_1	a	a	$\cdots$	b_n	b_n	a
a	a	a	a	$\cdots$	a	a	a

Lema 4.5 *$\mathcal{B}_n \models \Sigma_0$, tj. $\mathcal{B}_n$ zadovoljava sve identiteta skupa Σ_0.*

Dokaz. Pojasnimo definiciju operacije $\cdot$ u grupoidu datom prethodnom tablicom.

- za svako $x \in B_n$ važi $x \cdot a = a \cdot x = a$;
- $b_i \cdot b_i = b_i$;
- $b_i \cdot b_{i+1} = b_{i+1} \cdot b_i = b_{i+1}$, a takođe $b_n \cdot b_1 = b_1 \cdot b_n = b_1$;
- u ostalim slučajevima je $b_i \cdot b_j = a$.

Dakle struktura B_n je slična strukturi A_{n-1}, osnovna razlika je da važi $b_n \cdot b_1 = b_1$, a ne $b_n \cdot b_1 = a$ (zato ova struktura liči na kružnu strukturu).

Neka je $I \in \Sigma_0$ proizvoljan identitet. Neka on ima m promenljivih $x_1, \ldots, x_m$. Prema izbora broja n, važi $m < n$. Neka su $c_1, \ldots, c_m$ vrednosti koje uzimaju promenljive $x_1, \ldots, x_m$. Tada se među vrednostima $c_1, \ldots, c_m$ ne javljaju sve vrednosti $b_1, \ldots, b_n$. Neka je b_i element različit od elemenata $c_1, \ldots, c_m$. Kako se element b_i javlja samo kao rezultat primene operacije $\cdot$ na dva argumenta od kojih je bar jedan b_i, sledi da je $B_n \setminus \{b_i\}$ podgrupoid grupoida $\mathcal{B}_n$. Može se pokazati da je $B_n \setminus \{b_i\} \cong \mathcal{A}_{n-2}$. Jedan izomorfizam je npr. preslikavanje

$$\begin{array}{rcl} b_{i+1} & \mapsto & 0 \\ b_{i+2} & \mapsto & 1 \\ & \vdots & \\ b_n & \mapsto & n-i-1 \\ b_1 & \mapsto & n-i \\ b_2 & \mapsto & n-i+1 \\ & \vdots & \\ b_{i-1} & \mapsto & n-2 \\ a & \mapsto & a \end{array}$$

Pošto identitet I važi na $\mathcal{A}_2$, on važi i na $\mathcal{A}_{n-2}$, što znači da važi i na njemu izomorfnom grupoidu $B_n \setminus \{b_i\}$, pa kako su sve vrednosti $c_1, \ldots, c_m$ promenljivih $x_1, \ldots, x_m$ iz skupa $B_n \setminus \{b_i\}$, sledi da je za date vrednosti $c_1, \ldots, c_m$ identitet I zadovoljen u grupoidu $\mathcal{B}_n$.

Kako su vrednosti $c_1, \ldots, c_m$ bile proizvoljne, identitet važi za sve vrednosti $c_1, \ldots, c_m$, pa I važi na grupoidu B_n, a I je bio proizvoljan identitet iz Σ_0, pa $\mathcal{B}_n \models \Sigma_0$. ∎

Lema 4.6 *U grupoidu $\mathcal{B}_n$ ne važi identitet* $(*)$.

Dokaz. Dovoljno je naći niz vrednosti $c_1, \ldots, c_n$ za koje identitet $(*)$ nije zadovoljen. Neka promenljive $x_1, \ldots, x_n$ redom uzimaju vrednosti $b_1, \ldots, b_n$. Zbog "kružne strukture" grupoida $\mathcal{B}_n$, pošto su sve promenljive (pa time i njihove vrednosti) sa susednim indeksima, vrednost prvih j elemenata terma je sama vrednost c_j. Zato je vrednost leve strane jednakosti b_n, a desne b_1. Kako je $b_1 \neq b_n$, identitet nije zadovoljen. ∎

Tako smo na primeru grupoida $\mathcal{B}_n$ pokazali da $(*)$ nije posledica skupa formula Σ_0. Kako $(*)$ važi na $\mathcal{A}_2$, to je u kontradikciji sa pretpostavkom da je Σ_0 baza identiteta grupoida $\mathcal{A}_2$. Dakle pretpostavka da $\mathcal{A}_2$ ima konačnu bazu identiteta je pogrešna. Time smo pokazali da $\mathcal{A}_2$ nema konačnu bazu identiteta. ∎

4.3 O klonovima

Viševrednosna logika je grana matematike koja je nastala kao posledica potrebe za iskazima sa više od dve vrednosti. Ona je uvedena kao uopštenje dvovrednosne logike. Mnogi rezultati koji važe u dvovrednosnoj logici očuvani su i u viševrednosnoj logici, ali kao što neki rezultati koji su dobijeni u dvovrednosnoj logici ne mogu biti preneseni na viševrednosnu logiku, tako i neki rezultati dobijeni u viševrednosnoj logici ne važe u dvovrednosnoj logici. Viševrednosna logika je našla svoju primenu u kompjuterskim naukama. Pri sintezi velikih i kompleksnih sistema kao što su kompjuteri, mali broj osnovnih elemenata se koristi za izgradnju logičkih sklopova (logička, prekidačka kola). Skup osnovnih elemenata iz kojeg je moguće izgraditi svaki sklop se naziva kompletan skup. U proučavanju teorije kompletnosti veliku ulogu igra teorija klonova. Ova grana opšte algebre proučava algebre kao nezavisne objekte, i umesto veze sa drugim, sličnim algebrama, ispituje uzajamne veze operacija algebre i relacija koje se mogu uvesti na nosaču algebre. Klonovi su specijalne familije operacija koje izrastaju iz određenih skupova generišućih operacija.

Sada ćemo se baviti samo klonovima na troelementnom skupu. Neka je $E_3 = \{0, 1, 2\}$. Skup svih n-arnih operacija na E_3 označavamo sa $P_3^{(n)}$, a skup svih operacija na E_3 sa P_3. Tako

$$\begin{aligned} P_3^{(n)} &= \{f \mid f : E_3^n \to E_3\} \\ P_3 &= \bigcup_{n \geq 0} P_3^{(n)} \end{aligned}$$

Definicija 4.7 Neka su $i, n \in N$. *i-ta n-arna projekcija na E_3* je operacija $p_i^n : E_3^n \to E_3$ definisana sa

$$p_i^n(x_1, \ldots, x_n) = x_i$$

za sve $x_1, \ldots, x_n \in E_3$ i $0 \leq i \leq n$.

Skup svih takvih projekcija na E_3 označavamo sa Π_3.

Definicija 4.8 Neka su $m, n \in N$ i neka su $f \in P_3^{(n)}$ i $g_1, \ldots, g_n \in P_3^{(m)}$. *Kompozicija* operacija f i $g_1, \ldots, g_n$ je operacija $f(g_1, \ldots, g_n) \in P_3^{(m)}$ definisana sa

$$f(g_1, \ldots, g_n)(x_1, \ldots, x_m) \stackrel{\text{def}}{=} f(g_1(x_1, \ldots, x_m), \ldots, g_n(x_1, \ldots, x_m)).$$

Definicija 4.9 *Klon operacija $\mathcal{C}$* na E_3 je skup operacija na E_3 koji sadrži sve i-te n-arne projekcije i zatvoren je u odnosu na kompoziciju tj. $\mathcal{C}$ je skup operacija na E_3 koji zadovoljava sledeća dva uslova:

1. $\Pi_3 \subseteq \mathcal{C}$, i
2. Ako je f n-arna operacija iz $\mathcal{C}$ i ako su $g_1, \ldots, g_n$ m-arne operacije iz $\mathcal{C}$, tada je m-arna operacija $f(g_1, \ldots, g_m)$ takođe u $\mathcal{C}$.

Primer 4.10 Klonovi su Π_3 i P_3 u E_3. $\triangle$

Tvrđenje 4.11 *Neka je $\{\mathcal{C}_i \mid i \in N\}$ proizvoljna neprazna familija klonova operacija na E_3. Tada je $\cap_{i \in N} \mathcal{C}_i$ klon operacija na E_3.*

Dokaz. Iz definicije klona sledi da $\Pi_3 \subseteq \mathcal{C}_i$ za svako $i \in N$. Tada $\Pi_3 \subseteq \cap_{i \in N} \mathcal{C}_i$, pa važi 1.

Neka $f \in \cap_{i \in N} \mathcal{C}_i^{(n)}$ i $g_1, \ldots, g_n \in \cap_{i \in N} \mathcal{C}_i^{(m)}$. Sledi da $f \in C_i^{(n)}$ i $g_1, \ldots, g_n \in \mathcal{C}_i^{(m)}$, za svako $i \in N$. Prema definiciji klona tada i $f(g_1, \ldots, g_n) \in \mathcal{C}_i^{(m)}$ za svako $i \in N$, tj. $f(g_1, \ldots, g_n) \in \cap_{i \in N} C_i^{(m)}$, pa važi 2. ∎

Definicija 4.12 Sa L_3 označavamo skup svih klonova na E_3.

Definicija 4.13 Neka je F neki skup operacija na E_3. *Klon generisan skupom F* je klon

$$\langle F \rangle_{CL} \stackrel{\text{def}}{=} \cap \{\mathcal{C} \in L_3 \mid F \subseteq \mathcal{C}\}$$

tj. $\langle F \rangle_{CL}$ je najmanji klon koji sadrži F.

U E_3 važi sledeće tvrđenje.

Tvrđenje 4.14 (Janov, Mučnik) *L_3 ima kontinuum mnogo elemenata.*

Dokaz. Na konačnom skupu ima prebrojivo mnogo operacija, pa je L_3 najviše kardinalnosti kontinuum. Daćemo kontinuum mnogo različitih klonova operacija nad E_3.

Neka je $F = \{f_i \mid \mathrm{ar}(f_i) = i, i \geq 2\}$ gde je $f_i(1, 2, \ldots, 2) = f_i(2, 1, 2, \ldots, 2) = \cdots = f_i(2, 2, \ldots, 2, 1) = 1$ i $f_i(x_1, \ldots, x_i) = 0$ u svim drugim slučajevima. Pokažimo da $f_i \notin \langle F \setminus \{f_i\}\rangle_{CL}$. Odavde sledi da $H_1, H_2 \subseteq F$, $H_1 \neq H_2$ povlači $\langle H_1\rangle_{CL} \neq \langle H_2\rangle_{CL}$, što je dovoljno za dokaz tvrđenja.

Pretpostavimo da za neko $i \geq 2$ važi $f_i \in \langle F \setminus \{f_i\}\rangle_{CL}$. Tada je za neko $j \neq i$

$$f_i = f_j(g_1, \ldots, g_j) \tag{4.1}$$

gde za sve $1 \leq k \leq j$ važi $g_k \in \langle F \setminus \{f_i\}\rangle_{CL}$. Stoga imamo dve mogućnosti:

(1) $g_k = x_{i_k} = p^i_{i_k}$

(2) $g_k = f_{i_k}(g_{k_{i_1}}, \ldots, g_{k_{i_k}})$

Ako je (2) ispunjeno za bar dva različita indeksa k zamenom $x_1 = 1, x_2 = \cdots = x_i = 2$, odnosno ako je (2) ispunjeno za tačno jedan ideks k (recimo $k = 1$) zamenom $x_{i_2} = 1$, $x_j = 2$ za $j \neq i_2$, sledi kontradikcija sa 4.1.

Konačno pretpostavimo slučaj

$$f_i = f_j(x_{i_1}, \ldots, x_{i_j}).$$

Tada ne može biti $j < i$ jer bi tada f_i zavisilo od više promenljivih nego $f_j(x_{i_1}, \ldots, x_{i_j})$. Zato je $j > i$, pa među promenljivih x_{i_k} ima jednakih, npr. $i_1 = i_2$. Za vrednost $x_{i_1} = 1$, $x_j = 2$ za $j \neq i_1$ imamo kontradikciju kao i u prethodnom slučaju. ∎

Napomena 4.15 E. Post je pokazao da je L_2 prebrojiv skup. ⋄

Glava 5

Brojevi

5.1 Realni brojevi

Definicija 5.1 *Potpuno uređeno polje* **F** je algebarski sistem

$$\mathbf{F} = (F, +, \cdot, \leq)$$

gde je F neprazan skup, $+, \cdot : F^2 \to F$ binarne operacije skupa F, a $\leq \subseteq F^2$ binarna relacija skupa F, pri čemu važe sledeće aksiome:

1. $(F, +, \cdot)$ je polje;
2. relacija $\leq$ je refleksivna, antisimetrična, tranzitivna i totalno uređenje;
3. relacija $\leq$ je saglasna sa operacijama $+$ i $\cdot$ tj. važi
   (a) $(\forall a, b, c \in F)(a \leq b \Rightarrow a + c \leq b + c)$
   (b) $(\forall a, b \in F)(0 \leq a, 0 \leq b \Rightarrow 0 \leq a \cdot b)$
4. važi sledeća aksioma potpunosti:

   Neka je $\emptyset \neq A \subseteq F$ odozgo ograničen skup, tj. neka postoji $a \in F$ tako da za svako $b \in A$ važi $b < a$. Tada postoji *supremum* skupa A tj. broj m takav da važi:
   (a) m je gornje ograničenje skupa A: $(\forall b \in A)\, b \leq m$ i
   (b) m je manje od svih ostalih gornjih ograničenja: za svako $m_1 \in F$ koje je gornje ograničenje skupa, tj. za koje važi $(\forall b \in A)\, b \leq m_1$, važi $m \leq m_1$.

Aksioma potpunosti (4) govori da svaki odozgo ograničen neprazan podskup skupa F ima supremum (najmanje gornje ograničenje). Ovo svojstvo omogućava uvođenje merenja.

Pokazuje se da postoji potpuno uređeno polje i da su sva potpuno uređena polja izomorfna. Pa, pod realnim brojevima ubuduće podrazumevamo potpuno uređeno polje koje ćemo označavati sa $(R_e, +, \cdot, \leq)$.

Pošto je $(R_e, +, \cdot)$ polje, sve osobine polja važe u skupu realnih brojeva. Izvešćemo neke posledice aksioma koje se tiču odnosa operacija $+$ i $\cdot$ sa relacijom $\leq$. Koristimo uobičajenu oznaku $a \geq b$ za $b \leq a$, $a < b$ za $a \leq b \wedge a \neq b$ i $b > a$ za $a < b$.

Tvrđenje 5.2 *Za realne brojeve a i p važi:*

1. $a \geq 0 \Leftrightarrow -a \leq 0$
2. $a^2 \geq 0$
3. $1 > 0$
4. $a > 0 \Rightarrow a^{-1} > 0$
5. $p > 0 \Rightarrow (a < b \Rightarrow p \cdot a < p \cdot b)$

Dokaz.

1. Neka je $a \geq 0$. Prema aksiomi 3a, tada važi $a + (-a) \geq 0 + (-a)$, pa iz osobina polja sledi $-a \leq 0$. Obrnuto, neka je $-a \leq 0$. Tada primenom iste aksiome dobijamo $(-a) + a \leq a$, tj. $a \geq 0$.

2. Pošto je $\leq$ totalno uređenje, mora važiti $0 \leq a$ ili $a \leq 0$.

   (a) $0 \leq a$. Tada primenom aksiome 3b dobijamo $0 \leq a \cdot a = a^2$.

   (b) $a \leq 0$. Tada prema prethodno dokazanom slučaju 1 važi $0 \leq (-a)$. Odatle primenom aksiome 3b sledi $0 \leq (-a)(-a)$, a u polju je $(-a)(-a) = a^2$, pa je i u ovom slučaju $0 \leq a^2$.

3. Prema prethodnoj osobini je $1 = 1 \cdot 1 \geq 0$. Kako je $(R_e, +, \cdot)$ polje, važi $1 \neq 0$, pa je $1 > 0$.

4. Neka je $a > 0$. Pretpostavimo suprotno: $a^{-1} \leq 0$. Tada važi $0 \leq a$ i $0 \leq -a^{-1}$, pa prema aksiomi 3b sledi $0 \leq a \cdot (-a^{-1})$. Prema osobinama polja tada $0 \leq -(a \cdot a^{-1})$ tj. $0 \leq -1$, što primenom aksiome 3a daje $1 \leq 0$, a to je u kontradikciji sa prethodnom osobinom: $1 > 0$. Dakle pretpostavka $a^{-1} \leq 0$ je bila pogrešna, pa kako je $\leq$ totalno uređenje važi $0 \leq a^{-1}$, a kako je $0 \neq a^{-1}$, sledi $0 < a^{-1}$.

5. Neka je $p > 0$ i $a < b$. Pretpostavimo suprotno: $p \cdot b \leq p \cdot a$. Tada iz aksiome 3a sledi $p \cdot b - p \cdot a \leq 0$, pa iz distributivnosti sledi $0 \leq p \cdot (a - b)$. Kako je $p \neq 0$, postoji p^{-1}, a prema slučaju 4 ovog tvrđenja važi $0 < p^{-1}$. Odatle po aksiomi 3b sledi $0 \leq p^{-1} \cdot p \cdot (a - b)$ odnosno $0 \leq a - b$ što po aksiomi 3a povlači $b \leq a$, a to je kontradikcija sa pretpostavkom $a < b$ (zbog antisimetričnosti relacije $\leq$). Dakle pretpostavka $p \cdot a \geq p \cdot b$ je pogrešna, pa važi $p \cdot a < p \cdot b$.

■

Skup

$$R_e^+ = \{ x \mid x > 0\}$$

nazivamo skupom *pozitivnih* realnih brojeva. 1 je pozitivan realan broj, prema prethodnom tvrđenju, a primenom aksiome 3a dobijamo da su $2 \stackrel{\text{def}}{=} 1 + 1 > 1 + 0 = 1 > 0$, a zatim i $3 = 2 + 1, 4 = 3 + 1, \ldots$ pozitivni realni brojevi. Skup $N = \{1, 2, 3, \ldots\}$ dobijen na ovaj način zovemo *skup prirodnih brojeva*. Skup $N_0 = N \cup \{0\}$ zovemo *skup prirodnih brojeva sa nulom*, a skup $Z = N_0 \cup -N$ gde je $-N = \{-n \mid n \in N\}$ skup celih brojeva. $R_a = \{\frac{p}{q} \mid p, q \in Z, q \neq 0\}$ je skup racionalnih brojeva, a skup $\mathbf{I}_r = R_e \setminus R_a$ skup *iracionalnih* brojeva.

Neka $a, b \in R_e$ i $a < b$. Za broj c kažemo da je *između* brojeva a i b akko važi $a < c$ i $c < b$.

Tvrđenje 5.3 *Neka $a, b \in R_e$ i $a < b$. Tada postoji broj c koji je između brojeva a i b.*

Dokaz. Neka je $a < b$. Prema aksiomi 3a i komutativnosti sabiranja sledi

$$\begin{aligned} a + a &< a + b \\ a + b &< b + b. \end{aligned}$$

Primenom distributivnosti i osobine neutralnog elementa dobijamo $a + a = 1 \cdot a + 1 \cdot a = (1 + 1) \cdot a = 2a$, i analogno $b + b = 2b$, što znači da važi

$$\begin{aligned} 2a &< a + b \\ a + b &< 2b \end{aligned}$$

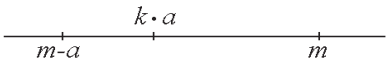
Pošto je $2 > 0$, postoji 2^{-1}. Prema tvrđenju 5.2 tada sledi $a < 2^{-1}(a + b)$ i $2^{-1}(a + b) < b$. Zato je $2^{-1}(a + b)$ traženi broj c koji se nalazi između a i b. ∎

Dakle u skupu R_e za svaka dva broja postoji broj između njih. Za skup koji ima ovu osobinu kažemo da je *gust*.

Tvrđenje 5.4 (Arhimedova nejednakost) *Neka je $a > 0$ i $b \in R_e$. Tada postoji $n \in N$ takav da je $na > b$.*

Dokaz. Neka su $a > 0$ i $b \in R_e$ proizvoljni. Pretpostavimo suprotno: za svako $n \in N$ važi $na \leq b$. Tada je skup $S = \{a, 2a, 3a, \ldots\}$ ograničen sa gornje strane, pa prema aksiomi potpunosti (4) postoji supremum m.

Ukoliko ne bi postojao ni jedan broj ka skupa S za koji važi $m - a < ka$, tada bi svi brojevi skupa S bili manji ili jednaki $m - a$, pa bi $m - a < m$ bilo gornje ograničenje, što je suprotnosti sa pretpostavkom da je m *najmanje* gornje ograničenje. Zato postoji



broj $ka \in S$ ($k \in N$) za koji važi $m - a < ka$. Tada i $k + 1 \in N$, pa $m = (m - a) + a < ka + a = (k + 1)a$. Kako $(k + 1)a \in S$, dobijamo da m nije gornje ograničenje, što je kontradikcija. Dakle postoji $n \in N$ tako da $na > b$. ∎

Napomena 5.5 Može se pokazati da postoji bijekcija između decimalnih zapisa realnih brojeva i skupa realnih brojeva R_e. ⋄

Definicija 5.6 Neka je $x \in R_e$. Tada je *apsolutna vrednost realnog broja* x data sa

$$|x| = \begin{cases} x, & x \geq 0 \\ -x, & x < 0. \end{cases}$$

Tvrđenje 5.7

1. $|0| = 0$
2. $x \neq 0 \Rightarrow |x| > 0$
3. $|x| = x \vee |x| = -x$
4. $-|x| \leq x \leq |x|$
5. $|-x| = |x|$
6. $|x| < a \Leftrightarrow -a < x < a$
7. $|xy| = |x||y|$
8. $|x + y| \leq |x| + |y|$

Dokaz. Osobine 1, 2, 3, 4 i 5 slede direktno iz definicije.

6. Osobina 6 je posledica činjenice da je

$$-a < x < a \quad \Leftrightarrow \quad -a < -x < a$$

7. Osobina 7 je posledica definicije i osobine 5.

8. Iz osobine 5 imamo $|x+y| = |-x-y|$, iz osobine 3 sledi $|x+y| = x+y \vee |x+y| = -x-y$, a iz 4 takođe $x \leq |x|$, $-x \leq |x|$, $-y \leq |y|$, $y \leq |y|$ odakle sledi $x+y \leq |x|+|y|$ i $-x-y \leq |x|+|y|$ tj. $|x+y| \leq |x|+|y|$.

■

Realni brojevi se mogu prikazati i u ravni pomoću realne prave. Neka je data prava p u ravni. Izaberimo dve različite tačke A i B na pravoj p i pridružimo im redom brojeve 0 i 1. Prenošenjem duži AB dobijamo celobrojne tačke na realnoj osi, a potom se odgovarajućim konstrukcijama pridruže tačke racionalnim brojevima. Korišćenjem osobine neprekidnosti realne prave dokazuje se da se i iracionalnim brojevima mogu dodeliti odgovarajuće tačke na pravoj. Može se pokazati da je takvo preslikavanje bijekcija. Dalje se može uspostaviti bijekcija skupa R_e^2 uređenih parova realnih brojeva i tačaka ravni, kao i bijekcija skupa R_e^3 trojki realnih brojeva i tačaka prostora.

5.2 Prirodni brojevi

Videli smo da se skup prirodnih brojeva sa nulom N_0 može uvesti kao podskup skupa realnih brojeva. Drugi način zasnivanja prirodnih brojeva su sledeće *Peanove aksiome*.

1. $0 \in N_0$.
2. Za svaki broj $n \in N_0$ postoji $n' \in N_0$ koji se naziva sledbenik broja n.
3. $m' = n' \Rightarrow m = n$.
4. 0 nije naslednik ni jednog broja iz N_0.
5. $M \subseteq N_0, \quad 0 \in M, \quad (n \in M \Rightarrow n' \in M) \Rightarrow M = N_0$.

Skupove celih i racionalnih brojeva moguće je definisati polazeći od skupa prirodnih brojeva. Dalje se pomoću racionalnih brojeva uvode realni brojevi.

Poslednja Peanova aksioma je aksioma indukcije. Onda predstavlja univerzalno tvrđenje koje se odnosi na sve podskupove M skupa N_0. U teoriji prvog reda ovo tvrđenje nije moguće izraziti jedinstvenom aksiomom. Zato uvodi sledeća šema-aksioma:

$$A(0) \wedge (\forall x)(A(x) \Rightarrow A(x')) \Rightarrow (\forall x)\, A(x)$$

za svaku formulu A predikatskog računa. Ovo je samo specijalni slučaj Peanove aksiome indukcije, jer svih podskupova M skupa N_0 ima kontinuum, a formula prvog reda ima samo prebrojivo mnogo.

U algebri $(N_0,')$ operacije sabiranja i množenja definišemo na sledeći način:

$$\begin{aligned} n+0 &= n \\ n+m' &= (n+m)' \end{aligned}$$

$$\begin{aligned} n\cdot 0 &= 0 \\ n\cdot m' &= n\cdot m+n. \end{aligned}$$

Primenom matematičke indukcije pokazujemo da važe poznate osobine prirodnih brojeva kao što su komutativnost i asocijativnost sabiranja i distributivnost množenja prema sabiranju.

Matematička indukcija se često koristi u nešto modifikovanom obliku. Ukoliko želimo da pokažemo da neko tvrđenje važi za sve prirodne brojeve počev od nekog broja n_0, tada pokazujemo da važi za n_0 i da važenje tvrđenja za neko $k \geq n_0$ povlači njegovo važenje za $k+1$.

Primer 5.8 Ilustrovaćemo način primene matematičke indukcije tako što ćemo pokazati da za svaki prirodan broj n važi

$$S(n): \qquad 1+2+\cdots+n = \frac{n(n+1)}{2}.$$

$S(1)$ se svodi na $1 = \frac{1\cdot 2}{2}$ što trivijalno važi.

Pretpostavimo da važi S_k:

$$1+2+\cdots+k = \frac{k(k+1)}{2}.$$

Ako i jednoj i drugoj strani dodamo $k+1$, dobijamo

$$1+2+\cdots+k+(k+1) = \frac{k(k+1)}{2}+(k+1),$$

što posle sređivanja daje

$$1+2+\cdots+k+(k+1) = \frac{(k+1)((k+1)+1)}{2},$$

a to je upravo $S(k+1)$. Dakle $S(k) \Rightarrow S(k+1)$, a kako važi $S(1)$, prema aksiomi matematičke indukcije sledi $(\forall n \in N)\, S(n)$. $\triangle$

Napomenimo da se uz određeno preciziranje meta matematičkih postupaka (posebno finitnosti) unutar vrlo široke klase formalnih teorija (u koje spadaju sve one koje sadrže elementarnu aritmetiku) ne može pokazati neprotivrečnost formalne teorije. Osim toga, za takve teorije važi da ukoliko su neprotivrečne, tada u njima postoje tvrđenja koja su neodlučiva. Dakle postoje izrazi koji su na dopušten način formirani u toj teoriji, takvi da ni izraz ni njegova negacija ne mogu biti izvedeni unutar teorije (Gedel (K. Gödel)).

