[1] Опис лиценци Креативне заједнице доступан је на адреси creativecommons.org.rs/?page_id=74.

Univerzitet u Novom Sadu
Prirodno-matematički fakultet
Departman za matematiku i informatiku

dr Nebojša Mudrinski

Predavanja iz algebre za informatičare

Novi Sad, 2017

Sadržaj

Predgovor **1**
0.1 Osnovni pojmovi i tvrđenja 3

1 Brojevi i polinomi **6**
1.1 Brojevne strukture 6
1.1.1 Teorija brojeva 12
1.2 Polinomi 18

2 Algebarske strukture **26**
2.1 Grupoidi. Kvazigrupe. 26
2.2 O polugrupama 29
2.3 Grupe 34
2.3.1 Definicija, osnovne osobine i primeri 35
2.3.2 Lagranžova teorema 36
2.3.3 Kejlijeva teorema reprezentacije 41
2.4 Prsteni i polja 45
2.5 Mreže i Bulove algebre 50
2.5.1 Mreža kao relacijska i algebarska struktura 50
2.5.2 Modularne i distributivne mreže 53
2.5.3 Bulove algebre 55

3 Linearna algebra **57**
3.1 Gausov algoritam. Vektorski prostori. Matrice 57
3.1.1 Sistemi jednačina 57
3.1.2 Vektorski prostori 60
3.1.3 Matrice 63
3.2 Determinante 65
3.3 Inverzne matrice i primena 70

Literatura **74**

Predgovor

Ova knjiga je pisana prema predavanjima koja sam držao iz predmeta Algebra za informatičare za studente prve godine smera informacione tehnologije. Svakako je mogu koristiti i ostali studenti koji slušaju neki predmet sa uvodnim sadržajem iz algebre. Iako se knjiga može čitati i samostalno, pretpostavlja se da je čitalac upoznat sa osnovnim pojmovima kao što su skupovi, relacije i funkcije kao i logika prvog reda.

Sadržaj je podeljen u tri glave koje nose sledeće nazive: Brojevi i polinomi, Algebarske strukture i Linearna algebra. U prvoj glavi obrađuju se teme pretežno poznate studentima iz srednje škole, sa ciljem da se znanje ponovi, dopuni i na adekvatan način koriguje uz filozofski uvod sa motivacijom uvođenja brojeva. Druga glava predstavlja jezgro ove knjige jer se u njoj izlažu osnove apstraktne algebre - algebarske strukture, gde se materijali iz prve glave navode kao glavni primeri. Među algebarskim strukturama koje se obrađuju akcenat je stavljen na grupe, jer se one provlače i kroz druge algebarske strukture kao što su prsteni, ali i linearnu algebru. U trećoj glavi se obrađuju elementi linearne algebre pretežno vezani za sisteme jednačina. Apstraktni pojam vektora i vektorskog prostora se tek površno ilustruje kroz neka tvrđenja.

Za uspešnu realizaciju ovog udžbenika zahvaljujem se recenzentima, Departmanu za matematiku i informatiku i Prirodno-matematičkom fakultetu u Novom Sadu.

Novi Sad, 16.5.2017. Nebojša Mudrinski

0.1 Osnovni pojmovi i tvrđenja

U ovom delu ćemo se ukratko podsetiti osnovnih pojmova vezanih za relacije i funkcije koje ćemo koristiti i nadograditi u materijalu koji sledi. Za one kojima je o ovome potrebno detaljnije izlaganje preporučujemo knjigu [9].

Za proizvoljan neprazan skup A i $n \in \mathbb{N}$ Dekartov stepen definišemo sa $A^n = \{(a_1, \ldots, a_n) \,|\, a_1, \ldots, a_n \in A\}$. Specijalno za $n = 2$ je $A^2 = A \times A = \{(a, b) \,|\, a, b \in A\}$. Oparacije preseka, unije i razlike skupova definišemo na uobičajeni način i označavamo redom sa $\cap, \cup, \setminus$, a skup svih podskupova nekog skupa A označavamo sa $\mathcal{P}(A)$.

Binarna relacija skupa A je svaki podskup od A^2. Relaciju A^2 ćemo zvati puna relacija. Binarne relacije obično označavamo malim grčkim slovima. Ukoliko je za neku binarnu relaciju θ i $p, q \in A$ $(p, q) \in \theta$ to onda čitamo da je element p u relaciji θ sa elementom q, što ćemo ponekad pisati i kao $p\theta q$.

Ako je svaki element skupa A u relaciji sa samim sobom kažemo da je relacija refleksivna. Ako se relacija sastoji samo od parova čije su komponente međusobno jednake onda je to dijagonala. Relacija α na A se naziva simetrična, ako za sve $x, y \in A$ važi $(x, y) \in \alpha \Rightarrow (y, x) \in \alpha$, a antisimetrična ako za sve $x, y \in A$ važi $(x, y) \in \alpha \wedge (y, x) \in \alpha \Rightarrow x = y$. Ako za sve $x, y, z \in A$ važi $(x, y) \in \alpha \wedge (y, z) \in \alpha \Rightarrow (x, z) \in \alpha$ onda kažemo da je α tranzitivna.

Ukoliko je neka relacija refleksivna, simetrična i tranzitivna naziva se relacija ekvivalencije. Trivijalno dijagonala i puna relacija su relacije ekvivalencije. Svaka relacija ekvivalencije particioniše skup na kome je definisana, drugim rečima deli taj skup na neprazne disjunktne podskupove čija je unija ceo skup. Elementi te particije su tačno klase ekvivalencije date relacije. Podsetimo se, klasa ekvivalencije nekog elementa je skup svih elemenata koji su sa njim u relaciji. Klasu elementa a u relaciji ekvivalencije α ćemo označavati sa a/α i prema već navedenom važi $a/\alpha = \{x \in A \,|\, x\alpha a\}$. Količnički skup je skup svih klasa ekvivalencije $A/\alpha = \{a/\alpha \,|\, a \in A\}$.

Ukoliko relacija jeste refleksivna, antisimetrična i tranzitivna nazivamo je relacija poretka. Sve relacije poretka delimo na relacije linearnog i parcijalnog poretka. Relacije linearnog poretka zadovoljavaju pored već navedenih osobina i uslov dihotomije: za svaka dva elementa a i b je a u relaciji sa b ili je b u relaciji sa a. Relacijsku strukturu koju čini skup sa definisanom relacijom poretka nazivamo i parcijalno uređenje. U parcijalnom uređenju za proizvoljna dva elementa možemo definisati pojam infimuma i supremuma. Naime, u parcijalnom uređenju (A, ρ) donje ograničenje za $\{a, b\} \subseteq A$ je skup onih elemenata x iz A za koje važi $x\rho a$ i $x\rho b$. Infimum za

dva elementa a i b, u oznaci $inf\{a,b\}$, je donje ograničenje za $\{a,b\}$, tako da za svako drugo donje ograničenje c iz A, važi $c\rho inf\{a,b\}$ ako takav element iz A postoji. Dualno, supremum dva elementa a i b, u oznaci $sup\{a,b\}$ je gornje ograničenje za $\{a,b\}$, tako da za svako drugo gornje ograničenje c iz A, važi $sup\{a,b\}\rho c$ ako takav element iz A postoji.

Podsetimo se još da za funkciju $f : A \to B$ kažemo da je "1-1" ili injekcija ako za sve $x, y \in A$ važi: $f(x) = f(y) \Rightarrow x = y$, a da za f kažemo da je "na" ili sirjekcija ako za svako $b \in B$ postoji $a \in A$ tako da je $f(a) = b$. Funkcija f se naziva bijekcija ako je i injekcija i sirjekcija. Bijekcija konačnog skupa u sebe sama naziva se još i permutacija. Funkcija ima inverzno preslikavanje ako i samo ako je bijekcija. Inverzno preslikavanje bijekcije je bijekcija. Podsetimo se i da kompoziciju preslikavanja $f, g : A \to A$ u oznaci $f \circ g$ definišemo kao preslikavanje iz A u A sa $(f \circ g)(x) = f(g(x))$, za sve $x \in A$. Uvodimo oznake $A^A = \{f \mid f : A \to A\}$ i $S_A = \{f \in A^A \mid f$ je bijekcija $\}$. Za sve $f, g, h \in A^A$ važi $(f \circ g) \circ h = f \circ (g \circ h)$. Ako $f : A \to B$, za $X \subseteq A$ je $f(X) = \{y \in B \mid (\exists x \in X) f(x) = y\}$, a za $Y \subseteq B$ definišemo $f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}$. Binarna relacija $kerf$ na A definisana za sve $x, y \in A$ sa $(x, y) \in kerf$ ako i samo ako je $f(x) = f(y)$, je relacija ekvivalencije na A. Slično za svaku relaciju ekvivalencije θ skupa A pod prirodnim preslikavanjem podrazumevamo $nat_\theta : A \to A/\theta$ dato sa $nat_\theta(a) = a/\theta$, za sve $a \in A$ i to preslikavanje je očigledno sirjekcija.

Glava 1

Brojevi i polinomi

U ovoj glavi dajemo bazično znanje iz kog ćemo u narednoj glavi crpiti primere i motivaciju za uvođenje apstraktnih algebarskih struktura. Naime, dajemo skicu i objašnjavamo osnovnu ideju aksiomatskog zasnivanja različitih skupova brojeva zajedno sa osnovnim operacijama na brojevima (sabiranje i množenje) kao i zasnivanje prirodnog poretka. Celi brojevi su nam zbog relacije deljivosti posebno interesantni i njima posvećujemo posebno predavanje. Po analogiji sa brojevima izlažemo osnovna tvrđenja o polinomima.

1.1 Brojevne strukture

U ovoj sekciji dokaz dajemo samo za pojedina tvrđenja gde ilustrujemo "mustru" po kojoj se dokazuju i ostala tvrđenja, ipak neke dokaze preskačemo i zbog svog obima koji bi čitaoca odvukli od ideje vodilje o zasnivanju brojeva koju treba da prati. Za one koje zanima, dokazi se mogu naći u [8].

Definicija 1.1 *Struktura prirodnih brojeva je uređena trojka* $(\mathbb{N}_0, ', 0)$ *gde je* $\mathbb{N}_0$ *skup,* $'$ *(prim) unarna operacija na* $\mathbb{N}_0$*, a* 0 *konstanta iz* $\mathbb{N}_0$ *tako da važi:*

(P1) $(\forall x)(0 \neq x')$*;*

(P2) $(\forall x, y)(x' = y' \Rightarrow x = y)$*;*

(P3) *Ako je* $M \subseteq \mathbb{N}_0$*, onda važi:*

$$0 \in M \wedge (\forall x)(x \in M \Rightarrow x' \in M) \Rightarrow M = \mathbb{N}_0.$$

Iskaze (P1), (P2) i (P3) nazivamo Peanove aksiome. Elemente skupa $\mathbb{N}_0$ nazivamo prirodni brojevi, a sam skup $\mathbb{N}_0$ skup prirodnih brojeva. Skup prirodnih brojeva bez 0 ćemo označavati sa $\mathbb{N}$. Element 0 nazivamo nula. Unarnu operaciju $'$ nazivamo sledbenik. Tada aksiomu (P1) čitamo: "Nula nije ničiji sledbenik.", a aksioma (P2) kaže da je funkcija sledbenika injektivna. Aksioma (P3) je poznatija pod imenom Princip matematičke indukcije. Uvodimo oznaku $0' = 1$.

DEFINICIJA 1.2 *Binarnu operaciju $+$ (sabiranje) na $\mathbb{N}_0$ definišemo na sledeći način:*

(S1) $x + 0 = x$;

(S2) $x + y' = (x + y)'$.

Binarnu operaciju $\cdot$ (množenje) na $\mathbb{N}_0$ definišemo na sledeći način:

(M1) $x \cdot 0 = 0$;

(M2) $x \cdot y' = x \cdot y + x$.

TEOREMA 1.3 *Neka je $\mathbb{N}_0$ skup prirodnih brojeva. Tada za sve $x, y, z \in \mathbb{N}_0$ važi:*

1. $x + (y + z) = (x + y) + z$ *(asocijativnost sabiranja);*
2. $x + y = y + x$ *(komutativnost sabiranja);*
3. $x + y = x + z \Rightarrow y = z$ *(leva kancelativnost sabiranja);*
4. $x \cdot y = y \cdot x$ *(komutativnost množenja);*
5. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ *(asocijativnost množenja);*
6. $x \cdot 1 = 1 \cdot x = x$ *(neutralni/jedinični element za množenje);*
7. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ *(leva distributivnost);*
8. $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ *(desna distributivnost);*
9. *Ako je $x \neq 0$ onda $x \cdot y = x \cdot z \Rightarrow y = z$ (kancelativnost množenja).*

Dokaz: Daćemo dokaz prvog tvrđenja, a ostali dokazi se izvode na sličan način. Dokaz dajemo indukcijom po z. Neka je

$$M = \{z \in \mathbb{N}_0 \mid (\forall x, y)((x + y) + z = x + (y + z))\}.$$

Jasno $0 \in M$ jer je $(x + y) + 0 = x + y = x + (y + 0)$ zbog (S1) (baza važi). Neka $z \in M$, pokažimo da $z' \in M$. Neka su x i y proizvoljni elementi iz $\mathbb{N}_0$. Korišćenjem (S2) nekoliko puta dobijamo: $(x + y) + z' = ((x + y) + z)' = (x + (y + z))' = x + (y + z)' = x + (y + z')$. Ovde smo indukcijsku hipotezu ($z \in M$) iskoristili u drugoj jednakosti. □

Definicija 1.4 *U skupu $\mathbb{N}_0$ uvodimo binarnu relaciju $\leq$ (manje ili jednako) na sledeći način: $x \leq y \Leftrightarrow (\exists z)(x + z = y)$.*

Propozicija 1.5 *$\leq$ je relacija linearnog poretka na skupu $\mathbb{N}_0$, takva da za sve $x, y, z \in \mathbb{N}_0$ važi:*

1. *$x \leq y \Rightarrow x + z \leq y + z$; (saglasnost linearnog poretka sa sabiranjem)*
2. *$x \leq y \Rightarrow xz \leq yz$; (saglasnost linearnog poretka sa množenjem)*

Definicija 1.6 *U skupu $\mathbb{N}$ uvodimo binarnu relaciju $\mid$ na sledeći način: $x \mid y \Leftrightarrow (\exists z)(x \cdot z = y)$.*

Propozicija 1.7 *$\mid$ je relacija parcijalnog poretka na skupu $\mathbb{N}$.*

Posmatrajmo jednačinu $a + x = b$, po x, gde su a i b unapred zadati prirodni brojevi. Ova jednačina ima rešenje u prirodnim brojevima samo u slučaju $a \leq b$. Ovaj problem nam govori da naš skup (prirodnih) brojeva nije dovoljno "dobar", pa ga proširujemo tako da pomenuta jednačina postane uvek rešiva.

Primetimo da jednačine:

$$0 + x = 0, 1 + x = 1, 2 + x = 2, \ldots$$

$$0 + x = 1, 1 + x = 2, 2 + x = 3, \ldots$$

$$\ldots$$

uvek imaju isto rešenje (ako su iz istog od nabrojanih nizova jednačina). Označimo njihova rešenja sa: $(0, 0), (1, 1), (2, 2), \ldots, (0, 1), (1, 2), (2, 3), \ldots$. Posmatramo i sledeće nizove jednačina:

$$1 + x = 0, 2 + x = 1, 3 + x = 2, \ldots$$

$$2 + x = 0, 3 + x = 1, 4 + x = 2, \ldots$$

Njihova rešenja ćemo označiti sa: $(1,0), (2,1), (3,2), \ldots, (2,0), (3,1), (4,2), \ldots$ Ovaj postupak nas navodi na sledeću definiciju.

DEFINICIJA 1.8 *Binarnu relaciju* $\approx$ *na skupu* $\mathbb{N}_0 \times \mathbb{N}_0$ *definišemo sa* $(a,b) \approx (c,d) \Leftrightarrow a + d = b + c$, *za sve* $a, b, c, d \in \mathbb{N}_0$.

PROPOZICIJA 1.9 $\approx$ *je relacija ekvivalencije na skupu* $\mathbb{N}_0 \times \mathbb{N}_0$.

Dokaz: Refleksivnost i simetričnost slede iz definicije relacije $\approx$ i komutativnosti sabiranja prirodnih brojeva. Pokažimo tranzitivnost. Neka su $a, b, c, d, e, f \in \mathbb{N}_0$ takvi da je $(a,b) \approx (c,d)$ i $(c,d) \approx (e,f)$. Po definiciji dobijamo da je $a + d = b + c$ i $c + f = d + e$. Sada iz prve jednakosti dobijamo da je $(a + d) + (e + f) = (b + c) + (e + f)$, pa primenom komutativnosti i asocijativnosti za sabiranje imamo $(a+f)+(d+e) = (b+e)+(c+f)$. Sada kancelativnost sabiranja daje $a + f = b + e$, jer je $d + e = c + f$. Po definiciji relacije $\approx$ dobijamo $(a,b) \approx (e,f)$. $\square$

DEFINICIJA 1.10

$$(a,b)/\approx + (c,d)/\approx = (a + c, b + d)/\approx;$$

$$(a,b)/\approx \cdot (c,d)/\approx = (ad + bc, ac + bd)/\approx;$$

za sve $a, b, c, d \in \mathbb{N}_0$.

PROPOZICIJA 1.11 *Operacije* $+$ *i* $\cdot$ *na skupu* $(\mathbb{N}_0 \times \mathbb{N}_0)/\approx$ *su dobro definisane.*

Napomenimo pre formulacije sledeé teoreme da ćemo rešenje jednačine $a + x = 0$ nazivati suprotan broj broja a.

TEOREMA 1.12 *U strukturi* $(\mathbb{N}_0 \times \mathbb{N}_0)/\approx$ *jednačina* $(a,b)/\approx + x = (c,d)/\approx$ *ima rešenje. Struktura* $(\{(0,n)/\approx \mid n \in \mathbb{N}_0\}, +, \cdot)$ *je izomorfna strukturi* $(\mathbb{N}_0, +, \cdot)$. *Operacije* $+$ *i* $\cdot$ *imaju sve osobine sabiranja i množenja u prirodnim brojevima. Takođe postoji suprotan broj u odnosu na element* $(0,0)/\approx$.

Ovde izomorfno znači da se operacije $+$ i $\cdot$ na skupu $\{(0,n)/\approx \mid n \in \mathbb{N}_0\}$ ponašaju kao sabiranje i množenje u prirodnim brojevima samo su ti prirodni brojevi drugačije obeleženi. Stoga, $(n,0)/\approx$ poistovećujemo sa negativnim brojevima, a skup $(\mathbb{N}_0 \times \mathbb{N}_0)/\approx$ označavamo sa $\mathbb{Z}$ i nazivamo skup celih brojeva. Klasu $(n,0)/\approx$ označavamo sa $-n$. Na osnovu toga uvodimo operaciju oduzimanja.

Definicija 1.13 *Binarnu operaciju $-$, oduzimanje na skupu celih brojeva definišemo sa $x - y = x + (-y)$, za sve $x, y \in \mathbb{Z}$.*

Jednačina $a \cdot x = b$ za proizvoljne unapred zadate cele brojeve $a \neq 0$ i b, po x, ima rešenje akko $a \mid b$. Ovaj problem nam govori da naš skup celih brojeva nije dovoljno "dobar", pa ga proširujemo tako da pomenuta jednačina postane uvek rešiva.

Primetimo da jednačine

$$1 \cdot x = 1, 2 \cdot x = 2, \ldots$$

$$1 \cdot x = 2, 2 \cdot x = 4, \ldots$$

$$\ldots$$

uvek imaju isto rešenje (ako su iz istog od nabrojanih nizova jednačina). Označimo njihova rešenja sa: $(1,1), (2,2), \ldots, (1,2), (2,4), \ldots$. Ovaj postupak nas navodi na sledeću definiciju.

Definicija 1.14 *$\sim$ definišemo kao binarnu relaciju na skupu $\mathbb{Z}\backslash\{0\} \times \mathbb{Z}$ sa $(p,q) \sim (r,s) \Leftrightarrow p \cdot s = r \cdot q$ za sve $p, r \in \mathbb{Z}\backslash\{0\}$ i $q, s \in \mathbb{Z}$.*

Propozicija 1.15 *Relacija $\sim$ je relacija ekvivalencije na skupu $\mathbb{Z}\backslash\{0\} \times \mathbb{Z}$.*

Dokaz: Slično dokazu Propozicije 1.9, ali kod tranzitivnosti treba obratiti pažnju na uslov za kancelativnost množenja. Tu se koristi činjenica da je proizvod dva broja jednak nuli akko je bar jedan od njih nula. □

Klasu elementa $(a,b)/\sim$ označavamo sa $\frac{b}{a}$.

Definicija 1.16 *$\frac{p}{q} + \frac{r}{s} = \frac{p \cdot s + r \cdot q}{q \cdot s}$ i $\frac{p}{q} \cdot \frac{r}{s} = \frac{p \cdot r}{q \cdot s}$, za sve $p, r \in \mathbb{Z}$ i $q, s \in \mathbb{Z}\backslash\{0\}$.*

Propozicija 1.17 *Operacije $+$ i $\cdot$ na skupu $(\mathbb{Z}\backslash\{0\} \times \mathbb{Z})/\sim$ su dobro definisane.*

Teorema 1.18 *U strukturi $(\mathbb{Z}\backslash\{0\} \times \mathbb{Z})/\sim$ jednačina $\frac{p}{q} \cdot x = \frac{r}{s}$ ima rešenje. Struktura $(\{\frac{p}{1} \mid p \in \mathbb{Z}\}, +, \cdot)$ je izomorfna sa $(\mathbb{Z}, +, \cdot)$, a operacije $+$ i $\cdot$ imaju sve osobine koje imaju sabiranje i množenje celih brojeva. Svi nenula elementi su invertibilni, odnosno za svaki nenula element t postoji recipročan element t^{-1} tako da kada se pomnože dobija se $\frac{1}{1}$ (jedinica).*

Skup $(\mathbb{Z}\backslash\{0\} \times \mathbb{Z})/\sim$ nazivamo skup racionalnih brojeva i označavamo sa $\mathbb{Q}$, a njegove elemente racionalni brojevi.

Definicija 1.19 *Ne skupu nenula racionalnih brojeva definišemo binarnu operaciju : deljenja sa* $x : y = x \cdot y^{-1}$*, za sve* $x, y \in \mathbb{Q}\backslash\{0\}$*, a* $0 : z = 0$*, za sve* $z \in \mathbb{Q}\backslash\{0\}$*.*

Kada se racionalni brojevi prikazuju u decimalnom zapisu on je konačan ili periodično beskonačan. Šta je sa brojevima koji imaju neperiodičan beskonačan decimalan zapis? Njih nazivamo iracionalni brojevi. Sve ove brojeve zajedno zovemo realni brojevi, a operacije sabiranja i množenja se prenose iz skupa racionalnih brojeva na prirodan način, kao i linearni poredak $\leq$. Međutim to nije moguće učiniti nekim sličnim proširenjem kao do sada (algebarskom konstrukcijom)! Zato se struktura realnih brojeva $(\mathbb{R}, +, \cdot, \leq)$ zasniva aksiomatski i jedinstvena je do na izomorfizam, ako zadovoljava sve osobine iz teoreme 1.3 za $+$, $\cdot$ i $\leq$ koje su zadovoljene u $\mathbb{Q}$ i još aksiomu potpunosti. U uvodnom delu definisali smo supremum za dva elementa u parcijalnom uređenju, ovde će nam trebati supremum čitavog poskupa, koji se definiše analogno, kao što sledi u narednoj definiciji.

Definicija 1.20 *Neka je* $\leq$ *relacija poretka na nepraznom skupu* A *i* $B \subseteq A$*. Tada je* $supB \in A$*, ako postoji, takav da je* $supB$ *gornje ograničenje za* B *i za svako drugo gornje ograničenje* a *za* B *je* $supB \leq a$*.*

Definicija 1.21 *(Aksioma potpunosti) Svaki neprazan skup ograničen sa gornje strane ima najmanje gornje ograničenje (supremum).*

I dalje postoje jednačine koje nisu rešive ni u realnim brojevima. Takva jednačina je $x^2 + 1 = 0$. Zbog toga proširujemo skup realnih brojeva na sledeći način.

Definicija 1.22 *Na skupu* $\mathbb{R} \times \mathbb{R}$ *definišemo binarne operacije* $+$ *i* $\cdot$ *sa:*

$$(a, b) + (c, d) = (a + c, b + d);$$

$$(a, b) \cdot (c, d) = (a \cdot c - b \cdot d, b \cdot c + a \cdot d),$$

za sve $a, b, c, d \in \mathbb{R}$*.*

Teorema 1.23 *Operacije* $+$ *i* $\cdot$ *imaju sve osobine sabiranja i množenja realnih brojeva., element* $(0, 0)$ *je nula za sabiranje, a element* $(1, 0)$ *je jedinica za množenje,* $(-a, -b)$ *je suprotan za element* (a, b)*, a* $(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$ *je recipročan za element* (a, b)*. Struktura* $(\{(r, 0) \mid r \in \mathbb{R}\}, +, \cdot)$ *je izomorfna strukturi* $(\mathbb{R}, +, \cdot)$*. Jednačina* $(x, y)^2 + (1, 0) = (0, 0)$ *je rešiva.*

$(\mathbb{R} \times \mathbb{R}, +, \cdot)$ označavamo sa $(\mathbb{C}, +, \cdot)$ i nazivamo struktura kompleksnih brojeva, a njene elemente kompleksni brojevi. Prvu komponentu a zovemo realni , a drugu b imaginarni deo za svaki kompleksan broj (a, b). Uvodimo oznaku $(0, 1) = i$ i pišemo $a + ib$ umesto (a, b). Poredak $\leq$ takav da ima osobine koje ima u realnim brojevima se ne može definisati.