5.3 Prsten celih brojeva

Jednačina $a+x=b$ nema uvek rešenje u skupu N_0. Zato se javlja potreba za uvođenjem strukture koja bi zadržala neka bitna svojstva strukture skupa N_0, ali u kojoj bi jednačina $a+x=b$ uvek imala rešenje. Zahtev da nova struktura zadrži neka bitna svojstva polazne strukture koja predstavljala motivaciju za njen nastanak, naziva se "Hankelov (H. Hankel) princip permanencije". Kada kažemo da smo skup prirodnih brojeva *proširili* skupom negativnih brojeva i tako dobili skup celih brojeva, znači da smo definisali novu strukturu celih brojeva koja kao svoju podstrukturu sadrži strukturu izomorfnu skupu prirodnih brojeva.

Opisaćemo konstrukciju pomoću koje od strukture prirodnih brojeva dolazimo do prstena celih brojeva.

Neka je $(A,+,\cdot)$ algebra tipa $(2,2)$ takva da su $+$ i $\cdot$ komutativne i asocijativne operacije, važi zakon skraćivanja za operaciju $+$ i zakon distributivnosti $\cdot$ prema $+$. (Primetimo da $(N_0,+,\cdot)$ zadovoljava ove osobine.) Definišimo operacije $+'$ i $\cdot'$ na skupu A^2 na sledeći način:

$$\begin{aligned}(x_1,x_2)+'(y_1,y_2) &\overset{\text{def}}{=} (x_1+y_1,x_2+y_2)\\ (x_1,x_2)\cdot'(y_1,y_2) &\overset{\text{def}}{=} (x_1\cdot y_1+x_2\cdot y_2,x_1\cdot y_2+x_2\cdot y_1)\end{aligned}$$

Primenom asocijativnosti, komutativnosti i distributivnosti operacija $+$ i $\cdot$, direktno se dobija da su i $+'$ i $\cdot'$ komutativne i asocijativne operacije na A^2 i da je $\cdot'$ distributivna prema $+'$. Definišimo relaciju $\sim$ na skupu A^2 na sledeći način:

$$(x_1,x_2)\sim(y_1,y_2)\overset{\text{def}}{\iff} x_1+y_2=y_1+x_2.$$

Pokazaćemo da je $\sim$ kongruencija algebre $(A^2,+',\cdot')$ tj. da je refleksivna, antisimetrična, tranzitivna, saglasna sa $+'$ i saglasna sa $\cdot'$.

Refleksivnost Kako je $x_1+x_2=x_1+x_2$, po definiciji sledi $(x_1,x_2)\sim(x_1,x_2)$ za proizvoljno $(x_1,x_2)\in A^2$.

Simetričnost Neka $(x_1,x_2)\sim(y_1,y_2)$. Tada $x_1+y_2=y_1+x_2$, pa $y_1+x_2=x_1+y_2$, što znači $(y_1,y_2)\sim(x_1,x_2)$.

Tranzitivnost Neka je $(x_1,x_2)\sim(y_1,y_2)$ i $(y_1,y_2)\sim(z_1,z_2)$. Tada $x_1+y_2=y_1+x_2$ i $y_1+z_2=z_1+y_2$. Sabiranjem ovih jednakosti dobijamo $(x_1+y_2)+(y_1+z_2)=(y_1+x_2)+(z_1+y_2)$. Odatle primenom asocijativnosti, komutativnosti i zakona skraćivanja za operaciju $+$ dobijamo $x_1+z_2=z_1+x_2$, pa je $(x_1,x_2)\sim(z_1,z_2)$.

Saglasnost sa $+'$ Pošto je $+'$ komutativna operacija, dovoljno je proveriti da važi

$$(x_1,x_2)\sim(y_1,y_2)\Rightarrow(x_1,x_2)+'(z_1,z_2)\sim(y_1,y_2)+'(z_1,z_2).$$

Neka je $(x_1, x_2) \sim (y_1, y_2)$. Tada je $x_1 + y_2 = y_1 + x_2$. Ako na obe strane dodamo $z_1 + z_2$ i primenimo asocijativnost i komutativnost za $+$ dobijamo

$$(x_1 + z_1) + (y_2 + z_2) = (y_1 + z_1) + (x_2 + z_2)$$

a to znači $(x_1 + z_1, x_2 + z_2) \sim (y_1 + z_1, y_2 + z_2)$ odnosno

$$(x_1, x_2) +' (z_1, z_2) \sim (y_1, y_2) +' (z_1, z_2).$$

Saglasnost sa $\cdot'$ I ovde je zbog komutativnosti operacije $\cdot'$ dovoljno proveriti

$$(x_1, x_2) \sim (y_1, y_2) \Rightarrow (x_1, x_2) \cdot' (z_1, z_2) \sim (y_1, y_2) \cdot' (z_1, z_2).$$

Neka je $(x_1, x_2) \sim (y_1, y_2)$. Tada je $x_1 + y_2 = y_1 + x_2$. Odatle sledi

$$(x_1 + y_2) \cdot z_1 = (y_1 + x_2) \cdot z_1. \qquad (*)$$

Kako je $+$ komutativna operacija, sledi $x_2 + y_1 = y_2 + x_1$, pa i

$$(x_2 + y_1) \cdot z_2 = (y_2 + x_1) \cdot z_2. \qquad (**)$$

Sabiranjem jednakosti $(*)$ i $(**)$ dobijamo

$$(x_1 + y_2) \cdot z_1 + (x_2 + y_1) \cdot z_2 = (y_1 + x_2) \cdot z_1 + (y_2 + x_1) \cdot z_2$$

što posle primene distributivnosti, kao i asocijativnosti i komutativnosti za $+$ daje

$$x_1 \cdot z_1 + x_2 \cdot z_2 + y_1 \cdot z_2 + y_2 \cdot z_1 = y_1 \cdot z_1 + y_2 \cdot z_2 + x_1 \cdot z_2 + x_2 \cdot z_1,$$

a to po definiciji znači

$$(x_1 \cdot z_1 + x_2 \cdot z_2, x_1 \cdot z_2 + x_2 \cdot z_1) \sim (y_1 \cdot z_1 + y_2 \cdot z_2, y_1 \cdot z_2 + y_2 \cdot z_1)$$

tj. $(x_1, x_2) \cdot' (z_1, z_2) \sim (y_1, y_2) \cdot' (z_1, z_2)$.

Dakle $\sim$ je kongruencija, pa postoji faktor-algebra $(A^2/_\sim, \oplus, \odot)$ algebre $(A^2, +', \cdot')$. Na faktor-algebru se prenosi komutativnost, asocijativnost i distributivnost operacija. Pokazaćemo da postoji neutralni element za $\oplus$ i inverzni elementi u odnosu na $\oplus$. Za proizvoljno $a \in A$ važi

$$(x_1, x_2)/_\sim \oplus (a, a)/_\sim = (x_1 + a, x_2 + a)/_\sim.$$

Kako je $x_1 + x_2 + a = x_1 + a + x_2$, sledi $(x_1, x_2) \sim (x_1 + a, x_2 + a)$, što znači $(x_1, x_2)/_\sim = (x_1 + a, x_2 + a)/_\sim$. Dakle $(a, a)/_\sim$ je neutralni element za $\oplus$. Neka je sada $(x_1, x_2)/_\sim \in A^2/_\sim$ proizvoljan. Tada je zbog komutativnosti za $+$

$$(x_1, x_2)/_\sim \oplus (x_2, x_1)/_\sim = (x_1 + x_2, x_2 + x_1)/_\sim = (a, a)/_\sim,$$

što znači da je $(x_2, x_1)/_\sim$ inverzni element elementa $(x_1, x_2)/_\sim$. Dakle $\oplus$ je asocijativna i komutativna operacija, postoji neutralni element i postoji inverzni element za svaki element iz $A^2/_\sim$, pa je $(A^2/_\sim, \oplus)$ grupa. Kako je $\odot$ asocijativna operacija i važi distributivnost $\odot$ prema $\oplus$, znači da je $(A^2/_\sim, \oplus, \odot)$ *prsten*.

Ako ovu konstrukciju sprovedemo za strukturu $(N_0, +, \cdot)$, tada dobijamo prsten $(N_0^2/_\sim, \oplus, \odot)$ koji nazivamo prsten celih brojeva i pišemo samo $\mathbf{Z} = (Z, +, \cdot)$. Podstruktura prstena $(Z, +, \cdot)$ koja je izomorfna sa $(N_0, +, \cdot)$ je određena skupom $\{\, (m, 0)/_\sim \mid m \in N_0\}$ i izomorfizam je upravo preslikavanje dato sa $f(n) = (n, 0)/_\sim$ za $n \in N_0$.

Videli smo da je skup realnih brojeva gust. Kada se na prirodan način uvede relacija totalnog poretka na skupovima N_0 i Z može se zaključiti da skupovi N_0 i Z nisu gusti, ali da u njima važi aksiom potpunosti.

5.4 Elementi teorije brojeva

Tvrđenje 5.9 (Deljenje sa ostatkom) *Neka je $a \in Z$ proizvoljan ceo broj i $b \in N$. Tada postoje jedinstveni brojevi q i r tako da $q \in Z$, $r \in \{0, 1, \ldots, b-1\}$ i važi*

$$a = qb + r$$

Dokaz.

Egzistencija p i q. Prvo ćemo dokazati da za $a \in N_0$ postoje odgovarajući q i r. Dokaz sprovodimo indukcijom po a. Ako je $a = 0$, tada je $a = 0 \cdot b + 0$ i važi $0 < b$, pa možemo staviti $q = 0$ i $r = 0$. Pretpostavimo da tvrđenje važi za a. Tada postoje q i r tako da je $a = qb + r$ i $0 \leq r \leq b - 1$. Treba da pokažemo da postoje q' i r' tako da važi $a + 1 = q'b + r'$ i $0 \leq r' \leq b - 1$. Razlikujemo dva slučaja.

1. $r \leq b - 2$. Tada je $a + 1 = qb + (r + 1)$ i važi $r + 1 \leq b - 1$, pa možemo staviti $q' = q$ i $r' = r + 1$.
2. $r = b - 1$. Tada je $a + 1 = qb + b - 1 + 1 = q(b + 1)$, pa možemo staviti $q' = q + 1$ i $r' = 0$.

Treba još pokazati da postoje odgovarajući q' i r' za $a \leq -1$. Tada je $-a - 1 \geq 0$, pa prema prethodnom razmatranju postoje q i r tako da važi $-a - 1 = qb + r$ i $0 \leq r \leq b-1$. Odatle sledi $a = (-q)b - r - 1$, odnosno $a = (-q-1)b + (b-1) - r$. Kako je $0 \leq (b-1) - r \leq b - 1$, možemo uzeti $q' = -q - 1$ i $r' = b - 1 - r$.

Jedinstvenost p i q Neka je $a = q_1 b + r_1$ i $a = q_2 b + r_2$ pri čemu $0 \leq r_1, r_2 \leq b - 1$. Tada je $(q_1 - q_2)b = r_2 - r_1$. Pri tome je $-(b-1) \leq r_2 - r_1 \leq b - 1$. Ako bi bilo $q_1 - q_2 \leq -1$ tada bi važilo $r_2 - r_1 = (q_1 - q_2)b \leq -b$, što je nemoguće. Ako bi važilo $q_1 - q_2 \geq 1$ tada bi bilo $r_2 - r_1 = (q_1 - q_2)b \geq b$, što je takođe nemoguće.

Dakle mora biti $q_1 - q_2 = 0$, odakle sledi $q_1 = q_2$, pa i $r_1 = r_2$, što znači da su q i r jedinstveni.

■

Broj q iz prethodnog tvrđenja se naziva *količnik*, a broj r *ostatak* deljenja broja a brojem b. Pišemo $q = a \operatorname{div} b$ i $r = a \bmod b$.

Definicija 5.10 Kažemo da ceo broj m *deli* ceo broj n (ili da je n *deljiv* sa m), u oznaci $m \mid n$, akko postoji $k \in Z$ tako da je $n = km$ (tj. $n \bmod m = 0$).

Lako se pokazuje da je relacija $\mid$ relacija parcijalnog uređenja na skupu N_0, dok na Z nije.

Definicija 5.11 Broj $d \in N$ je *najveći zajednički delilac* brojeva $a, b \in Z$, u oznaci $d = \mathrm{NZD}(a, b)$ ili $d = (a, b)$, akko

1. $d \mid a$ i $d \mid b$
2. za svako $d_1 \in Z$ za koje važi $d_1 \mid a$ i $d_1 \mid b$ važi i $d_1 \mid d$.

Za cele brojeve a i b kažemo da su *uzajamno prosti* ako je $\mathrm{NZD}(a, b) = 1$.

Definicija 5.12 $s \in N$ je *najmanji zajednički sadržalac* brojeva $a, b \in Z$, u oznaci $s = \mathrm{NZS}(a, b)$ ili $s = [a, b]$, akko

1. $a \mid s$ i $b \mid s$
2. za svako $s_1 \in Z$ za koje važi $a \mid s_1$ i $b \mid s_1$ važi i $s \mid s_1$.

Napomenimo, da u skupu prirpdnih brojeva relacija se sadrži je relacija parcijalnog poretka. U odnosu na relaciju $a \vee b = \sup\{a, b\} = NZS(a, b)$ je najmanji zajednički sadržalac za a i b, $a \wedge b = \inf\{a, b\} = NZD(a, b)$ je najveći zajednički delitelj za a i b. Dakle, imamo mrežu $(N, \vee, \wedge)$.

Tvrđenje 5.13 (Euklidov algoritam) *Neka su $a, b \in Z$ proizvoljni celi brojevi. Tada postoji jedinstven $d = \mathrm{NZD}(a, b)$ i postoje brojevi $\alpha, \beta \in Z$ tako da*

$$\alpha a + \beta b = d.$$

Dokaz. Neka su $a, b \in Z$ proizvoljni. Opisaćemo postupak kojim se efektivno nalazi $\mathrm{NZD}(a, b)$ i brojevi $\alpha, \beta \in Z$. Jedinstvenost $\mathrm{NZD}(a, b)$ je direktna posledica definicije za NZD i antisimetričnosti relacije $|$ na skupu N_0.

Lako se proverava da znak brojeva ne utiče na deljivost. Zato možemo posmatrati slučaj kada je $a, b \in N_0$. Iz definicije najvećeg zajedničkog delioca sledi $\mathrm{NZD}(a, b) = \mathrm{NZD}(b, a)$, što znači da možemo uzeti $a \geq b$. Neka je $a_0 = a$ i $b_0 = b$. Ako je $b_i \neq 0$ tada definišemo q_i, a_{i+1} i b_{i+1} na sledeći način:

$$\begin{aligned} q_i &= a_i \operatorname{div} b_i \\ a_{i+1} &= b_i \\ b_{i+1} &= a_i \bmod b_i. \end{aligned}$$

Tako možemo računati sledeće članove nizova na osnovu prethodnih sve dok je $b_i \neq 0$. Kada je $b_i = 0$, postupak je završen. Iz definicije sledi da je $b_{i+1} < b_i$. Zato su nizovi a_i i b_i strogo opadajući, pa postoji $k \in N_0$ tako da je $b_k = 0$. To znači da se postupak uvek završava u konačnom broju koraka. Pokazaćemo da je za svako $0 \leq i \leq k$ broj a_k najveći zajednički delilac brojeva a_i i b_i, odakle će slediti $a_k = \mathrm{NZD}(a, b)$. Za $i = k$ tvrđenje važi jer $a_k \mid a_k$ i $a_k \mid 0$, a za proizvoljan d_1 za koji važi $d_1 \mid a_k$ i $d_1 \mid 0$ važi $d_1 \mid a_k$, što po definiciji znači $a_k = \mathrm{NZD}(a_k, 0) = \mathrm{NZD}(a_k, b_k)$. Pretpostavimo sada da tvrđenje važi za $i+1$: neka je $a_k = \mathrm{NZD}(a_{i+1}, b_{i+1}) = \mathrm{NZD}(b_i, b_{i+1})$. Tada $a_k \mid b_i$ i $a_k \mid b_{i+1}$. Kako je $a_i = q_i b_i + b_{i+1}$, sledi $a_k \mid a_i$. Dakle, a_k jeste delilac brojeva a_i i b_i, treba još pokazati da je najveći. Neka $d' \mid a_i$ i $d' \mid b_i = a_{i+1}$. Kako je $b_{i+1} = a_i - q_i b_i$ sledi $d' \mid b_{i+1}$. Dakle imamo $d' \mid a_{i+1}$ i $d' \mid b_{i+1}$, pa pošto je po pretpostavci $a_k = \mathrm{NZD}(a_{i+1}, b_{i+1})$, sledi $d' \mid a_k$. Tada iz definicije sledi $a_k = \mathrm{NZD}(a_i, b_i)$. Dakle

$$a_k = \mathrm{NZD}(a_k, b_k) = \mathrm{NZD}(a_{k-1}, b_{k-1}) = \cdots = \mathrm{NZD}(a_0, b_0) = \mathrm{NZD}(a, b).$$

Sada ćemo opisati postupak za određivanje brojeva α i β koristeći konstruisane nizove a_i, b_i, q_i. Definišimo nizove $\alpha_k, \alpha_{k-1}, \ldots, \alpha_0$ i $\beta_k, \beta_{k-1}, \ldots, \beta_0$ na sledeći način:

$$\begin{aligned} &\alpha_k = 1, && \beta_k = 1 \\ &\alpha_i = \beta_{i+1}, && \beta_i = \alpha_{i+1} - \beta_{i+1} q_i \end{aligned}$$

Pokazaćemo da za $0 \leq i \leq k$ važi

$$\alpha_i a_i + \beta_i b_i = d.$$

Za $i = k$ tvrđenje se svodi na $1 \cdot d + 1 \cdot 0 = d$, što važi. Pretpostavimo da tvrđenje važi za $i + 1$:

$$\alpha_{i+1} a_{i+1} + \beta_{i+1} b_{i+1} = d.$$

Zamenjujući $a_{i+1} = b_i$ i $b_{i+1} = a_i - q_i b_i$ dobijamo

$$\alpha_{i+1} b_i + \beta_{i+1}(a_i - q_i b_i) = d,$$

tj.

$$\beta_{i+1}a_i + (\alpha_{i+1} - \beta_i q_i)b_i = d,$$

a to je upravo

$$\alpha_i a_i + \beta_i b_i = d.$$

Prema tome, važi i $\alpha_0 a_0 + \beta_0 b_0 = d$, pa možemo staviti $\alpha = \alpha_0$ i $\beta = \beta_0$. ∎

Primer 5.14 Pokažimo da je u cikličnoj grupi $\mathbf{C}_n$ reda n preslikavanje $f(x) = x^m$ automorfizam akko su m i n uzajamno prosti.

$\Leftarrow$) : Neka su m i n uzajamno prosti, tj. $\mathrm{NZD}(m,n) = 1$. Dokazujemo da je preslikavanje $f : C_n \to C_n$, definisano sa $f(x) = x^m$ automorfizam grupe $\mathbf{C}_m$. Kako je $\mathrm{NZD}(m,n) = 1$, postoje celi brojevi a i b takvi da je $am + bn = 1$. Pokažimo da je f 1-1 preslikavanje. Neka je $f(x) = f(y)$ tj. $x^m = y^m$. Pošto u grupi $\mathbf{C}_n$ za svaki element $z \in C_n$ važi $z^n = e$, sledi

$$\begin{aligned} x = x^1 = x^{am+bn} &= (x^m)^a (x^n)^b = (y^m)^a e^b \\ &= (y^m)^a (y^n)^b = y^{am+bn} = y^1 = y. \end{aligned}$$

Kako je f 1-1, a C_n konačan skup, sledi da je f i na. Konačno, kako je ciklična grupa komutativna,

$$f(xy) = (xy)^m = x^m y^m = f(x)f(y),$$

pa je f bijektivni homomorfizam, tj. automorfizam.

$\Rightarrow$) : Neka je $f(x) = x^m$ automorfizam i a generator grupe $\mathbf{C}_n$. Pretpostavimo da $\mathrm{NZD}(m,n) = d > 1$. Tada postoje k_1 i k_2 tako da $m = k_1 d$ i $n = k_2 d$. Kako $d > 1$ sledi $1 \leq k_2 < n$. Zato je $a^{k_2} \neq e$. Kako je

$$f(a^{k_2}) = a^{k_2 m} = a^{k_2 k_1 d} = (a^{k_2 d})^{k_1} = (a^n)^{k_1} = e = f(e),$$

sledi da f nije 1-1, što je kontradikcija sa pretpostavkom da je f automorfizam. △

Definicija 5.15 Za prirodan broj $p \geq 2$ kažemo da je *prost* akko nije deljiv ni sa jednim prirodnim brojem različitim od 1 i p. Prirodan broj veći od 2 je *složen* akko nije prost.

Primer 5.16 (*Mala Fermaova (P. Fermat) teorema)* Ako je p pozitivan prost broj, tada za svaki pozitivan ceo broj a važi

$$a^p \equiv a \pmod{p}$$

Dokaz. Indukcijom po a. Za $a = 1$ tvrđenje očigledno važi. Pretpostavimo da $p \mid a^p - a$. Treba da dokažemo da $p \mid (a+1)^p - (a+1)$. Kako je

$$(a+1)^p - (a+1) = (a^p - a) + \left(pa + \frac{p(p-1)}{2!} + \cdots + pa^{p-1} \right)$$

a oba sabirka na desnoj strani su deljiva sa p, sledi traženo tvrđenje. ∎ △

Lema 5.17 *Neka $a, b, c \in N$. Ako $c \mid ab$ i $\mathrm{NZD}(c, a) = 1$, tada $c \mid b$.*

Dokaz. Neka $a, b, c \in N$, $c \mid ab$ i $\mathrm{NZD}(c, a) = 1$. Tada prema Euklidovom algoritmu (5.13) postoje $\alpha, \beta \in Z$ tako da

$$\alpha c + \beta a = 1,$$

odakle sledi

$$\alpha cb + \beta ab = b.$$

Pošto $c \mid \alpha cb$ i $c \mid \beta ab$, sledi $c \mid b$. ∎

Lema 5.18 *Neka je p prost broj i $a, b \in Z$. Ako $p \mid ab$, tada $p \mid a$ ili $p \mid b$.*

Dokaz. Neka je p proizvoljan prost broj i $a, b \in Z$. Ukoliko $p \mid a$, tada tvrđenje važi. Ukoliko $p \nmid a$, tada je $\mathrm{NZD}(p, a) = 1$ jer su jedini delioci broja p broj 1 i sam broj p, a p nije delilac broja a. Prema prethodnoj lemi (5.17) $p \mid b$. ∎

Tvrđenje 5.19 (Osnovni stav aritmetike) *Neka je $n > 1$ prirodan broj. Tada se n na jedinstven način može napisati u obliku*

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \qquad (*)$$

gde su $p_1 < p_2 < \dots < p_k$ prosti brojevi i $\alpha_1, \dots, \alpha_k \in N$.

Dokaz. Prvo ćemo pokazati da se svaki prirodan broj može napisati u obliku $(*)$. Ako je $n = 2$ tada je $n = 2^1$, pa se može napisati u obliku $(*)$. Pretpostavimo da tvrđenje važi za sve brojeve manje od n. Ako je n prost broj, tada se on može napisati u obliku n^1. Ako je n složen, tada je $n = a \cdot b$ gde $1 < a, b < n$, pa za a i b važi induktivna hipoteza. Zato se a i b mogu napisati u obliku $(*)$. Tada primenom asocijativnosti i komutativnosti možemo sortirati redosled prostih činilaca u proizvodu $a \cdot b$ i sabrati eksponente. Tako dobijamo broj n predstavljen u obliku $(*)$. Dakle tvrđenje važi i za n.

Sada treba pokazati da je razlaganje na proste činioce jedinstveno. Pretpostavimo da su $p_1^{\alpha_1} \dots p_k^{\alpha_k}$ i $q_1^{\beta_1} \dots q_l^{\beta_l}$ dva razlaganja broja n na proste činioce. Tada je

$$p_1^{\alpha_1} \dots p_k^{\alpha_k} = q_1^{\beta_1} \dots q_l^{\beta_l}.$$

Pretpostavimo da su razlaganja različita, bilo da se neki od prostih brojeva sa jedne strane ne javlja sa druge, ili se javlja sa različitim eksponentom. Tada možemo skratiti sve činioce zajedničke za obe strane tako da bar sa jedne strane dobijemo broj različit od 1:

$$p_{i_1}^{\alpha_{i_1}} \dots p_{i_{k_1}}^{\alpha_{i_{k_1}}} = q_{j_1}^{\beta_{j_1}} \dots q_{j_{l_1}}^{\beta_{j_{l_1}}}.$$

Neka je npr. $\alpha_{i_1} > 0$. Tada p_{i_1} deli levu stranu, pa mora deliti i desnu. Prema lemi 5.18 prost broj p_{i_1} deli neki od prostih brojeva $q_{j_1}, \ldots, q_{j_{l_1}}$, a to je kontradikcija sa pretpostavkom da smo skratili sve zajedničke činioce. ∎

Tvrđenje 5.20 (Euklid) *Prostih brojeva ima beskonačno mnogo.*

Dokaz. Pretpostavimo suprotno: da postoji konačno mnogo prostih brojeva. Neka su $p_1, \ldots, p_k$ svi prosti brojevi. Stavimo

$$p = p_1 \cdot p_2 \cdots p_k + 1.$$

Broj p je veći od svih brojeva $p_1, \ldots, p_k$, pa mora biti složen. Zato se on može napisati kao proizvod prostih brojeva, što znači da je deljiv sa nekim od prostih brojeva $p_1, \ldots, p_k$, a to je kontradikcija jer p daje ostatak 1 pri deljenju sa svakim od brojeva $p_1, \ldots, p_k$. ∎

5.4.1 Linearne Diofantove jednačine

Ako su a i b celi brojevi i $a, b \neq 0$, tada se linearna jednačina oblika

$$ax + by = c$$

pri čemu promenljive x i y uzimaju vrednosti iz skupa celih brojeva, naziva linearna Diofantova jednačina. Jednačine ovog tipa proučavao je grčki matematičar Diofant u trećem veku pre naše ere. Zahtev da su rešenja celobrojna otežava njihovo rešavanje. Na primer, jednačina $x+y = 1$ ima beskonačno rešenja, dok jednačina $8x+12y = 13$ nema ni jedno, jer je leva strana prethodne jednakosti parna za sve celobrojne vrednosti x i y.

Tvrđenje 5.21 *Linearna Diofantova jednačina $ax + by = c$ ima rešenje akko $d \mid c$, gde je $d = \mathrm{NZD}(a, b)$.*

Dokaz. $\Rightarrow$) : Neka je $d = \mathrm{NZD}(a, b)$ i neka je (x_0, y_0) rešenje jednačine, tj. $ax_0 + by_0 = c$. Kako $d \mid a$ i $d \mid b$, sledi $d \mid ax_0 + by_0$ $(= c)$.

$\Leftarrow$) : Pretpostavimo da $d \mid c$. Tada postoji broj $k \in Z$ tako da $c = kd$. Na osnovu tvrđenja 5.13 postoje celi brojevi x' i y' takvi da je $ax' + by' = d$. Množeći poslednju jednakost sa k dobijamo $akx' + bky' = dk$, tj.

$$a(kx') + b(ky') = c,$$

pa je (kx', ky') jedno rešenje polazne linearne Diofantove jednačine. ∎

Primer 5.22 Rešimo Diofantovu jednačinu $13x + 32y = 5$. U ovom slučaju je $a = 13$, $b = 32$ i $c = 5$. Koristeći Euklidov algoritam dobijamo:

$$32 = 2 \cdot 13 + 6; \qquad 13 = 2 \cdot 6 + 1; \qquad 6 = 6 \cdot 1,$$

te su brojevi 32 i 13 uzajamno prosti, pa broj 1 možemo napisati kao

$$1 = 13 + (-2) \cdot 6 = 13 + (-2)(32 - 2 \cdot 13) = 5 \cdot 13 + (-2) \cdot 32.$$

Množenjem jednačine $1 = 5 \cdot 13 + (-2) \cdot 32$ sa 5 dobijamo $13 \cdot 25 + 32 \cdot (-10) = 5$, te je jedno rešenje polazne jednačine par $(25, -10)$. $\triangle$

5.5 Racionalni brojevi

Celi brojevi nam omogućavaju da rešavamo jednačinu oblika $a + x = b$, ali u skupu Z i dalje nije moguće rešiti sve jednačine oblika $x \cdot a = b$. Da bi smo omogućili rešavanje i ovih jednačina, rukovodeći se Hankelovim principom permanencije uvodimo skup racionalnih brojeva. Racionalni brojevi se definišu pomoću celih brojeva slično kao što se celi brojevi definišu pomoću prirodnih. Na skupu $Z \times (Z \setminus \{0\})$ se definiše relacija $(p, q) \sim (r, s) \overset{\text{def}}{\Longleftrightarrow} p \cdot s = r \cdot q$ i pokazuje da je $\sim$ kongruencija u odnosu na oeracije $+$ i $\cdot$ definisane sa

$$\begin{aligned} (b, a) + (d, c) &= (ad + bc, ac) \\ (b, a) \cdot (d, c) &= (bd, ac). \end{aligned}$$

Dobijeni faktor-prsten je prsten racionalnih brojeva, za koji se pokazuje da je polje. Pri radu sa racionalnim brojevima pogodno je izabrati jedinstvenog predstavnika svake klase $(p, q)/_\sim$. U ovom slučaju možemo uzeti predstavnika (p, q) za kojeg važi $\text{NZD}(p, q) = 1$. Klasu $(p, q)/_\sim$ tada označavamo sa $\frac{p}{q}$. Tako skup racionalnih brojeva možemo posmatrati i kao skup

$$R_a = \left\{ \frac{p}{q} \mid p, q \in Z,\ q \neq 0,\ \text{NZD}(p, q) = 1 \right\}.$$

Često skup R_a označavamo sa Q.

Skup racionalnih brojeva je gust, ali u njemu ne važi aksioma potpunosti. Naime, iz aksiome potpunosti bi sledilo, recimo, da postoji broj x tako da je $x^2 = 2$. Pokazaćemo da to nije slučaj (dokaz koji sledi potiče od Euklida). Naime, pretpostavimo suprotno, da postoji broj $x \in R_a$ takav da je $x^2 = 2$. Kako je $x \in R_a$, važi $x = \frac{a}{b}$ gde su a i b uzajamno prosti celi brojevi i $b \neq 0$. Dakle $\frac{a^2}{b^2} = 2$ tj. $a^2 = 2b^2$. Odavde sledi da je a^2 paran broj, pa je zato i a paran broj tj. može se napisati u obliku $a = 2p$ gde $p \in Z$. Iz

jednakosti $a^2 = 2b^2$ dobijamo sada $4p^2 = 2b^2$ tj. $2p^2 = b^2$. Sada sledi da je b paran broj, tj. da je $b = 2q$ gde $q \in Z$. Zaključujemo da a i b nisu uzajamno prosti brojevi, što je u suprotnosti sa početnom pretpostavkom.

Odgovarajućom konstrukcijom se od skupa racionalnih brojeva može konstruisati skup realnih brojeva u kome važi i aksioma potpunosti.

Napomenimo da zbir dve trigonometrijske periodične funkcije ne mora biti periodična funkcija. Tako $\cos x$ i $\sin\sqrt{2}x$ su periodične, a njihov zbir nije. Pretpostavimo suprotno, da postoji neki realan broj $T \neq 0$, takav da za svaki realan broj x važi:

$$\cos(x+T) + \sin\sqrt{2}(x+T) = \cos x + \sin\sqrt{2}x.$$

Za $x = 0$ dobijamo $\cos T + \sin\sqrt{2}T = 1$, a za $x = -T$ dobijamo $\cos T - \sin\sqrt{2}T = 1$. Odatle, $\cos T = 1$ i $\sin\sqrt{2}T = 0$, odnosno $T = 2n\pi$ i $T = \frac{m\pi}{\sqrt{2}}$, $n, m \in Z$. Izjednačavajući po T dobijamo $\sqrt{2} = \frac{m}{2n}$, odnosno da je $\sqrt{2}$ racionalan broj.

5.6 Kompleksni brojevi

Prilikom konstrukcije celih i racionalnih brojeva primenjivali smo osobine direktnog proizvoda i homomorfizma. Tako smo dobili strukture koje zadržavaju neke bitne osobine polaznih struktura. Može se, međutim, pokazati da direktni proizvod polja nije polje, a homomorfna slika polja je nula-prsten ili polje izomorfno početnom. Zato pri daljem "proširivanju" skupa realnih brojeva koristimo neke druge konstrukcije. Jednu takvu konstrukciju ćemo primeniti da bismo od polja realnih brojeva konstruisali polje kompleksnih brojeva.

Kako je za svaki realan broj $x^2 \geq 0$, sledi $x^2 + 1 > 0$, pa jednačina $x^2 + 1 = 0$ nema rešenja u skupu R_e. Kompleksni brojevi omogućavaju rešavanje i ovih jednačina. Definišemo ih kao strukturu $\mathbf{C} = (R_e^2, \oplus, \odot)$ gde je

$$(a,b) \oplus (c,d) = (a+c, b+d)$$
$$(a,b) \odot (c,d) = (ac - bd, ad + bc)$$

Može se pokazati da je $(R_e^2, \oplus, \odot)$ polje. $(0,0)$ je nula u polju, $(1,0)$ jedinica, $-(a,b) = (-a,-b)$, a za $(a,b) \neq (0,0)$ je

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right).$$

Struktura $(\{\,(a,0) \mid a \in R_e\}, \oplus, \odot)$ je potpolje polja $\mathbf{C}$ koje je izomorfno sa poljem $\boldsymbol{R_e}$. Izomorfizam je funkcija $f : R_e \to R_e^2$ definisana sa $f(a) = (a,0)$. Zato nema opasnosti

od zabune ukoliko $(a, 0)$ pišemo samo a. Umesto $\oplus$ i $\odot$ pišemo samo $+$ i $\cdot$. Ako sa i označimo $(0, 1)$ tada važi $i^2 = -1$ i svaki broj $z \in C$ se može napisati u obliku

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1) = a + bi.$$

Izraz $a + bi$ se naziva *algebarski oblik* kompleksnog broja (a, b). Ako je $z = (a, b)$ tada broj a nazivamo *realni deo kompleksnog broja* z i označavamo sa $\Re z$, a broj b nazivamo *imaginarni deo kompleksnog broja* z i označavamo sa $\Im z$.

Kao što je napomenuto, prilikom proširivanja skupa brojeva ne mogu se sačuvati sve osobine. Pokazaćemo da se proširivanjem skupa realnih na skup kompleksnih brojeva nužno gubi relacija totalnog uređenja saglasna sa $+$ i $\cdot$. Naime, pretpostavimo suprotno: postoji relacija totalnog uređenja $\leq$ na skupu C koja je saglasna sa $+$ i $\cdot$. Kako je $i \neq 0$, mora biti $i > 0$ ili $i < 0$. Ako je $i > 0$ tada je $0 < i$ i $0 < i$, pa $0 < i \cdot i$, tj. $0 < -1$. To povlači $1 + 0 < 1 + (-1)$, tj. $1 < 0$, što je kontradikcija sa tvrđenjem 5.2. Ako je $i < 0$ tada je $0 < -i$, pa dobijamo $0 < (-i) \cdot (-i)$, tj. $0 < -1$, a to opet vodi u kontradikciju.

Definicija 5.23 *Konjugovano kompleksni* broj broja $a + bi$, u oznaci $\overline{a + bi}$, je $a - bi$.

Definicija 5.24 *Moduo* kompleksnog broja $z = a+bi$, u oznaci $|z|$ je nenegativan realan broj $\sqrt{a^2 + b^2}$.

Sledeće osobine su posledice prethodnih definicija.

Tvrđenje 5.25

1. $\overline{\overline{z}} = z$
2. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
3. $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$
4. $\Re z = \frac{1}{2}(z + \overline{z})$
5. $\Im z = \frac{1}{2i}(z - \overline{z})$
6. $|\overline{z}| = |z|$

Kompleksne brojeve prikazujemo u *kompleksnoj ravni* tako što kompleksnom broju (a, b) pridružujemo tačku sa koordinatama a i b. Osa x se naziva *realna osa*, a osa y *imaginarna osa*. Geometrijski smisao modula kompleksnog broja (a, b) je udaljenost tačke (a, b) od koordinatnog početka. Ugao θ koji (za $(a, b) \neq (0, 0)$) zaklapa duž $(0, 0)(a, b)$ sa pozitivnim smerom x-ose se naziva *argument kompleksnog broja* i označava se sa $\arg z$. Može se definisati sa

$$\arg(a,b) = \begin{cases} \arccos \frac{a}{a^2+b^2}, & b \geq 0 \\ -\arccos \frac{a}{a^2+b^2}, & b < 0. \end{cases}$$

Definišemo i

$$\mathrm{Arg}\, z = \{\, \arg z + 2k\pi \mid k \in Z \,\}.$$

Tvrđenje 5.26

1. $|z|^2 = z\overline{z}$
2. $|z_1 z_2| = |z_1||z_2|$
3. $|\frac{z_1}{z_2}| = \frac{|z_1|}{|z_2|}$
4. $|z_1 + z_2| \leq |z_1| + |z_2|$

Dokaz. Neka je $z = a + bi$, $z_1 = a_1 + b_1 i$ i $z_2 = a_2 + b_2 i$.

1. $|z|^2 = (\sqrt{a^2+b^2})^2 = a^2 + b^2 = (a+bi)(a-bi) = z\overline{z}$.
2. $|z_1 z_2|^2 = z_1 z_2 \overline{z_1 z_2} = z_1 z_2 \overline{z_1}\ \overline{z_2} = z_1 \overline{z_1} z_2 \overline{z_2} = |z_1|^2 |z_2|^2$
3. Prema definiciji je

$$\overline{z^{-1}} = \overline{\left(\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2} i\right)} = \frac{a}{a^2+b^2} + \frac{b}{a^2+b^2} i = \frac{z}{z\overline{z}} = (\overline{z})^{-1}.$$

   Odatle je

$$\begin{aligned} \left|\frac{z_1}{z_2}\right| &= \frac{z_1}{z_2}\overline{\left(\frac{z_1}{z_2}\right)} = \frac{z_1}{z_2}\overline{\left(z_1 z_2^{-1}\right)} \\ &= \frac{z_1}{z_2}\overline{z_1}\overline{\left(z_2^{-1}\right)} = \frac{z_1}{z_2}\overline{z_1}(\overline{z_2})^{-1} = \frac{z_1\overline{z_1}}{z_2\overline{z_2}} = \frac{|z_1|}{|z_2|}. \end{aligned}$$

4. Koristeći formulu $z + \overline{z} = 2\Re z$ i $\Re z \leq |z|$, dobijamo $|z_1 + z_2|^2 = (z_1 + z_2)(\overline{z_1} + \overline{z_2}) = |z_1|^2 + |z_2|^2 + 2\Re(z_1\overline{z_2}) \leq |z_1|^2 + |z_2|^2 + 2|z_1||z_2| = (|z_1| + |z_2|)^2$, a kako za svako $z \in C$ važi $|z| \geq 0$, sledi $|z_1 + z_2| \leq |z_1| + |z_2|$.

■

Ako je $(a, b) = z \in C \setminus \{(0, 0)\}$ tada postoji $\theta = \arg z$ i važi $a = |z| \cos\theta$ i $b = |z| \sin\theta$. Tada je

$$z = a + bi = |z|(\cos\theta + i \sin\theta).$$

Poslednji izraz predstavlja *trigonometrijski oblik* kompleksnog broja i kraće se označava sa $|z| \operatorname{cis}\theta$. Primenom trigonometrijskih identiteta neposredno se pokazuje da za $z_1 = |z_1| \operatorname{cis}\theta_1$ i $z_2 = |z_2| \operatorname{cis}\theta_2$ važi

$$z_1 z_2 = |z_1||z_2| \operatorname{cis}(\theta_1 + \theta_2)$$

i $\frac{z_1}{z_2} = \frac{z_1}{z_2} \operatorname{cis}(\theta_1 - \theta_2)$. Matematičkom indukcijom se može pokazati da važi *Moavrova formula* (A. Moivre):

$$(\operatorname{cis}\theta)^n = \operatorname{cis} n\theta,$$

što se može koristiti za rešavanje jednačina oblika $z^n = a$ gde je $a \in C$.

Glava 6

Matrice

6.1 Gausov postupak

Neka je $(P, +, \cdot)$ polje. Sistem od m linearnih jednačina sa n nepoznatih je konjunkcija sledećih formula.

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & b_1 \\ \cdots & & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = & b_m \end{array} \qquad (S)$$

Elementi a_{ij} za $1 \leq i \leq m$ i $1 \leq j \leq n$ se nazivaju *koeficijenti*, a elementi b_i za $1 \leq i \leq m$ *slobodni članovi*. Pri tome slobodni članovi i koeficijenti uzimaju vrednosti iz polja. *Rešenje sistema* (S) je uređena n-torka $(c_1, \ldots, c_n)$ elemenata polja P koja zadovoljava sve jednačine sistema (S) (kada promenljive $x_1, \ldots, x_n$ redom uzmu vrednosti $c_1, \ldots, c_n$ identiteti važe u polju P). Skup rešenja sistema (S) je

$$R(S) = \{\, (c_1, \ldots, c_n) \mid (c_1, \ldots, c_n) \text{ je rešenje sistema } (S) \,\}.$$

Sistem jednačina je *homogen* ako je $b_i = 0$ za sve $1 \leq i \leq n$. Za homogeni sistem je $R(S) \neq \emptyset$ jer $(0, \ldots, 0) \in R(S)$. Rešenje $(0, \ldots, 0)$ se naziva *trivijalno rešenje*. Ako je $R(S) = \emptyset$ kažemo da je sistem S *protivrečan*. U suprotnom je sistem *neprotivrečan*. Ako je $|R(S)| = 1$ kažemo da sistem ima *jedinstveno rešenje*. Za $|R(S)| > 1$ sistem je *neodređen*. Sistemi S_1 i S_2 su *ekvivalentni* akko $R(S_1) = R(S_2)$.

Neka je $L = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ i $D = b$. Tada je svaka jednačina ovog sistema oblika $L = D$. Neka je $A = L - D$. Važe sledeća jednostavna tvrđenja.

Tvrđenje 6.1 $L = D \Leftrightarrow A = 0$.

Dokaz. Neka je $L = D$. Pošto je $(P, +)$ grupa, možemo i levoj i desnoj strani dodati $-D$. Tada dobijamo $L - D = 0$. Obrnuto, neka je $L - D = 0$. Ako dodamo D i levoj i desnoj strani, dobijamo $L = D$. ∎

Primenom prethodnog tvrđenja sve linearne jednačine u polju možemo posmatrati u obliku $A = 0$. Neka su $A = 0$ i $B = 0$ dve linearne jednačine i $k \in P$.

Tvrđenje 6.2 $A = 0 \wedge B = 0 \Leftrightarrow B = 0 \wedge A + kB = 0$.

Dokaz. Neka je $A = 0$ i $B = 0$. Tada je $A + kB = 0 + k \cdot 0 = 0$. Obrnuto, neka je $B = 0$ i $A + kB = 0$. Tada je $A + k \cdot 0 = 0$, tj. $A = 0$. ∎

Tvrđenje 6.3 *Neka su* $A = 0$ *i* $B = 0$ *jednačine u polju* P *i* $t \in P \setminus \{0\}$. *Tada*

$$A = 0 \Leftrightarrow t \cdot A = 0.$$

Dokaz. Neka je $A = 0$. Tada je $t \cdot A = 0$. Obrnuto, neka je $t \cdot A = 0$. Kako je $t \neq 0$, postoji $t^{-1} \in P$. Množenjem jednačine $t \cdot A = 0$ sa t^{-1} dobijamo $t^{-1} \cdot t \cdot A = t^{-1} \cdot 0$ tj. $A = 0$. ∎

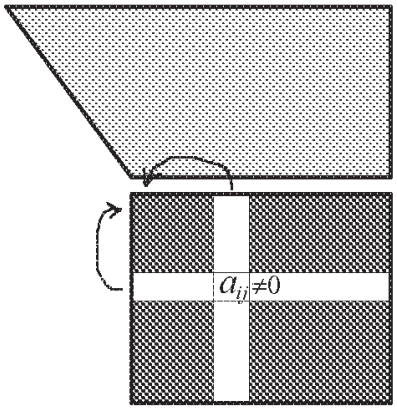
Za rešavanje sistema linearnih jednačina od posebnog su značaja sledeće *elementarne transformacije*:

1. promena mesta jednačinama u sistemu
2. množenje neke jednačine sistema elementom $k \in P$ različitim od 0
3. množenje neke jednačine elementom $t \in P$ i dodavanje nekoj drugoj jednačini sistema

Prva osobina je posledica komutativnosti i asocijativnosti konjunkcije. Druga osobina je posledica tvrđenja 6.2, a treća tvrđenja 6.3. Sistematskog primenom elementarnih transformacija dolazimo do *Gausovog algoritam* (K. Gaus).

Gausov algoritam Neka je sistem jednačina (S) konjukcija jednačina $J_1, \ldots, J_m$ sa po n promenljivih. U k-tom koraku algoritma ćemo eliminisati po jednu promenljivu iz svih jednačina $k + 1, k + 2, \ldots, m$, ukoliko je to moguće. Algoritam se završava kada nije moguće eliminisati ni jednu promenljivu ili kada je $k = m$. k-ti korak algoritma se sastoji u sledećem:

1. Pronaći proizvoljan koeficijent različit od nule u nekoj od jednačina $J_k, \ldots, J_m$. Ukoliko takav koeficijent ne postoji, tada se postupak završava. Ukoliko takav koeficijent postoji, neka je to a_{ij} u jednačini J_i gde je $i \geq k$.



2. Promeniti redosled jednačina $J_k, \ldots, J_m$ tako da se na k-tom mestu nalazi jednačina J_i. Promeniti redosled promenljivih $x_j, \ldots, x_n$ tako da je promenljiva x_j k-ta po redu. Sada se koeficijent a_{ij} nalazi na poziciji kk.

3. Svakoj od jednačina J_i za $k+1 \leq i \leq m$ dodati jednačinu J_k pomnoženu brojem $-a_{kk}^{-1} \cdot a_{ik}$. Tada će koeficijenti na poziciji ik biti

$$a_{ik} - a_{kk}^{-1} \cdot a_{ik} \cdot a_{kk} = 0,$$

čime smo eliminisali koeficijente uz x_k u jednačinama $J_{k+1}, \ldots, J_m$.

4. Ukoliko je $k = m$, postupak je završen. U suprotnom se k uvećava za 1 i postupak ponavlja.

Jasno je da se ovaj postupak mora završiti u najviše m koraka. Iz prethodnog razmatranja sledi da se svakim korakom dobija sistem ekvivalentat polaznom sistemu. Razmotrimo karakter rešenja sistema jednačina u zavisnosti od tačke u kojoj je algoritam završio sa radom.

1. Ukoliko se postupak završi u koraku 4, tada je polazni sistem ekvivalentan trouganom sistemu u kome je poslednja jednačina $a_{mm}x_m = b_m$. Množenjem te jednačine sa a_{mm}^{-1} koje postoji jer je prema uslovu koraka 1 $a_{mm} \neq 0$, dobijamo $x_m = b_m \cdot a_{mm}^{-1}$. Sada zamenom x_m u jednačinu J_{m-1} dobijamo jedinstvenu vrednost za x_{m-1}. Ponavljajući ovaj postupak dolazimo do jedinstvenog rešenja jednačine.

2. Ukoliko se postupak završi u koraku 1, tada su svi koeficijenti a_{ij} za $k \leq i \leq m$ i $k \leq j \leq n$ jednaki nuli. Razlikujemo dve mogućnosti.

(a) Svi slobodni članovi b_i za $k \leq i \leq m$ su jednaki nuli. Tada će sistem biti zadovoljen za proizvoljne vrednosti promenljivih $x_k, \ldots, x_m$, jer ostale promenljive možemo odrediti tako što zamenimo proizvoljne vrednosti $x_k, \ldots, x_m$ u jednačine J_1, ..., J_{k-1} čime se sistem svodi na trougaoni sistem iz prethodnog slučaja 1. Pošto vrednosti $m-k+1$ promenljivih možemo birati slobodno, kažemo da je sistem neodređen i ima $m-k+1$ *stepeni slobode*.

(b) Jedan od slobodnih članova je različit od nule, neka je to član b_i. Kako su leve strane svih jednačina jednake 0, jednakost J_i ne može biti zadovoljena, pa je sistem *protivrečan*.

Primer 6.4 Sistem linearnih jednačina u skupu realnih brojeva

$$\begin{aligned} x + \sqrt{2}\, y &= \sqrt{3} \\ \sqrt{2}\, x + 2y &= \sqrt{6} \end{aligned}$$

je neodređen, jer dodavanjem prve jednačine pomnožene sa $-\sqrt{2}$ drugoj jednačini dobijamo

$$\begin{aligned} x + \sqrt{2}y &= \sqrt{3} \\ 0 &= 0 \end{aligned}$$

pa sistem ima jedan stepen slobode. Zanimljivo je međutim da ako izvršimo aproksimaciju broja $\sqrt{2}$ proizvoljnim racionalnim brojem $\frac{p}{q}$, dobijamo sistem

$$\begin{aligned} x + \frac{p}{q}y &= \sqrt{3} \\ \frac{p}{q}x + 2y &= \sqrt{6} \end{aligned}$$

koji ima jedinstveno rešenje jer se ne može desiti da je $\frac{p}{q} \cdot \frac{p}{q} = 2$. Dakle priroda rešenja sistema je osobina koja je vrlo "osetljiva" na zaokruživanje. $\triangle$

Primer 6.5 Ukoliko sistem sadrži parametre na mestu koeficijenata, tada takođe možemo primeniti Gausov postupak, ali je egzistencija i vrednost rešenja funkcija datih parametara. Neka je dat sistem jednačina u polju realnih brojeva gde je $a \in R_e$ realan parametar.

$$\begin{aligned} x + ay &= a \\ ax + y &= a \end{aligned}$$

Primenimo Gausov postupak na ovaj sistem.

$$\begin{array}{rcll} x + & ay & = & a \qquad /\cdot(-a) \\ ax + & y & = & a \\ \hline x + & ay & = & a \\ & y(1-a^2) & = & a - a^2 \end{array}$$

Razlikujemo dva slučaja.

1. $1 - a^2 \neq 0$. Tada je $y = \frac{a-a^2}{1-a^2} = \frac{a}{1+a}$ i $x = \frac{a}{1+a}$.
2. $1 - a^2 = 0$. Tada je $a = 1$ ili $a = -1$.

   (a) $a = 1$. Sistem se svodi na

   $$\begin{aligned} x + y &= 1 \\ x + y &= 1 \end{aligned}$$

   i on je neodređen sa jednim stepenom slobode.

   (b) $a = -1$. Sistem se svodi na

   $$\begin{aligned} -x + y &= -1 \\ x \ - y &= -1. \end{aligned}$$

   Sabiranjem ove dve jednačine dobijamo $0 = -2$, pa je sistem protivrečan.

$\triangle$

6.2 Vektorski prostor

Neka je $(V, +)$ komutativna grupa i $(P, +, \cdot)$ polje. Elemente skupa V nazivamo *vektori* i označavamo sa x, y, z, a elemente skupa P *skalari* i označavamo sa a, b, c. Neka je $\cdot : P \times V \to V$ operacija koju nazivamo *spoljašnje množenje*. (Primetimo da smo znakom $\cdot$ označili i operaciju množenja polja i spoljašnje množenje. Istim znakom smo označili i operaciju sabiranja skalara u polju i operaciju sabiranja vektora. Prema konvenciji o označavanju objekata u datom kontekstu će biti jasno o kojoj se operaciji radi.) Kažemo da grupa $(V, +)$ čini *vektorski prostor* nad poljem $(P, +, \cdot)$ akko važe sledeće aksiome.

1. $(\forall a \in P)(\forall x, y \in V)\, a \cdot (x + y) = a \cdot x + a \cdot y$
2. $(\forall a, b \in P)(\forall x \in V)\, (a + b) \cdot x = a \cdot x + b \cdot x$
3. $(\forall a, b \in P)(\forall x \in V)\, (a \cdot b) \cdot x = a \cdot (b \cdot x)$
4. $(\forall x \in V)\, 1 \cdot x = x$ gde $1 \in P$ jedinica polja.

Napomena 6.6 Vektorski prostor u obliku u kojem smo ga upravo definisali nije algebarska struktura jer operacije nisu definisane na zajedničkom skupu. Vektorski prostor se može definisati i u obliku

$$(V, +, \{f_a\}_{a \in P}, 0)$$

gde su f_a, za $a \in P$ unarne operacija na skupu V. Operacija f_a odgovara spoljašnjem množenju elementom a polja $(P, +, \cdot)$, dakle $f_a(x) = a \cdot x$. Za svaki element polja $a \in P$ uvodi se operacija $f_a : V \to V$ tako da za beskonačno polje P dobijamo algebru sa beskonačno mnogo operacija. $\diamond$

Navešćemo dva primera vektorskog prostora.

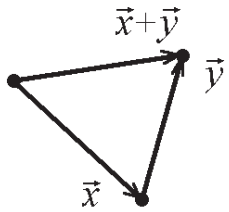
Primer 6.7 Neka je D^3 skup svih orjentisanih duži u prostoru. Uvedimo relaciju $\sim$ na skupu D^3. Ako su $x, y \in D^3$ duži u prostoru, tada $x \sim y$ akko x i y imaju isti

1. pravac,
2. smer (orjentaciju) i
3. dužinu.

Lako se pokazuje da je $\sim$ relacija ekvivalencije. Označimo sa V^3 skup $D^3/_\sim$. Elementi skupa V^3 se nazivaju *slobodni vektori* i označavaju se sa $\vec{x}, \vec{y}, \vec{z}$. *Intenzitet vektora* $\vec{x}$ je dužina proizvoljne duži koja predstavlja taj vektor i označava se sa $|\vec{x}|$. Na skupu V^3 definišemo operaciju sabiranja vektora sa

$$x/_\sim + y/_\sim = z/_\sim,$$

gde je $z/_\sim$ orjentisana duž dobijena nadovezivanjem orjentisanih duži x i y kao na slici.