U narednom odeljku (polinomi) će nam trebati pojam konjugovanja kompleksong broja, pa ćemo se ovde ukratko podsetiti njegovih osnovnih osobina.

Definicija 1.24 *Ako je $z = a + ib \in \mathbb{C}$, onda konjugovani broj broja z jeste $\overline{z} = a - ib$.*

Primetimo da konjugovanje "ne utiče" na realne brojeve, odnosno na kompleksne brojeve čiji je imaginarni deo jednak nuli.

Propozicija 1.25 *Za sve $x, y, z \in \mathbb{C}$ važi:*

1. $\overline{x + y} = \overline{x} + \overline{y}$;
2. $\overline{x \cdot y} = \overline{x} \cdot \overline{y}$;
3. $\overline{(\overline{z})} = z$.

Dokaz: Direktno iz definicije konjugovanja, sabiranja i monženja kompleksnih brojeva. □

1.1.1 Teorija brojeva

Propozicija 1.26 *Neka su $a, b \in \mathbb{N}$ takvi da $a|b$. Tada je $a \leq b$.*

Dokaz: Direktno iz definicije relacije $|$ i saglasnosti linearnog poretka sa množenjem prirodnih brojeva. □

Teorema 1.27 *Neka su $a, b \in \mathbb{Z}$ i $b > 0$. Tada postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da je $0 \leq r < b$ i $a = bq + r$.*

Dokaz: Tvrđenje dokazujemo najpre za $a \in \mathbb{N}_0$ indukcijom po a. Neka je $b > 0$ unapred dat prirodan broj. Za $a = 0$ uzimamo $q = r = 0$. Neka je $a \in \mathbb{N}_0$ i $q', r' \in \mathbb{Z}$, takvi da je $a = bq' + r'$, gde je $0 \leq r' < b'$. Tada je $a + 1 = bq' + r' + 1$. Ako je $r' + 1 < b$ uzimamo $q = q'$ i $r = r' + 1$. Neka je $r' + 1 = b$. Tada je $a + 1 = b(q' + 1)$, pa uzimamo $q = q' + 1$ i $r = 0$. Time je pokazan indukcijski korak.

Ako je $a < 0$ onda je $-a > 0$ pa postoje $q_1, r_1 \in \mathbb{Z}$ takvi da je $-a = bq_1 + r_1, 0 \leq r_1 < b$. Ako je $r_1 \neq 0$ onda je $a = b(-q_1) - r_1 = b(-q_1 - 1) + b - r_1$, gde je $0 < b - r_1 < b$, pa uzimamo $q = -q_1 - 1$ i $r = b - r_1$. Za $r_1 = 0$ uzimamo $r = 0$ i $q = -q_1$.

Pretpostavimo sada da za unapred date $a, b \in \mathbb{Z}$, gde je $b > 0$ postoje $q, q', r, r' \in \mathbb{Z}$ takvi da je $a = bq + r$ i $a = bq' + r'$ gde je $0 \leq r < b$ i $0 \leq r' < b'$. Neka je $r \leq r'$. Pretpostavimo da je $r \neq r'$. Iz datih jednakosti dobijamo da je $bq + r = bq' + r'$ odnosno $b(q - q') = r' - r$. Zato $b|(r' - r)$. Međutim $r' - r < b$. Kontradikcija sa propozicijom 1.26. Ostaje $bq = bq'$ što daje $q = q'$. Ovim je pokazana jedinstvenost celih brojeva q i r. □

Definicija 1.28 *Broj q iz prethodne teoreme zovemo količnik, a r ostatak pri deljenju celog broja a pozitivnim brojem b. Ako je $r = 0$ onda je b delitelj od a ili kažemo još i da je a deljivo sa b i pišemo $b|a$.*

Primer: $-5 = (-2) \cdot 4 + 3$, ovde je -2 količnik, a 3 ostatak pri deljenju broja -5 sa 4.

Propozicija 1.29 *Za $x \in \mathbb{N}$ i $\alpha, \beta, y, z \in \mathbb{Z}$ važi: $x|y \wedge x|z \Rightarrow x|(\alpha y + \beta z)$.*

Dokaz: Direktno po definiciji. □

Definicija 1.30 *Za $a, b \in \mathbb{Z}$ najveći zajednički delitelj je $NZD(a, b) \in \mathbb{N}$ takav da je:*

1. *$NZD(a, b)|a$ i $NZD(a, b)|b$;*
2. *$c|a \wedge c|b \Rightarrow c|NZD(a, b)$, za sve $c \in \mathbb{Z}$.*

Teorema 1.31 *Za svaka dva cela broja postoji najveći zajednički delilac koji je jedinstven.*

Dokaz: Bez umanjenja opštosti pretpostavimo da $a, b \in \mathbb{N}$. Tada postoje nizovi prirodnih brojeva $q_1, \ldots, q_k, \ldots, r_1, \ldots, r_k, \ldots$ takvi da je:

$$a = bq_1 + r_1, 0 \leq r_1 < b;$$

$$b = r_1 q_2 + r_2, 0 \leq r_2 < r_1;$$

$$\ldots$$

$$r_k = r_{k+1} q_{k+2} + r_{k+2}, 0 \leq r_{k+2} < r_{k+1};$$

...

Međutim kako je $r_1 > \ldots > r_k > \ldots$, postoji $n \in \mathbb{N}_0$ takav da je $r_{n+1} = 0$. Zato je $r_{n-1} = r_n q_{n+1}$, pa $r_n | r_{n-1}$. Iz jednakosti $r_{n-2} = r_{n-1}q_n + r_n$ dobijamo da $r_n | r_{n-2}$ po Propoziciji 1.29. Tako redom vraćajući sa ka prvoj od niza navedenih jednakosti dobijamo da $r_n | a$ i $r_n | b$. Neka sada neko $c \in \mathbb{N}$ ima osobinu da $c|a$ i $c|b$. Iz prve od jednakosti dobijamo da je $r_1 = a - bq_1$, pa koristeći ponovo Propoziciju 1.29 dobijamo da $c|r_1$. Druga jednakost daje $r_2 = b - r_1 q_2$, pa $c|r_2$ i tako nastavljajući ka poslednjoj jednakosti, odnosno njenom ekvivalentu $r_n = r_{n-2} - r_{n-1}q_{n-1}$ dobijamo da $c|r_n$. Po definciji smo dobili da je $r_n = NZD(a, b)$. Dokaz jedinstvenosti se izvodi na osnovu antisimetričnosti relacije $|$. □

Postupak opisan u dokazu prethodne teoreme je istovremeno i postupak za traženje najvećeg zajedničkog delitelja za dva prirodna broja i naziva se *Euklidov algoritam* i najstariji je poznati algoritam.

Primer: Pronađimo $NZD(2014, 2017)$. $2017 = 1 \cdot 2014 + 3$, $2014 = 671 \cdot 3 + 1$, pa je $NZD(2014, 2017) = 1$

Teorema 1.32 *Neka su $a, b \in \mathbb{Z}$. Tada postoje $x, y \in \mathbb{Z}$ takvi da je $ax+by = NZD(a, b)$.*

Dokaz: Pretpostavimo bez umanjenja opštosti da je $b > 0$. Tada postoji $n \in \mathbb{N}$ i celi brojevi $q_1, \ldots, q_{n+1}, r_1, \ldots, r_n$ takvi da je: $a = bq_1 + r_1$, $b = r_1q_2 + r_2$ i tako redom do $r_{n-2} = r_{n-1}q_n + r_n$, gde je $r_n = NZD(a, b)$. Koristeći ove jednakosti možemo pokazati indukcijom po n (sa korakom dva) da za sve $i \in \{1, \ldots, n\}$ postoje $x_i, y_i \in \mathbb{Z}$ takvi da je $r_i = x_i a + y_i b$. Iz prve jednakosti vidimo da je za $i = 1$ potrebno uzeti $x_1 = 1$ i $y_1 = -q_1$, a za $i = 2$, kako je $r_1 = a - bq_1$, a $r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = -aq_2 + b(1 + q_1q_2)$ pa uzmimo $x_2 = -q_2$ i $y_2 = 1 + q_1q_2$. Pretpostavimo da tvrđenje važi za r_i i r_{i+1} i dokažimo za r_{i+2}. Kako je $r_{i+2} = r_i - r_{i+1}q_{i+2}$ to je $r_{i+2} = x_ia + y_ib - (x_{i+1}a + y_{i+1}b)q_{i+2} = (x_i - x_{i+1}q_{i+2})a + (y_i - y_{i+1}q_{i+2})b$, pa uzimamo $x_{i+2} = x_i - x_{i+1}q_{i+2}$ i $y_{i+2} = y_i - y_{i+1}q_{i+2}$. □

Lema 1.33 *Neka su $a, b, c \in \mathbb{N}$. Ako $c|ab$ i $NZD(c, a) = 1$ onda je $c|b$.*

Dokaz: Po teoremi 1.32 znamo da postoje $\alpha, \beta \in \mathbb{Z}$ takvi da je $\alpha c + \beta a = 1$. Odavde je $\alpha cb + \beta ab = b$. Kako $c|ab$ znamo da $c|\beta ab$, pa po propoziciji 1.29, pa $c|(\alpha cb + \beta ab)$, odnosno $c|b$. □

Definicija 1.34 *Prirodan broj veći od* 1 *naziva se prost ako je deljiv jedino sa jedinicom i samim sobom, inače je složen. Broj* 1 *nije ni prost ni složen.*

PROPOZICIJA 1.35 *Neka je p prost broj i $a, b \in \mathbb{Z}$. Ako $p|ab$ onda $p|a$ ili $p|b$.*

Dokaz: Pretpostavimo da $p|ab$ i $p \not| a$. Tada je $NZD(p, a) = 1$, pa po lemi 1.33 dobijamo da $p|b$. □

TEOREMA 1.36 *(Osnovni stav aritmetike) Za svaki prirodan broj $n > 1$ jedinstveno postoje: broj $k \in \mathbb{N}$, prosti brojevi $p_1 < \ldots < p_k$ i $\alpha_1, \ldots \alpha_k \in \mathbb{N}$ takvi da je $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$.*

Dokaz: Indukcijom po n. Za $n = 2$ uzimamo $k = \alpha_1 = 1$ i $p_1 = 2$, pa je baza indukcije tačna. Pretpostavimo da tvrđenje važi za sve prirodne brojeve manje od n i dokažimo za prirodan broj n. Ako je n prost broj postupamo analogno slučaju baze. Pretpostavimo da je n složen broj. Tada je $n = n_1 m_1$ gde su $n_1, m_1 > 1$, pa za njih važi indukcijska pretpostavka. Odavde direktno dobijamo da važi tvrđenje za n, čime je završen indukcijski dokaz. Pokažimo još jedinstvenost faktorizacije. Pretpostavimo da postoje $k, m \in \mathbb{N}$, prosti brojevi $p_1 < \ldots < p_k, q_1 < \ldots < q_m$ i $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_m$ takvi da je $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} = q_1^{\beta_1} \cdot \ldots \cdot q_m^{\beta_m}$. Ako prost broj p_i figuriše sa leve strane, on deli desnu stranu pa po lemi 1.33 deli neki od prostih brojeva koji se pojavljuju u proizvodu sa desne strane, a to je moguće samo ako je jednak nekom od njih. Zato je svaki prost broj koji se javlja sa leve strane jednakosti jednak nekom prostom broju sa desne strane jednakosti i obratno. Dakle, $k = m$ i $p_i = q_i$, za sve $i \in \{1, \ldots, k\}$. Kada izvršimo sva moguća skraćivanja sa leve i desne strane ostaju proizvodi različitih prostih brojeva sa raznih strana jednakosti. Ponovo primenom leme 1.33 dolazimo do kontradikcije. □

PROPOZICIJA 1.37 *Prostih brojeva ima beskonačno mnogo.*

Dokaz: Pretpostavimo da ih ima samo konačno mnogo. Neka su to $p_1, \ldots, p_n$. Posmatrajmo broj $k = p_1 \cdot \ldots \cdot p_n + 1$. Ako je k prost on nije jednak ni jednom od brojeva $p_1, \ldots, p_n$, ako je složen mora imati neki prost delilac koji nije jednak ni jednom od $p_1, \ldots, p_n$. Svakako postoji još neki prost broj koji nije među nabrojanim. Kontradikcija. □

DEFINICIJA 1.38 *Za cele brojeve a, b i c jednačina $ax+by = c$ čija se rešenja po x i y traže u celim brojevima naziva se linearna Diofantova jednačina.*

TEOREMA 1.39 *Neka $a, b, c \in \mathbb{Z}$. Linearna Diofantova jednačina $ax+by = c$ ima rešenje ako i samo ako $NZD(a, b)|c$.*

Dokaz: Na osnovu propozicije 1.29 i teoreme 1.32. □

TEOREMA 1.40 *Neka je (x_0, y_0) jedno rešenje linearne Diofantove jednačine $ax + by = c$ i $d = NZD(a, b)$. Tada su sva rešenja data formulom: $(x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d})$, $k \in \mathbb{Z}$.*

Dokaz: Direktno proveravamo da navedeni uređeni par jeste rešenje, za svako $k \in \mathbb{Z}$, koristeći jednakost $ax_0 + by_0 = c$. Pokažimo još da je svako rešenje (u, v) jednačine $ax + by = c$ datog oblika. Sada koristimo da su ispunjene sledeće dve jednakosti:

$$\frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{c}{d}$$

$$\frac{a}{d}u + \frac{b}{d}v = \frac{c}{d}$$

Odavde je $\frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{a}{d}u + \frac{b}{d}v$ što je ekvivalentno sa $\frac{a}{d}(u - x_0) = \frac{b}{d}(y_0 - v)$. Kako je $NZD(\frac{a}{d}, \frac{b}{d}) = 1$ i $\frac{a}{d}|\frac{b}{d}(y_0 - v)$ po lemi 1.33 dobijamo da $\frac{a}{d}|(y_0 - v)$ odnosno $y_0 - v = \frac{a}{d}t$, za neko $t \in \mathbb{Z}$. Odavde je $v = y_o - \frac{a}{d}t$, a $u = x_0 + \frac{b}{d}t$. □

DEFINICIJA 1.41 *Neka su $a, b \in \mathbb{Z}$ i $m \in \mathbb{N}$. Kažemo da su a i b kongruentni po modulu m i pišemo $a \equiv b \pmod{m}$ ako i samo ako je $m|(a - b)$.*

PROPOZICIJA 1.42 *Relacija $\equiv \pmod{m}$ je relacija ekvivalencije na skupu celih brojeva. Takođe, za sve $x, y, z, t \in \mathbb{Z}$ važi:*

1. *ako je $x \equiv y \pmod{m}$ i $z \equiv t \pmod{m}$ onda je $x + z \equiv y + t \pmod{m}$; (saglasnost $\equiv \pmod{m}$ sa sabiranjem)*
2. *ako je $x \equiv y \pmod{m}$ i $z \equiv t \pmod{m}$ onda je $xz \equiv yt \pmod{m}$. (saglasnost $\equiv \pmod{m}$ sa množenjem)*

Dokaz: Refleksivnost i simetričnost slede direktno iz definicije relacije kongruentno po modulu. Tranzitivnost i saglasnost sa + se dobija korišćenjem propozicije 1.29. Za saglasnost sa $\cdot$ pokazujemo da iz $a \equiv b \pmod{m}$ sledi $ac \equiv bc \pmod{m}$ pomoću propozicije 1.29, a odatle sledi saglasnost za množenje. □

Skup ostataka $\{0, \ldots, m-1\}$ pri deljenju prirodnim brojem m označićemo sa $\mathbb{Z}_m$. Primetimo da je svaka klasa ekvivalencije relacije $\equiv \pmod{m}$ ustvari skup onih celih brojeva koji daju isti ostatak pri deljenju sa m. Dakle $\mathbb{Z}/\equiv \pmod{m} = \{0/\equiv \pmod{m}, \ldots, (m-1)/\equiv \pmod{m}\}$.

TEOREMA 1.43 *Neka $m \in \mathbb{N}$. U strukturi $(\mathbb{Z}_m, +_m, \cdot_m)$, gde je $a +_m b$ jednako ostatku pri deljenju $a + b$ sa m, a $a \cdot_m b$ jednako ostatku pri deljenju ab sa m, za sve $a, b \in \mathbb{Z}$, važi:*

1. *$+_m$ i $\cdot_m$ su komutativne operacije;*
2. *$+_m$ i $\cdot_m$ su asocijativne operacije;*
3. *$\cdot_m$ je distributivno u odnosu na $+_m$ sa svake strane;*
4. *$x +_m 0 = 0 +_m x = x$ za sve $x \in \mathbb{Z}_m$;*
5. *$x \cdot_m 1 = 1 \cdot_m x = x$ za sve $x \in \mathbb{Z}_m$; (1 je neutralni za $\cdot_m$)*
6. *$x +_m (m - x) = (m - x) +_m x = 0$ za sve $x \in \mathbb{Z}_m \backslash \{0\}$.*

Dokaz: Direktno iz definicije operacija $+_m$ i $\cdot_m$ i osobina sabiranja i množenja celih brojeva. □

TEOREMA 1.44 *Neka su $a, m \in \mathbb{N}$. Ako je $NZD(a, m) = 1$ onda kongruencija $ax \equiv b \pmod{m}$ ima rešenje po x u $\mathbb{Z}$ za sve $b \in \mathbb{Z}$. Svaka dva rešenja su kongruentna po modulu m, odnosno skup rešenja je jedinstvena klasa ekvivalencije relacije $\equiv \pmod{m}$.*

Dokaz: Po teoremi 1.32 znamo da postoje celi brojevi α i β takvi da je $a\alpha + m\beta = 1$. Odavde je $a\alpha \equiv 1 \pmod{m}$. Odnosno, zbog saglasnosti sa množenjem, propozicija 1.42, $ab\alpha \equiv b \pmod{m}$, pa se za jedno rešenje može uzeti broj $x_0 = b\alpha$. Takođe, znamo da za svaki broj $t \in \mathbb{Z}$ takav da je $x_0 \equiv t \pmod{m}$, važi $ax_0 \equiv at \pmod{m}$, pa je $at \equiv b \pmod{m}$, zbog tranzitivnosti relacije kongruentno po modulu. Dakle i svaki broj kongruentan sa rešenjem x_0 je takođe rešenje. Neka je sada $y \in \mathbb{Z}$ takav da je $ay \equiv b \pmod{m}$, tada je zbog tranzitivnosti opet $ax_0 \equiv ay \pmod{m}$. Ovo nam daje $m | a(x_0 - y)$, pa kako je $NZD(a, m) = 1$ po lemi 1.33 dobijamo $m | (x_0 - y)$ odnosno $x_0 \equiv y \pmod{m}$. □

TEOREMA 1.45 *Neka $m \in \mathbb{N}$. Za sve $n \in \{1, \ldots, m-1\}$ postoji $x \in \{1, \ldots, m-1\}$ takav da je $n \cdot_m x = 1$ ako i samo ako je m prost broj.*

Dokaz: ($\Rightarrow$) Neka je $k \in \{2, \ldots, m-1\}$. Po pretpostavci postoji $t \in \mathbb{Z}_m$ takav da je $k \cdot_m t = 1$, što je ekvivalentno sa $kt = mq + 1$, za neki količnik q. Iz poslednje jednakosti sledi da $k \not| m$. Zato je m prost broj. ($\Leftarrow$) Neka je sada m prost broj. Za bilo koje $k \in \{2, \ldots, m-1\}$ znamo da je $NZD(k, m) = 1$.

Po teoremi 1.44 znamo da postoji ceo broj $t \in \{0, \ldots, m-1\}$ takav da je $kt \equiv 1 \pmod{m}$, pa je $k \cdot_m t = 1$. Za $k = 1$ koristimo da važi $1 \cdot_m 1 = 1$. □

Osobinu operacije $\cdot_m$ opisanu u prethodnoj teoremi nazivamo postojanje inverza za operaciju $\cdot_m$ u odnosu na neutralni element 1.

TEOREMA 1.46 *(Kineska teorema o ostacima) Neka su $m_1, \ldots, m_k$ prirodni brojevi, dva po dva uzajamno prosti, odnosno $NZD(m_i, m_j) = 1$, za $i \neq j$. Tada za proizvoljne date cele brojeve $a_1, \ldots, a_k$ postoji ceo broj x takav da je $x \equiv a_i \pmod{m_i}$, za sve $i \in \{1, \ldots, k\}$. Sva rešenja ovog sistema kongruencija su klasa međusobno kongruentnih celih brojeva po modulu $m_1 \cdot \ldots \cdot m_k$.*

Dokaz: Neka je $M = m_1 \cdot \ldots \cdot m_k$ i za svako $i \in \{1, \ldots, k\}$ neka je $M_i = \frac{M}{m_i}$. Sada je po uslovu $NZD(M_i, m_i) = 1$ pa postoji $\alpha_i \in \mathbb{Z}$ takav da je $\alpha_i M_i \equiv 1 \pmod{m_i}$ za sve $i \in \{1, \ldots, k\}$ po teoremi 1.44. Sada je lako proveriti da je jedno rešenje datog sistema kongruencija oblika $x_0 = \alpha_1 M_1 a_1 + \ldots + \alpha_k M_k a_k$. Neka je x neko drugo rešenje. Tada je $x \equiv x_0 \pmod{m_i}$, za sve $i \in \{1, \ldots, k\}$, zbog tranzitivnosti relacije kongruentno po modulu. Kako su $m_1, \ldots, m_k$ po parovima uzajamno prosti dobijamo da je $x \equiv x_0 \pmod{M}$. Jasno da svako $y \in \mathbb{Z}$ koje je kongruentno x_0 po modulu M zadovoljava sve kongruencije sistema. □

Primer: Rešiti sistem kongruencija:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

Postupamo kao u dokazu Kineske teoreme. Formiramo $M = 15$, $M_1 = 5$ i $M_2 = 3$. Nije teško videti da je $\alpha_1 = \alpha_2 = 2$, pa je jedno rešenje $x_0 = \alpha_1 M_1 a_1 + \alpha_2 M_2 a_2 = 2 \cdot 5 \cdot 2 + 2 \cdot 3 \cdot 3 = 38$, a sva rešenja su data formulom $x = 38 + 15t$, $t \in \mathbb{Z}$.

1.2 Polinomi

Postoji više načina da se definiše polinom.

DEFINICIJA 1.47 *Neka je $(\mathbb{R}, +, \cdot)$ struktura realnih brojeva. Za $n \in \mathbb{N}_0$ i $a_n \in \mathbb{R}\backslash\{0\}$ izraz $a_0 + a_1 x + \ldots + a_n x^n$ je polinom sa realnim koeficijentima $a_0, \ldots, a_n$, gde je x promenljiva, a_0 slobodan član, $a_n x^n$ vodeći član, a $a_1 x, \ldots, a_{n-1} x^{n-1}$ ostali članovi. Stepen polinoma $p(x)$ je n. Jednočlani polinom naziva se monom, dvočlani binom, a tročlani trinom.*

Polinome definisane prethodnom definicijom nazivamo polinomi sa realnim koeficijentima, a analogno definišemo polinome sa celobrojnim, racionalnim ili kompleksnim koeficijentima. Skup svih polinoma sa realnim koeficijentima označavamo sa $\mathbb{R}[x]$, sa racionalnim $\mathbb{Q}[x]$, sa celobrojnim $\mathbb{Z}[x]$, a sa kompleksnim $\mathbb{C}[x]$. Polinome označavamo sa $p, q, r, \ldots$, a ako želimo naglasiti da je polinom p po promenljivoj x onda to pišemo $p(x)$. Funkciju koja svakom polinomu pridružuje njegov stepen (koji je prirodan broj) označavamo sa st. Tako je $st(x^3) = 3, st(1) = 0$. Naglašavamo da nula polinom nema definisan stepen.

DEFINICIJA 1.48 *Dva polinoma su jednaka ako imaju isti stepen i iste koeficijente uz odgovarajuće stepene.*

DEFINICIJA 1.49 *Neka* $p, q \in \mathbb{R}[x](\mathbb{C}[x], \mathbb{Q}[x], \mathbb{Z}[x])$. *Binarne operacije* $+$ *(sabiranje) i* $\cdot$ *(množenje) za* $a_n x^n + \ldots + a_1 x + a_0$ *i* $b_m x^m + \ldots + b_1 x + b_0$ *iz* $\mathbb{R}[x]$ *definišemo na sledeći način:*

$$(a_n x^n + \ldots + a_1 x + a_0) + (b_m x^m + \ldots + b_1 x + b_0) =$$
$$= a_n x^n + \ldots + (a_m + b_m) x^m + \ldots + (a_1 + b_1) x + (a_0 + b_0),$$

za $m \leq n$ *i*

$$(a_n x^n + \ldots + a_1 x + a_0) \cdot (b_m x^m + \ldots + b_1 x + b_0) =$$
$$= a_n b_m x^{n+m} + \ldots + (a_k b_0 + a_{k-1} b_1 + \ldots + a_0 b_k) x^k + \ldots + a_0 b_0.$$

PROPOZICIJA 1.50 *U strukturi* $(\mathbb{R}[x], +, \cdot)$ *važi:*

1. $p(x)+q(x) = q(x)+p(x)$ *i* $p(x)\cdot q(x) = q(x)\cdot p(x)$ *(*$+$ *i* $\cdot$ *su komutativne operacije);*

2. $(p(x) + q(x)) + r(x) = p(x) + (q(x) + r(x))$ *i* $(p(x) \cdot q(x)) \cdot r(x) = p(x) \cdot (q(x) \cdot r(x))$ *(*$+$ *i* $\cdot$ *su asocijativne operacije);*

3. $p(x) + 0 = 0 + p(x) = p(x)$ *(0 je neutralni element za* $+$*);*

4. $p(x) \cdot 1 = 1 \cdot p(x) = p(x)$ *(1 je neutralni element za* $\cdot$*);*

5. $p(x) + (-p(x)) = (-p(x)) + p(x) = 0$, *gde* $-p(x)$ *označava polinom sa suprotnim koeficijentima u odnosu na* $p(x)$ *(postoji inverz u odnosu na* $+$*);*

6. $p(x) \cdot (q(x)) + r(x)) = p(x) \cdot q(x) + p(x) \cdot r(x)$ *(distributivnost* $+$ *u odnosu na* $\cdot$*),*

za sve $p(x), q(x), r(x) \in \mathbb{R}[x]$.