Operacija $+$ na klasama je definisana preko svojih predstavnika i može se pokazati da je dobro definisana. Slično postupamo i sa ostalim operacijama. Suprotan vektor vektora $x/_\sim$ je vektor $y/_\sim$ gde je y orjentisana duž koja se od x razlikuje samo po tome što ima suprotan smer (dakle ima isti pravac i intenzitet). Za duži čija se početna i krajnja tačka poklapaju ne definišemo smer. Sve ovakve duži smatramo ekvivalentnim, a klasu ekvivalencije nazivamo nula-vektor i označavamo sa $\vec{0}$. Može se pokazati da je sa ovako definisanim operacijama $(V^3, +)$ grupa. Neka je $(R_e, +, \cdot)$ polje realnih brojeva. Ako je $a \in R_e$ i $\vec{x} \in V^3$, tada je $a \cdot \vec{x}$ vektor čiji je

1. pravac jednak pravcu vektora $\vec{x}$;
2. smer jednak smeru vektora $\vec{x}$ ako je $a > 0$, suprotan smeru vektora $\vec{x}$ ako je $a < 0$, a ako je $a = 0$ tada je $a \cdot \vec{x} = \vec{0}$;
3. intenzitet jednak $|a||\vec{x}|$.

Pokazuje se da je tada $(V^3, +)$ vektorski prostor nad poljem $(R_e, +, \cdot)$. $\triangle$

Primer 6.8 Neka je $(R_e^3, +) = (R_e, +)^3$ direktni stepen grupe realnih brojeva i $(R_e, +, \cdot)$ polje realnih brojeva. Proverom ustanovljavamo da $(R_e^3, +)$ čini vektorski prostor nad poljem $(R_e, +, \cdot)$ ako se operacija spoljašnjeg množenja definiše sa

$$a \cdot (x_1, x_2, x_3) = (ax_1, ax_2, ax_3).$$

Pokazuje se da je ovaj vektorski prostor izomorfan vektorskom prostoru slobodnih vektora. Izomorfizam pridružuje vektoru $(x_1, x_2, x_3) \in R_e^3$ slobodan vektor čiji je jedan predstavnik duž sa početnom tačkom u koordinatnom početku i krajnjom tačkom sa koordinatama (x_1, x_2, x_3) u Dekartovom koordinatnom sistemu. $\triangle$

Tvrđenje 6.9 *Neka je $(V, +)$ vektorski prostor nad poljem $(P, +, \cdot)$. Neka $x \in V$ i $a \in P$. Tada važe sledeća tvrđenja:*

1. $a \cdot \vec{0} = \vec{0}$
2. $0 \cdot x = \vec{0}$
3. $(-a) \cdot x = -(a \cdot x) = a \cdot (-x)$
4. $a \cdot x = \vec{0} \Rightarrow a = 0 \vee x = \vec{0}$.

Dokaz.

1. Kako je $a \cdot \vec{0} = a \cdot (\vec{0} + \vec{0}) = a \cdot \vec{0} + a \cdot \vec{0}$ i kako u grupi $(V, +)$ važi zakon skraćivanja, sledi $a \cdot \vec{0} = \vec{0}$.
2. Analogno prethodnom slučaju dobijamo $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, pa po zakonu skraćivanja $0 \cdot x = \vec{0}$.
3. Kako je $a \cdot x + (-a) \cdot x = (a + (-a)) \cdot x = 0 \cdot x = \vec{0}$ sledi da je $(-a) \cdot x$ inverzni element elementa $a \cdot x$ tj. $(-a) \cdot x = -(a \cdot x)$. Analogno, iz $a \cdot x + a \cdot (-x) = a \cdot (x + (-x)) = a \cdot \vec{0} = \vec{0}$ sledi $a \cdot (-x) = -(a \cdot x)$.
4. Neka je $a \cdot x = \vec{0}$. Ako je $a = 0$, tada tvrđenje važi. Ako je $a \neq 0$, tada postoji a^{-1}, pa je

   $$x = 1 \cdot x = (a^{-1} \cdot a) \cdot x = a^{-1} \cdot (a \cdot x) = a^{-1} \cdot \vec{0} = \vec{0},$$

   te tvrđenje važi i u ovom slučaju.

■

Definicija 6.10 *Linearna kombinacija* vektora $x^{(1)}, \ldots, x^{(n)} \in V$ je izraz oblika

$$a_1 x^{(1)} + \cdots + a_n x^{(n)},$$

gde $a_1, \ldots, a_n \in P$.

Ako za sve vrednosti $a_1, \ldots, a_n \in P$ važi

$$a_1 x^{(1)} + \cdots + a_n x^{(n)} = \vec{0} \qquad \Rightarrow \qquad a_1 = \cdots = a_n = 0,$$

onda za vektore $x^{(1)}, \ldots, x^{(n)}$ kažemo da su *linearno nezavisni*. U suprotnom kažemo da su linearno zavisni.

Primer 6.11 Posmatrajmo vektore $(1,0,0)$, $(0,1,0)$ i $(0,0,1)$ u prostoru $(R_e^3, +)$. Neka je

$$a_1(1,0,0) + a_2(0,1,0) + a_3(0,0,1) = (0,0,0).$$

Tada je

$$(a_1,0,0) + (0,a_2,0) + (0,0,a_3) = (0,0,0),$$

što povlači $(a_1, a_2, a_3) = (0,0,0)$, pa je $a_1 = a_2 = a_3 = 0$. Dakle vektori $(1,0,0)$, $(0,1,0)$ i $(0,0,1)$ su linearno nezavisni. $\triangle$

Primer 6.12 Posmatrajmo vektore $(1,0,1)$, $(0,1,0)$ i $(1,1,1)$. Zanima nas za koje vrednosti a_1, a_2, a_3 važi

$$a_1(1,0,1) + a_2(0,1,0) + a_3(1,1,1) = (0,0,0),$$

a to se svodi na

$$(a_1,0,a_1) + (0,a_2,0) + (a_3,a_3,a_3) = (0,0,0),$$

odnosno

$$\begin{aligned} a_1 + a_3 &= 0 \\ a_2 + a_3 &= 0 \\ a_1 + a_3 &= 0. \end{aligned}$$

Ovaj *homogen* sistem ima i netrivijalna rešenja. Jedno takvo rešenje je $a_1 = a_2 = 1$, $a_3 = -1$. Dakle vektori $(1,0,1)$, $(0,1,0)$ i $(1,1,1)$ nisu linearno nezavisni. $\triangle$

Definicija 6.13 Ako vektorski prostor $(V, +)$ sadrži n linearno nezavisnih vektora, a svakih $n+1$ vektora su linearno zavisni, kažemo da V ima *dimenziju* n i pišemo $\dim V = n$.

Definicija 6.14 *Baza* vektorskog prostora $(V,+)$ je skup vektora $B = \{e^{(1)},\dots,e^{(n)}\}$ tako da su vektori $e^{(1)},\dots,e^{(n)}$ linearno nezavisni, a za svaki vektor $x \in V$ vektori $e^{(1)},\dots,e^{(n)},x$ su linearno zavisni.

Iz prethodne definicije sledi sledeće tvrđenje.

Tvrđenje 6.15 *Neka je $B = \{e^{(1)},\dots,e^{(n)}\}$ baza vektorskog prostora. Tada za svaki vektor $x \in V$ postoje jedinstveni skalari $a_1,\dots,a_n$ tako da važi*

$$x = a_1e^{(1)} + \cdots + a_ne^{(n)}$$

Linearna zavisnost ima odgovarajuću geometrijsku interpretaciju ako se posmatraju slobodni vektori. Tako su u vektorskom prostoru slobodnih vektora vektori $e^{(1)}, e^{(2)}, e^{(3)}$ linearno nezavisni akko nisu komplanarni.

Definicija 6.16 Neka je $(V,+)$ vektorski prostor nad poljem $(P,+,\cdot)$. Preslikavanje $A : V \to V$ se naziva *linearna transformacija* akko važi:

$$\begin{aligned} A(x+y) &= A(x) + A(y) \\ A(a\cdot x) &= a\cdot A(x) \end{aligned}$$

Tvrđenje 6.17 *Neka je A linearna transformacija vektorskog prostora $(V,+)$ nad poljem $(P,+,\cdot)$. Tada je $A(\vec{0}) = \vec{0}$.*

Dokaz. Po definiciji linearne transformacije važi:

$$A(\vec{0}) = A(\vec{0}+\vec{0}) = A(\vec{0}) + A(\vec{0}),$$

a odatle primenom zakona skraćivanja sledi $A(\vec{0}) = \vec{0}$. ∎

6.3 Matrice

Matrica tipa (m,n) nad poljem $(P,+,\cdot)$ je preslikavanje $A : I \times J \to P$ gde je $I = \{1,\dots,m\}$ i $J = \{1,\dots,n\}$. Element $A(i,j)$ označavamo sa a_{ij}. Matricu A zapisujemo u obliku šeme:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Celu matricu zapisujemo i u obliku $[a_{ij}]_{m,n}$. Prema definiciji preslikavanja, $[a_{ij}]_{mn} = [b_{ij}]_{ts}$ važi akko $m = t$, $n = s$ i za sve $1 \leq i \leq m$ i $1 \leq j \leq n$ važi $a_{ij} = b_{ij}$. *Transponovana matrica* matrice $[a_{ij}]_{m,n}$, u oznaci $[a_{ij}]_{m,n}^T$ je matrica $[a_{ji}]_{n,m}$. Ako je $m = n$ matricu $[a_{ij}]_{mn}$ nazivamo *kvadratna matrica* reda m. *Jedinična matrica* je kvadratna matrica reda n kod koje je $a_{ii} = 1$, a $a_{ij} = 0$ za $i \neq j$:

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

Nula matrica tipa (m, n) je matrica $\mathbf{0} = [0]_{mn}$. Zbir matrica $[a_{ij}]_{m,n}$ i $[b_{ij}]_{m,n}$ istih formata je matrica data sa

$$[a_{ij}]_{m,n} + [b_{ij}]_{m,n} \stackrel{\text{def}}{=} [a_{ij} + b_{ij}]_{m,n}.$$

Ako je $[a_{ij}]_{m,n}$ proizvoljna matrica tada je rezultat njenog množenja brojem $k \in P$ matrica data sa

$$k \cdot [a_{ij}]_{m,n} = [k \cdot a_{ij}]_{m,n}.$$

Vektor je matrica tipa $(1, n)$ ili $(n, 1)$.

Na osnovu prethodnih definicija pokazuje se da važe sledeća tvrđenja.

Tvrđenje 6.18 *Skup matrica istog tipa u odnosu na sabiranje matrica je komutativna grupa.*

Tvrđenje 6.19 *Grupa matrica istog tipa u odnosu na množenje elementom polja* $(P, +, \cdot)$ *čini vektorski prostor nad poljem* $(P, +, \cdot)$.

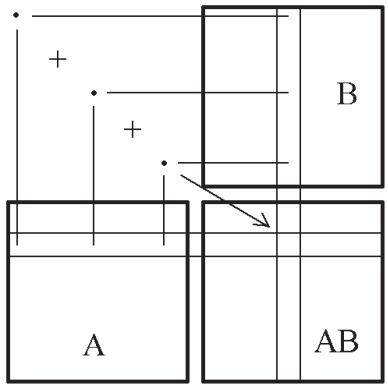
Definicija 6.20 Neka su date matrice $A = [a_{ij}]_{m,r}$ i $B = [b_{ij}]_{r,n}$. Proizvod matrica A i B je matrica tipa (m, n) data sa

$$[a_{ij}]_{m,r} \cdot [b_{ij}]_{r,n} = [a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ir} \cdot b_{rj}]_{m,n}$$

Ako postoji proizvod matrica A i B, ne mora postojati proizvod matrica B i A. Ako postoje oba proizvoda tada rezultat ne moraju biti matrice istog tipa, a ako i jesu istog tipa ne moraju biti jednake. Dakle, množenje matrica nije komutativno.

Primer 6.21

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



dok je

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

$\triangle$

Primer 6.22 Neka je u pravouglom koordinatnom sistemu xOy data tačka $M(x, y)$ i neka je izvršena rotacija koordinatnog sistema xOy oko koordinatnog početka O za ugao α u pozitivnom smeru. Neka su x_1 i x_2 koordinate tačke M u novom koordinatnom sistemu x_1Oy_1.

Tada važi

$$\begin{aligned} x &= x_1 \cos\alpha - y_1 \sin\alpha \\ y &= x_1 \sin\alpha + y_1 \cos\alpha \end{aligned}$$

ili u matričnom obliku

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}$$

Matrica

$$\begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$

dakle opisuje rotaciju u R^2_e oko koordinatnog početka za ugao α. $\triangle$

Može se pokazati da postoji bijekcija između linearnih transformacija i matrica, što ilustrujemo sledećim primerom.

Primer 6.23 Neka je $(V,+) = (R_e^3,+)$ vektorski prostor nad poljem $(R_e,+,\cdot)$. Neka je $A : R_e^3 \to R_e^3$ preslikavanje dato sa

$$A((x,y,z)) = (2x+y+z, x+2y, x-y-2z).$$

Direktno se proverava da je A linearna transformacija. Baza ovog vektorskog prostora je $B = \{(1,0,0),(0,1,0),(0,0,1)\}$. Nađimo slike elemanata baze pod transformacijom A.

$$A((1,0,0)) = (2,1,1)$$
$$A((0,1,0)) = (1,2,-1)$$
$$A((0,0,1)) = (1,0,-2)$$

Tada linearnoj transformaciji A odgovara matrica

$$\begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & -1 & -2 \end{bmatrix}$$

čije kolone odgovaraju slikama elemenata baze. $\triangle$

6.4 Determinante

Definicija 6.24 Permutacija f skupa A je bijektivno preslikavanje $f : A \to A$.

Mi ćemo posmatrati permutacije skupa $\{1,2,\ldots,n\}$. Skup svih takvih permutacija označavamo sa S_n. Sliku $p(i)$ elementa i permutacije $p \in S_n$ označavamo sa p_i, a celu permutaciju p sa $(p_1,\ldots,p_n)$. Nad skupom od n elemenata postoji $n!$ permutacija, što se lako proverava indukcijom.

Definicija 6.25 Elementi p_i i p_j permutacije p su u *inverziji* akko je $i < j$ i $p_i > p_j$.

Ukupan broj inverzija u permutaciji p označavamo sa $r(p)$. Ukoliko je taj broj paran, kažemo da je permutacija parna. U suprotnom kažemo da je permutacija neparna. Primetimo da je broj inverzija u permutaciji p jednak broju inverzija u njoj inverznoj permutaciji p^{-1}. To je zbog toga što svaka inverzija elemenata $p_i > p_j$ za $i < j$ u permutaciji p odgovara inverziji $p_k^{-1} > p_l^{-1}$ za $k < l$ ako stavimo $k = p_j$ i $l = p_i$.

Definicija 6.26 *Transpozicija* $t_{i,j}$ (za $i < j$) je permutacija koja menja mesta elementima i i j:

$$t_{i,j}(i) = j$$
$$t_{i,j}(j) = i$$
$$t_{i,j}(k) = k, \qquad k \neq i, k \neq j$$

Elementarna transpozicija je transpozicija oblika $t_{i,i+1}$ za $1 \leq i \leq n-1$.

Lema 6.27 *Svaka elementarna transpozicija menja parnost permutacije.*

Dokaz. Neka je p proizvoljna permutacija i $t_{i,i+1}$ elementarna transpozicija. Pokazaćemo da permutacija $t_{i,i+1} \circ p$ ima uvek jednu manje ili jednu više inverziju od permutacije p. Poredak elemenata p_i i p_j u odnosu na ostale elemente p_k za $k \neq i, j$ se primenom transpozicije ne menja, kao ni međusobni poredak elemenata p_k za $k \neq i, j$. Označimo sa q broj inverzija koji potiču od parova elemenata od kojih je bar jedan p_k za $k \neq i, j$. Ako je $p_i < p_{i+1}$ tada elementi p_i i p_{i+1} nisu u inverziji, pa je $r(p) = q$. U permutaciji $t_{i,i+1} \circ p$ elementi p_i i p_{i+1} zamene mesta pa su u inverziji, zato je $r(t_{i,i+1} \circ p) = q + 1$. Ako je pak $p_i > p_{i+1}$ tada su elementi p_i i p_{i+1} u inverziji u permutaciji p, ali nisu u inverziji u permutaciji $t_{i,i+1} \circ p$. Zato je $r(p) = q + 1$ i $r(t_{i,i+1} \circ p) = q$. U svakom slučaju $r(p)$ i $r(t_{i,i+1} \circ p)$ su različite parnosti, što je i trebalo dokazati. ∎

Lema 6.28 *Svaka transpozicija menja parnost permutacije.*

Dokaz. Neka je p proizvoljna permutacija, t_{ij} proizvoljna transpozicija i neka je $k = j - i - 1$. Između elemenata p_i i p_j se u permutaciji p nalazi k elemenata. Da bismo zamenili mesta elementima p_i i p_j možemo dovesti element p_i do elementa p_j primenom k elementarnih transpozicija, zatim promeniti mesta elementima p_i i p_j jednom elementarnom transpozicijom i potom vratiti element p_j na mesto gde je bio element p_i sa k elementarnih transpozicija. Ukupno je za zamenu mesta elemenata p_i i p_j potrebno $2k+1$ elementarnih transpozicija. Kako svaka elementarna transpozicija menja parnost permutacije, rezultujuća transpozicija $t_{i,j}$ će takođe menjati parnost permutacije. ∎

Definicija 6.29 *Determinanta* kvadratne matrice $[a_{ij}]_{n,n}$ nad poljem $(P, +, \cdot)$, u oznaci $\det A$ ili $|A|$, je data sa

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \ddots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \sum_{p \in S_n} (-1)^{r(p)} a_{1p_1} \cdots a_{np_n}.$$

Za matricu reda 1 dobijamo $\det[a_{11}] = a_{11}$. Za matricu reda 2 definicija se svodi na

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21},$$

a za matricu reda 3 dobijamo

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} =$$

$$a_{11}a_{22}a_{33} - a_{11}a_{23}a_{33} + a_{12}a_{23}a_{31} - a_{12}a_{21}a_{33} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}.$$

Za determinantu matrice reda 3 vrednost determinante se može računati i po sledećem Sarusovom pravilu (E. Sarrus):

$$\begin{array}{ccc|cc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array}$$

Trojke na opadajućoj dijagonali se računaju sa znakom $+$, a trojke na rastućoj dijagonali sa znakom $-$.

Postupak računanja determinanti se pojednostavljuje ako matrica sadrži nule. Zbog toga su posebno značajne transformacije matrice kojima se matrica može dovesti na oblik koji sadrži veći broj nula.

Tvrđenje 6.30 *Determinanta se ne menja ako se u matrici vrste zamene kolonama uz očuvanje poretka (dakle važi $|A| = |A^T|$ za svaku kvadratnu matricu A).*

Dokaz. Neka je data matrica $A = [a_{ij}]_{n,n}$ i neka je $B = [b_{ij}]_{n,n}$ njena transponovana matrica, gde je $b_{ij} = a_{ji}$. Posmatrajmo proizvoljni sabirak $s = (-1)^{r(p)} b_{1p_1}, \ldots, b_{np_n}$ u izrazu za determinantu matrice B. On je jednak $(-1)^{r(p)} a_{p_1 1}, \ldots, a_{p_n n}$. Primenom komutativnosti i asocijativnosti množenja možemo sortirati činioce u proizvodu po prvom indeksu. Ako u činiocu $a_{p_k k}$ stavimo $j = p_k$, tada iz $k = p_j^{-1}$ dobijamo $a_{p_k k} = a_{j p_j^{-1}}$, gde je p^{-1} inverzna permutacija permutacije p. Time $a_{p_1 1}, \ldots, a_{p_n n}$ postaje $a_{1 p_1^{-1}}, \ldots, a_{n p_n^{-1}}$. Kako je broj inverzija u permutaciji p jednak broju inverzija u njoj inverznoj permutaciji p^{-1}, dakle $r(p) = r(p^{-1})$, što povlači

$$s = (-1)^{r(p^{-1})} a_{1 p_1^{-1}} \ldots a_{n p_n^{-1}}$$

To znači da je sabirak s u izrazu za determinantu matrice B koji je određen permutacijom p jednak sabirku koji je određen permutacijom p^{-1} u izrazu za determinantu matrice A. Sumiranje po svim inverznim permutacijama permutacija skupa S_n je ekvivalentno sumiranju po svim permutacijama skupa S_n, pa su i cele determinante jednake. ∎

Prethodno tvrđenje pokazuje da su vrste i kolone ravnopravne kada se razmatraju determinante matrica. Zato ćemo u nastavku podrazumevati da tvrđenja koja navodimo za vrste analogno važe i za kolone (i obrnuto).

Tvrđenje 6.31 *Ako su u matrici A elementi jedne vrste jednaki elementima druge vrste, tada je $|A| = 0$.*

Dokaz. Neka je i-ta vrsta jednaka j-toj vrsti matrice A: $a_{ik} = a_{jk}$ za $1 \leq k \leq n$. Uočimo proizvoljan član s u izrazu za determinantu matrice A određen permutacijom p:

$$s = (-1)^{r(p)} a_{1p_1} \cdots a_{ip_i} \cdots a_{jp_j} \cdots a_{np_n}.$$

Izraz za determinantu takođe sadrži i član s' određen permutacijom $p' = t_{ij} \circ p$:

$$s' = (-1)^{r(p')} a_{1p_1} \cdots a_{ip_j} \cdots a_{jp_i} \cdots a_{np_n}.$$

Kako su i-ta i j-ta vrsta jednake, sledi $a_{ip_j} = a_{jp_j}$ i $a_{jp_i} = a_{ip_i}$, pa je

$$a_{1p_1} \cdots a_{ip_i} \cdots a_{jp_j} \cdots a_{np_n} = a_{1p_1} \cdots a_{ip_j} \cdots a_{jp_i} \cdots a_{np_n}. \qquad (*)$$

Permutacija p' je dobijena primenom transpozicije na permutaciju p, pa su permutacije različite parnosti, što povlači

$$(-1)^{r(p')} = -(-1)^{r(p)}. \qquad (**)$$

Iz $(*)$ i $(**)$ dobijamo $s' = -s$. Svakom sabirku s odgovara tačno jedan sabirak s' dobijen primenom transpozicije na permutaciju s, a sabirku s' odgovara upravo sabirak s. Tako se ceo zbir koji predstavlja vrednost determinante razbija na $n!/2$ parova čiji je zbir nula, pa je i $|A| = 0$. ∎

Tvrđenje 6.32 *Ako je matrica A_1 dobijena od matrice A tako što je svaki element jedne vrste matrice A pomnožen brojem λ, onda je $|A_1| = \lambda|A|$.*

Dokaz. Neka je matrica A_1 dobijena od matrice A množenjem vrste i brojem λ. Tada je

$$\begin{aligned} |A_1| &= \sum_{p \in S_n} (-1)^{r(p)} a_{1p_1} \cdots (\lambda a_{ip_i}) \cdots a_{np_n} \\ &= \lambda \sum_{p \in S_n} (-1)^{r(p)} a_{1p_1} \cdots a_{ip_i} \cdots a_{np_n} \\ &= \lambda |A|. \end{aligned}$$

∎

Tvrđenje 6.33 *Ako su u matrici A elementi jedne vrste proporcionalni elementima druge vrste, tada je $|A| = 0$.*

Dokaz. Neka su u matrici A elementi k-te vrste jednaki elementima l-te vrste pomnoženi brojem λ. Tada prema prethodnom tvrđenju važi $|A| = \lambda|A'|$ gde su u matrici A' vrste k i l jednake. Prema tvrđenju 6.31 tada je $|A'| = 0$, odakle sledi $|A| = 0$. ∎

Tvrđenje 6.34 *Ako se matrice A i B razlikuju samo po k-toj vrsti, tada je $|A| + |B| = |C|$ gde je k-ta vrsta matrice C jednaka zbiru k-tih vrsta matrica A i B, a ostale vrste su jednake odgovarajućim vrstama matrica A i B:*

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{k1}+c_{k1} & b_{k2}+c_{k2} & \cdots & b_{kn}+c_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{k1} & b_{k2} & \cdots & b_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{k1} & c_{k2} & \cdots & c_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

Dokaz.

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{k1}+c_{k1} & b_{k2}+c_{k2} & \cdots & b_{kn}+c_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} =$$

$$= \sum_{p\in S_n} (-1)^{r(p)} a_{1p_1} \cdots (b_{kp_k} + c_{kp_k}) \cdots a_{np_n}$$

$$= \sum_{p\in S_n} \left((-1)^{r(p)} a_{1p_1} \ldots b_{kp_k} \ldots a_{np_n} + (-1)^{r(p)} a_{1p_1} \ldots c_{kp_k} \ldots a_{np_n} \right)$$

$$= \sum_{p\in S_n} (-1)^{r(p)} a_{1p_1} \ldots b_{kp_k} \ldots a_{np_n} + \sum_{p\in S_n} (-1)^{r(p)} a_{1p_1} \ldots c_{kp_k} \ldots a_{np_n}$$

$$= \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{k1} & b_{k2} & \cdots & b_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{k1} & c_{k2} & \cdots & c_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

■

Tvrđenje 6.35 *Determinanta se ne menja ako se elementima jedne vrste dodaju elementi druge vrste prethodno pomnoženi istim brojem.*

Dokaz. Pokazaćemo da je determinanta matrice u kojoj je k-ta vrsta dodata l-toj vrsti jednaka polaznoj matrici koristeći tvrđenja 6.34 i 6.33.