Dokaz: Direktno iz definicija operacija $+$ i $\cdot$ i osobina tih operacija u realnim brojevima. □

Analogno tvrđenje važi i ako uzmemo polinome iz $\mathbb{C}[x]$ ili $\mathbb{Q}[x]$ ili $\mathbb{Z}[x]$.

PROPOZICIJA 1.51 *U* $\mathbb{R}[x], \mathbb{C}[x]$ *ili* $\mathbb{Q}[x]$ *jedini polinomi invertibilni za množenje su konstantni nenula polinomi. U* $\mathbb{Z}[x]$ *su to* 1 *i* -1.

Dokaz: Ovo je posledica definicije prozvoda polinoma i činjenice da je stepen proizvoda jednak zbiru stepena. □

Svakim polinomom sa realnim (kompleksnim) koeficijentima definišemo jedno preslikavanje na skupu realnih (kompleksnih) brojeva koje svakom realnom (kompleksnom) broju pridružuje vrednost polinoma koja se dobija kada se sva pojavljivanja promenljive zamene datim brojem, a potom izvrše operacije $+$ i $\cdot$ u realnim (kompleksnim) brojevima. Tako definisana funkcija se naziva *polinomna funkcija* i označavamo je takođe sa $p(x)$. Na primer $p : \mathbb{R} \to \mathbb{R}$ dato sa $p(x) = x + 1$ je jedna polinomna funkcija gde je $p(\sqrt{2}) = \sqrt{2} + 1$, $p(-1) = 0$, a $p(\frac{1}{2}) = \frac{3}{2}$.

TEOREMA 1.52 *Neka su* p *i* q *polinomi iz* $\mathbb{R}[x](\mathbb{Q}[x], \mathbb{C}[x])$ *i* $q(x) \neq 0$. *Tada postoje jedinstveni polinomi* s *i* r *takvi da važi* $p = s \cdot q + r$, *gde je* $r(x) = 0$ *ili je* $st(r) < st(q)$.

Dokaz: Za $p(x) = 0$ ili $st(p) < st(q)$ uzimamo $s(x) = 0$ i $r(x) = p(x)$. Pretpostavimo da je $st(q) \leq st(p)$. Dokažimo indukcijom po $st(p)$ da tvrđenje važi. Ako je $st(p) = 0$ ostaje i da je $st(q) = 0$, pa su i p i q konstantni polinomi, pa tvrđenje važi jer kako je $q \neq 0$, možemo uzeti $p = \frac{p}{q} \cdot q + 0$. Pretpostavimo da tvrđenje važi za polinome stepena $n \in \mathbb{N}_0$ i dokažimo da važi za polinom $p(x) = a_{n+1}x^{n+1} + \ldots + a_1x + a_0$, $a_{n+1} \neq 0$. Neka je $q(x) = b_mx^m + \ldots + b_1x + b_0$, $b_m \neq 0$, gde je $m \leq n+1$. Posmatrajmo polinom $p_1(x) = p(x) - \frac{a_{n+1}}{b_m}x^{n+1-m}q(x)$. Očigledno je $st(p_1) \leq n$. Ako je $st(q) > st(p_1)$ uzimamo $s(x) = \frac{a_{n+1}}{b_m}x^{n+1-m}$ i $r(x) = p_1(x)$. Pretpostavimo da je $st(q) \leq st(p_1)$. Po indukcijskoj hipotezi postoje s_1 i r_1 takvi da je $st(r_1) < st(q)$ ili je $r_1 = 0$ tako da je $p_1 = s_1 \cdot q + r_1$. Tada je $p(x) = (\frac{a_{n+1}}{b_m}x^{n+1-m} + s_1(x))q(x) + r_1(x)$, pa uzimamo $s(x) = \frac{a_{n+1}}{b_m}x^{n+1-m} + s_1(x)$ i $r(x) = r_1(x)$. Time je pokazan indukcijski korak.

Pokažimo još jedinstvenost. Neka postoje polinomi $s, s'r, r' \in \mathbb{R}[x]$ takvi da je $p = sq + r$ i $p = s'q + r'$, gde je $st(r), st(r') < st(q)$ ili je $r = 0$ ili je $r' = 0$. Odavde je $q(s - s') = (r' - r)$ i važi $st(r' - r) < st(q)$ ili je $r' - r = 0$. Kako je $st(q(s - s')) \geq st(q)$ ili je $s - s' = 0$, ostaje kao jedina mogućnost $s = s'$ i $r = r'$. □

Za polinome p, q, r i s iz prethodnog tvrđenja kažemo da je s količnik, a r ostatak pri deljenju polinoma p polinomom q. Ukoliko je $r = 0$ kažemo da je p deljivo sa q.

Posledica 1.53 *(Bezuova) Pri deljenju polinoma $p(x) \in \mathbb{R}[x](\mathbb{Q}[x], \mathbb{C}[x])$ polinomom $x - \alpha$, za $\alpha \in \mathbb{R}(\mathbb{Q}, \mathbb{C})$ dobija se ostatak $p(\alpha)$.*

Dokaz: Prema teoremi 1.52 dobijamo da postoje polinomi $q, r \in \mathbb{R}[x]$ takvi da je $p(x) = (x - \alpha)q(x) + r(x)$ i $st(r) < 1$ ili je $r = 0$. Ako je $r = 0$ onda je očigledno $p(\alpha) = 0$, pa tvrđenje važi. Ako je $r(x)$ konstanta onda opet uvrštavajući $x = \alpha$ dobijamo da je $r = p(\alpha)$. □

Posledica 1.54 *Polinom $p(x) \in \mathbb{R}[x](\mathbb{Q}[x], \mathbb{C}[x])$ je deljiv sa $x - \alpha$ za neko $\alpha \in \mathbb{R}(\mathbb{C}, \mathbb{Q})$ ako i samo ako je $p(\alpha) = 0$.*

Dokaz: Direktna posledica prethodnog tvrđenja. □

Prethodna posledica se može formulisati i ovako: α je nula polinoma $p(x)$ ako i samo ako je $p(x) = (x - \alpha)q(x)$, za neki polinom $q(x)$.

Definicija 1.55 *Broj α je k-tostruka nula polinoma $p(x)$ za neko $k \in \mathbb{N}$ ako je $p(x)$ deljivo sa $(x - \alpha)^k$, a nije deljivo sa $(x - \alpha)^{k+1}$.*

Definicija 1.56 *Polinom $p(x)$ se naziva nesvodljiv ako se ne može napisati kao proizvod dva polinoma različita od nule, stepena bar jedan.*

Propozicija 1.57 *Svaki linearan polinom je nesvodljiv.*

Dokaz: Direktno iz definicije množenja. □

Dokaz sledeće teoreme, koja se naziva još i *Osnovni stav algebre*, prevazilazi okvire ovog kursa. Ideju ovog dokaza zainteresovani čitalac može naći u [8, Tvrđenje 5.9, strana 304] kao i [10, Tvrđenje 7.12, strana 133].

Teorema 1.58 *(Gaus) Svaki polinom sa kompleksnim koeficijentima stepena bar jedan ima bar jednu kompleksnu nulu.*

Teorema 1.59 *Svaki polinom sa kompleksnim koeficijentima ima tačno onoliko nula u kompleksnim brojevima koliki mu je stepen računajući svaku nulu onoliko puta kolika joj je višestrukost.*

Dokaz: Sledi iz Bezuove i Gausove teoreme. □

Primer: Polinom $x^3 - x^2 - x + 1 = (x-1)^2(x+1)$ ima jednu dvostruku nulu jedinicu i jednu jednostruku nulu -1 što je zajedno tri i jednako je stepenu tog polinoma.

Teorema 1.60 *Kompleksan broj z je nula polinoma $p(x)$ sa realnim koeficijentima ako samo ako je $\overline{z}$ nula polinoma $p(x)$.*

Dokaz: Pokazujemo da je $p(z) = 0 \Leftrightarrow p(\overline{z}) = 0$ koristeći osobine konjugovanja iz propozicije 1.25 i da ne utiče na realne brojeve. □

Posledica 1.61 *Svaki polinom sa kompleksnim koeficijentima se može napisati kao proizvod linearnih i konstantnih polinoma sa kompleksnim koeficijentima. Svaki polinom sa realnim koeficijentima se može zapisati i kao prozvod konstantnih, linearnih i kvadratnih polinoma čiji su koeficijenti realni brojevi.*

Dokaz: Posledica prethodne teoreme. □

Propozicija 1.62 *Ako polinomi p, q sa kompleksnim koeficijentima, oba stepena najviše $n \in \mathbb{N}_0$, imaju jednake vrednosti za više od n različitih tačaka onda određuju istu polinomnu funkciju, odnosno $p(x) = q(x)$, za sve $x \in \mathbb{C}$.*

Dokaz: Posmatramo polinom $f(x) = p(x) - q(x)$ sa kompleksnim koeficijentima. Tada je $st(f) \leq n$, a ima bar $n+1$ nulu, pa i sam mora biti nula polinom, po teoremi 1.59. □

Teorema 1.63 *(Vijetove formule) Neka je $n \in \mathbb{N}_0$, $p(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{C}[x]$ i $\alpha_1, \ldots, \alpha_n$ nule polinoma $p(x)$, pri čemu su sve nule nabrojane onoliko puta kolika im je višestrukost. Tada važi:*

$$\begin{aligned}
\alpha_1 + \ldots + \alpha_n &= -\frac{a_{n-1}}{a_n} \\
\alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n &= \frac{a_{n-2}}{a_n} \\
&\ldots \\
\alpha_1 \cdot \ldots \cdot \alpha_n &= (-1)^n \frac{a_0}{a_n}.
\end{aligned}$$

Dokaz: Prema teoremi 1.59 $p(x) = a_n(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$, pa posle množenja, u datoj formuli izjednačavajući koeficijente uz odgovarajuće stepene dva izraza za $p(x)$ dobijamo nabrojane Vietove veze. □

TEOREMA 1.64 *Neka je* $n \in \mathbb{N}_0$, $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ *i* $\alpha \in \mathbb{Q}$ *nula polinoma* $f(x)$. *Ako je* $\alpha = \frac{p}{q}$, *za neke* $p, q \in \mathbb{Z}$ *takve da je* $NZD(p,q) = 1$, *onda* $q|a_n$ *i* $p|a_0$.

Dokaz: Kada uvrstimo svedeni razlomak $\frac{p}{q}$ za x u polinom $f(x)$, dobijamo $f(\frac{p}{q}) = 0$, odnosno

$$a_n(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + \ldots + a_1(\frac{p}{q}) + a_0 = 0$$
$$a_n\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \ldots + a_1\frac{p}{q} + a_0 = 0$$
$$a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_1 pq^{n-1} + a_0 q^n = 0$$

Iz poslednje jednakosti je $a_n p^n = -q(a_{n-1}p^{n-1} + \ldots + a_0 q^{n-1})$, pa kako je desna strana deljiva sa q to je i leva, odnosno $q|a_n p^n$, ali $NZD(p,q) = 1$, pa po lemi 1.33 je $q|a_n$. Takođe poslednju od gornjih jednakosti možemo zapisati i kao $a_0 q^n = -p(a_n p^{n-1} + \ldots + a_1 q^{n-1})$. Sada je desna strana deljiva sa p, pa $p|a_0 q^n$, ali $NZD(p,q) = 1$ pa po lemi 1.33 dobijamo da $p|a_0$. □

Iz prethodne teoreme se za dati polinom sa celobrojnim koeficijentima određuju kandidati za racionalne nule, a da li je neki od tih brojeva kandidata stvarno nula mora se proveriti direktno, jer je u teoremi dat samo potreban, ali ne i dovoljan uslov. U proveri da li je neki broj nula polinoma najčešće se koristi takozvana Hornerova šema. Za polinom $p(x) = a_n x^n + \ldots + a_1 x + a_0$ (sa koeficijentima u $\mathbb{C}$) ako je $c \in \mathbb{C}$ znamo po Bezuovoj teoremi da važi: $p(x) = (x-c)(b_0 + \ldots + b_{n-1}x^{n-1}) + p(c)$. Zanima nas kako odrediti koeficijente $b_0, \ldots, b_{n-1}$. Međutim kada izmnožimo drugu jednakost i izjednačimo koeficijente uz odgovarajuće stepene dobijamo: $a_0 + cb_0 = p(c)$, $b_0 = a_1 + cb_1$, …, $b_{n-2} = a_{n-1} + cb_{n-1}$ i $b_{n-1} = a_n$. Ovo se kraće zapisuje tabelarno:

c	a_n	a_{n-1}	$\ldots$	a_1	a_0
	b_{n-1}	b_{n-2}	$\ldots$	b_0	$p(c)$

Primer: Koristeći Hornerovu šemu rastavićemo polinom $x^3 - 2x^2 - x + 2 \in \mathbb{Z}[x]$. Kandidati za racionalne nule su $\{1, -1, 2, -2\}$. Proverimo najpre -2.

-2	1	-2	-1	2
	1	-4	7	-12

Kako u poslednjem polju druge vrste nije upisana nula, to -2 nije koren ovog polinoma. Pređimo na proveru da li je 1 nula.

1	1	-2	-1	2
	1	-1	-2	0

Sada je u poslednjem polju druge vrste nula pa jedinica jeste koren posmatranog polinoma i važi $x^3 - 2x^2 - x + 2 = (x - 1)(x^2 - x - 2)$. Ovde primećujemo da se koeficijenti u drugoj zagradi poklapaju redom sa brojevima u poljima u drugoj vrsti.

-1	1	-1	-2
	1	-2	0

Sada vidimo da je i -1 nula, pa dobijamo $x^3 - 2x^2 - x + 2 = (x - 1)(x + 1)(x - 2)$. Poslednja zagrada je već linearan polinom.

Glava 2

Algebarske strukture

U prethodnoj glavi uočili smo da neke zakonitosti za operacije sabiranja i množenja kao što su asocijativnost, komutativnost ili distributivnost važe kako na brojevima tako i na polinomima. Stoga apstrakujemo pojam operacije i strukture kao skupa sa operacijama na apstraktan pojam algebarske strukture, gde skup može biti proizvoljan i operacija proizvoljno zadata tako da ispunjavaju neke ili sve od navedenih zakonitosti ili eventualno neke dodatne osobine. Izučavaćemo algebarske strukture sa jednom ili dve binarne operacije.

2.1 Grupoidi. Kvazigrupe.

DEFINICIJA 2.1 *Neka je $A \neq \emptyset$ i $n \in \mathbb{N}_0$. Preslikavanje $f : A^n \to A$ nazivamo n-arna operacija na A. Za $n = 0$ govorimo o konstantnoj, za $n = 1$ o unarnoj, za $n = 2$ o binarnoj, a za $n = 3$ o ternarnoj operaciji. Ako je F skup nekih operacija na skupu A onda uređeni par (A, F) zovemo algebra (algebarska struktura ili univerzalna algebra). Skup A zovemo nosač ili domen date algebre.*

Primeri: Brojevne strukture: $(\mathbb{N}_0, ', 0)$, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}[x], +, \cdot)$, $(\mathbb{Z}, -)$, $(\mathbb{Z}_n, +_n, \cdot_n)$, za svako $n \in \mathbb{N}$, ali i konačne $(\{\top, \bot\}, \neg, \Rightarrow)$, $(\mathcal{P}(A), \cup)$ (koja je konačna za A konačan skup, a inače je beskonačna), ...

Binarne operacije zapisujemo između operanada: umesto $+(2, 3) = 5$ pišemo $2 + 3 = 5$, a ako binarnu operaciju označimo sa $\cdot$, onda je izostavljamo između operanada, sem kad želimo da je naglasimo. Binarnu operaciju označenu sa $+$ zovemo aditivna notacija, a sa $\cdot$ multiplikativna notacija. Često ćemo algebru navoditi tako što navedemo samo njen domen,

bez operacija za koje je jasno da sa navedenim domenom čine datu algebru. Jednoelementna algebra naziva se *trivijalna*.

DEFINICIJA 2.2 *Algebraska struktura $(G, \cdot)$, gde je $\cdot$ binarna operacija skupa G naziva se grupoid.*

Primeri: $(\mathbb{N}_0, +)$, $(\mathbb{N}_0, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}[x], +)$, $(\mathbb{Z}, -)$, $(\mathbb{Z}_n, +_n)$, $(\mathbb{Z}_n, \cdot_n)$, za svako $n \in \mathbb{N}$, ali i konačne $(\{\top, \bot\}, \Rightarrow)$, $(\mathcal{P}(A), \cup)$, ... Međutim $(\mathbb{N}_0, -)$ i $(\mathbb{Z}, :)$ nisu grupoidi jer $2 - 3 \notin \mathbb{N}_0$, a $2 : 3 \notin \mathbb{Z}$.

U slučaju da je G "mali" konačan skup binarnu operaciju možemo zadati i tabelarno, baš kao što to radimo u slučaju binarnih operacija iskazne algebre: $\wedge, \vee, \Rightarrow$ i $\Leftrightarrow$. Takva tablica se naziva *Kejlijeva tablica*.

Primer: Na skupu $\{a, b\}$ definišemo sledeću binarnu operaciju Kejlijevom tablicom:

$*$	a	b
a	a	a
b	b	a

Sada je $(\{a, b\}, *)$ jedan dvoelementni grupoid.

DEFINICIJA 2.3 *Neka je $(G, \cdot)$ grupoid. Element $e \in G$ naziva se leva (desna) jedinica grupoida $(G, \cdot)$ ako za sve $g \in G$ važi $eg = g (ge = g)$. Ako je element e istovremeno i leva i desna jedinica grupoida $(G, \cdot)$ onda se on naziva jedinica.*

Ako koristimo aditivnu notaciju onda umesto jedinice (jediničnog elementa) govorimo o neutralnom elementu, koga uvodimo analogno prethodnoj definiciji. Zato nadalje bez eksplicitnog maglašavanja ova dva pojma koristimo ravnopravno, ne formulišući svako tvrđenje ili defincinju za svaki pojam posebno, podrazumevajući da ono 'vsto važi u jednoj notaciji važi i u drugoj.

Primeri: $(\mathbb{N}_0, +)$, $(\mathbb{N}_0, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}[x], +)$, $(\mathbb{Z}_n, +_n)$, $(\mathbb{Z}_n, \cdot_n)$, za svako $n \in \mathbb{N}$, imaju jedinicu odnosno neutralni element, ali $(\mathbb{Z}, -)$ ima samo desni neutralni element, a $(\{\top, \bot\}, \Rightarrow)$ samo levi jedinični element, a $(\mathbb{N}, +)$ nema ni levi ni desni neutralni element.

PROPOZICIJA 2.4 *Ako grupoid ima i levi i desni neutralni element onda se oni poklapaju i to je neutralni element grupoida. Neutralni element grupoida je jedinstven.*

Dokaz: Neka su e_L levi, a e_D desni neutralni element grupoida $(G,+)$. Tada je $e_L + e_D = e_L$, jer je e_D desni neutralni element, ali je istovremeno i $e_L + e_D = e_D$, jer je e_L levi neutralni element. Zato je $e_L = e_D$ i taj element zadovoljava uslov za neutralni element datog grupoida. Analogno pokazujemo da je neutralni element jedinstven. □

Definicija 2.5 *Neka je $(G,\cdot)$ grupoid. Element $0 \in G$ naziva se leva (desna) nula grupoida $(G,\cdot)$ ako za sve $g \in G$ važi $0g = 0 (g0 = 0)$. Ako je element 0 istovremeno i leva i desna nula grupoida $(G,\cdot)$ onda se on naziva nula.*

Primeri: $(\mathbb{N}_0,\cdot)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Q},\cdot)$, $(\mathbb{R}[x],\cdot)$, $(\mathbb{Z}_n,\cdot_n)$, za svako $n \in \mathbb{N}$, imaju nulu, ali $(\mathcal{P}(A),\setminus)$ ima samo levu nulu, $(\{\top,\bot\},\Rightarrow)$ ima samo desnu nulu, a $(\mathbb{R},+)$ nema ni levu ni desnu nulu.

Kako je definicija nule analogna definiciji neutralnog elementa, važi i propozicija analogna propoziciji 2.4.

Propozicija 2.6 *Ako grupoid ima i levu i desnu nulu onda se one poklapaju i to je nula grupoida. Nula grupoida je jedinstvena.*

Dokaz: Analogno dokazu propozicije 2.4. □

Napomenimo da se levi(desni) jedinični element u Kejlijevoj tablici uočava tako što je jedna vrsta(kolona) jednaka vrsti (koloni) iznad gornje(leve) margine, a ako su jedna kolona i odgovarajuća po redu vrsta "prepisane" sa margina onda je odgovarajući element jedinični (neutralni) element.

Definicija 2.7 *Za grupoid $(G,\cdot)$ kažemo da je komutativan ako za sve $a,b \in G$ važi: $ab = ba$. Element $g \in G$ se naziva idempotent ako važi $gg = g$, a grupoid je idempotentan ako su mu svi elementi idempotenti.*

Primer: $(\mathbb{C},\cdot)$ je komutativan, a $(\{\top,\bot\},\Rightarrow)$ nije. Grupoid $(\mathbb{Z},\cdot)$ nije idempotentan, ali ima dva idempotentna elementa 0 i 1. Grupoid $(\{\top,\bot\},\wedge)$ jeste idempotentan.

Kod komutativnog grupoida Kejlijeva tablica je simetrična u odnosu na glavnu dijagonalu. Primetimo još da kod komutativnog grupoida postojanje bilo levog bilo desnog jediničnog elementa (nule) povlači postojanje jediničnog elemeta (nule).

Definicija 2.8 *Grupoid $(G,\cdot)$ je levo(desno) kancelativan ako važi: $ab = ac \Rightarrow b = c (ab = cb \Rightarrow a = c)$, za sve $a,b,c \in G$. Grupoid je kancelativan ako je levo i desno kancelativan.*

Primer: $(\mathbb{N}, +)$ je kancelativan grupoid, a $(\{\top, \bot\}, \vee)$ nije.

Ponovo kod komutativnih grupoida ne govorimo o levoj i desnoj kancelativnosti već samo o kancelativnosti.

DEFINICIJA 2.9 *Grupoid $(Q, \cdot)$ se naziva kvazigrupa ako su za sve $a, b \in Q$ jednačine $ax = b$ i $ya = b$ jednoznačno rešive po x i y.*

PROPOZICIJA 2.10 *Svaka kvazigrupa je kancelativni grupoid.*

Dokaz: Neka je za neke $a, b, c \in Q$ ispunjeno $ab = ac$, kako je $(Q, \cdot)$ kvazigrupa jednačina $ax = ac$ ima jedinstveno rešenje, pa je $b = c$. Analogno pokazujemo desnu kancelativnost. □

Kejlijeva tablica kvazigrupe je *latinski kvadrat*: u svakoj vrsti i svakoj koloni svaki element se pojavljuje tačno jednom.

2.2 O polugrupama

DEFINICIJA 2.11 *Polugrupa je algebarska struktura $(S, \cdot)$, gde je S neprazan skup i $\cdot : S \times S \to S$ binarna operacija, takva da za sve $a, b, c \in S$ važi:*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Ovo svojstvo nazivamo asocijativnost.

Primetimo da je polugrupa ustvari asocijativan grupoid. Zato u polugrupi S levu, desnu nulu (jedinicu), nulu (jedinicu) definišemo isto kao kod grupoida, kao i ostale osobine grupoida koje smo već naveli.

DEFINICIJA 2.12 *Monoid je polugrupa sa jedinicom.*

Primeri: $(\{\top, \bot\}, \Rightarrow)$ nije polugrupa, $(\mathbb{N}, +)$ jeste polugrupa, ali nije monoid, a $(\mathbb{N}, \cdot)$ je monoid.

Nula polugrupa je polugrupa sa nulom u kojoj je proizvod svaka dva elementa nula.

U sledećem tvrđenju uveden je *monoid reči.*

PROPOZICIJA 2.13 *Neka je Σ konačan skup, a Σ^* skup svih konačnih nizova iz Σ, koje ćemo zvati reči. Binarnu operaciju konkatenacije ili dopisivanja reči definišemo na prirodan način: $u \cdot v = uv$, za sve $u, v \in \Sigma^*$. Prazan niz označimo sa λ i nazovimo prazna reč. Tada je $(\Sigma^*, \cdot)$ monoid sa neutralnim elementom λ.*

Dokaz: Iz definicije operacije konkatenacije vidimo da je ona asocijativna i da je λ neutralni element. $\square$

Primer: Ako za Σ uzmemo $\{a, b\}$, tada je $\Sigma^* = \{\lambda, a, b, aa, ab, ba, bb, \ldots\}$ skup svih reči sastavljenih od slova a i b.

TEOREMA 2.14 *U polugrupi $(S, \cdot)$ proizvod konačno mnogo elemenata ne zavisi od rasporeda zagrada.*

Dokaz: Sa $a_1 \cdot \ldots \cdot a_n$ označićemo proizvod $(\ldots(a_1 \cdot a_2) \cdot \ldots \cdot a_n)$, za sve $n \in \mathbb{N}$ i $a_1, \ldots, a_n \in S$. Indukcijom po $m = k - i$ dokažimo da je $(a_1 \cdot \ldots \cdot a_i)(a_{i+1} \cdot \ldots \cdot a_k) = a_1 \cdot \ldots \cdot a_k$. Baza za $m = 1$ važi po dogovoru o zapisu $a_1 \cdot \ldots \cdot a_k$. Pretpostavimo da tvrđenje važi za m i dokažimo za $m+1$. Sada je $(a_1 \cdot \ldots \cdot a_i)(a_{i+1} \cdot \ldots \cdot a_{k+1}) = (a_1 \cdot \ldots \cdot a_i)((a_{i+1} \cdot \ldots \cdot a_k) \cdot a_{k+1}) = ((a_1 \cdot \ldots \cdot a_i) \cdot (a_{i+1} \cdot \ldots \cdot a_k)) \cdot a_{k+1} = (a_1 \cdot \ldots \cdot a_k) \cdot a_{k+1} = a_1 \cdot \ldots \cdot a_{k+1}$, čime je pokazan indukcijski korak. $\square$

Sada je sledeća definicija opravdana i predstavlja uvođenje pojma stepena.