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{l1}+\lambda a_{k1} & a_{l2}+\lambda a_{k2} & \cdots & a_{ln}+\lambda a_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

$$= \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{l1} & a_{l2} & \cdots & a_{ln} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ \lambda a_{k1} & \lambda a_{k2} & \cdots & \lambda a_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

$$= \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{l1} & a_{l2} & \cdots & a_{ln} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + 0 = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{l1} & a_{l2} & \cdots & a_{ln} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}.$$

■

Tvrđenje 6.36 *Ako dve vrste u matrici zamene mesta, determinanta matrice menja znak.*

Dokaz. Neka je A proizvoljna kvadratna matrica. Pokazaćemo da se zamenom vrsta k i

l menja znak determinante. Prvo primenom tvrđenja 6.35 vrstu l dodamo vrsti k:

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{l1} & a_{l2} & \cdots & a_{ln} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1}+a_{l1} & a_{k2}+a_{l2} & \cdots & a_{kn}+a_{l2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{l1} & a_{l2} & \cdots & a_{ln} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

Zatim primenom tvrđenja 6.35 vrstu k pomnoženu sa -1 dodamo vrsti l, dobijamo

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1}+a_{l1} & a_{k2}+a_{l2} & \cdots & a_{kn}+a_{l2} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{k1} & -a_{k2} & \cdots & -a_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

Konačno primenom tvrđenja 6.32 izvučemo -1 ispred determinante:

$$|A| = - \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{l1} & a_{l2} & \cdots & a_{l2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

■

Tvrđenje 6.37 *Neka su A i B kvadratne matrice reda n. Tada je*

$$|A \cdot B| = |A| \cdot |B|.$$

Dokaz. Za matrice $A = [a_{ij}]_{n,n}$ i $B = [b_{ij}]_{n,n}$ je $A \cdot B = [\sum_{k=1}^{n} a_{ik} b_{kj}]_{n,n}$. Na osnovu tvrđenja 6.34 dobijamo da je $|AB|$ jednaka zbiru determinanti oblika

$$\begin{vmatrix} a_{1p_1} b_{p_1 1} & a_{1p_2} b_{p_2 2} & \cdots & a_{1p_n} b_{p_n n} \\ a_{2p_1} b_{p_1 1} & a_{2p_2} b_{p_2 2} & \cdots & a_{2p_n} b_{p_n n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{np_1} b_{p_1 1} & a_{np_2} b_{p_2 2} & \cdots & a_{np_n} b_{p_n n} \end{vmatrix}$$

gde se sumiranje vrši po svim preslikavanjima $(p_1, \ldots, p_n)$ skupa $\{1, \ldots, n\}$ na sebe. Prema tvrđenju 6.32, svaki od ovih sabiraka je jednak

$$b_{p_1 1} b_{p_2 2} \cdots b_{p_n n} \begin{vmatrix} a_{1p_1} & a_{1p_2} & \cdots & a_{1p_n} \\ a_{2p_1} & a_{2p_2} & \cdots & a_{2p_n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{np_1} & a_{np_2} & \cdots & a_{np_n} \end{vmatrix} \tag{6.1}$$

Ako su neki od brojeva $p_1, \ldots, p_n$ jednaki, onda je sabirak 6.1 jednaka nuli (zbog tvrđenja 6.31). Ako su svi brojevi $p_1, \ldots, p_n$ međusobno različiti, tada je p permutacija, pa se sabirak 6.1 primenom tvrđenja 6.36 svodi na

$$(-1)^{r(p)} b_{p_1 1} \ldots b_{p_n n} |A|.$$

Tako dolazimo do

$$\begin{aligned} |A \cdot B| &= |A| \cdot \sum_{p \in S_n} (-1)^{r(p)} b_{p_1 1} \ldots b_{p_n n} \\ &= |A||B^T| = |A||B|. \end{aligned}$$

■

Definicija 6.38 Neka je data kvadratna matrica $A = [a_{ij}]_{n,n}$ reda n. *Minor* elementa a_{ij}, u oznaci M_{ij}, je determinanta kvadratne matrice reda $n-1$ koja se dobija od matrice A izbacivanjem i-te vrste i j-te kolone. *Algebarski komplement* elementa a_{ij}, u oznaci A_{ij}, je $(-1)^{i+1} M_{ij}$.

Tvrđenje 6.39

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \ddots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = a_{11} A_{11} + a_{12} A_{12} + \cdots + a_{1n} A_{1n}$$

Dokaz. Sve permutacije skupa S_n možemo razbiti prema prvom elementu p_1 na n klasa. U j-toj klasi se nalaze sve permutacije za koje je $p_1 = j$. Tada ostali elementi $(p_2, \ldots, p_n)$ čine permutaciju elemenata skupa $S' = \{1, \ldots, n\} \setminus \{j\}$, označimo tu permutaciju sa p'. Pošto je element j na prvom mestu, on je u inverziji sa svim elementima manjim od njega. Zato važi $r(p) = j - 1 + r(p')$. Stoga je

$$\begin{aligned} &(-1)^{r(p)} a_{1j} a_{2p_2} \cdots a_{np_n} \\ &\quad = a_{1j} (-1)^{j-1+r(p')} a_{2p_2} \cdots a_{np_n} \\ &\quad = a_{1j} (-1)^{j+1} (-1)^{r(p')} a_{2p_2} \cdots a_{np_n}. \end{aligned}$$

Zato možemo pisati

$$\begin{aligned} |A| &= \sum_{1\le j\le n}\sum_{p'\in S'} a_{1j}(-1)^{j+1}(-1)^{r(p')}a_{2p_2}\cdots a_{np_n} \\ &= \sum_{1\le j\le n} a_{1j}(-1)^{j+1}\sum_{p'\in S'}(-1)^{r(p')}a_{2p_2}\cdots a_{np_n} \\ &= \sum_{1\le j\le n} a_{1j}A_{1j}. \end{aligned}$$

■

Tvrđenje 6.40 (Laplas) *(M. Laplace) Neka je data matrica $A = [a_{ij}]_{n,n}$ i neka je $1 \le i \le n$. Tada je:*

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \ddots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in}.$$

Dokaz. Neka je B matrica dobijena od matrice A pomoću $i-1$ uzastopnih promena susednih vrsta tako da se i-ta vrsta matrice A nalazi na prvom mestu:

$$B = \begin{bmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \\ a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \ddots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}.$$

Prema tvrđenju 6.36 tada je $|A| = (-1)^{i-1}|B|$. Prema prethodnom tvrđenju 6.39, važi

$$|B| = \begin{vmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \\ a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \ddots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = a_{i1}(-1)^{1+1}M_{i1} + \cdots + a_{in}(-1)^{1+n}M_{1n}.$$

Iz prethodnih formula dobijamo

$$|A| = a_{i1}A_{i1} + \cdots + a_{in}A_{in}.$$

■

Tvrđenje Laplasa omogućava da determinantu reda n *razvijemo* po proizvoljnoj vrsti ili koloni i tako svedemo na n determinanti reda $n-1$. Pri tome obično biramo vrstu koja ima najveći broj nula jer su sabirci $a_{ij}A_{ij}$ za $a_{ij} = 0$ jednaki nuli, pa A_{ij} ne moramo računati. Specijalno, ako je cela vrsta ili kolona u matrici jednaka 0, tada je i determinanta matrice 0.

Tvrđenje 6.41 *Neka je $A = [a_{ij}]_{n,n}$ proizvoljna matrica, $1 \leq i, j \leq n$ i $i \neq j$. Tada je*

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + A_{in}A_{jn} = 0.$$

Dokaz. Prema definiciji algebarskog komplementa, vrednosti $A_{j1}, \ldots, A_{jn}$ ne zavise od elemenata koji se nalaze u j-toj vrsti. Neka je B matrica koja u j-toj vrsti ima elemente jednake i-toj vrsti matrice A, a elementi u ostalim vrstama su jednaki odgovarajućim elementima u matrici A. Tada je prema tvrđenju 6.40 (ako izvršimo razvoj po j-toj vrsti):

$$|B| = b_{j1}A_{j1} + \cdots + b_{jn}A_{jn} = a_{i1}A_{j1} + \cdots + a_{in}A_{jn}.$$

Kako je u matrici B i-ta vrsta jednaka j-toj vrsti, prema tvrđenju 6.31 važi $|B| = 0$, odakle sledi traženo tvrđenje. ∎

Van der Mondova determinanta Van der Mondova (A. Van der Mond) determinanta je determinanta sledeće matrice reda n:

$$A = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \cdots & \cdots & \ddots & \cdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{bmatrix}$$

Može se pokazati da je

$$|A| = \prod_{1 \leq i < j \leq n} (x_j - x_i),$$

odakle sledi da je $|A| \neq 0$ akko su svi elementi $x_1, \ldots, x_n$ različiti. Proverimo ovaj stav za Van der Mondovu determinantu reda 3. Primenićemo prethodno dokazana tvrđenja da bismo izračunali determinantu

$$\begin{vmatrix} 1 & 1 & 1 \\ x & y & z \\ x^2 & y^2 & z^2 \end{vmatrix}.$$

Ako prvu kolonu pomnoženu sa -1 dodamo drugoj i trećoj, dobijamo

$$\begin{vmatrix} 1 & 0 & 0 \\ x & y-x & z-x \\ x^2 & y^2-x^2 & z^2-x^2 \end{vmatrix}$$

što se izvlačenjem faktora $y - x$ iz druge i $z - x$ iz treće kolone svodi na

$$(y-x)(z-x) \begin{vmatrix} 1 & 0 & 0 \\ x & 1 & 1 \\ x^2 & y+x & z+x \end{vmatrix}$$

a to razvojem po prvoj vrsti daje

$$\begin{aligned}(y-x)(z-x)\begin{vmatrix}1 & 1\\ y+x & z+x\end{vmatrix} &= (y-x)(z-x)(z+x-y-x)\\ &= (y-x)(z-x)(z-y).\end{aligned}$$

Primer 6.42 Izračunajmo vrednost determinante:

$$D_n=\begin{vmatrix}a+1 & a & 0 & \cdots & 0 & 0\\ 1 & a+1 & a & \cdots & 0 & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & 0 & \cdots & a+1 & a\\ 0 & 0 & 0 & \cdots & 1 & a+1\end{vmatrix}$$

Razvijanjem D_n po elementima prve kolone, dobija se

$$D_n=(a+1)D_{n-1}-\begin{vmatrix}a & 0 & \cdots & 0 & 0\\ 1 & a+1 & \cdots & 0 & 0\\ \cdot & \cdot & \cdot & \cdot & \cdot\\ 0 & 0 & \cdots & a+1 & 0\\ 0 & 0 & \cdots & 1 & a\end{vmatrix}$$

tj. $D_n=(a+1)D_{n-1}-aD_{n-2}$. Služeći se ovom formulom možemo dobiti opšti izraz za D_n. Iz gornje formule imamo

$$D_n-aD_{n-1}=D_{n-1}-aD_{n-2}, \qquad \text{za } n>2.$$

Neposredno se proverava da je D_i-aD_{i-1} za sve $i=3,4,\ldots,n$ konstantna veličina. Kako su

$$\begin{aligned}D_2 &= \begin{vmatrix}a+1 & a\\ 1 & a+1\end{vmatrix}=a^2+a+1\\ D_3 &= \begin{vmatrix}a+1 & a & 0\\ 1 & a+1 & a\\ 0 & 1 & a+1\end{vmatrix}=a^3+a^2+a+1\end{aligned}$$

to je $D_3-aD_2=1$. Dakle, imamo $D_n-aD_{n-1}=1$ ili $D_n=aD_{n-1}+1$. Iz poslednje formule dobijamo sledeći sistem jednakosti:

$$\begin{aligned}D_n &= aD_{n-1}+1\\ D_{n-1} &= aD_{n-2}+1\\ &\cdots\\ D_3 &= aD_2+1.\end{aligned}$$

Odavde je

$$D_n = a(aD_{n-2} + 1) + 1 = \ldots = a^{n-2}D_2 + a^{n-3} + a^{n-4} + \cdots + a + 1.$$

Zamenjujući D_2 dobijamo na kraju

$$D_n = a^n + a^{n-1} + \cdots + a + 1.$$

$\triangle$

6.5 Sistemi n linearnih jednačina sa n nepoznatih

U ovom odeljku govorimo o vezi matrica i determinanti sa sistemima linearnih jednačina. Jednostavnosti radi, razmatraćemo samo sisteme od 3 jednačine sa 3 nepoznate, ali se tvrđenja koja ćemo navesti mogu uopštiti na proizvoljan sistem od n jednačina sa n nepoznatih za $n \in N$, i na analogan način dokazati.

Definicija 6.43 Neka je dat sistem od 3 jednačine sa tri nepoznate.

$$\begin{array}{l} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = b_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = b_3 \end{array} \qquad (S)$$

Determinanta sistema je data sa

$$D = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix},$$

a determinante promenljivih sa

$$D_1 = \begin{vmatrix} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & a_{23} \\ b_3 & a_{32} & a_{33} \end{vmatrix} \qquad D_2 = \begin{vmatrix} a_{11} & b_1 & a_{13} \\ a_{21} & b_2 & a_{23} \\ a_{31} & b_3 & a_{33} \end{vmatrix}$$

$$D_3 = \begin{vmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ a_{31} & a_{32} & b_3 \end{vmatrix}.$$

Tvrđenje 6.44 *Ako je $D \neq 0$, tada sistem ima jedinstveno rešenje i ono je dato* Kramerovim *(G. Cramer)* formulama*:*

$$x_1 = \frac{D_1}{D} \qquad x_2 = \frac{D_2}{D} \qquad x_3 = \frac{D_3}{D}.$$

Dokaz. Neka je (x_1, x_2, x_3) rešenje sistema (S). Tada je

$$x_1 D = x_1 \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a_{11}x_1 & a_{12} & a_{13} \\ a_{21}x_1 & a_{22} & a_{23} \\ a_{31}x_1 & a_{32} & a_{33} \end{vmatrix}$$

što posle dodavanja druge kolone pomnožene sa x_2 i treće kolone pomnožene sa x_3 prvoj koloni daje

$$\begin{vmatrix} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 & a_{12} & a_{13} \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 & a_{22} & a_{23} \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & a_{23} \\ b_3 & a_{32} & a_{33} \end{vmatrix} = D_1.$$

Dakle, $x_1 D = D_1$, a analogno se dobija i $x_2 D = D_2$ i $x_3 D = D_3$. Ako je $D \neq 0$ tada za svako rešenje (x_1, x_2, x_3) važi $x_1 = D_1/D$, $x_2 = D_2/D$ i $x_3 = D_3/D$, pa može postojati najviše jedno rešenje. Treba još pokazati da $(D_1/D, D_2/D, D_3/D)$ jeste rešenje sistema. Zamenimo vrednosti $(D_1/D, D_2/D, D_3/D)$ u i-tu jednačinu ($i \in \{1, 2, 3\}$).

$$a_{i1}\frac{D_1}{D} + a_{i2}\frac{D_2}{D} + a_{i3}\frac{D_3}{D} = \frac{1}{D}(a_{i1}D_1 + a_{i2}D_2 + a_{i3}D_3).$$

Ako D_1 razvijemo po prvoj, D_2 po drugoj, a D_3 po trećoj koloni, dobijamo

$$\frac{1}{D}\Big(a_{i1}(b_1A_{11} + b_2A_{21} + b_3A_{31}) + a_{i2}(b_1A_{12} + b_2A_{22} + b_3A_{32}) + a_{i3}(b_1A_{13} + b_2A_{23} + b_3A_{33})\Big),$$

što posle sređivanja postaje

$$\frac{1}{D}\Big(b_1(a_{i1}A_{11} + a_{i2}A_{12} + a_{i3}A_{13}) + b_2(a_{i1}A_{21} + a_{i2}A_{22} + a_{i3}A_{23}) + b_3(a_{i1}A_{31} + a_{i2}A_{32} + a_{i3}A_{33})\Big).$$

Prema tvrđenjima 6.40 i 6.41, izraz uz b_j ($j \in \{1, 2, 3\}$) će biti 0 za $j \neq i$, a D ako je $j = i$. Tako dobijamo

$$\frac{1}{D}b_i D = b_i$$

što znači da je i-ta jednačina zadovoljena. Dakle rešenje $(D_1/D,\ D_2/D,\ D_3/D)$ zadovoljava sve tri jednačine, a svako rešenje je tog oblika, pa je to jedinstveno rešenje. ∎

Ako je $D = 0$, onda se sistem rešava primenom Gausovog postupka.

Posmatrajmo sada homogen sistem. U njemu je $b_1 = b_2 = b_3 = 0$, pa svaka od determinanti D_1, D_2, D_3 ima u jednoj koloni samo nule. Zato je $D_1 = D_2 = D_3 = 0$. Ako je $D \neq 0$, tada je $x_1 = D_1/D = 0$, $x_2 = D_2/D = 0$ i $x_3 = D_3/D = 0$, pa sistem ima samo jedno, trivijalno rešenje. Dakle da bi sistem imao i netrivijalna rešenja, mora biti $D = 0$.

Dalje proučavanje sistema linearnih jednačina zahteva detaljnije poznavanje matričnog računa.

6.6 Inverzne matrice i primena

Pojmovi vezani za inverzne matrice se uvode za proizvoljnu kvadratnu matricu reda n. Mi ćemo se ovde ograničiti samo na matrice reda 3, mada sva tvrđenja važe za matrice proizvoljnog reda n i analogno se dokazuju.

Definicija 6.45 *Adjungovana matrica* matrice

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

je matrica

$$\operatorname{adj} A = \begin{bmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{bmatrix}.$$

Tvrđenje 6.46 *Neka je A matrica reda n. Tada je*

$$A \cdot \operatorname{adj} A = \operatorname{adj} A \cdot A = |A| \cdot I_n$$

gde je I_n jedinična matrica reda n.

Dokaz. Prema tvrđenju 6.40 proizvod i-te vrste matrice A i i-te kolone matrice $\operatorname{adj} A$ je jednak $|A|$. Prema tvrđenju 6.41 proizvod i-te vrste matrice A i j-te kolone matrice $\operatorname{adj} A$ za $j \neq i$ je jednak 0. Zato je

$$A \cdot \operatorname{adj} A = \begin{bmatrix} |A| & 0 & \dots & 0 \\ 0 & |A| & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & |A| \end{bmatrix} = |A| \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix},$$

a analogno se dobija i za $\operatorname{adj} A \cdot A$. ∎

Definicija 6.47 Ako za kvadratnu matricu A reda n postoji matrica B tako da važi $A \cdot B = B \cdot A = I_n$, kažemo da je B *inverzna matrica* matrice A.

Kako je množenje matrica asocijativno, iz tvrđenja 1.26 sledi da ako inverzna matrica postoji, onda je ona jedinstvena. Označavamo je sa A^{-1}.

Tvrđenje 6.48 *Kvadratna matrica A reda n ima inverznu matricu akko je $|A| \neq 0$. (Ako je $|A| \neq 0$, onda za matricu A kažemo da je regularna).*

Dokaz.

($\Rightarrow$): Neka A ima inverznu matricu A^{-1}. Tada je $A \cdot A^{-1} = I$. Prema tvrđenju 6.37 važi $1 = |I| = |A \cdot A^{-1}| = |A| \cdot |A^{-1}|$. Iz $|A| = 0$ bi sledilo $1 = 0$, pa je $|A| \neq 0$.

($\Leftarrow$): Neka je $|A| \neq 0$. Tada postoji $\frac{1}{|A|}$. Prema tvrđenju 6.46 tada važi

$$A \cdot \left(\frac{1}{|A|} \operatorname{adj} A \right) = \left(\frac{1}{|A|} \operatorname{adj} A \right) \cdot A = I,$$

pa je

$$A^{-1} = \frac{1}{|A|} \operatorname{adj} A.$$

■

Kramerove formule za sistem od n linearnih jednačina sa n nepoznatih se mogu izvesti primenom inverzne matrice.

Sistem jednačina

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\cdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= b_n \end{aligned}$$

može se zapisati u matričnom obliku

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{bmatrix},$$

tj. u obliku $A \cdot X = B$ gde je

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}, \qquad X = \begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{bmatrix}, \qquad B = \begin{bmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{bmatrix}.$$

Neka je $|A| \neq 0$. Tada rešavajući matričnu jednačinu

$$A \cdot X = B$$

po X tj. množeći sa A^{-1} i to sa leve strane jednačinu $A \cdot X = B$, dobijamo

$$\begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{bmatrix} = \frac{1}{|A|} \begin{bmatrix} b_1A_{11} + \cdots + b_nA_{n1} \\ b_1A_{12} + \cdots + b_nA_{n2} \\ \cdots \\ b_1A_{1n} + \cdots + b_nA_{nn} \end{bmatrix}$$

odakle sledi

$$x_k = \frac{1}{|A|}\left(b_1A_{1k} + b_2A_{2k} + \cdots + b_nA_{nk}\right)$$

za $k = 1, 2, \ldots, n$ tj.

$$x_k = \frac{D_k}{D}$$

gde je D determinanta sistema, tj. matrice A, a D_k determinanta promenljive x_k.

Primer 6.49 Neka je dat skup

$$A = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in R_e \right\}.$$

Pokazaćemo da je $\mathbf{A} = (A, +, \cdot)$ polje koje je izomorfno polju kompleksnih brojeva.

Dokaz. $(A, +)$ je Abelova grupa jer je sabiranje matrica asocijativno i komutativno, neutralni element je nula matrica $\mathbf{0} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, a svaka matrica ima suprotnu (za A to je $-A$), što je u ovom slučaju inverzni element za $+$.

$(A \setminus \{\mathbf{0}\}, \cdot)$ je Abelova grupa jer je za svake dve matrice iz $A \setminus \{\mathbf{0}\}$

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Množenje matrica je asocijativno, a neutralni element za $\cdot$ je jedinična matrica $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Kako za $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in A \setminus \{\mathbf{0}\}$ važi $\begin{vmatrix} a & b \\ -b & a \end{vmatrix} = a^2 + b^2 \neq 0$, to svaka matrica iz ovog skupa ima inverznu matricu koja pripada skupu $A \setminus \{\mathbf{0}\}$. Takođe za $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}, \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ je

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \cdot \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

pa je $\cdot$ komutativna operacija. Iz ovoga sledi da je $(A, +, \cdot)$ polje.

Pokažimo da je ovo polje izomorfno sa poljem $\mathbf{C}$. Uočimo preslikavanje $\phi : C \to A$ definisano ovako

$$\phi(a+ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}.$$

Tada iz $\phi(a+ib) = \phi(c+id)$ sledi $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ što povlači $a = c$ i $b = d$, pa je $a+ib = c+id$, dakle ϕ je 1-1. Ako je $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in A$ proizvoljan element, tada je $\phi(a+ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, pa je ϕ na. Preostaje još da proverimo da je ϕ homomorfizam:

$$\begin{aligned}
\phi(z+w) &= \phi((a+ib)+(c+id)) \\
&= \phi(a+c+i(b+d)) \\
&= \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} \\
&= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\
&= \phi(z) + \phi(w); \\
\phi(z \cdot w) &= \phi((a+ib)(c+id)) \\
&= \phi(ac-bd+i(ad+bc)) \\
&= \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} \\
&= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\
&= \phi(z) \cdot \phi(w). \\
\phi(0) &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \mathbf{0} \qquad \phi(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.
\end{aligned}$$

■ $\triangle$

Primer 6.50 Skup $GL(n, R)$ svih regularnih kvadratnih matrica reda n nad poljem realnih brojeva, u odnosu na operaciju množenja matrica, čini grupu koja za $n \geq 2$ nije komutativna. Grupa $GL(n, R)$ se zove **opšta linearna** ili **opšta matrična grupa**. $\triangle$

Glava 7

Polinomi

Posmatraćemo polinome nad komutativnim prstenom $(R, +, \cdot)$ sa jedinicom 1, a često ćemo zahtevati da taj prsten bude i polje. Pri tome strukture mogu biti kako konačne, tako i beskonačne.

7.1 Prsten polinoma

7.1.1 Prsten funkcija

Neka je $(R, +, \cdot)$ prsten i $X \neq \emptyset$. Tada postoji direktan stepen prstena $(R, +, \cdot)$:

$$(R, +, \cdot)^X = (R^X, \oplus, \odot).$$

pri tome je $R^X = \{f \mid f : X \to R\}$, a za $f, g \in R^X$ definišemo:

$$(f \oplus g)(x) = f(x) + g(x)$$
$$(f \odot g)(x) = f(x) \cdot g(x)$$

Struktura $(R^X, \oplus, \odot)$ je prsten koji se naziva *prsten funkcija*. Ako prsten $(R, +, \cdot)$ ima neutralni element 1, tada je funkcija $h : X \to R$, definisana sa $h(x) = 1$ za svako $x \in X$, jedinični element u prstenu funkcija. Ako je R komutativan prsten, tada je i prsten funkcija komutativan prsten.

7.1.2 Polinomi kao termi

Definicija 7.1 Neka je $(R, +, \cdot)$ komutativni prsten sa jedinicom 1, $n \in N_0$, $a_0, \ldots, a_n \in R$, x "promenljiva"i neka važi $a_n \neq 0$ ili $n = 0$. Tada term

$$p = a_0 + a_1 x + \cdots + a_n x^n.$$

nazivamo *polinom* nad prstenom $(R, +, \cdot)$.

Ako je $a_n \neq 0$, tada kažemo da je *stepen polinoma* p jednak n, i pišemo $\mathrm{st}(p) = n$. Konstanta je polinom $p = a$ gde je $a \in R$, i važi $\mathrm{st}(p) = 0$ ako je $a \neq 0$, a za $a = 0$ stepen polinoma p se ne definiše.

Ako je dat proizvoljan term

$$a_0 + a_1 x + \cdots + a_n x^n,$$

tada pod postupkom uklanjanja krajnjih nula podrazumevamo postupak odstranjivanja svih članova $a_i x^i$ za koje je $a_i = 0$, počev od člana $a_n x^n$, pa do prvog člana sa desne strane koji ima koeficijent različit od nule (ili do člana a_0 ukoliko su svi koeficijenti jednaki nuli). Time term postaje polinom prema definiciji 7.1.

Definicija 7.2 Ako su $p = a_0 + a_1 x + \cdots + a_n x^n$ i $q = b_0 + b_1 x + \cdots + b_m x^m$ polinomi i $n \leq m$ tada je *zbir* polinoma p i q polinom $p + q$

$$c_0 + c_1 x + \cdots + c_m x^m,$$

gde je

$$c_i = \begin{cases} a_i + b_i, & 1 \leq i \leq n \\ a_i, & n+1 \leq i \leq m. \end{cases}$$

Ako je $n > m$, tada $p + q$ definišemo kao $q + p$.

Definicija 7.3 Ako su $p = a_0 + a_1 x + \cdots + a_n x^n$ i $q = b_0 + b_1 x + \cdots + b_m x^m$ polinomi, tada je *proizvod* polinoma p i q polinom pq

$$c_0 + c_1 x + \cdots + c_{m+n} x^{m+n},$$

gde je

$$c_k = \sum_{\substack{i+j=k \\ i,j \geq 0}} a_i b_j.$$

Polinom 0 je neutralni element za sabiranje polinoma, a polinom 1 neutralni element za množenje polinoma. Inverzni element polinoma p u odnosu na sabiranje polinoma je polinom $-p$ čiji su koeficijenti suprotni koeficijentima polinoma p, jer posle uklanjanja suvišnih nula za zbir $p + (-p)$ dobijamo polinom 0. Takođe se pokazuje da je sabiranje i množenje polinoma asocijativno i komutativno. Ako sa $R[x]$ označimo skup svih polinoma nad prstenom $(R, +, \cdot)$, tada je $(R[x], +, \cdot)$ prsten koji se naziva prsten polinoma nad prstenom $(R, +, \cdot)$.

7.1.3 Polinomi kao nizovi

Definicija 7.4 Neka je $(R, +, \cdot)$ komutativni prsten sa jedinicom 1. *Polinom nad prstenom* $(R, +, \cdot)$ je svaki niz $a : N_0 \to R$:

$$(a_0, a_1, \ldots, a_n, 0, 0, \ldots)$$

koji sadrži samo konačno mnogo elemenata različitih od nule.

Skup svih nizova koji imaju konačno mnogo elemenata različitih od nule označavamo sa $(R^N)_0$. Nad takvim nizovima definišemo operacije $+$ i $\cdot$. Ako je $n \leq m$, tada je

$$\begin{aligned}(a_0, a_1, \ldots, a_n, 0, 0, \ldots) + (b_0, b_1, \ldots, b_m, 0, 0, \ldots)\\ = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, a_{n+1}, \ldots, a_m, 0, 0, \ldots),\end{aligned}$$

a za proizvoljne m i n definišemo

$$\begin{aligned}(a_0, a_1, \ldots, a_n, 0, 0, \ldots) \cdot (b_0, b_1, \ldots, b_m, 0, 0, \ldots)\\ = (c_0, c_1, \ldots, c_{m+n}, 0, 0, \ldots)\end{aligned}$$

gde je

$$c_k = \sum_{\substack{i+j=k \\ i,j \geq 0}} a_i b_j,$$

za $0 \leq k \leq m + n$. Tada je $\Big((R^N)_0, +, \cdot\Big)$ komutativni prsten sa jedinicom.

Označimo niz $(0, 1, 0, 0, \ldots)$ sa x. Lako se proverava da važi $x^n = (0, \ldots, 1, 0, \ldots)$ pri čemu se jedinica javlja na $(n + 1)$-vom mestu.

Preslikavanje $\mu : R \to (R^N)_0$ definisano sa $\mu(a) = (a, 0, 0, \ldots)$ je monomorfizam. To znači da prsten $\Big((R^N)_0, +, \cdot\Big)$ sadrži potprsten izomorfan sa prstenom $(R, +, \cdot)$, zato sa a, gde je $a \in R$ označavamo $\mu(a) \in (R^N)_0$. Tada za svaki niz $(a_0, \ldots, a_n, 0, \ldots)$ važi

$$\begin{aligned}&(a_0, \ldots, a_n, 0, \ldots) =\\ &\quad = (a_0, 0, \ldots) + (0, a_1, 0, \ldots) + \cdots + (0, \ldots, a_n, 0, \ldots)\\ &\quad = a_0(1, 0, \ldots) + a_1(0, 1, 0, \ldots) + \cdots + a_n(0, \ldots, 1, 0, \ldots)\\ &\quad = a_0 + a_1 x + \cdots a_n x^n.\end{aligned}$$

Tako ponovo dolazimo do terma koji predstavlja polinom.

7.1.4 Polinomne funkcije

Definicija 7.5 Neka je dat polinom $p = a_0 + a_1x + \cdots + a_nx^n$ nad komutativnim prstenom $(R, +, \cdot)$ sa jedinicom 1. *Polinomna funkcija* polinoma p je $h(p) : R \to R$ definisana sa

$$h(p)(t) = a_0 + a_1t + \cdots + a_nt^n$$

za svako $t \in R$.

Preslikavanje h pridružuje svakom polinomu iz $R[x]$ funkciju iz R^R. Operacije sabiranja i množenja polinoma su tako definisane da je preslikavanje h homomorfizam prstena polinoma $(R[x], +, \cdot)$ u prsten funkcija $(R^R, \oplus, \odot)$. Pri tome je $h(R[x])$ potprsten prstena R^R čiji se elementi nazivaju polinomne funkcije.

Sledeći primer pokazuje da homomorfizam h ne mora biti monomorfizam.

Primer 7.6 Neka je $(Z_3, +, \cdot)$ konačno polje gde je $Z_3 = \{0, 1, 2\}$, $+$ sabiranje, a $\cdot$ množenje po modulu 3. Neka su $p = 2x^3 + 2x + 1$ i $q = x + 1$ polinomi. Pošto imaju različite koeficijente (a nisu ni istog stepena), polinomi p i q su različiti. Pokazaćemo međutim da su njihove polinomne funkcije, kao preslivakanja $Z_3 \to Z_3$ jednake. Zaista,

$$\begin{aligned} h(p)(0) &= 2 \cdot 0^3 + 2 \cdot 0 + 1 = 1 \\ h(p)(1) &= 2 \cdot 1^3 + 2 \cdot 1 + 1 = 2 \\ h(p)(2) &= 2 \cdot 2^3 + 2 \cdot 2 + 1 = 0 \end{aligned}$$

$$\begin{aligned} h(q)(0) &= 0 + 1 = 1 \\ h(q)(1) &= 1 + 1 = 2 \\ h(q)(2) &= 2 + 1 = 0 \end{aligned}$$

$h(p)$ i $h(q)$ se poklapaju za sve vrednosti skupa $\{0, 1, 2\}$, pa je $h(p) = h(q)$. Dakle h nije 1-1. $\triangle$

Može se pokazati da ako je R beskonačno polje (npr. polje kompleksnih brojeva $\mathbf{C}$), tada je prsten polinoma izomorfan sa prstenom polinomnih funkcija.

Neka je $\alpha \in R$ element prstena. Kada je to iz konteksta jasno, vrednost polinomne funkcije koja odgovara polinomu p u tački α umesto sa $h(p)(\alpha)$, označavamo sa $p(\alpha)$.

7.2 Deljenje polinoma

Neka je $(R, +, \cdot)$ polje. Polinomi $R[x]$ nad tim poljem čine prsten. U osnovi sledećeg tvrđenja je Euklidov algoritam deljenja polinoma (u induktivnom koraku dokaza se krije rekurzivna definicija algoritma deljenja).

Tvrđenje 7.7 *Neka je f proizvoljan polinom i g polinom različit od nule. Tada postoje jedinstveni polinomi q i r tako da*

$$f = qg + r$$

i važi $r = 0$ ili $\mathrm{st}(r) < \mathrm{st}(g)$.

Dokaz. Neka je f proizvoljan polinom i g polinom različit od nule. Prvo ćemo pokazati da postoje q i r tako da važi $f = qg + r$ i pri tome $r = 0$ ili $\mathrm{st}(r) < \mathrm{st}(g)$. Ukoliko je $f = 0$, tada je $f = 0 \cdot g + 0$, pa možemo uzeti $q = 0$ i $r = 0$. Neka je sada $f \neq 0$. Tada postoji $\mathrm{st}(f)$. Pokazaćemo indukcijom po $\mathrm{st}(f)$ da postoje traženi q i r.

1. $\mathrm{st}(f) = 0$. Tada je $f = a_0$. Razlikujemo dva slučaja.

   (a) $\mathrm{st}(g) = 0$. Tada je $g = b_0$. Kako je

   $$f = a_0 = (a_0 b_0^{-1})g + 0,$$

   možemo uzeti $q = a_0 b_0^{-1}$ i $r = 0$.

   (b) $\mathrm{st}(g) > 0$. Kako je

   $$f = 0 \cdot g + f$$

   i kako je $\mathrm{st}(f) = 0 < \mathrm{st}(g)$, možemo staviti $q = 0$ i $r = f$.

2. Pretpostavimo da tvrđenje važi za sve polinome za koje je $\mathrm{st}(f) = k$ gde je $k < n$. Neka je f proizvoljan polinom za koji je $\mathrm{st}(f) = n$. Postoje dve mogućnosti.

   (a) $\mathrm{st}(g) > \mathrm{st}(f)$. Pošto važi

   $$f = 0 \cdot g + f$$

   i $\mathrm{st}(f) < \mathrm{st}(g)$, možemo staviti $q = 0$ i $r = f$.

   (b) $\mathrm{st}(g) \leq \mathrm{st}(f)$. Neka je

   $$f = a_0 + a_1 x + \cdots + a_n x^n$$
   $$g = b_0 + b_1 x + \cdots + b_m x^m.$$

   Da bismo sveli ovaj slučaj na induktivnu hipotezu, eliminisaćemo član $a_n x^n$ tako što ćemo pronaći polinom koji ima $a_n x^n$ kao prvi koeficijent i deljiv je sa g. (ovaj korak odgovara nalaženju količnika člana $a_n x^n$ i $b_m x^m$ u postupku deljenja Euklidovim algoritmom). Ako stavimo $h = a_n b_m^{-1} x^{n-m} \cdot g$, vidimo da je h deljiv sa g, a važi

   $$a_n b_m^{-1} x^{n-m} \cdot b_m x^m = a_n x^n,$$

pa je $\mathrm{st}(h) = n$ i koeficijent uz član x^n je jednak koeficijentu uz x^n u polinomu f. Zato za ostatak $f_1 = f - h$ važi $\mathrm{st}(f_1) < n$, pa po induktivnoj hipotezi postoje q_1 i r_1 tako da važi

$$f_1 = q_1 g + r_1.$$

i $\mathrm{st}(r_1) < \mathrm{st}(g)$ ili $r_1 = 0$. Tada je

$$f = h + f_1 = a_n b_m^{-1} x^{n-m} g + q_1 g + r_1 = (a_n b_m^{-1} x^{n-m} + q_1) g + r_1.$$

Kako je $\mathrm{st}(r_1) < \mathrm{st}(g)$ ili $r_1 = 0$, možemo uzeti

$$\begin{aligned} q &= a_n b_m^{-1} x^{n-m} + q_1 \\ r &= r_1. \end{aligned}$$

Time smo pokazali egzistenciju polinoma q i r koji zadovoljavaju tražene uslove. Treba još pokazati jedinstvenost. Neka su q, r i q', r' dva para polinoma za koje važi

$$\begin{aligned} f &= qg + r, && \mathrm{st}(r) < \mathrm{st}(g) \text{ ili } r = 0 \\ f &= q'g + r' && \mathrm{st}(r') < \mathrm{st}(g) \text{ ili } r' = 0. \end{aligned}$$

Tada važi

$$(q - q')g = r' - r.$$

Pretpostavimo da je $q - q' \neq 0$. Kako je $g \neq 0$, važiće $(q - q')g \neq 0$ i pri tome $\mathrm{st}((q - q')g) \geq \mathrm{st}(g)$. Odatle sledi $r' - r \neq 0$ i $\mathrm{st}(r' - r) \geq \mathrm{st}(g)$, što je kontradikcija sa uslovom

$$(\mathrm{st}(r) < \mathrm{st}(g) \vee \mathrm{st}(r) = 0) \ \wedge \ (\mathrm{st}(r') < \mathrm{st}(g) \vee \mathrm{st}(r') = 0).$$

Do kontradikcije smo došli jer smo pretpostavili $q - q' \neq 0$. Dakle mora biti $q - q' = 0$ tj. $q = q'$. Odatle sledi

$$r = f - qg = f - q'g = r',$$

čime smo pokazali jedinstvenost polinoma q i r. ∎

Polinom q iz prethodnog tvrđenja nazivamo *količnik*, a polinom r *ostatak* pri deljenju polinoma f polinomom g. Ako je $r = 0$ kažemo da polinom g *deli* polinom f.

7.3 Nule polinoma

Nula polinoma $p = a_0 + a_1 x + \cdots + a_n x^n$ nad prstenom $(R, +, \cdot)$ je vrednost $\alpha \in R$ za koju polinomna funkcija $h(p)$ ima vrednost 0 tj. za koju važi

$$a_0 + a_1 \alpha + \cdots + a_n \alpha^n = 0.$$

U nastavku ćemo uglavnom posmatrati polinome nad poljem kompleksnih brojeva $\mathbf{C}$.

Tvrđenje 7.8 (Bezuov stav) *Ostatak pri deljenju polinoma f polinomom $x - c$ je $f(c)$.*

Dokaz. Prema tvrđenju 7.7 polinom f se na jedinstven način može napisati u obliku

$$f = q(x - c) + r$$

pri čemu je $r = 0$ ili $\mathrm{st}(r) < \mathrm{st}(x - c) = 1$. Dakle $r \in C$. Kako je $f(c) = q(c)(c - c) + r(c) = r(c)$, a r je konstanta, mora biti $r = f(c)$. ∎

Posledica 7.9 *Broj c je nula polinoma f akko $x - c$ deli f.*

7.3.1 Hornerova šema

Hornerova šema (G. Horner) se koristi za brzo deljenje polinoma f polinomom $x - c$. Neka je $f = a_0 + a_1x + \cdots + a_nx^n$. Neka je $q = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ količnik deljenja f sa $x - c$. Tada važi

$$\begin{aligned} & a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \\ = \quad & (x - c)(b_0 + b_1x + \cdots + b_{n-2}x^{n-2} + b_{n-1}x^{n-1}) + r \end{aligned}$$

gde je r konstanta. Izjednačavanjem koeficijenata sa leve i desne strane dobijamo

$$\begin{aligned} a_n &= b_{n-1} \\ a_{n-1} &= b_{n-2} - cb_{n-1} \\ &\vdots \\ a_1 &= b_0 - cb_1 \\ a_0 &= r - cb_0, \end{aligned}$$

iz čega sledi

$$\begin{aligned} b_{n-1} &= a_n \\ b_{n-2} &= a_{n-1} + cb_{n-1} \\ &\vdots \\ b_0 &= a_1 + cb_1 \\ r &= a_0 + cb_0. \end{aligned}$$

Ove formule nam omogućavaju da u n koraka izračunamo količnik deljenja polinoma f polinomom $x - c$. Postupak se zapisuje u obliku tablice.

c	a_n	a_{n-1}	$\cdots$	a_1	a_0
	b_{n-1}	b_{n-2}	$\cdots$	b_0	r

Donja vrsta matrice daje količnik q i ostatak r pri deljenju, a popunjava se tako što se na mesto b_{n-1} prepiše a_n, a zatim se popunjavaju ostale kolone prema formuli $b_j = a_{j+1} + cb_{j+1}$, koristeći poznate vrednosti c i prethodno izračunatu vrednost b_{j+1}.

Primer 7.10 Podelimo polinom $15x^4 - 13x^3 + 2x - 1$ sa $x - 2$.

2	15	-13	0	2	-1
	15	17	34	70	139

Dakle količnik deljenja je $15x^3 + 17x^2 + 34x + 70$, a ostatak 139. $\triangle$

Definicija 7.11 Broj c je *nula k-tog reda* ($k \in N$) polinoma f akko postoji polinom q tako da

$$f = (x - c)^k q$$

i $q(c) \neq 0$.

7.3.2 Osnovni stav algebre

Tvrđenje 7.12 (Gaus) *Svaki polinom nad poljem kompleksnih brojeva stepena bar jedan ima bar jednu nulu u skupu kompleksnih brojeva.*

Skica dokaza. Neka je dat proizvoljan polinom

$$f = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0.$$

Kako je jednačina

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0 = 0$$

ekvivalentna sa jednačinom

$$z^n + \frac{a_{n-1}}{a_n} z^{n-1} + \cdots + \frac{a_0}{a_n} = 0$$

koja se dobija množenjem sa a_n^{-1}, polinom f ima iste nule kao i polinom $a_n^{-1} \cdot f$. Zato je dovoljno posmatrati slučaj kada je $a_n = 1$. Ako je $a_0 = 0$, tada je $f(0) = 0$, pa je 0 tražena nula, zato je dovoljno razmatrati slučaj $a_0 \neq 0$.

Pokazaćemo da je polinomna funkcija $z \mapsto f(z)$ (dalje označena samo sa f) neprekidna funkcija na skupu kompleksnih brojeva tj. da važi

$$(\forall \varepsilon \in R_e^+)(\exists \delta \in R_e^+)(\forall h \in C)(|h| < \delta \Rightarrow |f(z + h) - f(z)| < \varepsilon),$$

gde su $|h|$ i $|f(z + h) - f(z)|$ moduli datih kompleksnih brojeva.

Neka je $z \in C$ proizvoljan kompleksan broj. Pokazaćemo da je f neprekidna u tački z. Neka je $\varepsilon \in R_e^+$ proizvoljno. Tada važi

$$\begin{aligned} f(z+h)-f(z) &= \sum_{k=0}^{n} a_k \left((z+h)^k - z^k\right) \\ &= \sum_{k=0}^{n} a_k \left(\sum_{i=0}^{k} \binom{k}{i} z^{k-i}h^i - z^k\right) \\ &= \sum_{k=1}^{n} a_k \sum_{i=1}^{k} \binom{k}{i} z^{k-i}h^i \\ &= h\sum_{k=1}^{n} a_k \sum_{i=1}^{k} \binom{k}{i} z^{k-i}h^{i-1}, \end{aligned}$$

odakle za $|h|<1$ sledi

$$\begin{aligned} |f(z+h)-f(z)| &= |h|\left|\sum_{k=1}^{n}\sum_{i=1}^{k} a_k \binom{k}{i} z^{k-i}h^{i-1}\right| \\ &\le |h|\sum_{k=1}^{n}\sum_{i=1}^{k} |a_k| \binom{k}{i} |z|^{k-i}|h|^{i-1} \\ &\le |h|\sum_{k=1}^{n}\sum_{i=1}^{k} |a_k| \binom{k}{i} |z|^{k-i} \\ &= |h|c, \end{aligned}$$

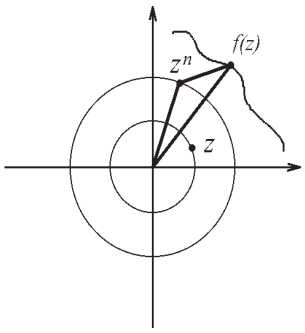
gde je $c = \sum_{k=1}^{n}\sum_{i=1}^{k} |a_k|\binom{k}{i}|z|^{k-i}$ veličina koja ne zavisi od h. Ako stavimo $\delta = \dfrac{\varepsilon}{c}$, tada za $|h|<\delta$ dobijamo

$$|f(z+h)-f(z)| \le |h|c < \frac{\varepsilon}{c}c = \varepsilon.$$

Dakle možemo staviti $\delta = \min\left\{1, \dfrac{\varepsilon}{c}\right\}$. Time je pokazana neprekidnost funkcije f u proizvoljnoj tački $z \in C$, pa je f neprekidna na skupu C.

Posmatrajmo brojeve $z \in C$ za koje važi $|z| = r$ gde je $r > M$ za $M = \max\{1, |a_0| + \cdots + |a_{n-1}|\}$. Tada je

$$\begin{aligned} |f(z)-z^n| &= |a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \cdots + a_0| \\ &\le |a_{n-1}||z|^{n-1} + |a_{n-2}||z|^{n-2} + \cdots + |a_0| \\ &= |a_{n-1}|r^{n-1} + |a_{n-2}|r^{n-2} + \cdots + |a_0| \\ &\le |a_{n-1}|r^{n-1} + |a_{n-2}|r^{n-1} + \cdots + |a_0|r^{n-1} \qquad \text{(jer je } r>1\text{)} \\ &= r^{n-1}(|a_{n-1}| + \cdots + |a_0|) \\ &< r^{n-1}r = r^n = |z|^n. \end{aligned}$$



To znači da je rastojanje tačke $f(z)$ od tačke z^n u kompleksnoj ravni *manje* od rastojanja tačke z^n od koordinatnog početka. Kada je $|z| = r$, a argument kompleksnog broja z prolazi od 0 do 2π, tačka z^n opiše n krugova poluprečnika r^n. Za to vreme tačka $f(z)$ "prati" tačku z^n (na osnovu prethodne nejednakosti), pa i ona opiše zatvorenu krivu liniju koja u svojoj unutrašnjosti sadrži koordinatni početak. To važi za $r > M$, a kada je $r = 0$, tj. $z = 0$, tada je $f(z) = a_0 \neq 0$, što znači da se kriva linija koju $f(z)$ opisuje degenerisala u tačku. Pošto je funkcija f neprekidna, krugovi koje $f(z)$ opisuje za vrednosti z za koje je $0 < |z| < r$ se neprekidno transformišu od krive linije koja obuhvata koordinatni početak, do tačke $a_0 \neq 0$. Odatle sledi da će za neko $0 < r_1 < r$ kriva linija koju opisuje $f(z)$ za $|z| = r_1$ prolaziti kroz koordinatni početak, što znači da postoji z za koje je $|z| = r_1$ i važi $f(z) = 0$. Dakle, u krugu poluprečnika M u kompleksnoj ravni polinom ima kompleksnu nulu. Time smo završili skicu dokaza.

Neka je $p = a_n x^n + \cdots + a_0$. proizvoljni polinom stepena n za $n > 0$. Prema osnovnom stavu algebre on ima kompleksnu nulu α_1. Prema Bezuovom stavu (7.8) tada je p deljiv sa $x - \alpha_1$, pa se može napisati u obliku $p = (x - \alpha_1)p_1$, gde je p_1 polinom stepena $n-1$. Neka je $n-1 > 0$. Primenjujući osnovni stav algebre na polinom p_1, dobijamo da postoji α_2 tako da važi $p_1 = (x - \alpha_2)p_2$ gde je $\mathrm{st}(p_2) = n - 2$. Ponavljajući ovaj postupak sve do polinoma p_n koji je konstanta, dobijamo da se svaki polinom p može zapisati u obliku

$$p = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)a,$$

gde je $a \in C$ konstanta. Izjednačavanjem koeficijenata polinoma p i njegovog zapisa, zaključujemo da je $a = a_n \neq 0$. Može se pokazati da je ovakav prikaz jedinstven. Ako je $\beta = \alpha_i$ za neko $1 \leq i \leq n$ tada je $p(\beta) = 0$. Ako je pak $\beta \neq \alpha_i$ za $1 \leq i \leq n$ tada su svi činioci u definiciji polinoma različiti od nule, pa je i $p(\beta) \neq 0$. Dakle važi sledeća posledica.

Posledica 7.13 *Svaki polinom stepena n u polju komleksnih brojeva ima tačno n nula.*

Primetimo da ovo tvrđenje važi i za $n = 0$, jer polinom stepena nula (to je broj različit od nule) nema nula. Jedino se za broj 0 ne može primeniti posledica 7.13, jer se za polinom 0 ne definiše stepen.

Tvrđenje 7.14 *Ako polinomi f i g nad skupom C za koje važi $\mathrm{st}(f), \mathrm{st}(g) \leq n$ imaju jednake vrednosti za više od n različitih tačaka, onda je $f = g$.*

Dokaz. Polinom $f(x) - g(x)$ ima stepen najviše n. Sa druge strane, on ima više od n nula. Dakle $f(x) - g(x) = 0$. ∎

7.3.3 Lagranžov interpolacioni polinom

Zbog svoje jednostavnosti polinomi se često koriste za interpolaciju i aproksimaciju funkcija. Interpolacija je problem određivanja funkcije koja u datim tačkama uzima date vrednosti. Neka su date različite vrednosti $x_1, \ldots, x_n$ i proizvoljne vrednosti $y_1, \ldots, y_n$. *Lagranžov interpolacioni polinom* je polinom $(n-1)$-vog stepena za koji važi $f(x_1) = y_1, \ldots, f(x_n) = y_n$. Za date različite vrednosti $x_1, \ldots, x_n$ i proizvoljne vrednosti $y_1, \ldots, y_n$ postoji jedinstven Lagranžov interpolacioni polinom. Za $n = 3$ on je dat sa

$$p(x) = \frac{(x-x_2)(x-x_3)}{(x_1-x_2)(x_1-x_3)}y_1 + \frac{(x-x_1)(x-x_3)}{(x_2-x_1)(x_2-x_3)}y_2 + \frac{(x-x_1)(x-x_2)}{(x_3-x_1)(x_3-x_2)}y_3.$$

Lako se proverava da ovaj polinom prolazi kroz tačke (x_i, y_i) za $1 \leq i \leq n$. Svaki drugi polinom p' stepena $n-1$ koji prolazi kroz sve tačke (x_i, y_i) za $1 \leq i \leq n$ ima iste vrednosti kao i p u $n > n-1$ tačaka, pa prema tvrđenju 7.14 mora biti $p' = p$. Dakle p je jedinstven.

7.3.4 Vijetove formule

Neka je $p = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ proizvoljan polinom n-tog stepena. Prema prethodnom razmatranju on se na jedinstven način može napisati u obliku

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 = a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

gde su $\alpha_1, \ldots, \alpha_n$ nule polinoma. Izjednačavanjem koeficijenata sa obe strane dobijamo:

$$\begin{aligned}
a_{n-1} &= a_n(-\alpha_1 - \alpha_2 \cdots - \alpha_n) \\
a_{n-2} &= a_n(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_n\alpha_{n-1}) \\
&\vdots \\
a_1 &= a_n(-1)^{n-1}(\alpha_1\alpha_2\cdots\alpha_{n-1} + \cdots + \alpha_2\alpha_3\cdots\alpha_n) \\
a_0 &= a_n(-1)^n\alpha_1\alpha_2\cdots\alpha_n,
\end{aligned}$$

a odatle slede sledeće *Vijetove formule* (F. R. Viete):

$$\begin{aligned}
\alpha_1+\alpha_2+\cdots+\alpha_n &= -\frac{a_{n-1}}{a_n}\\
\alpha_1\alpha_2+\alpha_2\alpha_3+\cdots+\alpha_{n-1}\alpha_n &= \frac{a_{n-2}}{a_n}\\
&\vdots\\
\alpha_1\alpha_2\cdots\alpha_{n-1}+\cdots+\alpha_2\alpha_3\cdots\alpha_n &= (-1)^{n-1}\frac{a_1}{a_n}\\
\alpha_1\alpha_2\cdots\alpha_n &= (-1)^n\frac{a_0}{a_n}.
\end{aligned}$$

Primer 7.15 [DM] Neka koreni jednačine

$$x^n+a_1x^{n-1}+\cdots+a_n=0$$

čine n uzastopnih članova aritmetičke progresije. Pokazaćemo da se oni onda mogu odrediti.

Neka su koreni $x_1=\alpha$, $x_2=\alpha+d$, …, $x_n=\alpha+(n-1)d$. Koristeći Vijetove formule dobijamo:

$$\begin{aligned}
&x_1+x_2+\cdots+x_n=\\
&\quad=\alpha+\alpha+d+\cdots+\alpha+(n-1)d\\
&\quad=n\alpha+d\frac{n(n-1)}{2}=-a_1. \qquad (*)
\end{aligned}$$

Kako je

$$(x_1+\cdots+x_n)^2-2(x_1x_2+x_1x_3+\cdots+x_{n-1}x_n)=x_1^2+\cdots+x_n^2$$

i važi $x_1x_2+\cdots+x_{n-1}x_n=a_2$, sledi

$$\begin{aligned}
(-a_1)^2-2a_2 &= \alpha^2+(\alpha+d)^2+\cdots+(\alpha+(n-1)d)^2\\
&= n\alpha^2+\alpha n(n-1)d+n(n-1)(2n-1)\frac{d^2}{6}
\end{aligned}$$

tj.

$$\alpha+\alpha d(n-1)+(n-1)(2n-1)\frac{d^2}{6}=\frac{a_1^2-2a_2}{n}. \qquad (**)$$

Rešavanjem sistema jednačina $(*)$ i $(**)$ po α i d mogu se odrediti rešenja polazne jednačine $x_1,\ldots,x_n$. $\triangle$

7.3.5 O rešavanju opštih algebarskih jednačina

Opšta algebarska jednačina n-tog stepena je jednačina $p(x) = 0$ gde je p polinom n-tog stepena. Iz osnovnog stava algebre sledi da svaka algebarska jednačina n-tog stepena ima tačno n (ne obavezno različitih) rešenja, ali ostaje problem nalaženja tih rešenja. U 9. veku je rešavana kvadratna jednačina: ustanovljeno je da su rešenja jednačine

$$a_2x^2 + a_1x + a_0 = 0$$

brojevi

$$\alpha_1 = \frac{-a_1 + \sqrt{D}}{2a_2} \qquad \text{i} \qquad \alpha_2 = \frac{-a_1 - \sqrt{D}}{2a_2}$$

gde je $D = a_1^2 - 4a_2a_0$. Kasnije su pronadjena rešenja i za jednačine $3.$ i $4.$ stepena, takođe u vidu formula u kojima učestvuju koeficijenti jednačine i operacije $+$, $\cdot$, $-$, $/$, x^n i $\sqrt[n]{x}$. Ovakva rešenja se nazivaju *rešenja putem radikala*. Posle rešavanja jednačina $3.$ i $4.$ reda ostalo je otvoreno pitanje rešavanja jednačina stepena većeg od 4. Na ovom problemu je radio Vijet, Abel je da osnovnu ideju o rešenju problema, a Galoa (E. Galois) je konačno dokazao da za jednačinu stepena većeg od 4 u opštem slučaju ne postoji rešenje putem radikala. Dokaz ovog tvrđenja se oslanja na teoriju grupa i polja.