DEFINICIJA 2.15 *Ako je $(S, \cdot)$ monoid sa jedinicom 1 onda je za sve $a \in S$ $a^0 = 1$, $a^{n+1} = a^n a$, za sve $n \in \mathbb{N}_0$. U aditivnoj notaciji: $0a = 0$, $(n+1)a = na + a$, za sve $n \in \mathbb{N}_0$.*

Veoma važna i dosta proučavana klasa u teoriji polugrupa je klasa regularnih polugrupa. Ove polugrupe predstavljaju jedno uopštenje grupa, algebarskih struktura kojima ćemo se kasnije detaljno posvetiti. Opširnije o regularnim polugrupama se može naći u [3].

DEFINICIJA 2.16 *Za element a proizvoljne polugrupe S kažemo da je regularan ako postoji $x \in S$ tako da je $axa = a$. Polugrupa je regularna ako su joj svi elementi regularni.*

Primetimo da su idempotenti uvek regularni elementi polugrupe.

TEOREMA 2.17 *Svaka regularna i kancelativna polugrupa je kvazigrupa.*

Dokaz: Neka je $(S, \cdot)$ polugrupa. Za date a i b zbog regularnosti postoje $a_1, b_1 \in S$ takvi da je $aa_1a = a$ i $bb_1b = b$. Sada su $x = a_1b$ i $y = ba_1$ rešenja jednačina $ax = b$ i $ya = b$, redom, što se utvrđuje direktnom proverom korišćenjem kancelativnosti. Kancelativnost daje i jedinstvenost navedenih

rešenja jednačina. Dakle, za sve $a, b \in S$ su jednoznačno rešive jednačine $ax = b$ i $ya = b$ po x i y, pa je $(S, \cdot)$ kvazigrupa. □

Podsetimo se da za $\emptyset \neq B \subseteq A$ i n-arnu operaciju f na A, za $n \in \mathbb{N}_0$ preslikavanje $g : B^n \to A$ definisano sa $g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$,za sve $x_1, \ldots, x_n \in B$ zovemo restrikcija preslikavanja f na B i označavamo sa $f|_{B^n}$.

Definicija 2.18 *Neka je $(S, \cdot)$ polugrupa. Za $\emptyset \neq P \subseteq S$ kažemo da je nosač (domen) potpolugrupe ako je $(P, \cdot|_{P^2})$ polugrupa.*

Primer: $(\mathbb{Z}, +)$ je potpolugrupa od $(\mathbb{Q}, +)$, ali $(\mathbb{R}\backslash\mathbb{Q}, +)$ nije potpolugrupa od $(\mathbb{R}, +)$, jer na primer $\sqrt{2}, -\sqrt{2} \in \mathbb{R}\backslash\mathbb{Q}$, a $\sqrt{2} + (-\sqrt{2}) \in \mathbb{Q}$. Lako je videti da ako polugrupa ima idempotentan element on sam za sebe obrazuje trivijalnu potpolugrupu.

Umesto provere po definiciji da li je neki neprazan podskup nosač potpolugrupe praktičniji je za proveru uslov dat u sledećoj propoziciji.

Propozicija 2.19 *Ako je $(S, \cdot)$ polugrupa, onda je $\emptyset \neq P \subseteq S$ nosač (domen) potpolugrupe ako i samo ako za sve $a, b \in P$ važi $ab \in P$.*

Dokaz: ($\Rightarrow$) Očigledno važi. ($\Leftarrow$) Ako je ispunjen dati uslov onda je $(P, \cdot|_{P^2})$ grupoid, a asocijativnost važi jer važi na širem skupu. □

Definicija 2.20 *Preslikavanje $f : S_1 \to S_2$, gde su $(S_1, \cdot)$ i $(S_2, *)$ proizvoljne polugrupe, tako da za proizvoljne $a, b \in S_1$ važi:*

$$f(a \cdot b) = f(a) * f(b)$$

naziva se homomorfizam. Ako je to preslikavanje polugrupe u sebe samu naziva se endomorfizam. Injektivni homomorfizam nazivamo potapanje (monomorfizam), sirjektivni epimorfizam, a bijektivni izomorfizam. Izomorfizam polugrupe u sebe samu nazivamo automorfizam.

Ako je $f : S_1 \to S_2$ epimorfizam onda kažemo da je polugrupa S_2 ustvari homomorfna slika polugrupe S_1. Ako je polugrupa S_1 izomorfna polugrupi S_2 onda pišemo $S_1 \cong S_2$.

Lema 2.21 *Kompozicija dva homomorfizma je ponovo homomorfizam.*

Dokaz: Neka su $(S_1, \cdot_1), (S_2, \cdot_2)$ i $(S_3, \cdot_3)$ tri polugrupe i $f : S_2 \to S_3$ i $g : S_1 \to S_2$ homomorfizmi. Pokažimo da je $f \circ g : S_1 \to S_3$ homomorfizam. Neka $a, b \in S_1$, računamo: $(f \circ g)(a \cdot_1 b) = f(g(a \cdot_1 b)) = f(g(a) \cdot_2 g(b)) = f(g(a)) \cdot_3 f(g(b)) = (f \circ g)(a) \cdot_3 (f \circ g)(b)$. □

PROPOZICIJA 2.22 *Neka su* $(S_1, \cdot_1), (S_2, \cdot_2)$ *i* $(S_3, \cdot_3)$ *tri polugrupe. Tada važi:*

1. $S_1 \cong S_1$;
2. *Ako je* $S_1 \cong S_2$ *onda je* $S_2 \cong S_1$;
3. *Ako je* $S_1 \cong S_2$ *i* $S_2 \cong S_3$ *onda je* $S_1 \cong S_3$.

Dokaz: 1. Važi jer identičko preslikavanje na S_1 predstavlja izomorfizam (automorfizam). 2. Važi jer je inverzno preslikavanje bijekcije opet bijekcija. Dokažimo još da je inverzno preslikavanje izomorfizma i homomorfizam. Neka je $f : S_1 \to S_2$ izomorfizam i $f^{-1} : S_2 \to S_1$. Za proizvoljne $a, b \in S_2$ postoje $c, d \in S_1$ takvi da je $f(c) = a$ i $f(d) = b$. Sada dobijamo: $f^{-1}(a \cdot_2 b) = f^{-1}(f(c) \cdot_2 f(d)) = f^{-1}(f(c \cdot_1 d)) = c \cdot_1 d = f^{-1}(a) \cdot_1 f^{-1}(b)$. 3. je posledica činjenice da je kompozicija dve bijekcije ponovo bijekcija i da je kompozicija dva homomorfizma opet homomorfizam po lemi 2.21. □

Da su dve polugrupe izomorfne ustvari znači da se one razlikuju samo u nazivu elemenata nosača. To drugačije kažemo da su iste do na preimenovanje elemenata. U algebri nije važno kako smo elemente nazvali već kako deluje operacija te polugrupe, pa zato izomorfne polugrupe u algebri poistovećujemo. Sam izomorfizam kao preslikavanje ustvari i daje način na koji treba da preimenujemo elemente jedne polugrupe u elemente druge polugrupe i time od Kejlijeve tablice prve dobijemo Kejlijevu tablicu druge polugrupe.

Primer: Svake dve trivijalne polugrupe su izomorfne, jer preslikavanje koje jedinstvenom elementu jedne dodeljuje jedinstveni element druge polugrupe očigledno jeste i bijekcija i homomorfizam. Evo jednog netrivijalnog primera: $(\mathbb{Z}_2, \cdot_2) \cong (\{\top, \bot\}, \vee)$ pomoću izomorfizma $\varphi(0) = \top$ i $\varphi(1) = \bot$. Kejlijeva tablica polugrupe $(\{\top, \bot\}, \vee)$ se može zaista dobiti iz Kejlijeve tablice $(\mathbb{Z}_2, \cdot_2)$ ako umesto nule pišemo $\top$, a umesto jedinice $\bot$. Pri tome ćemo naravno umesto operacijskog znaka $\cdot_2$ upisati operacijski znak $\vee$.

$\cdot_2$	0	1
0	0	0
1	0	1

$\vee$	$\top$	$\bot$
$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$

DEFINICIJA 2.23 *Neka je* $(M, \cdot)$ *monoid sa jedinicom* 1. *Tada je* S *nosač podmonoida ako* $1 \in S$ *i* S *je nosač potpolugrupe od* S.

PROPOZICIJA 2.24 *Neka je* $(S, \cdot)$ *polugrupa. Tada je:*

1. *neprazan presek dve potpolugrupe potpolugrupa;*

2. *neprazan presek konačno mnogo potpolugrupa ponovo potpolugrupa;*

3. *neprazan presek proizvoljne familije potpolugrupa ponovo potpolugrupa.*

Dokaz: Neka su P_1 i P_2 nosači dve potpolugrupe od $(S, \cdot)$. Ako je $P_1 \cap P_2 \neq \emptyset$, neka $a, b \in P_1 \cap P_2$. Tada $a, b \in P_1$ i $a, b \in P_2$, pa $ab \in P_1$ i $ab \in P_2$ pa je $ab \in P_1 \cap P_2$. Time je pokazano prvo tvrđenje na osnovu propozicije 2.19. Koristeći se tim i matematičkom indukcijom dokazujemo drugo tvrđenje. Neka je sad $\{P_i \mid i \in I\}$, za $I \neq \emptyset$ familija (nosača) potpolugrupa od S takva da je $\cap_{i \in I} P_i \neq \emptyset$. Ako $a, b \in \cap_{i \in I} P_i$ to znači da za sve $i \in I$ važi $a, b \in P_i$, a onda $ab \in P_i$, pa po definiciji preseka familije skupova dobijamo da $ab \in \cap_{i \in I} P_i$. □

Dokaz sledećeg tvrđenja o monoidima je sličan dokazu prethodnog tvrđenja samo zahteva dodatno razmatranje jedinice.

Propozicija 2.25 *Neka je $(S, \cdot)$ monoid sa jedinicom 1. Tada je:*

1. *Presek dva podmonoida podmonoid;*

2. *Presek konačno mnogo podmonoida ponovo podmonoid;*

3. *Presek proizvoljne familije podmonoida ponovo podmonoid.*

Ako je $(S, \cdot)$ polugrupa i $\emptyset \neq X \subseteq S$ onda u opštem slučaju X ne mora biti nosač potpolugrupe od S. Možemo se pitati kako izgleda nosač najmanje (u odnosu na relaciju $\subseteq$) potpolugrupe od S koji sadrži X. Takvu potpolugrupu zovemo *potpolugrupa generisana sa X*, a njen nosač označavamo sa $< X >$. Ovaj pojam formalnije uvodimo sledećom definicijom.

Definicija 2.26 *Ako je $(S, \cdot)$ polugrupa i $\emptyset \neq X \subseteq S$ onda je $< X >$ nosač potpolugrupe generisane sa X ako je $X \subseteq < X >$, $< X >$ je nosač potpolugrupe od $(S, \cdot)$ i za svaki domen P potpolugrupe od $(S, \cdot)$ takav da je $X \subseteq P$, važi $< X > \subseteq P$.*

Propozicija 2.27 *Ako je $(S, \cdot)$ polugrupa i $\emptyset \neq X \subseteq S$ onda je*

1. $< X > = \cap\{P \in \mathcal{P}(S) \mid X \subseteq P, (P, \cdot)$ *je potpolugrupa od* $(S, \cdot)\}$;

2. $< X > = \{x_1 \cdot \ldots \cdot x_n \mid n \in \mathbb{N}, x_1, \ldots, x_n \in X\}$.

Dokaz: 1. Skup sa desne strane jednakosti jeste nosač potpolugrupe od S koji sadrži X zbog osobina preseka skupova i propozicije 2.19. Takođe je i najmanji u odnosu na poredak $\subseteq$ što direktno sledi.

2. Označimo skup sa desne strane sa Y i dokažimo da je $< X >= Y$. Jasno, $X \subseteq Y$, a po propoziciji 2.19 lako proveravamo da je Y domen potpolugrupe od $(S, \cdot)$. Zato je $< X > \subseteq Y$. Ako je P nosač neke potpolugrupe od S takav da je $X \subseteq P$, onda opet po propoziciji 2.19 dobijamo da je $Y \subseteq P$. Odavde je $Y \subseteq < X >$. □

Primer: U polugrupi $(\mathbb{Z}_3, +_3)$ je $< 0 >= \{0\}$, ali $< 1 >= \mathbb{Z}_3$.

Propozicija 2.28 *Ako je $(S, \cdot)$ monoid sa jedinicom 1 i $X \subseteq S$ onda je*

1. $< X >= \cap\{P \in \mathcal{P}(S) \mid X \subseteq P, (P, \cdot)$ *je podmonoid od* $(S, \cdot)\}$;

2. $< X >= \{x_1 \cdot \ldots \cdot x_n \mid \forall n \in \mathbb{N}, x_1, \ldots, x_n \in X\} \cup \{1\}$.

Dokaz: Posledica propozicije 2.40. □

Sledeća teorema objašnjava zašto su polugrupe reči posebno važan primer polugrupa. Više o polugrupama reči može se naći u [1].

Teorema 2.29 *Neka je Σ proizvoljan konačan skup, a $(M, \cdot)$ monoid sa jedinicom 1. Ako postoji preslikavanje $\varphi : \Sigma \to M$, onda postoji homomorfizam $\phi : \Sigma^* \to M$ takav da je $\phi|_\Sigma = \varphi$.*

Dokaz: Preslikavanje $\phi : \Sigma^* \to M$ definišemo sa: $\phi(a_1 \ldots a_n) = \varphi(a_1) \cdot \ldots \cdot \varphi(a_n)$ i $\phi(\lambda) = 1$. Jasno, $\phi(a) = \varphi(a)$, za sve $a \in \Sigma$, pa $\phi|_\Sigma = \varphi$. Homomorfnost: neka su $a_1 \ldots a_n, b_1 \ldots b_m \in \Sigma^*$, gde $n, m \in \mathbb{N}$, tada je $\phi(a_1 \ldots a_n b_1 \ldots b_m) = \varphi(a_1) \cdot \ldots \cdot \varphi(a_n) \cdot \varphi(b_1) \cdot \ldots \cdot \varphi(b_m) = \phi(a_1 \ldots a_n) \cdot \phi(b_1 \ldots b_m)$. □

2.3 Grupe

Zbog svog značaja u drugim granama matematike, ali i fizici i srodnim naukama grupe zauzimaju centralno mesto u klasičnoj algebri. Mi do pojma grupa stižemo preko već dobro pripremljene osnove, naime grupoida i polugrupa. Iako je grupama posvećen značajan deo celokupnog materijala, ipak to predstavlja samo mali uvod u ono što se o grupama danas zna. Više o grupama zainteresovani čitalac na srpskom jeziku može naći u [2].

2.3.1 Definicija, osnovne osobine i primeri

DEFINICIJA 2.30 *Neka je $(G, \cdot)$ monoid sa jedinicom (neutralnim elementom) 1. Ako za svako $g \in G$ postoji $h \in G$ takvo da je $hg = gh = 1$ onda algebru $(G, \cdot)$ nazivamo grupa.*

Primeri: $(\mathbb{Z}, +)$ jeste, ali $(\mathbb{Q}, \cdot)$ nije grupa jer za 0 ne postoji racionalan broj r takava da je $0r = r0 = 1$. $(\mathbb{Q}\backslash\{0\}, \cdot)$ jeste grupa.

PROPOZICIJA 2.31 *Neka je $(G, \cdot)$ grupa sa neutralnim elementom 1. Tada za svako $g \in G$ postoji jedinstveno $h \in G$ takvo da je $hg = gh = 1$.*

Dokaz: Pretpostavimo da za neko $g \in G$ postoje $h, h' \in G$ takvi da je $hg = gh = 1$ i $h'g = gh' = 1$. Sada je $h = h \cdot 1 = h(gh') = (hg)h' = 1 \cdot h' = h'$. □

Zbog prethodnog tvrđenja opravdana je sledeća definicija.

DEFINICIJA 2.32 *Ako je $(G, \cdot)$ grupa sa neutralnim elementom 1 onda se jedinstveni element $h \in G$ za dati element $g \in G$, takav da je $gh = hg = 1$, naziva inverzni element elementa g i označava sa g^{-1}.*

Sada se prethodna propozicija može formulisati na sledeći način: inverzni element svakog elementa grupe je jedinstven.

PROPOZICIJA 2.33 *Neka je $(G, \cdot)$ grupa sa neutralnim elementom 1. Tada važi:*

1. *leva i desna kancelativnost;*
2. *$(g^{-1})^{-1} = g$, za sve $g \in G$;*
3. *$(ab)^{-1} = b^{-1}a^{-1}$, za sve $a, b \in G$;*
4. *1 je jedini idempotent;*
5. *$(G, \cdot)$ je kvazigrupa.*

Dokaz: 5. Neka $a, b \in G$. Tada je jedinstveno rešenje jednačine $ax = b$ ustvari $x = a^{-1}b$, a jedinstveno rešenje jednačine $ya = b$, $y = ba^{-1}$, što se lako neposredno proverava, a jedinstvenost sledi zbog jedinstvenosti inverznog elementa. Sada koristeći propoziciju 2.10 dobijamo 1. Dokažimo 4. Ako je za neko $a \in G$ ispunjeno $a^2 = a$ onda množeći ovu jednakost sa a^{-1} dobijamo $a = 1$. Za svako $g \in G$ bilo da g^{-1} množimo sa g ili sa $(g^{-1})^{-1}$ sa bilo koje strane uvek dobijamo 1. Zbog jedinstvenosti inverza za g^{-1} sledi 2. Analogno dokazujemo 3. tako što posmatramo inverze elementa ab. □

Definicija 2.34 *Grupa $(G,\cdot)$ u kojoj važi: $ab=ba$, za sve $a,b\in G$ naziva se Abelova grupa.*

Primeri: $(\mathbb{R},+)$ je Abelova grupa. Za dati neprazan skup A sa S_A ćemo označiti skup svih bijekcija skupa A u skup A. Tada je $(S_A,\circ)$, gde je $\circ$ kompozicija preslikavanja, grupa koja nije Abelova, jer kompozicija preslikavanja nije komutativna u opštem slučaju. Grupa $(S_A,\circ)$ se naziva *simetrična grupa skupa A*. Ukoliko skup A jeste konačan sa $n\in\mathbb{N}$ elemenata onda za domen odgovarajuće grupe permutacija koristimo i oznaku S_n.

2.3.2 Lagranžova teorema

Definicija 2.35 *Neka je $(G,\cdot)$ grupa. Za $\emptyset\neq H\subseteq G$ kažemo da je nosač (domen) podgrupe ako je $(H,\cdot|_{H^2})$ grupa.*

Primeri: $(\mathbb{Z},+)$ je podgrupa od $(\mathbb{Q},+)$, a ona opet podgrupa od $(\mathbb{R},+)$. $(\mathbb{Z}\backslash\{0\},\cdot)$ nije podgrupa od $(\mathbb{Q}\backslash\{0\},\cdot)$.

Propozicija 2.36 *Ako je $(G,\cdot)$ grupa, onda je $\emptyset\neq H\subseteq G$ nosač (domen) podgrupe ako i samo ako za sve $a,b\in H$ važi $ab\in H$ i $a^{-1}\in H$.*

Dokaz: Ako je H domen podgrupe onda jasno za sve $a,b\in H$ važi $ab\in H$ i $a^{-1}\in H$. Pokažimo obratno. Neka je neutralni element grupe $e\in G$. Ako je $\emptyset\neq H\subseteq G$ onda postoji neko $h\in H$, pa $h^{-1}\in H$ po pretpostavci, pa $e=hh^{-1}\in H$. Kako je H zatvoreno za proizvode to je H nosač potpolugrupe po propoziciji 2.19, a kako sadrži e to je H domen podmonoida. Iz pretpostavke da je H zatvoreno za inverze sledi da je H domen podgrupe. □

Propozicija 2.37 *Ako je $(G,\cdot)$ grupa, onda je $\emptyset\neq H\subseteq G$ nosač (domen) podgrupe ako i samo ako za sve $a,b\in H$ važi $a^{-1}b\in H$.*

Dokaz: Ako je H domen podgrupe onda jasno za sve $a,b\in H$ važi $a^{-1}b\in H$. Pokažimo obratno. Neka je neutralni element grupe $e\in G$. Ako je $\emptyset\neq H\subseteq G$ onda postoji neko $h\in H$, pa $e=h^{-1}h\in H$ po pretpostavci. Odavde za svako $a\in H$ je $a^{-1}=a^{-1}e\in H$, pa je i za sve $b\in H$ $ab=(a^{-1})^{-1}b\in H$. Sada kako je H zatvoreno za proizvode i inverze to je H nosač podgrupe po propoziciji 2.36. □

Propozicija 2.38 *Neka je $(G,\cdot)$ grupa. Tada je:*

1. *presek domena dve podgrupe domen podgrupe;*

2. *presek konačno mnogo domena podgrupa ponovo domen podgrupe;*

3. *presek proizvoljne familije domena podgrupa ponovo domen podgrupe.*

Dokaz: Dokaz sličan dokazu tvrđenja o polugrupama (propozicija 2.25), na osnovu propozicije 2.36. □

Definicija 2.39 *Ako je $(G,\cdot)$ grupa i $\emptyset \neq X \subseteq G$ onda je $< X >$ nosač podgrupe generisane sa X ako je $X \subseteq < X >$, $< X >$ je nosač podgrupe od $(G,\cdot)$ i za svaki domen H podgrupe od $(G,\cdot)$ takav da je $X \subseteq H$, važi $< X > \subseteq H$.*

Propozicija 2.40 *Ako je $(G,\cdot)$ grupa i $\emptyset \neq X \subseteq G$ onda je*

1. $< X >= \cap\{H \in \mathcal{P}(G) \mid X \subseteq H, (H,\cdot)$ *je podgrupa od* $(G,\cdot)\}$;

2. $< X >= \{x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} \mid n \in \mathbb{N}, x_1, \ldots, x_n \in X, \alpha_1, \ldots, \alpha_n \in \{1,-1\}\}$.

Dokaz: 1. Skup sa desne strane jednakosti jeste nosač podgrupe od G koji sadrži X zbog osobina preseka skupova i propozicije 2.36. Takođe je i najmanji u odnosu na poredak $\subseteq$ što direktno sledi.

2. Označimo skup sa desne strane sa Y i dokažimo da je $< X >= Y$. Jasno, $X \subseteq Y$, a po propozicijama 2.33 i 2.36 lako proveravamo da je Y domen podgrupe od $(G,\cdot)$. Zato je $< X > \subseteq Y$. Ako je H nosač neke podgrupe od G takav da je $X \subseteq H$, onda opet po propozicijama 2.33 i 2.36 dobijamo da je $Y \subseteq H$. Odavde je $Y \subseteq < X >$. □

Definicija 2.41 *Neka je $(G,\cdot)$ grupa i $a \in G$. Broj elemenata $< a >$ nazivamo red elementa a i označavamo sa $red(a)$. Podgrupu $(< a >,\cdot)$ zovemo ciklička podgrupa generisana sa a. Ako je $< a >= G$ onda G zovemo ciklička grupa generisana sa a.*

Primer: $(\mathbb{Z},+)$ je ciklična grupa generisana sa 1, $(\mathbb{Z}_m,+_m)$ je ciklična grupa generisana sa 1. Takođe je $(\mathbb{Z},+)$ ciklička podgrupa od $(\mathbb{Q},+)$.

Propozicija 2.42 *Neka je $a \in G$, gde je $(G,\cdot)$ grupa sa neutralnim elementom e. Tada je $red(a)$ najmanji prirodan broj n takav da je $a^n = e$, ako takav broj postoji inače je $red(a)$ beskonačan.*

Dokaz: Neka je $red(a) = n \in \mathbb{N}$, tada skup $\{e, a, \ldots, a^{n-1}\}$ jeste nosač podgrupe i važi $a^n = a^k$, gde je $k \in \{0, \ldots, n-2\}$, ali dolazi u obzir samo mogućnost $k = 0$, jer bi u suprotnom bilo $|\{e, a, \ldots, a^{n-1}\}| = n - k < n$. Sličnim rezonom ni za jedno $m \in \mathbb{N}_0$ koje je manje od n ne može važiti $a^m = e$, jer bi tada bilo $|\{e, a, \ldots, a^{n-1}\}| = m < n$. □

Primer: Element -1 je element reda 2 u grupi $(\mathbb{Q}\backslash\{0\}, \cdot)$, neutralni element je reda 1, a ostali elementi su beskonačnog reda.