7.3.6 Nule realnih polinoma

Tvrđenje 7.16 *Neka je $p = a_0 + a_1x + \cdots + a_nx^n$ polinom nad poljem kompleksnih brojeva pri čemu su koeficijenti $a_1, \ldots, a_n$ iz skupa realnih brojeva. Ako za $\alpha \in C$ važi $p(\alpha) = 0$, tada važi i $p(\overline{\alpha}) = 0$.*

Dokaz. Neka važi

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Odatle sledi

$$\overline{a_0 + a_1\alpha + \cdots + a_n\alpha^n} = \overline{0}.$$

Primenom osobina operacije $x \mapsto \overline{x}$ dobijamo

$$\begin{aligned} \overline{a_0} + \overline{a_1\alpha} + \cdots + \overline{a_n\alpha^n} &= 0 \\ \overline{a_0} + \overline{a_1}\,\overline{\alpha} + \cdots + \overline{a_n}\overline{\alpha^n} &= 0 \\ a_0 + a_1\overline{\alpha} + \cdots + a_n\,(\overline{\alpha})^n &= 0, \end{aligned}$$

a to znači $p(\overline{\alpha}) = 0$. ∎

Tvrđenje 7.17 *Neka je racionalan broj* $\frac{p}{q} \in R_a$ *(*$\mathrm{NZD}(p,q) = 1$*), rešenje jednačine*

$$a_n x^n + \cdots + a_0 = 0$$

pri čemu $a_0, \ldots, a_n \in Z$*. Tada* $p \mid a_0$ *i* $q \mid a_n$*.*

Dokaz. Neka je $\frac{p}{q}$ nula jednačine $a_n x^n + \cdots + a_0 = 0$. Zamenom $\frac{p}{q}$ u jednačinu dobijamo:

$$\begin{aligned} a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1 \frac{p}{q} + a_0 &= 0 \\ \frac{a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n}{q^n} &= 0. \end{aligned}$$

Odatle sledi $a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$. Kako su prvih n sabiraka deljivi sa p, mora biti $p \mid a_0 q^n$. Kako $\mathrm{NZD}(p,q) = 1$, sledi $p \mid a_0$. Analogno, poslednjih n sabiraka su deljivi sa q, pa $q \mid a_n p^n$, odakle sledi $q \mid a_n$. ∎

Ako je dat proizvoljan polinom

$$p(x) = \frac{a_n}{b_n} x^n + \cdots + \frac{a_0}{b_0}$$

sa racionalnim koeficijentima, tada možemo posmatrati polinom

$$p'(x) = p(x) \cdot \mathrm{NZS}(b_n, \ldots, b_0).$$

Polinom $p'(x)$ ima iste nule kao i polinom $p(x)$, a ima celobrojne koeficijente, pa na njega možemo primeniti prethodno tvrđenje.

Primer 7.18 [MMV] Neka je dat polinom $p = 30x^5 - 9x^4 - 10x^3 + 3x^2 - 40x + 12$. Delioci broja 12 su $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$, a delioci broja 30 su $\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30$. Zato se sve racionalne nule polinoma p nalaze među brojevima

$$\pm 1, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{1}{5}, \ldots, \pm\frac{12}{30}.$$

Neposrednom zamenom proveravamo da je od datih brojeva jedino $\frac{3}{10}$ nula polinoma p. Sada Hornerovom šemom možemo naći polinom q tako da važi $p = \left(x - \frac{3}{10}\right) q$. Pri tome je polinom q stepena 4, pa možemo primeniti odgovarajuću formulu. △

Napomena 7.19 Za kompleksan broj α kažemo da je **algebarski** ako je on nula nekog polinoma sa celim (odnosno racionalnim) koeficijentima koji nisu svi jednaki nuli. Ako

takav polinom za broj α ne postoji, onda kažemo da je α **transcedentan** broj. J. Liuvil je pokazao 1844. godine da je broj

$$L = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \cdots + \frac{1}{10^{k!}} + \cdots$$

transcedentan. (Videti [KU]). Takođe su i brojevi π, e transcedentni. Inače, algebarskih brojeva ima prebrojivo mnogo, a transcedentnih ima kontinuum mnogo. (Zaťo?). $\diamond$

Napomena 7.20 Funkcija f je *algebarska*, ako postoji polinom

$$p(u) = a_0(x) + a_1(x)u + \cdots + a_n(x)u^n,\ n \in N$$

gde su $a_0(x), a_1(x), ..., a_n(x)$ polinomi sa realnim koeficijentima, koji nisu svi istovremeneo identički jednaki nuli, tako da $p(f(x))$ je indentički jednaka nuli za x iz domena funkcije f. Funkcija f je *transcedentna*, ako nije algebarska. Tako je funkcije $\sin$ transcedentna. Pretpostavimo suprotno, to jest da važi

$$a_0(x) + a_1(x)\sin x + \cdots + a_n(x)\sin^n x = 0,$$

gde polinom $a_0(x)$ nije identički jednak nuli za $x \in R$. Neka je $a_0(x)$ polinom stepena $m \in N$. Tada za $k \in Z$ je $a_0(k\pi) = 0$, pa polinom $a_0(x)$ iam beskonačno različitih nula, a to je suprotno sa posledicom 7.13.

Iz prethodnog neposredno sledi da ne postoje polinomi $a_0(x)$ i $a_1(x)$ sa realnim koeficijentima tako da je

$$\sin x = \frac{a_0(x)}{a_1(x)}.$$

Takodje , transcedentne su i ostale trigonometrijske funkcije, kao i logaritamske i eskponencijalne funkcije. $\diamond$

Glava 8

Vektori

U odeljku 6.2 data je definicija vektorskog prostora. U ovom odeljku ćemo se baviti trodimenzionalnim vektorskim prostorom R^3_e i vektorskim prostorom slobodnih vektora V^3.

8.1 Vektori u $\mathbf{R}^3$

8.1.1 Skalarni proizvod u $\mathbf{R}^3$

Definicija 8.1 Skalarni proizvod vektora $(a_1, a_2, a_3), (b_1, b_2, b_3) \in R^3_e$, u oznaci

$$(a_1, a_2, a_3) \cdot (b_1, b_2, b_3),$$

je skalar $a_1b_1 + a_2b_2 + a_3b_3$.

Primer 8.2 Ako su vektori $\vec{a} = (1, 2, 3)$ i $\vec{b} = (2, 0, -1)$, onda je

$$\vec{a} \cdot \vec{b} = 1 \cdot 2 + 2 \cdot 0 + 3 \cdot (-1) = -1.$$

$\triangle$

Primer 8.3 Ako su vektori $\vec{a} = (1, -1, 1)$ i $\vec{b} = (2, 3, 1)$ onda je

$$\vec{a} \cdot \vec{b} = 0.$$

$\triangle$

Za dva vektora različita od nula vektora kažemo da su *normalna* ako je njihov skalarni proizvod nula.

Navedimo sada neke osobine skalarnog proizvoda.

Tvrđenje 8.4 *Neka $\vec{a}, \vec{b}, \vec{c} \in R_e^3$ i $k \in R_e$. Tada važi:*

1. $\vec{a} \cdot \vec{b} = \vec{b} \cdot \vec{a}$
2. $\vec{a} \cdot (\vec{b} + \vec{c}) = \vec{a} \cdot \vec{b} + \vec{a} \cdot \vec{c}$
3. $k(\vec{a} \cdot \vec{b}) = (k \cdot \vec{a}) \cdot \vec{b} = \vec{a} \cdot (k\vec{b})$
4. $\vec{a} \cdot \vec{a} \geq 0$; $\qquad \vec{a} \cdot \vec{a} = 0 \Leftrightarrow \vec{a} = \vec{0}$.

Dokaz. Proističe direktno iz definicije, na primer za 1:

$$\vec{a} \cdot \vec{b} = a_1b_1 + a_2b_2 + a_3b_3 = b_1a_1 + b_2a_2 + b_3a_3 = \vec{b} \cdot \vec{a}.$$

■

Definicija 8.5 *Intenzitet vektora* $\vec{a} = (a_1, a_2, a_3)$, u oznaci $|\vec{a}|$, je

$$\sqrt{\vec{a} \cdot \vec{a}} = \sqrt{a_1^2 + a_2^2 + a_3^2}.$$

Kako je dijagonala pravouglog paralelepipeda sa stranama a_1, a_2 i a_3 jednaka $\sqrt{a_1^2 + a_2^2 + a_3^2}$, to geometrijski smisao $|\vec{a}|$ jeste dužina vektora $\vec{a}$, od $(0, 0, 0)$ do (a_1, a_2, a_3).

Vektor $\vec{a}$ za koji je $|\vec{a}| = 1$ zovemo jedinični vektor i označavamo ga sa $\vec{a}_0$.

Tvrđenje 8.6 (Nejednakost Koši-Bunjakovskog) *(A. Cauchy, B. Bunjakovskij) Za proizvoljne $\vec{a}, \vec{b} \in R_e^3$ važi*

$$|\vec{a} \cdot \vec{b}| \leq |\vec{a}||\vec{b}|.$$

Dokaz. Prema tvrđenju 8.4 važi

$$\begin{aligned} (\vec{a} - k \cdot \vec{b})(\vec{a} - k \cdot \vec{b}) &\geq 0 \\ \vec{a} \cdot \vec{a} - 2k\vec{a} \cdot \vec{b} + k^2\vec{b} \cdot \vec{b} &\geq 0 \\ (\vec{b} \cdot \vec{b})k^2 + (-2)(\vec{a} \cdot \vec{b})k + \vec{a} \cdot \vec{a} &\geq 0. \end{aligned}$$

Posmatrajmo levu stranu nejednakosti kao funkciju od realnog broja k. Nejednakost važi za sve vrednosti broja k, a kako je $\vec{b} \cdot \vec{b} \geq 0$, za diskriminantu D kvadratne funkcije mora važiti $D \leq 0$. Zato je

$$(-2)^2(\vec{a} \cdot \vec{b})^2 - 4 \cdot (\vec{b} \cdot \vec{b})(\vec{a} \cdot \vec{a}) \leq 0,$$

odatle sledi $(\vec{a} \cdot \vec{b})^2 \leq \vec{a}^2 \cdot \vec{b}^2$. Nalaženjem kvadratnog korena obe strane dobijamo traženu nejednakost. ■

Tvrđenje 8.7 (Nejednakost trougla za vektore)

$$|\vec{a}+\vec{b}| \leq |\vec{a}|+|\vec{b}|$$

Dokaz. Pokazaćemo da važi $|\vec{a}+\vec{b}|^2 \leq \left(|\vec{a}|+|\vec{b}|\right)^2$. Primenom nejednakosti Koši-Bunjakovskog (tvrđenje 8.6), dobijamo

$$|\vec{a}+\vec{b}|^2 = (\vec{a}+\vec{b})(\vec{a}+\vec{b}) = |\vec{a}|^2 + 2\vec{a}\vec{b} + |\vec{b}|^2 \leq |\vec{a}|^2 + 2|\vec{a}||\vec{b}| + |\vec{b}|^2 = \left(|\vec{a}|+|\vec{b}|\right)^2.$$

■

Jedinični vektori su

$$\begin{aligned} \vec{\imath} &= (1,0,0) \\ \vec{\jmath} &= (0,1,0) \\ \vec{k} &= (0,0,1). \end{aligned}$$

Oni čine bazu prostora R^3_e. Vektor $\vec{\imath}$ se zove koordinatni vektor x-ose, vektor $\vec{\jmath}$ koordinatni vektor y-ose, a vektor $\vec{k}$ koordinatni vektor z-ose.

Skalarni proizvodi jediničnih vektora dati su sledećom Kejlijevom tablicom:

$\cdot$	$\vec{\imath}$	$\vec{\jmath}$	$\vec{k}$
$\vec{\imath}$	1	0	0
$\vec{\jmath}$	0	1	0
$\vec{k}$	0	0	1

Tako je, na primer, $\vec{\imath}\cdot\vec{\jmath}=0$, a $\vec{k}\cdot\vec{k}=1$.

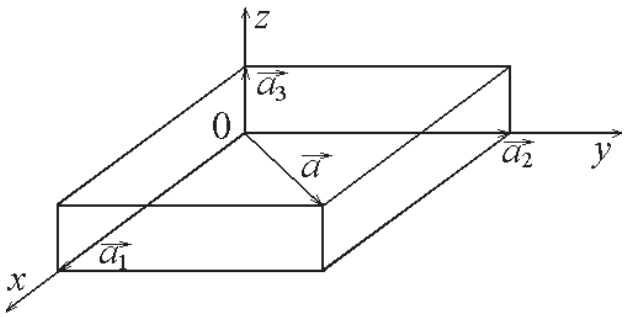
Tvrđenje 8.8 *Svaki vektor $\vec{a}=(a_1,a_2,a_3)$ može biti predstavljen kao zbir tri vektrora $\vec{a}_1 = a_1\vec{\imath}$, $\vec{a}_2 = a_2\vec{\jmath}$ i $\vec{a}_3 = a_3\vec{k}$, koji imaju iste pravce redom kao i vektori $\vec{\imath}$, $\vec{\jmath}$ i $\vec{k}$ (tj. kolinearni su sa $\vec{\imath}$, $\vec{\jmath}$, $\vec{k}$ redom), dakle:*

$$\vec{a} = a_1\vec{\imath} + a_2\vec{\jmath} + a_3\vec{k}.$$

Dokaz. Iz definicije množenja vektora skalarom dobijamo $a_1\vec{\imath} = (a_1,0,0)$, $a_2\vec{\jmath} = (0,a_2,0)$ i $a_3\vec{k} = (0,0,a_3)$. Dakle (vidi sliku):

$$\vec{a} = (a_1,a_2,a_3) = a_1\vec{\imath} + a_2\vec{\jmath} + a_3\vec{k}.$$

■



Ako su α, β i γ uglovi između vektora $\vec{a} = (a_1, a_2, a_3) \neq \vec{0}$ i jediničnih vektora $\vec{i}$, $\vec{j}$, $\vec{k}$ respektivno, onda važi da je

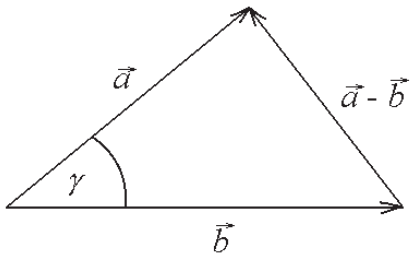
$$\cos^2 \alpha + \cos^2 \beta + \cos^2 \gamma = 1.$$

Ova formula neposredno sledi ako se uzme u obzir da su *kosinusi pravca* vektora $\vec{a}$ dati sa

$$\cos \alpha = \frac{a_1}{|\vec{a}|}, \qquad \cos \beta = \frac{a_2}{|\vec{a}|}, \qquad \cos \gamma = \frac{a_3}{|\vec{a}|}.$$

Nula vektoru $\vec{0}$ se ne pridružuje pravac.

Napomena 8.9 Ako su $\vec{a}$ i $\vec{b}$ dva vektora različita od $\vec{0}$, tada $\vec{a}$, $\vec{b}$ i $\vec{a} - \vec{b}$ obrazuju trougao.



Na osnovu kosinusne teoreme imamo:

$$|\vec{a} - \vec{b}|^2 = |\vec{a}|^2 + |\vec{b}|^2 - 2|\vec{a}||\vec{b}| \cos \gamma,$$

tj.

$$(\vec{a} - \vec{b}) \cdot (\vec{a} - \vec{b}) = \vec{a} \cdot \vec{a} + \vec{b} \cdot \vec{b} - 2|\vec{a}||\vec{b}| \cos \gamma,$$

odakle se dobija

$$\vec{a} \cdot \vec{b} = |\vec{a}||\vec{b}| \cos \gamma.$$

Poslednja formula je geometrijska definicija skalarnog proizvoda (u V^3). $\diamond$

Primer 8.10 Neka je jedna baza vektorskog prostora R^3 data sa $(\vec{a}_1, \vec{a}_2, \vec{a}_3)$. Nađimo novu bazu tako da su vektori nove baze jedinični i međusobno normalni.

Neka je, na primer, $\vec{a}_1 = \vec{v}_1$. Prvi jedinični vektor dobijamo sa

$$\vec{u}_1 = \frac{\vec{v}_1}{|\vec{v}_1|}.$$

Uočimo sada vektor

$$\vec{v}_2 = \vec{a}_2 - \alpha\vec{u}_1,$$

pri čemu α određujemo iz uslova da vektor $\vec{v}_2$ bude normalan na $\vec{u}_1$, tj. da važi

$$\vec{v}_2\vec{u}_1 = \vec{a}_2\vec{u}_1 - \alpha\vec{u}_1\vec{u}_1 = 0.$$

(primetiti da je $\vec{u}_1 \cdot \vec{u}_1 = 1$). Odatle je $\alpha = \vec{a}_2 \cdot \vec{u}_1$, i

$$\vec{v}_2 = \vec{a}_2 - (\vec{a}_2\vec{u}_1)\vec{u}_1.$$

Vektor $\vec{u}_2 = \vec{v}_2/|\vec{v}_2|$ je drugi traženi vektor. Sada uočimo vektor

$$\vec{v}_3 = \vec{a}_3 - \beta\vec{u}_1 - \gamma\vec{u}_2$$

gde β i γ određujemo iz uslova da vektor $\vec{v}_3$ bude normalan i na $\vec{u}_1$ i na $\vec{u}_2$ tj. da važi $0 = \vec{v}_3\vec{u}_1 = \vec{a}_3\vec{u}_1 - \beta$ i $0 = \vec{v}_3\vec{u}_2 = \vec{a}_3\vec{u}_2 - \gamma$. Dakle,

$$\beta = \vec{a}_3\vec{u}_1 \qquad \text{i} \qquad \gamma = \vec{a}_3\vec{u}_2,$$

pa dobijamo $\vec{v}_3 = \vec{a}_3 - (\vec{a}_3\vec{u}_1)\vec{u}_1 - (\vec{a}_3\vec{u}_2)\vec{u}_2$. Poslednji traženi vektor je $\vec{u}_3 = \vec{v}_3/|\vec{v}_3|$. Opisani postupak zove se *Gram-Šmitov postupak* (J. Gram, E. Schmidt). △

8.1.2 Vektorski proizvod u $\mathbf{R}^3$

Definicija 8.11 Ako su dati vektori $\vec{a} = (a_1, a_2, a_3)$ i $\vec{b} = (b_1, b_2, b_3)$, onda pod *vektorskim proizvodom* tih vektora podrazumevamo vektor označen sa $\vec{a} \times \vec{b}$, definisan sa

$$\vec{a} \times \vec{b} \stackrel{\text{def}}{=} (a_2b_3 - a_3b_2, a_3b_1 - a_1b_3, a_1b_2 - a_2b_1)$$

tj.

$$\vec{a} \times \vec{b} = (a_2b_3 - a_3b_2)\vec{\imath} + (a_3b_1 - a_1b_3)\vec{\jmath} + (a_1b_2 - a_2b_1)\vec{k}.$$

Prethodnu formulu možemo zapisati i u obliku sledeće *simboličke determinante*:

$$\vec{a} \times \vec{b} = \begin{vmatrix} \vec{\imath} & \vec{\jmath} & \vec{k} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}.$$

Značajna osobina vektorskog proizvoda koja sledi iz definicije jeste:

$$\vec{a} \times \vec{b} = -\vec{b} \times \vec{a}.$$

Primer 8.12 Ako je $\vec{a} = (1, 1, -3)$ i $\vec{b} = (-1, -2, -3)$, onda je:

$$\begin{aligned} \vec{a} \times \vec{b} &= \begin{vmatrix} \vec{\imath} & \vec{\jmath} & \vec{k} \\ 1 & 1 & -3 \\ -1 & -2 & -3 \end{vmatrix} \\ &= (-9)\vec{\imath} + 6\vec{\jmath} + (-1)\vec{k} = (-9, 6, -1). \end{aligned}$$

△

Tvrđenje 8.13 *Vektori $\vec{a} \neq \vec{0}$ i $\vec{b} \neq \vec{0}$ su kolinearni akko $\vec{a} \times \vec{b} = \vec{0}$.*

Dokaz. Neka je $\vec{a} = (a_1, a_2, a_3)$ i $\vec{b} = (b_1, b_2, b_3)$ i neka su oni kolinearni, tj. $\vec{a} = k\vec{b}$. Tada je

$$\vec{a} \times \vec{b} = \begin{vmatrix} \vec{\imath} & \vec{\jmath} & \vec{k} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} = \begin{vmatrix} \vec{\imath} & \vec{\jmath} & \vec{k} \\ a_1 & a_2 & a_3 \\ ka_1 & ka_2 & ka_3 \end{vmatrix} = \vec{0}$$

po tvrđenju 6.33.

Ako je $\vec{a} \times \vec{b} = \vec{0}$, tada iz definicije vektorskog proizvoda imamo:

$$a_2 b_3 - a_3 b_2 = 0 \tag{8.1}$$

$$a_3 b_1 - a_1 b_3 = 0 \tag{8.2}$$

$$a_1 b_2 - a_2 b_1 = 0. \tag{8.3}$$

Kako je $\vec{b} \neq \vec{0}$, važi $b_i \neq 0$ za neko $i \in \{1, 2, 3\}$. Neka je npr. $b_1 \neq 0$ (za $b_2 \neq 0$ i $b_3 \neq 0$ dokaz je analogan). Neka je $k = a_1/b_1$. Tada je $a_1 = kb_1$. Iz 8.2 sledi $a_3 = kb_3$, a iz 8.3 sledi $a_2 = kb_2$. Zato je

$$(a_1, a_2, a_3) = (kb_1, kb_2, kb_3) = k(b_1, b_2, b_3)$$

tj. $\vec{a} = k\vec{b}$, što znači da su vektori kolinearni. ∎

Vektorski proizvod jediničnih vektora $\vec{\imath}$, $\vec{\jmath}$, $\vec{k}$ dat je sa

$\times$	$\vec{\imath}$	$\vec{\jmath}$	$\vec{k}$
$\vec{\imath}$	0	$\vec{k}$	$-\vec{\jmath}$
$\vec{\jmath}$	$-\vec{k}$	0	$\vec{\imath}$
$\vec{k}$	$\vec{\jmath}$	$-\vec{\imath}$	0

Na primer, $\vec{\imath} \times \vec{\imath} = \vec{0}$, a $\vec{\jmath} \times \vec{\imath} = -\vec{k}$.

Za vektorski proizvod ne važi asocijativni zakon. Tako imamo:

$$(\vec{\imath} \times \vec{\imath}) \times \vec{\jmath} = \vec{0}, \quad \text{a} \quad \vec{\imath} \times (\vec{\imath} \times \vec{\jmath}) = -\vec{\jmath}.$$

Za vektorski proizvod važe sledeće osobine koje neposredno slede iz njegove definicije.

Tvrđenje 8.14 *Neka $\vec{a}, \vec{b}, \vec{c} \in R_e^3$ i $t \in R_e$. Tada*

$$\vec{a} \times (\vec{b} + \vec{c}) = \vec{a} \times \vec{b} + \vec{a} \times \vec{c}$$

$$(\vec{a} + \vec{b}) \times \vec{c} = \vec{a} \times \vec{c} + \vec{b} \times \vec{c}$$

$$t(\vec{a} \times \vec{b}) = (t\vec{a}) \times \vec{b}.$$

Napomena 8.15 Vektor $\vec{a} \times \vec{b}$ normalan je na vektore $\vec{a}$ i $\vec{b}$ (proveri) i triedar vektora $\vec{a}$, $\vec{b}$, $\vec{a} \times \vec{b}$ čini triedar desne orijentacije. Pri tom je koordinatni sistem u kojem su date koordinate vektora desno orijentisan. $\diamond$

8.1.3 Mešoviti proizvod u $\mathbf{R}^3$

Definicija 8.16 Mešoviti proizvod vektora $\vec{a}, \vec{b}, \vec{c} \in R_e^3$ je skalar definisan sa $\vec{a} \cdot (\vec{b} \times \vec{c})$.

Iz definicije skalarnog i vektorskog proizvoda sledi da je:

$$\begin{aligned} &\vec{a} \cdot (\vec{b} \times \vec{c}) = \\ &= a_1(b_2c_3 - b_3c_2) + a_2(b_3c_1 - b_1c_3) + a_3(b_1c_2 - b_2c_1). \end{aligned}$$

Izraz na desnoj strani je vrednost determinante

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$$

tj.

$$\vec{a} \cdot (\vec{b} \times \vec{c}) = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$$

8.2 Vektorski prostor slobodnih vektora V^3

8.2.1 Skalarni proizvod u V^3

Videli smo da vektore možemo posmatrati kao orijentisane duži, zatim kako se sabiraju dva vektora i kako se oni množe skalarom. Kao što znamo, za dva vektora kažemo da su kolinearni ako se nalaze na istoj ili paralelnim pravama. Vektor $\vec{0}$ je kolinearan sa svakim vektorom.

Tvrđenje 8.17 *Ako su vektori $\vec{a}$ i $\vec{b}$ kolinearni, tada postoje brojevi $m, n \in R_e$ od kojih je bar jedan različit od nule, tako da važi $n\vec{a} + m\vec{b} = \vec{0}$.*

Dokaz. Ako je jedan od vektora $\vec{a}$ ili $\vec{b}$ nula vektor, na primer $\vec{a} = \vec{0}$, tada za $m = 1$ i $n = 0$ važi formula (1). Ako je $\vec{a} \neq \vec{0}$ i $\vec{b} \neq \vec{0}$, tada je moguće naći broj $t > 0$ tako da je $t|\vec{b}| = |\vec{a}|$. Ako su vektori $\vec{a}$ i $\vec{b}$ istog smera, tada je

$$1\vec{a} - t\vec{b} = \vec{0},$$

a ako su suprotnog smera

$$1\vec{a} + t\vec{b} = \vec{0}.$$

■

Napomena 8.18 Prisetimo se da su dva vektora linearno zavisni ako je ispunjen jedan od sledeća dva uslova:

1. jedan od ta dva vektora je nula vektor;
2. postoje brojevi $m \neq 0$ i $n \neq 0$ takvi da je $m\vec{a} + n\vec{b} = \vec{0}$ (tj. $\vec{a} = -\frac{m}{n}\vec{b}$).

Prema ovome i tvrđenju 8.17 imamo: dva vektora su kolinearna akko su linearno zavisni. ◇

Za tri vektora kažemo da su *komplanarni* ako leže u istoj ravni ili su paralelni istoj ravni.

Tvrđenje 8.19 *Vektori $\vec{a}, \vec{b}, \vec{c} \in V$ su linearno zavisni akko su komplanarni.*

Dokaz. Ako su vektori $\vec{a}$, $\vec{b}$ i $\vec{c}$ linearno zavisni, tada postoje brojevi m, n i t od kojih je bar jedan različit od nule tako da je $m\vec{a} + n\vec{b} + t\vec{c} = \vec{0}$, a to znači da vektori $m\vec{a}$, $n\vec{b}$ i $t\vec{c}$ obrazuju trougao, tj. leže u jednoj ravni. Kako su vektori $\vec{a}$, $\vec{b}$ i $\vec{c}$ kolinearni sa $m\vec{a}$, $n\vec{b}$ i $t\vec{c}$, sledi da i oni leže u istoj ravni.