Definicija 2.43 *Neka je $(G, \cdot)$ grupa i $H \subseteq G$. Tada je za svako $g \in G$, $gH = \{gh \,|\, h \in H\}$ levi suskup od H i $Hg = \{hg \,|\, h \in H\}$ desni suskup od H. Levu i desnu binarnu relaciju $\pmod H$ na G definišemo sa $a \equiv b \pmod{{}_L H}$ akko $a^{-1}b \in H$, a $a \equiv b \pmod{{}_D H}$ akko $ab^{-1} \in H$, za sve $a, b \in G$.*

Propozicija 2.44 *Neka je $(G, \cdot)$ grupa i H domen podgrupe grupe G. Relacija $\equiv \pmod{{}_L H}$ ($\equiv \pmod{{}_D H}$) je relacija ekvivalencije na G i klase ekvivalencije su tačno levi (desni) suskupovi od H.*

Dokaz: Označimo neutralni element date grupe sa e. Refleksivnost: $a \equiv a \pmod{{}_L H}$ jer je $a^{-1}a = e \in H$, za svako $a \in G$. Simetričnost: Pretpostavimo da je $a \equiv b \pmod{{}_L H}$, za neke $a, b \in G$, tada je $a^{-1}b \in H$, ali kako je H nosač podgrupe onda je $(a^{-1}b)^{-1} \in H$. Odavde je $b^{-1}a \in H$, pa je $b \equiv a \pmod{{}_L H}$. Tranzitivnost: neka za neke $a, b, c \in G$ važi: $a \equiv b \pmod{{}_L H}$ i $b \equiv c \pmod{{}_L H}$. Tada imamo $a^{-1}b \in H$ i $b^{-1}c \in H$, pa kako je H domen podgrupe dobijamo da je $a^{-1}bb^{-1}c \in H$, odnosno $a^{-1}c \in H$. Zato je $a \equiv c \pmod{{}_L H}$. Ovim je pokazano da je relacija $\equiv \pmod{{}_L H}$ relacija ekvivalencije na G. Primetimo da je $xH = H$, za sve $x \in H$, da je $eH = H$ i da $a \in aH$ jer $e \in H$. Koristeći se time dokažimo da je levi suskup od H tačno klasa ekvivalencije $\equiv \pmod{{}_L H}$: $a \equiv b \pmod{{}_L H}$ akko $a^{-1}b \in H$ akko $a^{-1}bH = H$ akko $aa^{-1}bH = aH$ akko $bH = aH$, za sve $a, b \in G$. □

Lema 2.45 *Svi levi (desni) suskupovi nosača podgrupe neke grupe su iste kardinalnosti. (imaju isti broj elemenata)*

Dokaz: Neka je H domen podgrupe neke grupe $(G, \cdot)$ i $g \in G$. Posmatrajmo preslikavanje $f : H \to gH$ zadato sa $f(x) = gx$, za sve $x \in H$. Kako je svaka grupa kvazigrupa lako se vidi da je f bijekcija, pa je $|H| = |gH|$. □

Red grupe je broj elemenata domena te grupe.

TEOREMA 2.46 *(Lagranžova teorema) Neka je $(G, \cdot)$ grupa konačnog reda. Tada red svake podgrupe deli red grupe.*

Dokaz: Neka je H domen podgrupe. Kako je G konačan skup, to relacija $\equiv \pmod{{}_L H}$ ima samo konačno mnogo klasa. Neka su to $H, g_1H, \ldots, g_nH$, za neko $n \in \mathbb{N}_0$, gde je $g_0H = H$. Tada je $G = \bigcup_{x \in \{g_0, \ldots, g_n\}} xH$. Time je skup G prikazan kao unija međusobno disjunktnih i po broju elemenata jednakih skupova, pa važi $|G| = (n+1)|H|$, zbog leme 2.45. □

POSLEDICA 2.47 *Ako je grupa konačna, onda red svakog elementa deli red grupe.*

Dokaz: Red elementa je red odgovarajuće cikličke podgrupe, pa po Lagranžovoj teoremi deli red grupe. □

DEFINICIJA 2.48 *Neka je $(G, \cdot)$ grupa. Ako za domen podgrupe H važi $gH = Hg$, za sve $g \in G$ onda je H domen normalne podgrupe grupe $(G, \cdot)$.*

Primer: U Abelovim grupama sve podgrupe su normalne.

PROPOZICIJA 2.49 *Neka je $(G, \cdot)$ grupa i $(H, \cdot)$ njena podgrupa. Tada je H domen njene normalne podgrupe ako i samo ako se relacije $\equiv \pmod{{}_L H}$ i $\equiv \pmod{{}_D H}$ poklapaju.*

Dokaz: ($\Rightarrow$) Za proizvoljne $x, y \in G$ važi: $x \equiv y \pmod{{}_L H}$ akko $xH = yH$ akko $Hx = Hy$ akko $x \equiv y \pmod{{}_D H}$, koristeći propoziciju 2.44. ($\Leftarrow$) Ako se $\equiv \pmod{{}_L H}$ i $\equiv \pmod{{}_D H}$ poklapaju onda im se poklapaju i odgovarajuće klase ekvivalencije. Zato je za sve $g \in G$ ispunjeno $gH = Hg$, pa je H nosač normalne podgrupe. □

Zbog prethodne propozicije, u slučaju domena normalne podgrupe ne razlikujemo levu i desnu relaciju već obe označavamo sa $\equiv \pmod{H}$.

DEFINICIJA 2.50 *Neka je $(G, \cdot)$ grupa. Binarna relacija θ na G naziva se kongruencija ako je relacija ekvivalencije i za sve $a, b, c, d \in G$ važi: $a\theta b \wedge c\theta d \Rightarrow ac\theta bd$ (kompatibilnost ili saglasnost sa operacijom grupe).*

Primer: U grupi $(\mathbb{Z}, +)$ relacija $\equiv \pmod{m}$ je kongruencija za svaki prirodan broj m. Primetimo da su dijagonala i puna relacija uvek kongruencije svake grupe.

PROPOZICIJA 2.51 *Ako je ρ kongruencija grupe $(G,\cdot)$ onda za sve $a,b\in G$ važi: $a\rho b\Rightarrow a^{-1}\rho b^{-1}$.*

Dokaz: Neka za neke $a,b\in G$ važi $a\rho b$. Kako je $a^{-1}\rho a^{-1}$, zbog kompatibilnosti relacije ρ dobijamo da je $aa^{-1}\rho ba^{-1}$, odnosno $e\rho ba^{-1}$, gde je e neutralni element date grupe. Takođe znamo da je $b^{-1}\rho b^{-1}$ pa ponovo zbog kompatibilnosti dobijamo $b^{-1}e\rho b^{-1}ba^{-1}$, odakle je $b^{-1}\rho a^{-1}$, što zbog simetričnosti daje $a^{-1}\rho b^{-1}$. □

TEOREMA 2.52 *Neka je $(G,\cdot)$ grupa sa neutralnim elementom e. Ako je ρ kongruencija date grupe onda je e/ρ domen njene normalne podgrupe. Ako je H domen normalne podgrupe, onda je $\equiv \pmod H$ kongruencija grupe $(G,\cdot)$.*

Dokaz: Neka je ρ kongruencija. Tada je $\emptyset\neq e/\rho\subseteq G$. Ako $a,b\in e/\rho$, onda je $a\rho e$ i $b\rho e$ pa je zbog kompatibilnosti $ab\rho e$, a zbog propozicije 2.51 dobijamo $a^{-1}\rho e$. Zato je $ab,a^{-1}\in e/\rho$, pa po propoziciji 2.36 dobijamo da je e/ρ nosač podgrupe od G. Kako je za sve $a,b\in G$ ispunjeno $a^{-1}b\in e/\rho$ akko $b\rho a$ akko $e\rho ab^{-1}$ akko $ab^{-1}\in e/\rho$, dobijamo da je e/ρ nosač normalne podgrupe od G po propoziciji 2.49. Ako je H domen normalne podgrupe onda je $\equiv \pmod H$ svakako relacija ekvivalencije na G po propoziciji 2.44. Dokažimo da je $\equiv \pmod H$ kompatibilna. Neka je $a\equiv b \pmod H$ i $c\equiv d \pmod H$. Sada je $c^{-1}d\in H$, pa je $c^{-1}a^{-1}ad\in H$, odnosno $(ac)^{-1}ad\in H$, odnosno $ac\equiv ad \pmod H$. Takođe iz $add^{-1}b^{-1}\in H$ dobijamo $ad(bd)^{-1}\in H$, pa je $ad\equiv bd \pmod H$. Iz tranzitivnosti sada sledi $ac\equiv bd \pmod H$. □

Primer: Označimo sa $2\mathbb{Z}$ skup svih parnih celih brojeva. U grupi $(\mathbb{Z},+)$ je $(2\mathbb{Z},+)$ normalna podgrupa, a $\equiv \pmod{2\mathbb{Z}}$ je ustvari $\equiv \pmod 2$. Obratno, $0/{\equiv} \pmod 2 = 2\mathbb{Z}$.

PROPOZICIJA 2.53 *Neka je θ kongruencija grupe $(G,\cdot)$. Tada je $\odot$, gde je*

$$a/\theta\odot b/\theta = ab/\theta,$$

za sve $a/\theta,b/\theta\in G/\theta$ dobro definisana binarna operacija na količničkom skupu G/θ. Struktura $(G/\theta,\odot)$ je grupa.

Dokaz: Ako je $c\in a/\theta$ i $d\in b/\theta$ onda treba dokazati da je $a/\theta\odot b/\theta = c/\theta\odot d/\theta$. Po definiciji je $c/\theta\odot d/\theta = cd/\theta$. Iz $c\in a/\theta$ dobijamo da je $a\theta c$, a iz $d\in b/\theta$ dobijamo da je $b\theta d$, pa zbog kompatibilnosti za θ imamo

$ab\theta cd$, odnosno $ab/\theta = cd/\theta$. Da u strukturi $(G/\theta, \odot)$ važi asocijativnost se direktno proverava na osnovu toga što u strukturi $(G, \cdot)$ važi asocijativnost. Neutralni element je e/θ, za neutralni element e grupe G, a za inverz elementa g/θ uzimamo klasu g^{-1}/θ. □

Grupa nastala na način opisan u prethodnom tvrđenju naziva se *faktor grupa*.

2.3.3 Kejlijeva teorema reprezentacije

Kako grupe jesu i polugrupe, pojam homomorfizma (epimorfizma, monomorfizma, izomorfizma, endomorfizma i automorfizma) se prenosi. Naravno da kako grupe imaju "bogatiju" strukturu od polugrupa ovi homomorfizmi imaju dodatne osobine, od kojih ćemo sada neke i pokazati.

PROPOZICIJA 2.54 *Neka su $(G, \cdot)$ i $(H, +)$ grupe čiji su neutralni elementi redom $1 \in G$ i $0 \in H$. Ako je $f : G \to H$ homomorfizam (odgovarajućih polugrupa) onda je $f(1) = 0$ i $f(g^{-1}) = (f(g))^{-1}$, za sve $g \in G$.*

Dokaz: Koristeći homomorfnost preslikavanja f dobijamo da je $f(1) = f(1 \cdot 1) = f(1) + f(1)$, pa je $f(1)$ idempotent u grupi H, što po propoziciji 2.33 daje da je $f(1) = 0$. Neka je $g \in G$. Sada je $0 = f(1) = f(g \cdot g^{-1}) = f(g) + f(g^{-1})$, analogno je i $f(g^{-1}) + f(g) = 0$, pa je $f(g^{-1})$ inverz za $f(g)$ u grupi H. □

PROPOZICIJA 2.55 *Neka je $(G, \cdot)$ grupa i θ njena kongruencija, a $(G/\theta, \odot)$ odgovarajuća faktor grupa. Tada je prirodno preslikavanje $nat_\theta : G \to G/\theta$, dato sa $nat_\theta(g) = g/\theta$, za sve $g \in G$ epimorfizam.*

Dokaz: Jasno je da je nat_θ "na", jer svaka klasa kongruencije θ sadrži bar jedan element. Homomorfnost sledi iz definicije operacije u faktor grupi. □

PROPOZICIJA 2.56 *Neka je $f : G \to H$ homomorfizam grupe $(G, \cdot)$ u grupu $(H, +)$. Ako je 0 neutralni element grupe $(H, +)$, onda je $f^{-1}(\{0\})$ normalna podgrupa grupe $(G, \cdot)$.*

Dokaz: Kako je $f(1) = 0$ po propoziciji 2.54, to je $\emptyset \neq f^{-1}(\{0\}) \subseteq G$. Neka $a, b \in f^{-1}(\{0\})$, tada je $f(a) = f(b) = 0$, pa je $f(ab) = f(a) + f(b) = 0 + 0 = 0$. Zato $ab \in f^{-1}(\{0\})$. Iz $f(a) = 0$ dobijamo da je $f(a^{-1}) = -f(a) = 0$, po propoziciji 2.54, pa $a^{-1} \in f^{-1}(\{0\})$. Zato je $f^{-1}(\{0\})$ domen

podgrupe od G. Ako je $g \in f^{-1}(\{0\})$ i $a \in G$ onda je $ag \in af^{-1}(\{0\})$, a $aga^{-1} \in f^{-1}(\{0\})$, jer je $f(aga^{-1}) = f(a) + f(g) - f(a) = 0$ koristeći osobine homomorfizma f, pa postoji $b \in f^{-1}(\{0\})$ takvo da je $aga^{-1} = b$ odnosno $ag = ba \in f^{-1}(\{0\})a$. Zato je $af^{-1}(\{0\}) \subseteq f^{-1}(\{0\})a$. Analogno dokazujemo i obratnu inkluziju i time smo pokazali tvrđenje. □

PROPOZICIJA 2.57 *Neka je $f : G \to H$ homomorfizam grupe $(G, \cdot)$ u grupu $(H, +)$. Tada je jezgro homomorfizma f kongruencija grupe $(G, \cdot)$.*

Dokaz: Znamo da je $kerf$ relacija ekvivalencije na skupu G. Dokažimo još kompatibilnost sa operacijom $\cdot$. Neka su $a, b, c, d \in G$ takvi da je $a \, kerf \, b$ i $c \, kerf \, d$. Tada je $f(a) = f(b)$ i $f(c) = f(d)$, pa je $f(a)+f(c) = f(b)+f(d)$, odnosno $f(a \cdot c) = f(b \cdot d)$. Zato je $a \cdot c \, kerf \, b \cdot d$, pa je $kerf$ kongruencija. □

PROPOZICIJA 2.58 *Neka je $f : G \to H$ homomorfizam grupe $(G, \cdot)$ u grupu $(H, +)$. Tada je $f^{-1}(\{0\}) = 1/kerf$, gde su $0 \in H$ i $1 \in G$ odgovarajući neutralni elementi.*

Dokaz: Neka $x \in G$. Tada $x \in f^{-1}(\{0\})$ akko $f(x) = 0$ akko $f(x) = f(1)$ akko $x \, kerf \, 1$ akko $x \in 1/kerf$. □

PROPOZICIJA 2.59 *Neka je $f : G \to H$ homomorfizam grupe $(G, \cdot)$ u grupu $(H, +)$. Tada je $f(G)$ domen podgrupe grupe $(H, +)$.*

Dokaz: Ako $a, b \in f(G)$ onda postoje $c, d \in G$ takvi da je $a = f(c)$ i $b = f(d)$ koristeći propoziciju 2.54, dobijamo da je $-a = f(c^{-1}) \in f(G)$ i $a + b = f(c) + f(d) = f(cd) \in f(G)$. □

TEOREMA 2.60 *Homomorfna slika svake grupe je izomorfna faktor grupi po jezgru tog homomorfizma.*

Dokaz: Neka je $f : G \to H$ homomorfizam grupe $(G, \cdot)$ u grupu $(H, +)$. Dokažimo da je $(G/kerf, \odot) \cong (f(G), +)$. Definišimo preslikavanje $\varphi : G/kerf \to f(G)$ sa $\varphi(g/kerf) = f(g)$, za sve $g \in G$. Sada za $g, h \in G$ imamo: $\varphi(g/kerf) = \varphi(h/kerf)$ akko $f(g) = f(h)$ akko $gkerfh$ akko $g/kerf = h/kerf$, što dokazuje da je φ dobro definisano "1-1" preslikavanje. Osobina "na" važi očigledno. Pokažimo homomorfnost. $\varphi(a/kerf \odot b/kerf) = \varphi(ab/kerf) = f(ab) = f(a) + f(b) = \varphi(a/kerf) + \varphi(b/kef)$, za sve $a/kerf, b/kerf \in G/kerf$. □

TEOREMA 2.61 *(Kejlijeva teorema) Svaka grupa je izomorfna nekoj podgrupi grupe permutacija.*

Dokaz: Neka je $(G, \cdot)$ grupa. Za prozvoljno $a \in G$ definišimo preslikavanje $t_a : G \to G$ sa $t_a(x) = ax$, za sve $x \in G$. Svako ovako definisano preslikavanje je bijekcija. Sirjektivnost sledi jer je svaka grupa kvazigrupa, a injektivnost jer je svaka grupa kancelativna. Posmatrajmo skup $T = \{t_a \,|\, a \in G\}$. Dokažimo da je T domen podgrupe grupe permutacija S_G. Jasno je da je T neprazan podskup od G. Ako $t_a, t_b \in T$, onda imamo $t_a \circ t_b(x) = t_a(t_b(x)) = abx = t_{ab}(x)$, za sve $x \in G$. Zato $t_a \circ t_b \in T$. Ako $a \in G$ tada je $t_a^{-1} = t_{a^{-1}}$, što se direktno proverava. Zato $t_a^{-1} \in T$. Ostaje još da se pokaže da je $(G, \cdot) \cong (S_G, \circ)$. Definišimo preslikavanje $\varphi : G \to T$ sa $\varphi(g) = t_g$, za sve $g \in G$. Očigledno je φ sirjektivno. Neka je za neke $a, b \in G$ ispunjeno $\varphi(a) = \varphi(b)$. Tada je $t_a = t_b$, pa je $t_a(1) = t_b(1)$, gde je 1 neutralni element za G. Dakle, $a = b$. Zato je φ bijekcija. Dokažimo homomorfnost. Neka $a, b \in G$. Tada je $\varphi(ab) = t_{ab} = t_a \circ t_b = \varphi(a) \circ \varphi(b)$. □

Primer: Posmatrajmo grupu $(\mathbb{Z}_3, +_3)$ i grupu permutacija skupa $\{0, 1, 2\}$. Skup $\{t_0, t_1, t_2\}$, gde je $t_0 = id$, $t_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$, a $t_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$, jeste domen podgrupe grupe $(S_{\{0,1,2\}}, \circ)$, jer je $t_1^{-1} = t_2$ i $t_2^{-1} = t_1$, a $t_1 \circ t_1 = t_2$ i $t_2 \circ t_2 = t_1$. Odavde možemo formirati Kejlijevu tablicu grupe $(\{t_0, t_1, t_2\}, \circ)$:

$\circ$	t_0	t_1	t_2
t_0	t_0	t_1	t_2
t_1	t_1	t_2	t_0
t_2	t_2	t_0	t_1

Iz tablice vidimo da je $(\mathbb{Z}_3, +_3) \cong (\{t_0, t_1, t_2\}, \circ)$.

TEOREMA 2.62 *Sve cikličke grupe istog reda su izomorfne.*

Dokaz: Neka su $(G, *)$ i $(H, \cdot)$ dve beskonačne cikličke grupe i $G =< g >$, a $H =< h >$. Definišimo preslikavanje $\varphi : G \to H$ sa $\varphi(g^k) = h^k$, $k \in \mathbb{N}$. Očigledno je φ "na". Neka je za neke $m, n \in \mathbb{N}$ ispunjeno $\varphi(g^n) = \varphi(g^m)$, tada je $h^n = h^m$. Neka je bez umanjenja opštosti $n > m$. Međutim onda dobijamo $h^{n-m} = 1$, pa bi onda H bila konačna ciklička grupa. Zato φ jeste "1-1", pa je bijekcija. Pokažimo homomorfnost. Za $n, m \in \mathbb{N}$ imamo $\varphi(g^n * g^m) = \varphi(g^{n+m}) = h^{n+m} = h^n \cdot h^m = \varphi(g^n) \cdot \varphi(g^m)$. U slučaju konačnih cikličkih grupa postoji samo razlika u dokazu injektivnosti preslikavanja φ,

gde u slučaju da injektivnost ne važi dobijamo da je generatorni element manjeg reda od reda cikličke grupe što je nemoguće. □

Napomena: Na osnovu prethodne teoreme mi ustvari do na izomorfizam poznajemo sve cikličke grupe: trivijalna, $(\mathbb{Z}_2, +_2), \ldots, (\mathbb{Z}_n, +_n), \ldots, (\mathbb{Z}, +)$.

PROPOZICIJA 2.63 *Neka $n \in \mathbb{N}$ i neka su $(G_1, \cdot_1), \ldots, (G_n, \cdot_n)$ grupe. Tada je $(G_1 \times \ldots \times G_n, \odot)$, gde je $\odot$ binarna operacija na $G_1 \times \ldots \times G_n$ data sa*

$$(a_1, \ldots, a_n) \odot (b_1, \ldots, b_n) = (a_1 \cdot_1 b_1, \ldots, a_n \cdot_n b_n),$$

za sve $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in G_1 \times \ldots \times G_n$, grupa.

Dokaz: Asocijativnost se direktno proverava na osnovu toga što važi na svakoj komponenti. Neutralni element je n-torka $(1_1, \ldots, 1_n)$, a inverzni element za neku n-torku je n-torka čije su komponente redom inverzi odgovarajućih elemenata u datim grupama $G_1, \ldots, G_n$. □

Novonastala grupa iz prethodnog tvrđenja naziva se *direktan proizvod grupa*.

PROPOZICIJA 2.64 *Neka $n \in \mathbb{N}$ i neka su $(G_1, \cdot_1), \ldots, (G_n, \cdot_n)$ grupe. Tada je preslikavanje $\pi_i : G_1 \times \ldots \times G_n \to G_i$ dato sa $\varphi(a_1, \ldots, a_n) = a_i$, za sve $(a_1, \ldots, a_n) \in G_1 \times \ldots \times G_n$ epimorfizam.*

Dokaz: Direktno. □

Epimorfizam iz prethodnog tvrđenja naziva se još i *i-ta projekcija*.

PROPOZICIJA 2.65 *Direktan proizvod grupa je komutativan ako i samo ako je svaka od grupa iz tog proizvoda komutativna.*

Dokaz: Direktno se proverava da je direktan proizvod Abelovih grupa Abelova grupa. Za obrat pokažimo da je homomorfna slika Abelove grupe Abelova. Neka je $(G, \cdot)$ Abelova i $f : G \to H$ epimofizam na grupu $(H, +)$. Tada za sve $a, b \in H$ postoje $c, d \in G$ takvi da je $f(c) = a$ i $f(d) = b$. Sada je $a + b = f(c) + f(d) = f(cd) = f(dc) = f(d) + f(c) = b + a$. Da bi dokazali tvrđenje iskoristićemo da su odgovarajuće projekcije epimorfizmi. □

LEMA 2.66 *Neka je $(G, \cdot)$ grupa i $g \in G$ reda $n \in \mathbb{N}$. Ako za neko $m \in \mathbb{N}$ važi $g^m = e$, onda $n|m$.*

Dokaz: Neka je $m = nq + r$, gde je $0 \leq r < n$. Sada je $e = g^m = g^{nq+r} = g^{nq}g^r = (g^n)^q g^r = g^r$. Zbog definicije reda elementa g znamo da je n najmanji prirodan broj sa osobinom da kada g stepenujemo na taj prirodan broj dobija se neutralni element e, pa mora biti $r = 0$, a onda $n|m$. □

TEOREMA 2.67 *Direktan proizvod dve konačne ciklične grupe je ciklična grupa ako i samo ako su njihovi redovi uzajamno prosti brojevi.*

Dokaz: ($\Rightarrow$) Neka su $(G, \cdot)$ i $(H, *)$ dve ciklične grupe takve da je $(G \times H, \odot)$ ciklička grupa. Neka je $G \times H =< (g, h) >$ i $|G| = m$, $|H| = n$, za neke $m, n \in \mathbb{N}$. Tada je $|G \times H| = |G||H| = mn$. Neka je $NZD(m, n) = d$, $m' = m : d$, a $n' = n : d$. Dokažimo da element (g, h) ima red najviše $n'm'd$. To važi jer je $(g, h)^{n'm'd} = (g^{n'm'd}, h^{n'm'd}) = ((g^{m'd})^{n'}, (h^{n'd})^{m'}) = ((g^m)^{n'}, (h^n)^{m'}) = (1_G^{n'}, 1_H^{m'}) = (1_G, 1_H)$, pa je $red(g, h) \leq n'm'd < nm$, za $d > 1$. Kontradikcija.

($\Leftarrow$) Neka su $(G, \cdot)$ i $(H, *)$ dve ciklične grupe takve da je $G =< g >$ i $H =< h >$ i $|G| = m$, $|H| = n$, za neke $m, n \in \mathbb{N}$, gde je $NZD(m, n) = 1$. Tada je $|G \times H| = |G||H| = mn$. Neka je $\alpha \in \mathbb{N}$ takav da je $red(g, h) = \alpha$. Dobijamo $(g, h)^\alpha = (1_G, 1_H)$, odavde je $(g^\alpha, h^\alpha) = (1_G, 1_H)$, odnosno $g^\alpha = 1_G$ i $h^\alpha = 1_H$. Zato $m|\alpha$ i $n|\alpha$ po lemi 2.66, pa kako su m i n uzajamno prosti dobijamo da $mn|\alpha$. Sa druge strane $\alpha|mn$ po Lagranžovoj teoremi pa je $\alpha = mn$, a onda je (g, h) generator grupe $(G \times H, \odot)$, pa je ona ciklična. □

2.4 Prsteni i polja

U ovoj i narednoj sekciji bavimo se algebrama koje imaju dve binarne operacije. Za početak krenućemo sa jednom grupnom i jednom polugrup=nom operacijom, baš kao što se uvodi u sledećoj definiciji.

DEFINICIJA 2.68 *Struktura $(P, +, \cdot)$, gde je $(P, +)$ Abelova grupa, a $(P, \cdot)$ polugrupa, takva da za sve $a, b, c \in P$ važi $a(b+c) = ab+ac$ i $(a+b)c = ac+bc$, naziva se prsten.*

Napomena: Prsten možemo definisati i kao algebarsku strukturu $(P, +, \cdot)$ u kojoj postoji $0 \in P$ tako da za sve $x, y, z \in P$ važi:

1. $x + y = y + x$;

2. $(x + y) + z = x + (y + z)$;
3. $x + 0 = 0 + x = x$;
4. $(\forall x)(\exists y)x + y = y + x = 0$;
5. $(xy)z = x(yz)$;
6. $x(y + z) = xy + xz$;
7. $(x + y)z = xz + yz$.