Obratno, ako su vektori $\vec{a}$, $\vec{b}$ i $\vec{c}$ komplanarni, onda možemo naći skalare α, β, γ od kojih je bar jedan različit od 0 tako da važi

$$\alpha\vec{a} + \beta\vec{b} + \gamma\vec{c} = \vec{0}.$$

■

Definicija 8.20 *Skalarni proizvod* dva vektora $\vec{a}$ i $\vec{b}$ definiše se sa

$$\vec{a} \cdot \vec{b} \stackrel{\text{def}}{=} |\vec{a}||\vec{b}| \cos \angle(\vec{a}, \vec{b})$$

tj. $\vec{a} \cdot \vec{b}$ je skalar jednak proizvodu dužine oba vektora $\vec{a}$ i $\vec{b}$ i kosinusa ugla zahvaćenog sa $\vec{a}$ i $\vec{b}$.

Iz osobina kosinusa sledi da je $\vec{a} \cdot \vec{b} = \vec{b} \cdot \vec{a}$ tj. važi komutativni zakon za skalarni proizvod.

Koristeći definiciju 8.20 možemo naći ugao između dva vektora $\vec{a}$ i $\vec{b}$:

$$\cos \angle(\vec{a}, vb) = \frac{\vec{a} \cdot \vec{b}}{|\vec{a}||\vec{b}|}.$$

Primer 8.21 Odredimo ugao između jediničnih vektora $\vec{a}$ i $\vec{b}$ ako je njihov skalarni proizvod $\frac{\sqrt{2}}{2}$.

Iz formule $\cos \alpha = \frac{\vec{a} \cdot \vec{b}}{|\vec{a}||\vec{b}|}$ sledi da je $\cos \alpha = \frac{\sqrt{2}}{2}$, dakle $\alpha = \frac{\pi}{4}$. $\triangle$

Tvrđenje 8.22 *Ako $\vec{a} \neq \vec{0}$ i $\vec{b} \neq \vec{0}$, onda je $\vec{a}$ normalan na $\vec{b}$ akko je $\vec{a} \cdot \vec{b} = 0$.*

Dokaz. $\vec{a} \cdot \vec{b} = 0$ akko $\angle(\vec{a}, \vec{b}) = \frac{\pi}{2}$ ili $\angle(\vec{a}, \vec{b}) = \frac{3\pi}{2}$, tj. $\vec{a}$ je normalan na $\vec{b}$. ∎

Za skalarni proizvod značajne su i sledeće osobine:

$$(t\vec{a}) \cdot \vec{b} = t(\vec{a} \cdot \vec{b}) = \vec{a} \cdot (t\vec{b})$$

kao i

$$\vec{a} \cdot (\vec{b} + \vec{c}) = \vec{a} \cdot \vec{b} + \vec{a} \cdot \vec{c}.$$

Koristeći distributivnost dobijamo da iz $\vec{a} \cdot \vec{c} = \vec{b} \cdot \vec{c}$ sledi $(\vec{a} - \vec{b}) \cdot \vec{c} = 0$. Primenom tvrđenja 8.22 dobijamo da je vektor $\vec{a} - \vec{b}$ normalan na $\vec{c}$.

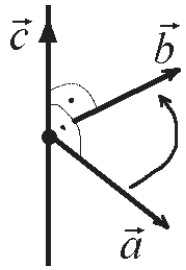
Napomena 8.23 Definicija skalarnog proizvoda u analitičkom obliku se može neposredno dobiti iz geometrijske definicije korišćenjem jediničnih koordinatnih vektora i distributivnog zakona. Vektori $\vec{i}$, $\vec{j}$ i $\vec{k}$ koji odgovaraju osaa x, y i z uvode se kao tri međusobno normalna jedinična vektora. $\diamond$

8.2.2 Vektorski proizvod u V^3

Definicija 8.24 Neka su $\vec{a}$ i $\vec{b}$ proizvoljni vektori različiti od $\vec{0}$. Tada definišemo vektor $\vec{a} \times \vec{b}$ na sledeći način.

1. pravac vektora $\vec{a} \times \vec{b}$ je pravac normale ravni određene vektorima $\vec{a}$ i $\vec{b}$;
2. smer vektora $\vec{a} \times \vec{b}$ je takav da vektori $\vec{a}, \vec{b}, \vec{b} \times \vec{c}$, tim redom, obrazuju desni triedar;
3. intenzitet je dat izrazom
$$|\vec{a} \times \vec{b}| = |\vec{a}||\vec{b}| \sin \angle(\vec{a}, \vec{b}),$$
gde je $\angle(\vec{a}, \vec{b})$ ugao između vektora $\vec{a}$ i $\vec{b}$ ($\angle(\vec{a}, \vec{b}) \in [0, \pi)$).

Ako je $\vec{a} = \vec{0}$ ili $\vec{b} = \vec{0}$, tada $\vec{a} \times \vec{b} = \vec{0}$.



Intenzitet vektorskog proizvoda $\vec{a} \times \vec{b}$ ima brojnu vrednost površine paralelograma konstruisanog nad vektorima $\vec{a}$ i $\vec{b}$ dovedenim u zajednički početak.

Tvrđenje 8.25 *Ako su $\vec{a}$ i $\vec{b}$ vektori, tada je $\vec{a} \times \vec{b} = \vec{0}$ akko je $\vec{a}$ kolinearan sa $\vec{b}$ ili je bar jedan od vektora $\vec{a}$, $\vec{b}$ jednak $\vec{0}$.*

Dokaz. Sledi direktno iz definicije. ∎

Tvrđenje 8.26 *Ako su $\vec{a}$ i $\vec{b}$ vektori, tada važi*
$$\vec{a} \times \vec{b} = -\vec{b} \times \vec{a}.$$

Dokaz. Sledi iz definicije $\vec{a} \times \vec{b}$. Promenom mesta $\vec{a}$ i $\vec{b}$ u proizvodu, jedino dolazi do promene smera u suprotan. ∎

Navodimo još neke značajne osobine vektorskog proivoda.
$$(t\vec{a}) \times \vec{b} = t(\vec{a} \times \vec{b}) = \vec{a} \times (t\vec{b})$$
i
$$(\vec{a} + \vec{b}) \times \vec{c} = \vec{a} \times \vec{c} + \vec{b} \times \vec{c}.$$

Primenom tvrđenja 8.26 na prethodnu jednakost dobija se
$$\vec{a} \times (\vec{b} + \vec{c}) = \vec{a} \times \vec{b} + \vec{a} \times \vec{c}.$$

Napomena 8.27 Koristeći geometrijsku definiciju vektorskog proizvoda može se lako dobiti analitička definicija. Iz analitičke definicije se može dobiti geometrijska, što ćemo i pokazati. Kako je

$$\begin{aligned} |\vec{a}\times\vec{b}|^2 &= (a_2b_3-a_3b_2)^2+(a_3b_1-a_1b_3)^2+(a_1b_2-a_2b_1) \\ &= (a_1^2+a_2^2+a_3^2)(b_1^2+b_2^2+b_3^2)-(a_1b_1+a_2b_2+a_3b_3)^2 \\ &= |\vec{a}|^2|\vec{b}|^2-(\vec{a}\cdot\vec{b})^2 \\ &= |\vec{a}|^2|\vec{b}|^2-|\vec{a}|^2|\vec{b}|^2\cos^2\angle(\vec{a},\vec{b}) \\ &= |\vec{a}|^2|\vec{b}|^2\sin^2\angle(\vec{a},\vec{b}). \end{aligned}$$

Sledi da je intenzitet vektora $\vec{a}\times\vec{b}$ dat sa

$$|\vec{a}\times\vec{b}| = |\vec{a}||\vec{b}|\sin\angle(\vec{a},\vec{b}).$$

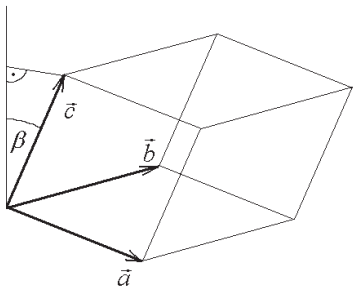
Neposredno se proverava da $\vec{a}$, $\vec{b}$ i $\vec{a}\times\vec{b}$ čine desni triedar, kao i da je $\vec{a}\times\vec{b}$ normalan i na $\vec{a}$ i na $\vec{b}$. $\diamond$

8.2.3 Mešoviti proizvod u V^3

Definicija 8.28 Mešoviti proizvod vektora $\vec{a}$, $\vec{b}$, $\vec{c}$ je skalar $(\vec{a}\times\vec{b})\cdot\vec{c}$.

Tvrđenje 8.29 *Apsolutna vrednost mešovitog proizvoda vektora $\vec{a},\vec{b},\vec{c}\in V^3$ jednaka je zapremini paralelepipeda obrazovanog nad vektorima $\vec{a}$, $\vec{b}$, $\vec{c}$.*

Dokaz. Neka vektori $\vec{a}$, $\vec{b}$ i $\vec{c}$ obrazuju triedar desne orijentacije (vidi sliku).



Označimo sa $\vec{p}$ vektor $\vec{a}\times\vec{b}$. Tada važi

$$\begin{aligned} (\vec{a}\times\vec{b})\cdot\vec{c} &= \vec{p}\cdot\vec{c}=|\vec{p}|\vec{p}_0\cdot\vec{c} \\ &= |\vec{p}||\vec{p}_0|\cdot|\vec{c}|\cos\angle(\vec{p}_0,\vec{c}). \end{aligned}$$

Kako je $|\vec{a} \times \vec{b}| = B$ jednako mernom broju površine paralelograma obrazovanog nad vektorima $\vec{a}$ i $\vec{b}$, a visina paralelepipeda iznosi $|\vec{c}| \cos \angle(\vec{p}, \vec{c}) = H$, to je

$$(\vec{a} \times \vec{b}) \cdot \vec{c} = B \cdot H = V.$$

gde je V zapremina paralelepipeda.

Ako vektori $\vec{a}$, $\vec{b}$ i $\vec{c}$ obrazuju triedar leve orijentacije, tada je $\cos \angle(\vec{p}, \vec{c}) < 0$, pa je $(\vec{a} \times \vec{b}) \cdot \vec{c} = -V$. ∎

Mešoviti proizvod vektora $\vec{a}, \vec{b}, \vec{c}$ jednak je nuli ako je bar jedan od vektora $\vec{a}$, $\vec{b}$ ili $\vec{c}$ nula-vektor ili ako sva tri vektora leže u jednoj ravni, tj. ako su komplanarni. U slučaju komplanarnosti tri vektora zapremina paralelepipeda konstruisanog nad ovim vektorima je jednaka nuli, pa je $(\vec{a} \times \vec{b}) \cdot \vec{c} = 0$.

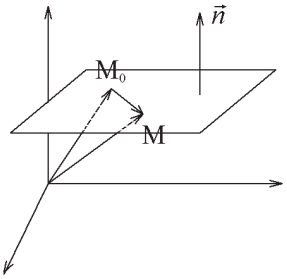
Napomena 8.30 Kako su skalarni i vektorski proizvodi dati u R^3_e i V^3 ekvivalentni, to su i mešoviti proizvodi takvi. ⋄

8.3 Jednačine ravni i prave

Koristeći osobine vektora izvešćemo jednačine ravni i prave. Sa $\overrightarrow{AB}$ označavamo vektor čiji je jedan predstavnik orjentisana duž AB. Ako je O koordinatni početak, tada sa $\vec{M}$ označavamo vektor $\overrightarrow{OM}$.

8.3.1 Jednačina ravni

Neka je M_0 data tačka u prostoru i neka je $\vec{n} \neq \vec{0}$ dati vektor. Skup svih tačaka M takvih da je vektor $\overrightarrow{M_0M}$ normalan na vektor $\vec{n}$ naziva se *ravan* kroz tačku M_0 (vektor $\vec{n}$ se naziva *vektor normale*).



Vektor $\overrightarrow{M_0M}$ se može izraziti preko vektora $\overrightarrow{OM_0}$ i $\overrightarrow{OM}$ tj.

$$\overrightarrow{OM} - \overrightarrow{OM_0} = \overrightarrow{M_0M}\,.$$

Kako su vektori $\overrightarrow{M_0M}$ i $\vec{n}$ normalni, njihov skalarni proizvod je jednak nuli:

$$\vec{n} \cdot (\overrightarrow{OM} - \overrightarrow{OM_0}) = 0. \tag{8.4}$$

Ako je $\vec{n} = (A,\, B,\, C)$, $\overrightarrow{OM_0} = (x_0,\, y_0,\, z_0)$, $\overrightarrow{OM} = (x,\, y,\, z)$, tada jednačina 8.4 u analitičkom obliku glasi

$$Ax + By + Cz - Ax_0 - By_0 - Cz_0 = 0 \tag{8.5}$$

Ako označimo $Ax_0 + By_0 + Cz_0$ sa D, dobijamo

$$Ax + By + Cz = D. \tag{8.6}$$

To je *opšti oblik jednačine ravni u analitičkom obliku.*

Napomena 8.31 Jednačina 8.6 je linearna jednačina po x, y i z. Važi i obrnuto, tj. ako je data jednačina $Ax + By + Cz = D$ kod koje je bar jedan od brojeva A, B, C različit od 0, onda je ona jednačina ravni. Neka je (x_0, y_0, z_0) jedno rešenje jednačine $Ax + By + Cz = D$. Ako sada stavimo da je $\vec{n} = (A, B, C)$ i ako tačka M_0 ima koordinate (x_0, y_0, z_0), onda dolazimo do jednačine $\vec{n} \times (\overrightarrow{OM} - \overrightarrow{OM_0}) = \vec{0}$ koju zadovoljava svako rešenje jednačine $Ax + By + Cz = D$. $\diamond$

Kako je $\vec{n} = (A, B, C)$ i $\vec{r} = \overrightarrow{OM} = (x, y, z)$ (tj. vektor položaja proizvoljne tačke M), to geometrijski oblik jednačine ravni jeste:

$$\vec{r} \cdot \vec{n} = D.$$

Koristeći jednačinu 8.5 možemo zapisati i analitički oblik jednačine ravni kroz tačku M_0, normalnu na vektor normale $\vec{n}$. To je jednačina

$$A(x - x_0) + B(y - y_0) + C(z - z_0) = 0.$$

Dve ravni su *paralelne* ako su im vektori normala $\vec{n}_1$ i $\vec{n}_2$ kolinearni, a *normalne* ako su im vektori normala međusobno normalni.

Ako su date tri različite tačke M_1, M_2 i M_3 koje ne leže na jednoj pravoj onda možemo odrediti *jednačinu ravni kroz date tri tačke*, na sledeći način. Neka je M proizvoljna tačka ravni, tada su vektori $\overrightarrow{M_1M}$, $\overrightarrow{M_1M_2}$ i $\overrightarrow{M_1M_3}$ kolinearni, pa je njihov mešoviti proizvod jednak nuli tj.

$$\overrightarrow{M_1M} \cdot (\overrightarrow{M_1M_2} \times \overrightarrow{M_1M_3}) = 0.$$

Kako je

$$\begin{aligned}
\overrightarrow{M_1M} &= \overrightarrow{OM} - \overrightarrow{OM_1} = (x,y,z) - (x_1,y_1,z_1) \\
&= (x-x_1, y-y_1, z-z_1) \\
\overrightarrow{M_1M_2} &= \overrightarrow{OM_2} - \overrightarrow{OM_1} = (x_2-x_1, y_2-y_1, z_2-z_1) \\
\overrightarrow{M_1M_3} &= \overrightarrow{OM_3} - \overrightarrow{OM_1} = (x_3-x_1, y_3-y_1, z_3-z_1),
\end{aligned}$$

dobijamo analitički oblik jednačine ravni kroz tačke M_1, M_2 i M_3:

$$\begin{vmatrix} x-x_1 & y-y_1 & z-z_1 \\ x_2-x_1 & y_2-y_1 & z_2-z_1 \\ x_3-x_1 & y_3-y_1 & z_3-z_1 \end{vmatrix} = 0$$

Primer 8.32 Napisati jednačinu ravni kroz date tri tačke $M_1(1,2,3)$, $M_2(-1,0,0)$ i $M_3(3,0,1)$. Tražena ravan je

$$\begin{vmatrix} x-1 & y-2 & z-3 \\ -2 & -2 & -3 \\ 2 & -2 & -2 \end{vmatrix} = 0,$$

tj. $x+5y-4z+1=0$. $\triangle$

8.3.2 Jednačina prave

Kako je prava presek dve ravni koje nisu paralelne, to se jednačina prave može dati skupom jednačina dvaju ravni:

$$\vec{r}\cdot\vec{n}_1 = D_1 \qquad \text{i} \qquad \vec{r}\cdot\vec{n}_2 = D_2,$$

ili u analitičkom obliku:

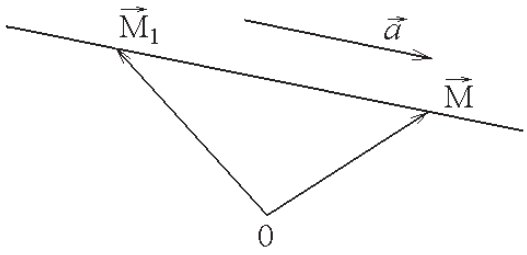
$$A_1x + B_1y + C_1z = D_1, \qquad A_2x + B_2y + C_2z = D_2.$$

Prava u prostoru je određena ako je poznata tačka M_1 kroz koju ona prolazi i vektor $\vec{a} \neq \vec{0}$ kome je prava paralelna, dakle

$$\overrightarrow{OM} = \overrightarrow{OM_1} + \overrightarrow{M_1M}\,.$$

Kako je vektor $\overrightarrow{M_1M}$ kolinearan sa $\vec{a}$, tj. $\overrightarrow{M_1M} = k\vec{a}$, dobijamo

$$\overrightarrow{OM} = \overrightarrow{OM_1} + k\vec{a} \tag{8.7}$$



i

$$\overrightarrow{OM} - \overrightarrow{OM_1} = k\vec{a}.$$

Poslednju jednačinu možemo napisati u obliku

$$(\overrightarrow{OM} - \overrightarrow{OM_1}) \times \vec{a} = \vec{0}.$$

Ako su dati vektori $\overrightarrow{OM} = (x, y, z)$, $\overrightarrow{OM_1} = (x_1, y_1, z_1)$ i $\vec{a} = (m, n, p)$, tada vektorskoj jednačini 8.7 odgovaraju tri skalarne jednačine date sistemom:

$$\begin{array}{rcl} x & = & x_1 + mk \\ y & = & y_1 + nk \\ z & = & z_1 + pk. \end{array} \tag{8.8}$$

Ove jednačine predstavljaju tzv. *parametarski oblik* jednačine prave. Ako su m, n i p različiti od 0, onda možemo eliminisati parametar k i dobiti jednačinu prave u *segmentnom obliku*:

$$\frac{x - x_1}{m} = \frac{y - y_1}{n} = \frac{z - z_1}{p}.$$

Ako je, na primer, $p = 0$, onda se sistem 8.8 može napisati u obliku:

$$\frac{x - x_1}{m} = \frac{y - y_1}{n}, \qquad z = z_1 \tag{8.9}$$

a ako su na primer n i p jednaki nuli, sistem 8.8 glasi

$$x = x_1 + m \cdot k, \qquad y = y_1, \qquad z = z_1. \tag{8.10}$$

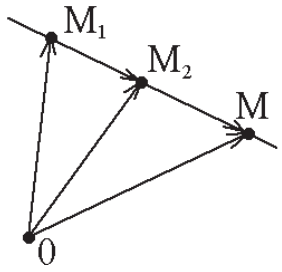
Primer 8.33 Nađimo jednačinu prave kroz tačku $(1, 2, 3)$ paralelnu sa vektorom $\vec{a} = (1, -2, 1)$. Prema prethodnom razmatranju dobijamo

$$\frac{x - 1}{1} = \frac{y - 2}{-2} = \frac{z - 3}{1}.$$

$\triangle$

Prava je određena dvema tačkama M_1 i M_2. Vektor $\vec{a}$ pravca prave je $\overrightarrow{M_1M_2}$. Ako sada u jednačini 8.7 stavimo $\overrightarrow{M_1M_2}$ umesto $\vec{a}$, dobijamo *jednačinu prave kroz dve tačke* M_1 i M_2:

$$\overrightarrow{OM} = \overrightarrow{OM_1} + k\,\overrightarrow{M_1M_2}\,. \tag{8.11}$$



Ako je $\overrightarrow{OM} = (x, y, z)$, $\overrightarrow{OM_1} = (x_1, y_1, z_1)$ i $\overrightarrow{M_1M_2} = (x_2 - x_1, y_2 - y_1, z_2 - z_1)$, tada iz jednačine 8.11 dobijamo *parametarski oblik jednačine prave kroz dve tačke* M_1 i M_2, dat sistemom

$$\begin{array}{rcl} x & = & x_1 + k(x_2 - x_1) \\ y & = & y_1 + k(y_2 - y_1) \\ z & = & z_1 + k(z_2 - z_1), \end{array} \tag{8.12}$$

a iz 8.12 eliminacijom k dobijamo *simetrični oblik jednačine prave*:

$$\frac{x - x_1}{x_2 - x_1} = \frac{y - y_1}{y_2 - y_1} = \frac{z - z_1}{z_2 - z_1} \qquad (\overrightarrow{M_1M_2} \neq \vec{0}). \tag{8.13}$$

Primer 8.34 Prava kroz tačke $(1, 0, -2)$ i $(2, -1, 3)$ zadata je jednačinom

$$\frac{x - 1}{1} = \frac{y}{-1} = \frac{z + 2}{5}.$$

$\triangle$

Neka je data prava

$$a: \quad \frac{x - x_1}{m} = \frac{y - y_1}{n} = \frac{z - z_1}{p} = k$$

i neka je data ravan α sa

$$Ax + By + Cz + D = 0.$$

Odredimo prodor prave a kroz ravan α. Iz jednačine prave izrazimo x, y, z preko k, pa uvrstimo x, y, z u jednačinu α. Tako dobijamo jednačinu po k. Nalazeći to k i zamenjujući ga u $x = x_1 + mk$, $y = y_1 + nk$, $z = z_1 + pk$, dobijamo koordinate prodora.

Bibliografija

[GB] G. Birkhoff: *Lattice theory*, The AMS, New York, 1948.

[BC] S. M. Bogdanović, M. D. Ćirić: *Polugrupe*, Prosveta, Niš, 1993.

[BM] N. Božović, Ž. Mijajlović: *Uvod u teoriju grupa*, Naučna knjiga, Beograd, 1990.

[BS] S. Burris, H. P. Sankappanavar: *A Course in Universal Algebra*, Springer Verlag, New York-Heidelberg-Berlin, 1981.

[CS] D. M. Cvetković, S. K. Simić: *Kombinatorika - klasična i moderna*, Naučna knjiga, Beograd, 1984.

[CDM] S. Crvenković, I. Dolinka, R. Madarász: *Odabrane teme opšte algebre*, PMF, Novi Sad, 1997.

[GCBT] G. Čupona, B. Trpenovski: *Predavanja po algebre* II, Skopje, 1976.

[VD] V. Dašić: *Algebra*, NIO "Univerzitetska riječ", Podgorica, 1987.

[RD] R. Doroslovački: *Elementi opšte i linearne algebre*, FTN, Novi Sad, 1997.

[JD] J. Dudek: *A Note on Model of Identities*, Algebra Universalis (1988), pp 400-401.

[GL] K. Gilezan, B. Latinović: *Bulova algebra i primene*, Matematički institut, Beograd, 1977.

[GG] G. Grätzer: *Universal Algebra*, D. Van Nostrand Comp. Inc., 1968.

[MG] M. Grulović: *Osnovi teorije grupa*, Institut za Matematiku, Novi Sad, 1997.

[SH] S. Hedman: First cours in Logic, Oxford, 2004.

[SJ] S. Jablonskii: *Vvedenie v diskretnuju matematiku*, Nauka, Moskva, 1979.

[GK] G. Kalajdžić: *Algebra*, BS Procesor - Matematički fakultet, 1992.

[KU] M. Kac, S. Ulam: Matematika i logika, Školska knjiga, Zagreb, 1977.

[JK] J. Kečkić: *Linearna algebra*, Naučna knjiga, Beograd, 1985.

[AKO] A. I. Kostrikin: *Vvedenie v algebru*, Nauka, Moskva, 1977.

[DJK] Đ. Kurepa: *Viša algebra I, II*, Zavod za izdavanje udžbenika, Beograd, 1971.

[SK] S. Kurepa: *Konačno dimenzionalni vektorski prostori i primjene*, Tehnička knjiga, Zagreb, 1967.

[AG74] A. Kuroš: *Obščaja algebra*, Nauka, Moskva, 1974.

[AL] A. Lipkovski: *Linearna algebra i analitička geometrija*, Naučna knjiga, Beograd, 1992.

[MC] S. R. Madarász, S. Crvenković: *Relacione algebre*, Matematički institut, Beograd, 1992.

[MGA] S. Markovski, D. Gligorski, S. Andova, *Using quasigroups for one-one secure encoding*, Proceedings of the VII Conference on Logic and Computer Science *LIRA '97*, pp. 157-162, Novi Sad, 1997.

[SMA] S. Mardešić: *Matematička analiza I*, Školska knjiga, Zagreb, 1974.

[MK] V. Mičić, Z. Kadelburg: *Uvod u teoriju brojeva,*Društvo matemativcara SR Srbije, Beograd, 1989.

[ZM] Ž. Mijajlović: *Algebra I*, Milgor, Beograd - Moskva, 1993.

[SM84] S. Milić: *Elementi algebre*, Institut za matematiku, Novi Sad, 1984.

[DM] D. Mitrinović: *Zbornik matematičkih problema III*, Zavod za izdavanje udžbenika Srbije, Beograd, 1960.

[MMV] D. S. Mitrinović, D. Mihailović, P. M. Vasić: *Linearna algebra, polinomi, analitička geometrija*, Građevinska knjiga, Beograd, 1983.

[VP] V. Perić: *Algebra I, II*, Svjetlost, Sarajevo, 1980.

[MR] M. Radić: *Algebra I, II*, Školska knjiga, Zagreb, 1989.

[LS] L. A. Skornjakov: *Elementi obšćej algebri*, Nauka, Moskva, 1982.

[MS58] M. D. Stojaković: *Elementi linearne algebre*, Zavod za izdavanje udžbenika, Beograd, 1958.

[MS73] M. D. Stojaković: *Teorija jednačina*, Naučna knjiga, Beograd, 1973.

[SP] Z. Stojaković, Đ. Paunić: *Zbirka zadataka iz algebre*, Građevinska knjiga, Beograd, 1993.

[TV] R. Tošić, V. Vukosavljević: *Elementi teorije brojeva*, ALEF, Novi Sad, 1995.

[GV] G. Vojvodić: *Algebra*, Institut za matematiku, Novi Sad, 1992.

[GV1] G. Vojvodić: Predavanja iz matematičke logike i algebre, Univerzitet u Novom Sadu, Novi Sad, 1998.

[VS] G. Vojvodić, B. Šobot: Zbirka zadataka iz matematičke logike iz algebre, Univerzitet u Novom Sadu, Novi Sad, 2003.