Primeri: Trivijalan prsten, nula prsten, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, ...

Uobičajeno je da se u prstenu $(P, +, \cdot)$ sa 0 označava neutralni element za $+$, a da $-$ bude oznaka za inverz u odnosu na grupnu operaciju $+$.

PROPOZICIJA 2.69 *Neka je $(P, +, \cdot)$ prsten. Tada za sve $x, y \in P$ važi:*

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

Dokaz: Koristeći levu distributivnost, za proizvoljno $x \in P$ dobijamo $x(0 + 0) = x \cdot 0 + x \cdot 0$, odnosno $x \cdot 0 = x \cdot 0 + x \cdot 0$, pa je $x \cdot 0$ idempotent u grupi $(P, +)$, pa mora biti $x \cdot 0 = 0$. Analogno pokazujemo $0 \cdot x = 0$, samo što umesto leve koristimo desnu distributivnost. Sada koristeći i ovu osobinu dobijamo preostale dve tvrdnje. Ako $x, y \in P$ onda je $0 = x \cdot 0 = x(y + (-y)) = xy + x(-y)$, ali je i $0 = x(-y) + xy$ iz komutativnosti za $+$, pa je zbog jedinstvenosti inverznog elementa za xy u grupi $(P, +)$ ispunjeno $-(xy) = x(-y)$. Analogno dokazujemo da je $(-x)y = -(xy)$. Treće tvrđenje je direktna posledica drugog tvrđenja i osobine da je inverz inverznog elementa u grupi polazni element. □

DEFINICIJA 2.70 *Prsten $(P, +, \cdot)$ je komutativan ako je polugrupa $(P, \cdot)$ komutativna. Kažemo da $(P, +, \cdot)$ ima jedinicu ako je $(P, \cdot)$ monoid. Ako postoje $a, b \in P$ takvi da je $ab = 0$ i $a, b \neq 0$, onda a zovemo levi, a b desni delitelj nule. Ako komutativan prsten sa jedinicom nema delitelja nule onda se on naziva integralni domen.*

Primeri: $(\mathbb{Z}, +, \cdot)$ je integralni domen. $(\mathbb{Z}_4, +_4)$ nije integralni domen jer ima delitelj nule $2 \cdot_4 2 = 0$, ali jeste komutativan prsten sa jedinicom.

PROPOZICIJA 2.71 *Ako je* $(P, +, \cdot)$ *netrivijalan prsten sa jedinicom* 1*, onda* 1 *nije neutralni element za* $+$*.*

Dokaz: Pretpostavimo da je $1 = 0$. Tada je za svako $x \in P$ ispunjeno $x = x \cdot 1 = x \cdot 0 = 0$. Kontradikcija. □

U sledećoj teoremi koristićemo binomni koeficijent $\binom{n}{k}$. Podsetimo se da je $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, za sve $n \in \mathbb{N}_0$ i $k \in \{0, \ldots, n\}$, gde je $0! = 1$. Pojam binomnog koeficijenta je predmet izučavanja diskretne matematike pa se više o tome kao i sledeća teorema formulisana za prsten realnih brojeva može naći u [5]. U dokazu ćemo koristiti takozvani Paskalov identitet $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ čiji algebarski dokaz ostavljamo čitaocu za vežbu, a nalazi se u [5, Teorema 1.27 b), strana 28].

TEOREMA 2.72 *(Njutnova binomna formula) Neka je* $(P, +, \cdot)$ *komutativan prsten sa jedinicom. Tada za svaka dva elementa* $x, y \in P$ *važi:* $(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$*, za sve* $n \in \mathbb{N}$*.*

Dokaz: Dokaz dajemo indukcijom po n. Baza: za $n = 1$ trivijalno važi. Pretpostavimo da tvrđenje važi za n i dokažimo za $n+1$. Koristićemo sledeće osobine binomnog koeficijenta koje slede direktno iz definicije: $\binom{n}{0} = \binom{n}{n} = 1$, za sve $n \in \mathbb{N}_0$ i $k \in \{1, \ldots, n\}$.

$(x + y)^{n+1} = (x + y)^n (x + y)$
$= (\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k)(x + y)$
$= \sum_{k=0}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k+1}$
$= x^{n+1} + \sum_{k=1}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n-1} \binom{n}{k} x^{n-k} y^{k+1} + y^{n+1}$
$= \binom{n+1}{0} x^{n+1} + \sum_{k=1}^{n} \binom{n}{k} x^{n+1-k} y^k + \sum_{k=1}^{n} \binom{n}{k-1} x^{n-(k-1)} y^k + \binom{n+1}{0} y^{n+1}$
$= \binom{n+1}{0} x^{n+1} + \sum_{k=1}^{n} (\binom{n}{k} + \binom{n}{k-1}) x^{n+1-k} y^k + \binom{n+1}{0} y^{n+1}$
$= \binom{n+1}{0} x^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^{n+1-k} y^k + \binom{n+1}{0} y^{n+1}$
$= \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k$. □

DEFINICIJA 2.73 *Karakteristika prstena* $(P, +, \cdot)$ *je najmanji prirodan broj* n*, ako takav postoji, da je ispunjeno* $nx = \underbrace{x + \ldots + x}_{n} = 0$*, za sve* $x \in P$*, gde je* 0 *neutralni element za* $+$*. Inače je prsten beskonačne karakteristike. Karakteristiku prstena* $(P, +, \cdot)$ *označavamo sa* $Char(P)$*.*

PROPOZICIJA 2.74 *Neka je* $(P, +, \cdot)$ *prsten sa jedinicom. Tada je* $Char(P)$ *najmanji prirodan broj* n *različit od nule takav da je* $n1 = 0$*, gde je* 1 *jedinica, a* 0 *neutralni element za* $+$*.*

Dokaz: Naka je $n \in \mathbb{N}$ najmanji sa osobinom $n1 = 0$. Tada je $nx = \underbrace{1 \cdot x + \ldots + 1 \cdot x}_{n} = (\underbrace{1 + \ldots + 1}_{n}) \cdot x = 0 \cdot x = 0$. Ako je za sve $x \in P$ ispunjeno $mx = 0$, za neko $m \in \mathbb{N}$ onda je $m1 = 0$, što daje $m \geq n$. Zato je po definiciji $Char(R) = n$. □

Definicija 2.75 *Ako je u prstenu $(P, +, \cdot)$, 0 neutralni element za $+$, a $(P\backslash\{0\}, \cdot)$ grupa, onda algebarsku strukturu $(P, +, \cdot)$ nazivamo telo, a ako je $(P\backslash\{0\}, \cdot)$ Abelova grupa, onda algebarsku strukturu $(P, +, \cdot)$ nazivamo polje.*

Primeri: $(\mathbb{Q}, +, \cdot)$ je polje, ali i $(\mathbb{Z}_p, +_p, \cdot_p)$, za svaki prost broj p jeste polje.

Teorema 2.76 *Svako polje je integralni domen. Konačan integralni domen jeste polje.*

Dokaz: Svako polje jeste komutativan prsten sa jedinicom jer nula komutira sa svakim elementom u odnosu na drugu operaciju. Ako bi $a, b \in P$ bili delitelji nule polja $(P, +, \cdot)$ onda $(P\backslash\{0\}, \cdot)$ ne bi uopšte bio grupoid, pa je to nemoguće. Neka je sada $(P, +, \cdot)$ konačan integralni domen. Tada je $(P\backslash\{0\}, \cdot)$ konačan monoid. Zato za proizvoljno $a \in P$, $a \neq 0$ postoje $m, n \in \mathbb{N}$ takvi da je $a^m = a^n$ i neka je bez umanjenja opštosti $m > n$. Iz poslednje jednakosti dobijamo $a^m - a^n = 0$ odnosno $a^n(a^{m-n} - 1) = 0$. Kako u integralnom domenu nema delitelja nule i $a \neq 0$ ostaje $a^{m-n} - 1 = 0$ odnosno $a^{m-n} = 1$ odakle zaključujemo da postoji inverz za a u odnosu na operaciju $\cdot$, pa P jeste polje. □

Propozicija 2.77 *Karakteristika polja je prost broj.*

Dokaz: Pretpostavimo da je karakteristika polja $(P, +, \cdot)$ složen broj. Tada je $Char(P) = n \cdot m$, gde $m, n \in \mathbb{N}\backslash\{1\}$. Kako polje nema delitelja nule, a ima jedinicu važi $nm1 = 0$, odnosno

$$0 = \underbrace{1 + \ldots + 1}_{nm} = \underbrace{\underbrace{(1 + \ldots + 1)}_{n} + \ldots + \underbrace{(1 + \ldots + 1)}_{n}}_{m}$$

$$= \underbrace{1 \cdot \underbrace{(1 + \ldots + 1)}_{n} + \ldots + 1 \cdot \underbrace{(1 + \ldots + 1)}_{n}}_{m} = \underbrace{(1 + \ldots + 1)}_{m} \cdot \underbrace{(1 + \ldots + 1)}_{n},$$

pa je $\underbrace{1 + \ldots + 1}_{m} = 0$ ili je $\underbrace{1 + \ldots + 1}_{n} = 0$, ali tada lako pokazujemo (kao u propoziciji 2.74) da je $mx = 0$ i $nx = 0$, za sve $x \in P$. Kako je $m, n < mn$ dolazimo u kontradikciju sa činjenicom da je $Char(P) = mn$. □

DEFINICIJA 2.78 *Neka je $(P,+,\cdot)$ prsten i $\emptyset \neq R \subseteq P$. Tada je R nosač potprstena od $(P,+,\cdot)$ ako je $(R,+|_{R^2},\cdot|_{R^2})$ prsten.*

Primer: $(\mathbb{Q},+,\cdot)$ je potprsten od $(\mathbb{R},+,\cdot)$ koji je potprsten od $(\mathbb{C},+,\cdot)$.

PROPOZICIJA 2.79 *Neka je $(P,+,\cdot)$ prsten i $\emptyset \neq R \subseteq P$. Tada je R nosač potprstena od $(P,+,\cdot)$ ako i samo ako je za sve $a,b \in P$ ispunjeno $a-b \in P$ i $ab \in P$.*

Dokaz: Tvrđenje je posledica kriterijuma za domen podgrupe (propozicija 2.36) i potpolugrupe (propozicija 2.19). □

DEFINICIJA 2.80 *Neka je $(P,+,\cdot)$ prsten i $\emptyset \neq I \subseteq P$. Tada je I ideal ako za sve $a,b \in I$ važi $a-b \in I$ i za sve $r \in P$ je $ar, ra \in I$.*

Napomena: Primetimo da svaki ideal jeste domen potprstena, a da obratno ne mora da važi. Nije teško proveriti [8, zadatak 2.4, strana 98] da je $(\mathcal{P}(A),\triangle,\cap)$ prsten za proizvoljan skup A, gde je binarana operacija $\triangle$ definisana sa:

$$X \triangle Y = (X \backslash Y) \cup (Y \backslash X),$$

za sve $X, Y \subseteq A$. Ako je $A = \{a,b\}$ onda je $\{\emptyset, A\}$ nosač potprstena koji nije ideal, jer $\{a,b\} \cap \{a\} = \{a\} \notin \{\emptyset, A\}$.

Ideal u prstenu ima ulogu analognu normalnoj podgrupi u grupama, što ćemo videti u nastavku.

DEFINICIJA 2.81 *Relacija ekvivalencije θ na skupu P se naziva kongruencija prstena $(P,+,\cdot)$ ako za sve $a,b,c,d \in P$ važi ako je $a\theta b$ i $c\theta d$ onda je $(a+b)\ \theta\ (c+d)$ i $ab\,\theta\,cd$. Kraće, kažemo da θ treba da bude kompatibilna sa operacijama $+$ i $\cdot$.*

PROPOZICIJA 2.82 *Ako je ρ kongruencija prstena $(P,+,\cdot)$ sa neutralnim elementom 0 za $+$, onda je $0/\rho$ ideal tog prstena. Ako je I ideal prstena $(P,+,\cdot)$ onda je binarna relacija $\sim_I$ na P definisana sa $a \sim_I b \Leftrightarrow a-b \in I$, za sve $a,b \in P$, kongruencija tog prstena. Za svaki ideal I prstena $(P,+,\cdot)$ važi $I = 0/\sim_I$.*

Dokaz: Neka je ρ kongruencija prstena $(P,+,\cdot)$. Tada $0 \in 0/\rho$, pa je $\emptyset \neq 0/\rho \subseteq P$. Neka $a,b \in 0/\rho$ i $r \in P$. Tada je $a\,\rho\,0$ i $b\,\rho\,0$, pa $b+(-b)\ \rho\ -b$ odnosno $0\,\rho\,-b$, pa je $-b\,\rho 0$. To daje $(a-b)\ \rho\,0$ odnosno $a-b \in 0/\rho$. Takođe je $ra\,\rho\,r\cdot 0$ i $ar\,\rho\,0\cdot r$ pa $ar, ra \in 0/\rho$. Time smo pokazali da je

$0/\rho$ ideal. Neka je sada I ideal datog prstena. Refleksivnost za $\sim_I$ sledi jer $0 \in I$, simetričnost iz činjenice da ako $x \in I$ onda $-x \in I$, za sve $x \in P$, a tranzitivnost zbog zatvorenosti I za $+$. Pokažimo saglasnost za $+$ i $\cdot$. Neka $a, b, c, d \in P$ takvi da je $a \sim_I b$ i $c \sim_I d$, to znači da je $a - b \in I$ i $c - d \in I$. Iz zatvorenosti ideala za $+$ dobijamo $a - b + c - d \in I$, što je ekvivalentno sa $(a+c)-(b+d) \in I$, odnosno $(a+c) \sim_I (b+d)$. Da bi pokazali saglasnost sa $\cdot$, iskoristimo da iz $c \in P$ i $a-b \in I$ dobijamo $(a-b)c \in I$, odnosno $ac-bc \in I$. Analogno, iz $b \in P$ i $c - d \in I$ dobijamo $b(c-d) \in I$, odnosno $bc - bd \in I$. Zbog zatvorenosti I za $+$ imamo $ac - bc + bc - bd \in I$, što daje $ac - bd \in I$, odnosno $ac \sim_I bd$. Jasno, $x \in I \Leftrightarrow x - 0 \in I \Leftrightarrow x \sim_I 0 \Leftrightarrow x \in 0/\sim_I$. □

Teorema 2.83 *Sve kongruencije prstena $(\mathbb{Z}, +, \cdot)$ su kongruencije po modulu.*

Dokaz: Neka je I ideal prstena $(\mathbb{Z}, +, \cdot)$. Uočimo najmanji nenula prirodan broj koji pripada I. Neka je to $n \in \mathbb{N}$. Ako neko $a \in I$, po teoremi 1.27 znamo da postoje $q \in \mathbb{Z}$ i $r \in \{0, \ldots, n-1\}$ takvi da je $a = nq + r$. Odavde je $r = a - nq$, pa kako $n \in I$, to je $nq \in I$, pa je $a - nq \in I$. Zato je $r \in I$, ali $r < n$, pa mora biti $r = 0$. Dakle, $n|a$, a jasno da svi umnošci od n jesu u I. Zato je $I = \{kn \mid k \in \mathbb{Z}\}$ ili kraće $I = n\mathbb{Z}$. Odgovarajuća kongruencija je $\sim_{n\mathbb{Z}}$, gde $a \sim_{n\mathbb{Z}} b$ akko $a - b \in n\mathbb{Z}$ odnosno $a \equiv b \pmod{n}$ ili ekvivalentno $\sim_{n\mathbb{Z}} = \equiv \pmod{n}$. Zbog propozicije 1.42, znamo da svaka kongruencija po modulu jeste kongruencija prstena $(\mathbb{Z}, +, \cdot)$. □

Definicija 2.84 *Neka su $(P, +, \cdot)$ i $(P', +', \cdot')$ dva prstena. Tada je preslikavanje $f : P \to P'$ homomorfizam prstena ako za sve $x, y \in P$ važi $f(x + y) = f(x) +' f(y)$ i $f(x \cdot y) = f(x) \cdot' f(y)$.*

2.5 Mreže i Bulove algebre

Evo jedne drugačije algebarske strukture sa dve binarne operacije.

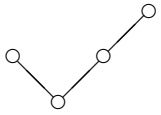
2.5.1 Mreža kao relacijska i algebarska struktura

Definicija 2.85 *Neka je $A \neq \emptyset$ i $\leq$ relacija poretka na skupu A. Ako za svaka dva elementa $a, b \in A$ postoje $inf\{a, b\}$ i $sup\{a, b\}$ onda se relacijska struktura $(A, \leq)$ naziva mreža.*

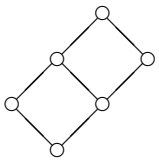
Primeri: $(\mathbb{R}, \leq)$, infimum za dva broja je manji, a supremum veći od njih. $(\mathbb{N}, |)$, infimum za dva prirodna broja je njihov najveći zajednički delilac, a

supremum njihov najmanji zajednički sadržalac. $(\mathcal{P}(A), \subseteq)$, za svaki skup A, ovde je infimum presek, a supremum unija podskupova.

Kao i parcijalna uređenja mreže možemo predstavljati Haseovim dijagramom.



parcijalno uređenje koje nije mreža



Haseov dijagram jedne šestoelementne mreže

Na prethodnoj slici Haseov dijagram levo predstavlja parcijalno uređenje u kome neuporedivi elementi nemaju supremume pa zato nije mreža.

DEFINICIJA 2.86 *Algebarska struktura $(L, \wedge, \vee)$ takva da za sve $x, y, z \in L$ važi:*

1. $x \wedge y = y \wedge x$ *i* $x \vee y = y \vee x$; *(komutativnost)*
2. $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ *i* $(x \vee y) \vee z = x \vee (y \vee z)$; *(asocijativnost)*
3. $x \wedge x = x \vee x = x$; *(idempotentnost)*
4. $(x \wedge y) \vee x = (x \vee y) \wedge x = x$. *(apsorpcija)*

naziva se mreža.

Iz ove definicije vidimo da su operacije $\wedge$ i $\vee$ dualne, što znači da "sve" što važi za jednu važi i za drugu, a dokaz se dobija prepravkom znaka $\wedge$ u znak $\vee$ i obratno.

TEOREMA 2.87 *Neka je $(L, \leq)$ mreža. Tada je (L, inf, sup) takođe mreža. Ako je $(L, \wedge, \vee)$ mreža, tada je $(L, \leq)$, gde je $a \leq b \Leftrightarrow a \wedge b = a$, za sve $a, b \in L$, takođe mreža i pri tom je $a \leq b$ ekvivalentno sa $a \vee b = b$.*

Dokaz: Neka je $(L, \leq)$ mreža, onda jasno važi $inf\{a, b\} = inf\{b, a\}$ i $sup\{a, b\} = sup\{b, a\}$, za sve $a, b \in L$. Još očiglednije važi idempotentost za operacije infimum i supremum. Neka je sada $c = \inf\{a, b\}$, za neke $a, b \in L$.

Dokažimo da je $sup\{c,a\}=a$. Jasno $a\leq sup\{c,a\}$. Kako je $\inf\{a,b\}\leq a$ to je a jedno gornje ograničenje za $\{c,a\}$, pa je $sup\{c,a\}\leq a$. Sada iz anitsimetričnosti za $\leq$ dobijamo da je $a=sup\{inf\{a,b\},a\}$. Analogno se pokazuje da je $a=inf\{sup\{a,b\},a\}$, pa važe zakoni apsorpcije. Neka su sada $a,b,c\in L$. Kako je $inf\{a,b\}\leq b$, to je $inf\{inf\{a,b\},c\}\leq b$. Jasno $inf\{inf\{a,b\},c\}\leq c$, pa je $inf\{inf\{a,b\},c\}\leq inf\{b,c\}$, a kako je $inf\{a,b\}\leq a$, to je $inf\{inf\{a,b\},c\}\leq a$, pa dobijamo $inf\{inf\{a,b\},c\}\leq inf\{a,inf\{b,c\}\}$. Analognim razmatranjem proizilazi $inf\{a,inf\{b,c\}\}\leq inf\{inf\{a,b\},c\}$ odakle zbog antisimetričnosti za $\leq$ sledi asocijativnost za inf. Na sličan način se dokazuje i da je sup asocijatvna operacija.

Neka je sada $(L,\wedge,\vee)$ mreža i binarna relacija $\leq$ na L definisana sa $a\leq b\Longleftrightarrow a\wedge b=a$, za sve $a,b\in L$. Dokažimo da je $\leq$ pre svega relacija poretka. Refleksivnost važi zbog idempotentnosti za $\wedge$. Antisimetričnost sledi iz komutativnosti za $\wedge$, na osnovu definicije za $\leq$. Za dokaz tranzitivnosti neka $a,b,c\in L$ takvi da je $a\leq b$ i $b\leq c$. Tada je $a\wedge b=a$ i $b\wedge c=b$, pa je $a\wedge c=(a\wedge b)\wedge c=a\wedge(b\wedge c)=a\wedge b=a$, pa je $a\leq c$.

Za proizvoljne $a,b\in L$ važi $a\wedge b=a\wedge(a\wedge b)=(a\wedge b)\wedge b$, pa je $a\wedge b$ jedno donje ograničenje za skup $\{a,b\}$. Neka je $c\leq a$ i $c\leq b$. Tada je $c\wedge(a\wedge b)=(c\wedge a)\wedge b=c\wedge b=c$, pa je $c\leq a\wedge b$. Zato je $a\wedge b$ infimum za $\{a,b\}$. Dokažimo sada da je za proizvoljne $a,b\in L$ ispunjeno $a\wedge b=a\Leftrightarrow a\vee b=b$. Ako je $a\wedge b=a$ onda je $a\vee b=(a\wedge b)\vee b=b$, po apsorpciji. Obratno ako je $a\vee b=b$ onda je $a\wedge b=a\wedge(a\vee b)=a$. Dakle $a\leq b$ je ekvivalentno sa $a\vee b=b$, za sve $a,b\in L$. Znajući ovo dokazujemo da je supremum za skup $\{a,b\}\subseteq L$ ustvari $a\vee b$ potpuno dualno dokazu da je infimum za taj skup $a\wedge b$. Zato je $(L,\leq)$ mreža. □

Napomena: Zbog prethodne teoreme ćemo bez eksplicitnog pozivanja koristiti mrežu i kao relacijsku i kao algebarsku strukturu i koristiti poredak na uvedeni način.

Definicija 2.88 *Neka je $(L,\wedge,\vee)$ mreža i $\emptyset\neq L'\subseteq L$. Tada je L' domen podmreže ako je $(L',\wedge|_{L'^2},\vee|_{L'^2})$ mreža.*

Propozicija 2.89 *Neka je $(L,\wedge,\vee)$ mreža i $\emptyset\neq L'\subseteq L$. Tada je L' domen podmreže ako za sve $a,b\in L'$ važi $a\wedge b,a\vee b\in L'$.*

Dokaz: Ako je ispunjen dati uslov onda su $\wedge$ i $\vee$ binarne operacije na skupu L', a kako komutativnost, asocijativnost, idempotentnost i apsorpcija važe na L važe i na njegovom podskupu L'. □

DEFINICIJA 2.90 *Neka su* $(L, \wedge, \vee)$ *i* $(L', \wedge', \vee')$ *dve mreže. Tada je* $f : L \to L'$ *homomorfizam mreža ako za sve* $x, y \in L$ *važi:* $f(x \wedge y) = f(x) \wedge' f(y)$ *i* $f(x \vee y) = f(x) \vee' f(y)$.

PROPOZICIJA 2.91 *Neka je* $(S, \wedge, \vee)$ *mreža. Tada za sve* $x, y, z, t \in S$ *važi:*

1. *Iz* $x \leq y$ *i* $z \leq t$ *sledi* $x \wedge z \leq y \wedge t$ *i* $x \vee z \leq y \vee t$;
2. *Iz* $x \leq z$ *sledi* $x \vee (y \wedge z) \leq (x \vee y) \wedge z$;
3. $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$;
4. $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$.

Dokaz: (1) Pretpostavimo da je $x \leq y$ i $z \leq t$. Tada je $x \wedge y = x$ i $z \wedge t = z$. Odavde je $(x \wedge z) \wedge (y \wedge t) = (x \wedge y) \wedge (z \wedge t) = x \wedge z$. Zato je $x \wedge z \leq y \wedge t$. Dualno pokazujemo deo sa $\vee$ koristeći da je $x \vee y = y$ i $z \vee t = t$.

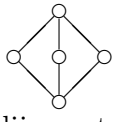
(2) Neka je $x \leq z$. Lako se proverava da važi $y \wedge z \leq z$. Zbog (1) imamo da je $x \vee (y \wedge z) \leq z \vee z = z$. Iz $y \wedge z \leq y$ što lako sledi po definiciji $\leq$ dobijamo koristeći (1) i $x \leq x$ da je $x \vee (y \wedge z) \leq x \vee y$. Sada je $x \vee (y \wedge z) \leq (x \vee y) \wedge z$.

(3) Kako je očito $x \wedge y \leq x$ i $x \wedge z \leq x$ to je $(x \wedge y) \vee (x \wedge z) \leq x \vee x = x$. Slično, $x \wedge y \leq y$ i $x \wedge z \leq z$ pa je $(x \wedge y) \vee (x \wedge z) \leq y \vee z$. Zato važi nejednakost iz tvrđenja. □

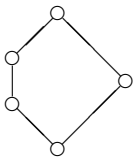
2.5.2 Modularne i distributivne mreže

DEFINICIJA 2.92 *Mreža* $(L, \wedge, \vee)$ *je modularna ako za sve* $x, y, z \in L$ *važi:* $x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z$. *Mreža* $(L, \wedge, \vee)$ *je distributivna ako za sve* $x, y, z \in L$ *važi:* $(x \wedge y) \vee (x \wedge z) = x \wedge (y \vee z)$.

Primer: Mreža M_3 (dijamant) je modularna, ali nije distributivna, a mreža N_5 (pentagon) nije modularna. Mreža $(\mathcal{P}(A), \cap, \cup)$ je distributivna.



M_3 dijamant



N_5 pentagon

Ako u M_3 označimo elemente sa $0, a, b, c, 1$, tako da je 0 najmanji, a 1 najveći element onda je $a \wedge b = a \wedge c = 0$, što daje $(a \wedge b) \vee (a \wedge c) = 0 \neq a = a \wedge 1 = a \wedge (b \vee c)$. Ako na isti način uvedemo oznake elemenata u N_5, pri čemu neka bude $a \leq b$ onda je $a \vee (c \wedge b) = a \vee 0 = a \neq b = 1 \wedge b = (a \vee c) \wedge b$.

PROPOZICIJA 2.93 *Mreža $(L, \wedge, \vee)$ je distributivna ako i samo ako važi: $(x \vee y) \wedge (x \vee z) = x \vee (y \wedge z)$, za sve $x, y, z \in L$.*

Dokaz: ($\Leftarrow$) Koristeći distributivnost računamo $(x \vee y) \wedge (x \vee z) = (x \wedge (x \vee z)) \vee (y \wedge (x \vee z)) = x \vee (y \wedge x) \vee (y \wedge z) = x \vee (y \wedge z)$. ($\Rightarrow$) Dualno prethodnom smeru. □

PROPOZICIJA 2.94 *Svaka distributivna mreža je modularna.*

Dokaz: Neka je $(L, \wedge, \vee)$ distributivna mreža. Pretpostavimo da je $a \leq b$, za neke $a, b, c \in L$. Tada je $a \vee (c \wedge b) = (a \vee c) \wedge (a \vee b) = (a \vee c) \wedge b$, koristeći distributivnost. □

PROPOZICIJA 2.95 *Mreža $(L, \wedge, \vee)$ je modularna ako i samo ako za sve $x, y, z \in L$ važi: $x \wedge ((x \wedge y) \vee z) = (x \wedge y) \vee (x \wedge z)$.*

Dokaz: Neka je $(L, \wedge, \vee)$ modularna mreža. Tada kako je $x \wedge y \leq x$ to važi $((x \wedge y) \vee z) \wedge x = (x \wedge y) \vee (z \wedge x)$, pa iz komutativnosti za $\wedge$ dobijamo traženu jednakost. Neka sada važi $x \wedge ((x \wedge y) \vee z) = (x \wedge y) \vee (x \wedge z)$, za sve $x, y, z \in L$. Tada ako je za neke $a, b, c \in L$ ispunjeno $a \leq c$ onda uvrštavajući $y = a$, $z = b$ i $x = c$ dobijamo $c \wedge (a \vee b) = a \vee (c \wedge b)$. Pa za sve $x, y, z \in L$ važi: $x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z$. □

Sledeće dve teoreme navedene su bez dokaza, da bi se izbeglo nagomilavanje tehničkih detalja. Zainteresovanima preporučujemo da dokaz Dedekindove teoreme pogledaju u [7, Teorema 3.5, strana 23]. Dokaz Birkhofove teoreme može se naći u [4, Teorema 4.6, strana 70].

TEOREMA 2.96 *(Dedekindova) Mreža je modularna ako i samo ako ne sadrži pentagon kao podmrežu.*

TEOREMA 2.97 *(Birkhofova) Mreža je distributivna ako i samo ako ne sadrži ni pentagon ni dijamant kao podmreže.*

PROPOZICIJA 2.98 *Neka je $(L, \wedge, \vee)$ distributivna mreža. Tada za sve $x, y, z \in L$ važi: ako je $x \wedge y = x \wedge z$ i $x \vee y = x \vee z$ onda je $y = z$.*

Dokaz: Pretpostavimo da za neke $a, b, c \in L$ važi $a \wedge b = a \wedge c$ i $a \vee b = a \vee c$. Tada je $b = b \vee (a \wedge b) = b \vee (a \wedge c) = (b \vee a) \wedge (b \vee c) = (c \vee a) \wedge (c \vee b) = c \vee (a \wedge b) = c \vee (a \wedge c) = c$. □

2.5.3 Bulove algebre

DEFINICIJA 2.99 *Neka je $(L, \wedge, \vee)$ distributivna mreža takva da postoje elementi $0, 1 \in L$ za koje je $0 \leq x \leq 1$, za sve $x \in L$. Ako za svako $x \in L$ postoji $y \in L$ tako da važi $x \wedge y = 0$ i $x \vee y = 1$, onda se $(L, \wedge, \vee)$ naziva Bulova algebra.*

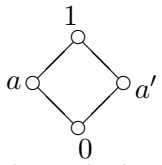
PROPOZICIJA 2.100 *Neka je $(L, \wedge, \vee)$ Bulova algebra, sa najmanjim elementom 0 i najvećim elementom 1. Tada za svako $x \in L$ jedinstveno postoji $y \in L$ tako da je $x \wedge y = 0$ i $x \vee y = 1$.*

Dokaz: Neka za neko $x \in L$ postoje $y, z \in L$ da važi $x \wedge y = 0$ i $x \vee y = 1$, kao i $x \wedge z = 0$ i $x \vee z = 1$. Tada je $x \wedge y = x \wedge z$ i $x \vee y = x \vee z$, pa po propoziciji 2.98 dobijamo $y = z$. □

Zbog prethodnog tvrđenja možemo uvesti pojam komplementa elementa u Bulovoj algebri, koji označavamo sa x', za element x. To je jedinstveno x' takvo da je $x \wedge x' = 0$ i $x \vee x' = 1$. Napomenimo da se Bulova algebra zato može definisati kao distributivna mreža sa najmanjim i najvećim elementom u kojoj svaki element ima komplement. Takođe postoji i definicija Bulove algebre kao algebarske strukture $(B, \wedge, \vee, ', 0, 1)$ gde je $(B, \wedge, \vee)$ distributivna mreža i za sve $x \in B$ važi:

1. $x \wedge 0 = 0$;
2. $x \vee 1 = 1$;
3. $x \wedge x' = 0$;
4. $x \vee x' = 1$.

Primer: Za svaki skup A je $(\mathcal{P}(A), \cap, \cup, ', \emptyset, A)$ Bulova algebra.



Bulova algebra
sa četiri elementa

DEFINICIJA 2.101 *Za dve Bulove algebre $(B, \wedge, \vee)$ i $(B', \wedge', \vee')$ kažemo da su izomorfne, ako postoji homomorfizam odgovarajućih mreža koji je bijekcija.*

TEOREMA 2.102 *(Teorema reprezentacije konačnih Bulovih algebri) Svaka konačna Bulova algebra izomorfna je Bulovoj algebri* $(\mathcal{P}(A), \cap, \cup, ', \emptyset, A)$*, za neki skup* A*.*

Dokaz: Element a neke mreže $(L, \leq)$ sa najmanjim elementom 0 naziva se atom ako je $\{x \in L \mid x \leq a\} = \{0, a\}$. Neka je sada $(B, \wedge, \vee, ', 0, 1)$ Bulova algebra takva da je $A = \{a \in B \mid a \text{ je atom u } B\}$. Definišimo preslikavanje $f : B \to \mathcal{P}(A)$ sa $f(x) = \{y \in A \mid y \leq x\}$. Pokažimo sada da je f izomorfizam Bulovih algebri. Neka $a, b \in B$. Sada $c \in f(a \vee b)$ akko $c \leq a \vee b$ akko $c = c \wedge (a \vee b) = (c \wedge a) \vee (c \wedge b)$ akko $c = c \wedge a$ ili $c = c \wedge b$ akko $c \leq a$ ili $c \leq b$ akko $c \in f(a)$ ili $c \in f(b)$ akko $c \in f(a) \cup f(b)$. Zato je $f(a \vee b) = f(a) \cup f(b)$. Ovde ekvivalencija $c = (c \wedge a) \vee (c \wedge b)$ akko $c = c \wedge a$ ili $c = c \wedge b$ važi jer je c atom. Slično, $c \in f(a \wedge b)$ akko $c \leq a \wedge b$ akko $c \leq a$ i $c \leq b$ akko $c \in f(a)$ i $c \in f(b)$ akko $c \in f(a) \cap f(b)$. Ovde ekvivalencija $c \leq a \wedge b$ akko $c \leq a$ ili $c \leq b$ važi jer je $a \wedge b$ infimum za $\{a, b\}$ i $\wedge$ je saglasno sa $\leq$. Zato je $f(a \wedge b) = f(a) \cap f(b)$. Sirjektivnost za f je posledica činjenice da je $f(a) = \{a\}$, za sve $a \in A$ i homomorfnosti za f. Jasno za sve $a \in A$ važi $a \in f(1) = f(x) \cup f(x')$ i $a \notin f(0) = f(x) \cap f(x')$, pa svaki atom jeste element tačno jednog od skupova $f(x)$ ili $f(x')$, za sve $x \in B$. Nije teško videti da je za svaka dva elementa $x, y \in B$ ispunjeno $x \leq y \Leftrightarrow x \wedge y' = 0$. Zato ako je $x \neq y$ onda bez umanjenja opštosti pretpostavimo da nije $x \leq y$. Tada je $x \wedge y' \neq 0$ pa postoji atom a takav da je $a \leq x$ i $a \leq y'$, ali onda nije $a \leq y$, pa je $f(x) \neq f(y)$. Zato je f injektivno pa je bijekcija. □

Glava 3

Linearna algebra

3.1 Gausov algoritam. Vektorski prostori. Matrice

3.1.1 Sistemi jednačina

DEFINICIJA 3.1 *Neka je $(F, +, \cdot)$ polje, $m, n \in \mathbb{N}$ i $a_{ij}, b_i \in F$, gde $i \in \{1, \ldots, m\}$, a $j \in \{1, \ldots, n\}$. Tada se konjunkcija jednačina*

$$a_{11}x_1 + \ldots + a_{1n}x_n = b_1$$

$$a_{21}x_1 + \ldots + a_{2n}x_n = b_2$$

$$\ldots\ldots\ldots\ldots$$

$$a_{m1}x_1 + \ldots + a_{mn}x_n = b_m$$

naziva sistem jednačina sa n nepoznatih $x_1, \ldots, x_n$, $a_{11}, \ldots, a_{mn}$ su koeficijenti, a $b_1, \ldots, b_m$ se nazivaju slobodni članovi. Rešenje navedenog sistema je svaka n-torka $(\alpha_1, \ldots, \alpha_n)$ elemenata iz F takva da kada uvrstimo umesto x_1 element α_1,..., umesto x_n element α_n u svaku od jednačina dobijamo tačne jednakosti. Ako takva n-torka ne postoji sistem se naziva protivrečan ili nesaglasan, a ako postoji naziva se neprotivrečan ili saglasan sistem. Saglasni sistemi koji imaju tačno jedno rešenje nazivaju se određeni, a koji imaju više rešenja nazivaju se neodređeni. Ukoliko je $m = n$ sistem se naziva kvadratni.

Primeri: Sistem $x + 2y = 3$ nad poljem realnih brojeva je saglasan, ali neodređen jer su rešenja svi uređeni parovi realnih brojeva $(3 - 2t, t)$, gde $t \in \mathbb{R}$. Kažemo još i da je ovaj sistem neodređen sa jednim stepenom

slobode, jer jednu nepoznatu možemo birati po volji iz skupa realnih brojeva, a onda je druga nepoznata jednoznačno određena. Međutim sistem $x+2y = 3 \wedge 2x + 4y = 4$ je protivrečan jer nema rešenja.

Definicija 3.2 *Ukoliko su u sistemu jednačina svi slobodni članovi jednaki nuli takav sistem se naziva homogen sistem.*

Napomena: Homogen sistem je uvek saglasan jer ima bar jedno rešenje $(0, \ldots, 0)$. To rešenje se naziva trivijalno rešenje.

Definicija 3.3 *Dva sistema jednačina nad istim poljem i istim brojem nepoznatih nazivamo ekvivalentnim ako imaju isti skup rešenja.*

Propozicija 3.4 *Svaki sistem se može svesti na oblik takav da su sa desne strane jednakosti u svakoj od jednačina nule. U novonastalom sistemu ako pomnožimo bilo koju jednačinu nenula elementom polja dobijamo ekvivalentan sistem. Takođe ako bilo kojoj jednačini dodamo neku drugu prethodno pomnoženu bilo kojim elementom polja dobijamo ekvivalentan sistem.*

Dokaz: Neka je dati sistem nad poljem $(F, +, \cdot)$. Označimo leve strane jednačina sa L, a desne sa D. Tada svaka jednačina posmatranog sistema ima oblik $L = D$, a kako je $D \in F$ i $(F, +)$ grupa to je $L = D \Leftrightarrow L - D = 0$. Ako je u novonastalom sistemu neka jednačina $J = 0$ i $k \in F\backslash\{0\}$ onda je $kJ = 0 \Leftrightarrow J = 0$ i konačno ako su $J_1 = 0$ i $J_2 = 0$ dve jednačine novonastalog sistema onda je $J_1 + kJ_2 = 0 + k \cdot 0 = 0 + 0 = 0$. Ako je $J_1 + kJ_2 = 0 \wedge J_2 = 0$ onda je $J_1 = 0$. Zato je $J_1 = 0 \wedge J_2 = 0 \Leftrightarrow J_1 + kJ_2 = 0 \wedge J_2 = 0$. □

Definicija 3.5 *Elementarnom transformacijom sistema nazivamo:*

1. *zamenu mesta dveju jednačina sistema;*
2. *množenje neke jednačine elementom odgovarajućeg polja različitim od nule;*
3. *dodavanje neke jednačine prethodno pomnožene nekim elementom odgovarajućeg polja nekoj drugoj jednačini.*

Posledica 3.6 *Svakom elementarnom transformacijom se sistem prevodi u ekvivalentan sistem.*

Dokaz: Sledi iz prethodne definicije i propozicije 3.4. Prva elementarna transformacija ostavlja sistem ekvivalentan polaznom zbog asocijativnosti i komutativnosti konjunkcije. □

Gausov postupak se sastoji u tome da primenom elementarnih transformacija od polaznog sistema dobijemo ekvivalentan sistem koji ima "trougaoni" ili "trapezni" oblik. Preciznije ako je sistem sa n nepoznatih i m jednačina, k-ti korak se sastoji od sledećih potkoraka:

1. Među jednačinama od k. do m. uočimo jednačinu kod koje je neki koeficijent različit od nule. Ukoliko takav koeficijent ne postoji postupak se završava.

2. Zamenimo mesta odgovarajućih jednačina tako da uočena jednačina bude na k. mestu i zamenimo mesta promenljivih tako da promenljiva uz uočeni nenula koeficijent bude k. po redu.

3. Dodavanjem sad k. jednačine prethodno pomnožene sa odgovarajućim koeficijentom svim ostalim jednačinama eleminišemo nepoznatu x_k iz $k+1$. do m. jednačine.

4. Ukoliko je $k < m$ prelazimo na $k+1$. korak.

Ishod Gausovog algoritma je sledeći:

Ukoliko je postupak završen u 4. potkoraku tada je dobijeni sistem ekvivalentan polaznom sistemu trougaoni:

$$\begin{aligned} a'_{11}x_1 + a'_{22}x_2 + \ldots + a'_{1m}x_m &= b'_1 \\ a'_{22}x_2 + \ldots + a'_{2m}x_m &= b'_2 \\ \ldots & \\ a'_{mm}x_m &= b'_m \end{aligned}$$

i tada iz poslednje jednačine dobijamo x_m jedinstveno, pa iz pretposlednje x_{m-1} jedinstveno i tako redom do prve jednačine koja će za poznate $x_2, \ldots, x_m$, dati x_1 jedinstveno i sistem je saglasan i određen.

Ukoliko se postupak završio u 1. potkoraku nekog k. koraka tada su svi koeficijenti uz $x_{k+1}, \ldots, x_m$ u jednačinama od $k+1$. do m. jednaki nuli. Ukoliko je bar jedan od slobodnih članova u jednačinama $k+1$. do m. različit od nule dobijamo protivrečan sistem. Ukoliko su slobodni članovi u svim tim jednačinama jednaki nuli (trapezni sistem) sistem je saglasan, ali neodređen i birajući proizvoljno vrednosti iz polja za $x_{k+1}, \ldots, x_n$ dobijamo jedinstvene vrednosti za nepoznate $x_1, \ldots, x_k$.

Primer: Rešimo sistem jednačina:

$$x + y + 2z = 5$$

$$\begin{aligned} x+2y+z &= 0 \\ 2x+y+z &= 3 \end{aligned}$$

Kako je u prvoj jednačini koeficijent uz x jedan (različit od nule) eleminisaćemo x is druge jednačine tako što ćemo dodati prvu jednačinu drugoj prethodno pomnoženu sa -1 i dobijamo:

$$\begin{aligned} x+y+2z &= 5 \\ y-z &= -5 \\ 2x+y+z &= 3 \end{aligned}$$

Zatim ćemo eleminisati x is treće jednačine tako što ćemo dodati prvu jednačinu trećoj prethodno pomnoženu sa -2 i dobijamo:

$$\begin{aligned} x+y+2z &= 5 \\ y-z &= -5 \\ -y-3z &= -7 \end{aligned}$$

Time je završen prvi korak, prelazimo na drugi korak Gausovog postupka. Sada posmatramo drugu i treću jednačinu. Kako je u drugoj jednačini koeficijent uz y jedan (različit od nule) eleminisaćemo y iz treće jednačine. Zato ćemo drugu jednačinu dodati trećoj. Tako dobijamo:

$$\begin{aligned} x+y+2z &= 5 \\ y-z &= -5 \\ -4z &= -12 \end{aligned}$$

Na taj način dobijamo trougaoni sistem i time je Gausov postupak završen. Sada iz treće jednačine dobijamo $z=3$, iz druge dobijamo da je $y=-2$, a onda uvrštavajući to u prvu jednačinu dobijamo da je $x=1$. Jedinstveno rešenje posmatranog sistema jednačina je $(x,y,z)=(1,-2,3)$.

3.1.2 Vektorski prostori

Definicija 3.7 *Neka je $(V,+)$ Abelova grupa, $(F,+,\cdot)$ polje i operacija skalarnog množenja kao preslikavanje iz $F\times V$ u V u oznaci αv, za $\alpha\in F$ i $v\in V$ zadovoljava:*

1. $\alpha(x+y)=\alpha x+\alpha y$;

2. $(\alpha+\beta)x = \alpha x + \beta x$*;*

3. $(\alpha\beta)x = \alpha(\beta x)$*;*

4. $1x = x$*,*

za sve $x, y \in V$ *i* $\alpha, \beta \in F$*, gde je* $1 \in F$ *jedinica polja* $(F, +, \cdot)$*, onda kažemo da* $(V, +)$ *čini vektorski prostor nad poljem* $(F, +, \cdot)$*. Elemente polja* F *nazivamo skalari, a elemente Abelove grupe* V *vektori.*

Primeri: Vektori u geometriji koji se sabiraju po pravilu paralelograma, a množe realnim brojem na uobičajeni način čine vektorski prostor nad poljem realnih brojeva. Takođe za proizvoljno polje $(F, +, \cdot)$, za svako $n \in \mathbb{N}$ je $(F^n, \oplus)$ vektorski prostor nad poljem F gde je:

$$(a_1, \ldots, a_n) \oplus (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$

$$\alpha(a_1, \ldots, a_n) = (\alpha a_1, \ldots, \alpha a_n),$$

za sve $a_1, \ldots, a_n, b_1, \ldots, b_n, \alpha \in F$.

Propozicija 3.8 *Neka je* $(V, +)$ *vektorski prostor nad poljem* F*. Tada je*

1. $\alpha 0 = 0$*;*

2. $0x = 0$*;*

3. $(-\alpha)x = -(\alpha x) = \alpha(-x)$*;*

4. $\alpha x = 0 \Rightarrow \alpha = 0 \vee x = 0$*,*

za sve $x \in V$ *i* $\alpha \in F$*.*

Dokaz: 1. $\alpha 0 = \alpha(0+0) = \alpha 0 + \alpha 0$, pa je $\alpha 0$ idempotent u grupi $(V, +)$, pa je $\alpha 0 = 0$.

2. Analogno 1.

3. $0 = 0x = (\alpha + (-\alpha))x = \alpha x + (-\alpha)x$, pa je $(-\alpha)x$ suprotan za αx. Slično pokazujemo $-(\alpha x) = \alpha(-x)$.

4. Neka je $\alpha x = 0$ i $\alpha \neq 0$. Tada postoji $\alpha^{-1} \in F$, pa je $x = 1x = \alpha^{-1}\alpha x = \alpha^{-1}0 = 0$ koristeći 1. □

Definicija 3.9 *Neka je* $(V, +)$ *vektorski prostor nad poljem* F*,* $n \in \mathbb{N}$*,* $v_1, \ldots, v_n \in V$ *i* $\alpha_1, \ldots, \alpha_n \in F$*. Tada je* $\alpha_1 v_1 + \ldots + \alpha_n v_n$ *linearna kombinacija vektora* $v_1, \ldots, v_n$*. Vektori* $v_1, \ldots, v_n$ *se nazivaju linearno zavisni ako postoji linearna kombinacija jednaka nuli u kojoj nisu svi skalari jednaki nuli, inače su vektori* $v_1, \ldots, v_n$ *linearno nezavisni.*

Primer: U geometriji su dva kolinearna vektora linearno zavisni, a tri nekomplanarna vektora linearno nezavisni.

DEFINICIJA 3.10 *Neka je $(V,+)$ vektorski prostor nad poljem F, $n \in \mathbb{N}$. Skup $\{v_1,\ldots,v_n\}$ vektora je baza vektorskog prostora V ako su $v_1,\ldots,v_n$ linearno nezavisni vektori tako da su za svaki vektor $u \in V$ vektori $v_1,\ldots,v_n,u$ linearno zavisni.*

TEOREMA 3.11 *Neka je $\{v_1,\ldots,v_n\}$ baza vektorskog prostora $(V,+)$ nad poljem F. Tada za svaki vektor $x \in V$ jedinstveno postoje skalari $\alpha_1,\ldots,\alpha_n$ u F takvi da je $x = \alpha_1 v_1 + \ldots + \alpha_n v_n$.*

Dokaz: Jasno je da je prikazivanje nula vektora kao linearne kombinacije vektora $v_1,\ldots,v_n$ jedinstveno zbog linearne nezavisnosti baze. Kako je $\{v_1,\ldots,v_n\}$ baza to su vektori $v_1,\ldots,v_n,x$, za svako $x \in V$ linearno zavisni, pa postoje skalari $\alpha_1,\ldots,\alpha_{n+1} \in F$ od kojih bar jedan nije nula takvi da je $\alpha_1 v_1 + \ldots + \alpha_{n+1} x = 0$. Ako je $\alpha_{n+1} = 0$ onda dobijamo da su vektori baze linearno zavisni. Zato je $\alpha_{n+1} \neq 0$, pa je $x = -\frac{\alpha_1}{\alpha_{n+1}} v_1 + \ldots + (-\frac{\alpha_n}{\alpha_{n+1}} v_n)$. Ako je $x = \alpha_1 v_1 + \ldots + \alpha_n v_n$ i $x = \beta_1 v_1 + \ldots + \beta_n v_n$, za neke $\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_n \in F$ takve da postoji $i \in \{1,\ldots,n\}$ takvo da je $\alpha_i \neq \beta_i$ onda se nula vektor može prikazati kao linearna kombinacija na dva načina. Kontradikcija. □

DEFINICIJA 3.12 *Ako vektorski prostor $(V,+)$ sadrži n, $n \in \mathbb{N}$, linearno nezavisnih vektora, a svakih $n+1$ vektora su linearno zavisni, onda kažemo da taj vektorski prostor ima dimenziju n i pišemo $dimV = n$.*

POSLEDICA 3.13 *U vektorskom prostoru dimenzije n, $n \in \mathbb{N}$, sve baze imaju n elemenata.*

Dokaz: Direktno iz definicije baze i definicije dimenzije. □

Primer: Tri jedinična međusobno ortogonalna vektora su baza vektora u geometriji.

DEFINICIJA 3.14 *Neka je $(V,+)$ vektorski prostor nad poljem F. Tada je $f : V \to V$ linearna transformacija vektorskog prostora V ako za sve $x,y \in V$ i $\alpha \in F$ važi:*

$$f(x+y) = f(x) + f(y)$$

$$f(\alpha x) = \alpha f(x)$$

Napomena: linearna transformacija je ustvari endomorfizam (homomorfizam u sebe sama) vektorskog prostora.

PROPOZICIJA 3.15 *Neka je $(V,+)$ vektorski prostor nad poljem F i $f : V \to V$ linearna transformacija. Tada je $f(0) = 0$.*

Dokaz: $f(0) = f(0+0) = f(0) + f(0)$, pa je $f(0)$ idempotent u grupi $(V,+)$. Zato važi tvrđenje. □

TEOREMA 3.16 *Neka je $\{e_1, \ldots, e_n\}$, za $n \in \mathbb{N}$, baza vektorskog prostora $(V,+)$ nad poljem F i f i g dve linearne transformacije iz V u V. Ako je $f(e_i) = g(e_i)$, za sve $i \in \{1, \ldots, n\}$ onda je $f = g$.*

Dokaz: Neka je $x \in V$. Tada jedinstveno postoje $\alpha_1, \ldots \alpha_n \in F$ po teoremi 3.11 takvi da je $x = \alpha_1 e_1 + \ldots + \alpha_n e_n$. Sada koristeći linearnost za f i g dobijamo: $f(x) = f(\alpha_1 e_1 + \ldots + \alpha_n e_n) = \alpha_1 f(e_1) + \ldots + \alpha_n f(e_n) = \alpha_1 g(e_1) + \ldots + \alpha_n g(e_n) = g(\alpha_1 e_1 + \ldots + \alpha_n e_n) = g(x)$. □

3.1.3 Matrice

DEFINICIJA 3.17 *Neka $m, n \in \mathbb{N}$ i neka je $(F,+,\cdot)$ polje. Tada pravougaonu šemu*

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix},$$

gde $a_{ij} \in F$, za sve $i \in \{1, \ldots, m\}$ i $j \in \{1, \ldots, n\}$ nazivamo matrica formata $m \times n$ i označavamo kraće sa $[a_{ij}]_{m\times n}$. Ako je $m = n$ onda matricu $[a_{ij}]_{m\times n}$ nazivamo kvadratna. Matrica čiji su svi elementi nule naziva se nula matrica. Matrica čiji su svi elementi van glavne dijagonale nule, a na glavnoj dijagonali su svi elementi jednaki jedinici se naziva jedinična matrica. Dve matrice su jednake ako su istog formata i ako su im odgovarajući elementi jednaki. Skup svih matrica formata $m \times n$ nad unapred određenim poljem označavaćemo sa $\mathcal{M}_{m,n}$.

DEFINICIJA 3.18 *Neka $m, n, p \in \mathbb{N}$ i neka je $(F,+,\cdot)$ polje. Tada je*

1. $[a_{ij}]_{m\times n} + [b_{ij}]_{m\times n} = [a_{ij} + b_{ij}]_{m\times n}$,
2. $\alpha[a_{ij}]_{m\times n} = [\alpha a_{ij}]_{m\times n}$ *i*

3. $[a_{ij}]_{m\times n}\cdot[b_{ij}]_{n\times p}=[c_{ij}]_{m\times p}$*, gde je* $c_{ij}=\Sigma_{k=1}^{n}a_{ik}b_{kj}$*,*

za sve $a_{ij},b_{ij},\alpha\in F$*.*

Teorema 3.19 *Neka* $m,n\in\mathbb{N}$ *i neka je* $(F,+,\cdot)$ *polje. Tada je*

1. $(\mathcal{M}_{m,n},+)$ *Abelova grupa.*

2. $(\mathcal{M}_{n,n},+,\cdot)$ *prsten.*

3. $(\mathcal{M}_{m,n},+)$ *vektorski prostor nad poljem* F*.*

Dokaz: 1. $(\mathcal{M}_{m,n},+)$ je grupa jer je nula matrica neutralni element, matrica čiji su svi elementi suprotni odgovarajućim inverzni element za $+$, a asocijativnost i komutativnost sa lako proveravaju koristeći da važe u polju i definiciju.

2. Koristeći 1. ostaje da ispitamo asocijativnost za množenje kvadratnih matrica i distributivnost množenja prema sabiranju kvadratnih matrica. Neka $[a_{ij}],[b_{ij}],[c_{ij}]\in\mathcal{M}_{n,n}$. Sada je $[a_{ij}]([b_{ij}]+[c_{ij}])=[a_{ij}][b_{ij}+c_{ij}]=[\Sigma_{k=1}^{n}a_{ik}(b_{kj}+c_{kj})]=[\Sigma_{k=1}^{n}a_{ik}b_{kj}+\Sigma_{k=1}^{n}a_{ik}c_{kj}]=[\Sigma_{k=1}^{n}a_{ik}b_{kj}]+[\Sigma_{k=1}^{n}a_{ik}c_{kj}]=[a_{ij}][b_{ij}]+[a_{ij}][c_{ij}]$, čime je pokazana distributivnost množenja prema sabiranju. Pokažimo još asocijativnost množenja:

$([a_{ij}][b_{ij}])[c_{ij}]=[\Sigma_{k=1}^{n}a_{ik}b_{kj}][c_{ij}]$
$=[\Sigma_{t=1}^{n}(\Sigma_{k=1}^{n}a_{ik}b_{kt})c_{tj}]$
$=[\Sigma_{t=1}^{n}\Sigma_{k=1}^{n}(a_{ik}b_{kt})c_{tj}]$
$=[\Sigma_{t=1}^{n}\Sigma_{k=1}^{n}a_{ik}(b_{kt}c_{tj})]$
$=[\Sigma_{k=1}^{n}\Sigma_{t=1}^{n}a_{ik}(b_{kt}c_{tj})]$
$=[\Sigma_{k=1}^{n}a_{ik}\Sigma_{t=1}^{n}(b_{kt}c_{tj})]$
$=[a_{ij}][\Sigma_{t=1}^{n}(b_{it}c_{tj})]$
$=[a_{ij}]([b_{ij}][c_{ij}])$.

3. Na osnovu 1. je $(\mathcal{M}_{m,n},+)$ Abelova grupa. Osobine množenja skalarom slede direktno na osnovu definicije množenja matrice elementom polja i na osnovu asocijativnosti množenja i distributivnosti za množenje prema sabiranju u polju. □

Definicija 3.20 *Neka je* $(F,+,\cdot)$ *polje i* $m,n\in\mathbb{N}$*. Tada za* $[a_{ij}]\in\mathcal{M}_{m,n}$ *definišemo* $[a_{ij}]^T\in\mathcal{M}_{n,m}$ *sa* $[a_{ij}]^T=[b_{ij}]$*, gde je* $b_{ij}=a_{ji}$*, za svako* $i\in\{1,\dots,n\}$ *i* $j\in\{1,\dots,m\}$*. Matricu* $[b_{ij}]_{n\times m}$ *nazivamo transponovana matrica matrice* $[a_{ij}]_{m\times n}$*.*

Zbog teoreme 3.16 svakom matricom je jednoznačno određena jedna linearna transformacija. Naime znamo da je dovoljno odrediti slike vektora baze i time je jedinstveno određena linearna transformacija, ali slike vektora baze možemo na jedinstven način predstaviti kao linearne kombinacije vektora te iste baze. Sada koeficijente upisujemo kao odgovarajuće vektor kolone u matricu i time formiramo matricu polazne linearne transformacije.

Neka je $v_1, \ldots, v_n$ baza nekog vektorskog prostora $(V, +)$ nad poljem F. Proizvoljan vektor $x \in V$ predstavimo kao linearnu kombinaciju vektora baze na jedinstven način

$$x = x_1 v_1 + \ldots + x_n v_n$$

ili kao $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, što nekad zovemo vektor kolona. Ako je A linearna transformacija takva da je:

$$A(v_j) = \alpha_{1j} v_1 + \ldots + \alpha_{nj} v_n,$$

za sve $j \in \{1, \ldots, n\}$, onda matricu te linearne transformacije u oznaci $[A]$ dobijamo kao $[\alpha_{ij}]_{n \times n}$. Pokažimo da je $[A(x)] = [A][x]$. Izračunajmo $A(x) = x_1 A(v_1) + \ldots + x_n A(v_n) = x_1(\alpha_{11} v_1 + \ldots + \alpha_{n1} v_n) + \ldots + x_n(\alpha_{1n} v_1 + \ldots + \alpha_{nn} v_n) = (x_1\alpha_{11} + \ldots + x_n\alpha_{1n})v_1 + \ldots + (x_1\alpha_{n1} + \ldots + x_n\alpha_{nn})v_n$, pa je $[A(x)] = \begin{bmatrix} x_1\alpha_{11} + \ldots + x_n\alpha_{1n} \\ \vdots \\ x_1\alpha_{n1} + \ldots + x_n\alpha_{nn} \end{bmatrix} = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \ldots & \alpha_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$.

3.2 Determinante

Podsetimo se da je permutacija nekog konačnog skupa ustvari bijekcija tog konačnog skupa u sebe sama i da sve permutacije na nekom konačnom skupu u odnosu na kompoziciju preslikavanja čine grupu koju još nazivamo i grupa permutacija.

Definicija 3.21 *Ako je za neku permutaciju $\pi : \{1, \ldots, n\}$ ispunjeno $i < j$, a $\pi(i) > \pi(j)$, za neke $i, j \in \{1, \ldots, n\}$, onda kažemo da permutacija π ima inverziju (ij). Ukoliko je broj inverzija neke permutacije paran, onda je ta permutacija parna, a inače je neparna.*

Primer: Permutacija $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ ima dve inverzije: (12) i (13) i zato je parna.

DEFINICIJA 3.22 *Neka je $n \in \mathbb{N}$ i $A = [a_{ij}]_{n\times n}$ kvadratna matrica nad poljem $(F, +, \cdot)$. Tada je determinanta matrice A u oznaci $|A|$ ili $detA$ jednaka sa*

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \sum_{\pi\in S_n} (-1)^{Inv\pi} a_{1\pi(1)} \cdot \ldots \cdot a_{n\pi(n)}.$$

Primer: $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \sum_{\pi\in S_2}(-1)^{Inv\pi} a_{1\pi(1)}a_{2\pi(2)} = a_{11}a_{22} - a_{12}a_{21}$. Kraće kažemo da determinantu reda dva računamo tako što od proizvoda elemenata na glavnoj dijagonali oduzmemo proizvod elemenata na sporednoj dijagonali.

Primer: $\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \sum_{\pi\in S_3}(-1)^{Inv\pi} a_{1\pi(1)}a_{2\pi(2)}a_{3\pi(3)}$

$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$.

Ovo pravilo za računanje determinante trećeg reda naziva se Sarusovo pravilo i često se formuliše na sledeći način. Prve dve kolone determinante prepišemo sdesna, a onda od proizvoda elementa na glavnoj dijagonali sabranoj sa proizvodima elemenata na njoj dvema paralelnim dijagonalama oduzimamo proizvode elemenata na sporednim dijagonalama.

PROPOZICIJA 3.23 *Determinanta neke matrice jednaka je determinanti njoj transponovane matrice.*

Zahvaljujući prethodnom tvrđenju naredna ćemo formulisati za vrste, a važiće analogna tvrđenja i za kolone.

PROPOZICIJA 3.24 *Determinanta matrice koja ima dve jednake vrste jednaka je nuli.*

PROPOZICIJA 3.25 *Ako sve elemente jedne vrste neke matrice pomnožimo nekim elementom $\lambda \neq 0$ onda se vrednost determinante dobija tako što se determinanta polazne matrice množi sa λ.*

Dokaz: U svakom sabirku u izrazu za determinantu se javlja tačno jedan element uočene vrste i svaki od njih se javlja tačno jednom, pa zbog distributivnosti množenja prema sabiranju u polju taj element izvlačimo ispred zagrade. □

Za dve vrste (kolone) matrice kažemo da su proporcionalne, ako se elementi jedne dobijaju od elemenata druge množenjem nekom konstantom različitom od nule.

Propozicija 3.26 *Ako su dve vrste matrice proporcionalne onda je determinanta te matrice jednaka nuli.*

Dokaz: Posledica tvrđenja 3.24 i 3.25. □

Propozicija 3.27 *Zbir dve determinante matrica koje imaju sve jednake odgovarajuće elemente sem na i-toj vrsti jednaka je determinanti matrice koja ima sve jednake elemente polaznim matricama na svim vrstama sem i-te, a na i-toj vrsti su elementi jednaki zbirovima odgovarajućih elemenata polaznih matrica.*

Dokaz: Kao i u dokazu propozicije 3.25 u svakom sabirku u izrazu za determinantu se javlja tačno jedan element uočene vrste i svaki od njih se javlja tačno jednom, pa zbog distributivnosti množenja prema sabiranju u polju svaki od sabiraka možemo napisati kao zbir dva od kojih je jedan iz prve, a jedan iz druge matrice na odgovarajućoj poziciji, pa suma postaje suma dva izraza za determinante prve i druge matrice od kojih smo pošli. □

Propozicija 3.28 *Vrednost determinante se ne menja ako u odgovarajućoj matrici elementima jedne vrste dodamo prethodno pomnožene nekim elementom, odgovarajuće elemente neke druge vrste.*

Dokaz: Na osnovu propozicija 3.26 i 3.27. □

Propozicija 3.29 *Ako zamenimo mesta dvama vrstama neke matrice njena determinanta menja znak.*

Dokaz: Koristićemo propoziciju 3.28 više puta. Ako želimo zameniti mesta i-toj i j-toj vrsti onda tako dobijenu determinantu možemo dobiti tako što i-toj vrsti najpre dodamo j-tu vrstu pa u tako dobijenoj matrici, novu i-tu vrstu oduzmemo od j-te i onda konačno tu j-tu vrstu dodamo

i-toj vrsti novonastale matrice. Sad matrica ima u i-toj vrsti elemente j-te vrste polazne matrice, a u j-toj vrsti elemente i-te vrste polazne matrice sa promenjenim znakom. Koristeći propoziciju 3.25 kompletiramo dokaz. □

Sledeću teoremu navodimo bez dokaza. Dokaz se može pogledati u [6, Teorema 8.4.3 2), strana 188].

Teorema 3.30 *Za dve kvadratne matrice A i B istog formata nad istim poljem važi: $|AB| = |A||B|$.*

Definicija 3.31 *Minor M_{ij} koji odgovara elementu a_{ij} neke kvadratne matrice formata $n \times n$, za $n \in \mathbb{N}$ dobija se kao determinanta matrice koja je od polazne nastala tako što su izbačene i-ta vrsta i j-ta kolona. Algebarski komplement elementa a_{ij} je $(-1)^{i+j}M_{ij}$.*

Teorema 3.32 *(Laplasova teorema) Neka je $[a_{ij}]_{n\times n}$, $n \in \mathbb{N}$, kvadratna matrica nad nekim poljem. Tada je*

$$|[a_{ij}]_{n\times n}| = \sum_{j=1}^{n} a_{ij}A_{ij},$$

za svako $i \in \{1, \ldots, n\}$. Takođe, $\sum_{j=1}^{n} a_{ij}A_{kj} = 0$, za $i \neq k$.

Dokaz: Teoremu ćemo dokazati najpre za $i = 1$ da važi. Sve permutacije skupa $\{1, \ldots, n\}$ razbijamo na klase prema tome gde se preslikava 1. Ako je $\pi(1) = k$, tada ostali elementi $(\pi(2), \ldots, \pi(n))$ čine permutaciju skupa $\{1, \ldots, n\}\backslash\{k\}$. Označimo to preslikavanje sa π'. Primetimo da je $Inv\pi = k - 1 + Inv\pi'$. Sada je

$$\sum_{\pi\in S_n} (-1)^{Inv\pi} a_{1\pi(1)} \cdot \ldots \cdot a_{n\pi(n)}$$

$$= \sum_{k=1}^{n} \Big(\sum_{\pi\in S_n, \pi(1)=k} (-1)^{Inv\pi} a_{1k}a_{2\pi(2)} \cdot \ldots \cdot a_{n\pi(n)} \Big)$$

$$= \sum_{k=1}^{n} \Big(\sum_{\pi\in S_n, \pi(1)=k} (-1)^{k-1+Inv\pi'} a_{1k}a_{2\pi(2)} \cdot \ldots \cdot a_{n\pi(n)} \Big)$$

$$= \sum_{k=1}^{n} a_{1k}(-1)^{1+k} \Big(\sum_{\pi\in S_n, \pi(1)=k} (-1)^{Inv\pi'} a_{2\pi(2)} \cdot \ldots \cdot a_{n\pi(n)} \Big)$$

$$= \sum_{k=1}^{n} a_{1k}(-1)^{1+k}\Big(\sum_{\pi' \in S'_{n-1}} (-1)^{Inv\pi'} a_{2\pi'(2)} \cdot \ldots \cdot a_{n\pi'(n)}\Big)$$

$$= \sum_{k=1}^{n} a_{1k}(-1)^{1+k} M_{1k} = \sum_{k=1}^{n} a_{1k} A_{1k}.$$

Za $i \in \{2, \ldots, n\}$ dokazujemo tako što najpre zamenimo mesta i-te i prve vrste, ali tako što menjamo mesta $i-1$ puta pomerajući i-tu vrstu ka prvoj u svakoj zameni sa vrstom iznad. Za $i \neq k$ vidimo da je to Laplasov razvoj determinante u kojoj su i-ta i k-ta vrsta jednake, pa je po propoziciji 3.24 ta determinanta jednaka nuli. □

Determinante igraju važnu ulogu u određivanju prirode rešenja kvadratnih sistema jednačina. Determinantu kvadratnog sistema dobijamo kada upišemo koeficijente tog sistema redom kao elemente matrice i onda nađemo njenu determinantu.

Teorema 3.33 *(Kramerova) Ako je determinanta D kvadratnog sistema jednačina sa n nepoznatih, $n \in \mathbb{N}$ različita od nule, onda taj sistem ima jedinstveno rešenje. Ako sa D_i označimo determinantu dobijenu od determinante sistema tako što su koeficijenti uz nepoznatu x_i zamenjeni odgovarajućim slobodnim čalanovima, onda važi $x_i = \frac{D_i}{D}$, za sve $i \in \{1, \ldots, n\}$.*

Dokaz: Dokazaćemo teoremu za kvadratni sistem sa tri nepoznate. Dakle posmatramo sistem

$$a_{11}x + a_{12}y + a_{13}z = b_1$$

$$a_{21}x + a_{22}y + a_{23}z = b_2$$

$$a_{31}x + a_{32}y + a_{33}z = b_3$$

Pretpostavimo da je (x, y, z) rešenje tog sistema. Sada računamo $xD = x\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a_{11}x & a_{12} & a_{13} \\ a_{21}x & a_{22} & a_{23} \\ a_{31}x & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} b_1 - a_{12}y - a_{13}z & a_{12} & a_{13} \\ b_2 - a_{22}y - a_{23}z & a_{22} & a_{23} \\ b_3 - a_{32}y - a_{33}z & a_{32} & a_{33} \end{vmatrix} = D_1$, kada prvoj koloni dodamo drugu pomnoženu sa y, a treću pomnoženu sa z, po propoziciji 3.28 i 3.29. Analogno pokazujemo da je $yD = D_2$ i $zD = D_3$. Ako je $D \neq 0$ onda je svako rešenje oblika navedenog u tvrđenju. Dokažimo još da $(\frac{D_1}{D}, \frac{D_2}{D}, \frac{D_3}{D})$ jeste rešenje. Zamenimo $x = \frac{D_1}{D}$, $y = \frac{D_2}{D}$ i $z = \frac{D_3}{D}$ u prvu jednačinu. Dobijamo:

$$a_{11}\frac{D_1}{D} + a_{12}\frac{D_2}{D} + a_{13}\frac{D_3}{D} = \frac{1}{D}(a_{11}D_1 + a_{12}D_2 + a_{13}D_3)$$

$$= \frac{1}{D}(a_{11}(b_1A_{11} + b_2A_{21} + b_3A_{31}) + a_{12}(b_1A_{12} + b_2A_{22} + b_3A_{32})$$
$$+a_{13}(b_1A_{13} + b_2A_{23} + b_3A_{33})$$
$$= \frac{1}{D}(b_1(a_{11}A_{11} + a_{12}A_{12} + a_{13}A_{13}) + b_2(a_{11}A_{21} + a_{12}A_{22} + a_{13}A_{23})$$
$$+b_3(a_{11}A_{31} + a_{12}A_{32} + a_{13}A_{33}))$$
$$= \frac{1}{D}b_1(a_{11}A_{11} + a_{12}A_{12} + a_{13}A_{13}) = b_1.$$

Analogno pokazujemo da su druga i treća jednakost tačne. □

Posledica 3.34 *Ako kvadratni homogeni sistem jednačina ima netrivijalna rešenja onda je determinanta sistema jednaka nuli.*

Dokaz: Kako je homogeni sistem uvek saglasan, odnosno kako uvek postoji bar trivijalno rešenje, znamo da rešenje nije jedinstveno, pa zbog Kramerove teoreme determinanta mora biti nula. □

3.3 Inverzne matrice i primena

Definicija 3.35 *Neka je $n \in \mathbb{N}$ i $A = [a_{ij}]_{n\times n}$ kvadratna matrica nad poljem $(F, +, \cdot)$. Adjungovanu matricu matrice A u oznaci $adjA$ definišemo kao kvadratnu matricu $[A_{ij}]^T_{n\times n}$, gde A_{ij} jeste algebarski komplement elementa a_{ij}, za sve $i, j \in \{1, \ldots, n\}$.*

Primer: Neka je $A = \begin{bmatrix} 1 & 2 & 1 \\ 3 & 5 & 0 \\ 1 & 2 & 0 \end{bmatrix}$. Tada je $adjA = \begin{bmatrix} 0 & 2 & -5 \\ 0 & -1 & 3 \\ 1 & 0 & -1 \end{bmatrix}$.

Propozicija 3.36 *Neka je $n \in \mathbb{N}$ i $(F, +, \cdot)$ neko polje. Tada za svaku kvadratnu matricu A reda n nad tim poljem važi: $A \cdot adjA = adjA \cdot A = |A|E$.*

Dokaz: Iz Laplasove teoreme dobijamo da je $A \cdot adjA = adjA \cdot A = \begin{bmatrix} |A| & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & |A| \end{bmatrix} = |A|E$. □

Propozicija 3.37 *Neka je $n \in \mathbb{N}$ i $A = [a_{ij}]_{n\times n}$ kvadratna matrica nad poljem $(F, +, \cdot)$. Ako postoji kvadratna matrica B nad istim poljem i istog reda kao A takva da je $AB = BA = E$, onda je matrica B jedinstvena.*

Dokaz: Skup $L_n(F) = \{A \in \mathcal{M}_{n,n} \mid (\exists B \in \mathcal{M}_{n,n}) AB = BA = E\}$ zajedno sa operacijom množenja matrica čini grupu: ako $A, A' \in L_n(F)$ onda postoje $B, B' \in \mathcal{M}_{n,n}$ takve da je $AB = BA = A'B' = B'A' = E$, a tada je $A'ABB' = BB'A'A = E$, gde $BB' \in \mathcal{M}_{n,n}$, pa $A'A \in L_n(F)$. Zato je $L_n(F)$ nosač potpolugrupe od $(\mathcal{M}_{n,n}, \cdot)$ i jasno $E \in L_n(F)$, pa je podmonoid. Zato je $L_n(F)$ nosač monoida koji je grupa. □

Definicija 3.38 *Neka je $n \in \mathbb{N}$ i $A = [a_{ij}]_{n\times n}$ kvadratna matrica nad poljem $(F, +, \cdot)$. Jedinstvena kvadratna matrica B nad istim poljem i istog reda kao A takva da je $AB = BA = E$, ako postoji, naziva se inverzna matrica matrice A i označava sa A^{-1}.*

Teorema 3.39 *Kvadratna matrica nad nekim poljem ima inverznu matricu ako i samo ako je njena determinanta različita od nule.*

Dokaz: Ako je $|A| \neq 0$ onda iz propozicije 3.36 dobijamo $A^{-1} = \frac{1}{|A|} adjA$. Ako postoji A^{-1} onda je $AA^{-1} = E$, pa je po teoremi 3.30, $1 = |E| = |A||A^{-1}|$, što u polju ne može biti tačno ako je $|A| = 0$. □

Posledica 3.40 *Skup svih kvadratnih matrica istog reda nad nekim poljem kojima je determinanta različita od nule zajedno sa množenjem matrica čini grupu.*

Dokaz: $L_n(F) = \{A \in \mathcal{M}_{n,n} \mid |A| \neq 0\}$, gde je $n \in \mathbb{N}$, $(F, +, \cdot)$ polje. Prema prethodno izloženom je $(L_n(F), \cdot)$ grupa. □

Napomena: Grupa iz prethodnog tvrđenja nije Abelova.

Inverzne matrice imaju primenu u rešavanju kvadratnih sistema linearnih jednačina. Neka je

$$\begin{aligned} a_{11}x_1 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + \ldots + a_{2n}x_n &= b_2 \\ \ldots\ldots\ldots\ldots & \\ a_{n1}x_1 + \ldots + a_{nn}x_n &= b_n \end{aligned}$$

sistem jednačina nad nekim poljem $(F, +, \cdot)$. Tada je zbog definicije množenja i jednakosti matrica

$$\begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}.$$

Ako je determinanta sistema $|A| = |[a_{ij}]_{n\times n}|$ različita od nule, onda po Kramerovoj teoremi sistem ima jedinstveno rešenje. Ako je determinanta različita od nule onda postoji inverzna matrica A^{-1} za A i $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = A^{-1} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$.

Literatura

[1] S. Crvenković, R. Szilágyi Madarász, *Uvod u teoriju automata i formalnih jezika*, Univerzitetski udžbenik 15, Stylos, Novi Sad, 1995.

[2] M.Z. Grulović, *Osnovi teorije grupa*, Feljton, Novi Sad, 1997.

[3] J.M. Howie, *An Introduction to Semigroup Theory*, Academic Press, London, New York, San Francisko, 1976.

[4] R. Madarász Szilágyi, *Od skupova do univerzalnih algebri*, Univerzitet u Novom Sadu, Prirodno-matematički fakultet, Novi Sad, 2006.

[5] D. Mašulović, *Diskretna matematika za informatičare 1*, Prirodno-matematički fakultet Novi Sad, Novi Sad, 2014.

[6] S. Milić, *Elementi algebre*, Carić, Beograd, 1995.

[7] B. Šešelja, *Matematika informatike*, Institut za matematiku Novi Sad, Novi Sad, 1990.

[8] A. Tepavčević, B. Šešelja, *Algebra 1*, Univerzitet u Novom Sadu, Prirodno-matematički fakultet, Novi Sad, 2000.

[9] B. Šobot, *Teorijske osnove informatike I*, Prirodno-matematički fakultet, Novi Sad, 2017.

[10] G. Vojvodić, *Predavanja iz algebre*, Univerzitetski udžbenik, Novi Sad, 2007.

CIP - Каталогизација у публикацији
Библиотека Матице српске, Нови Сад

512(075.8)

МУДРИНСКИ, Небојша
Predavanja iz algebre za informatičare [Elektronski izvor] / Nebojša Mudrinski. - Novi Sad : Prirodno-matematički fakultet, Departman za matematiku i informatiku, 2018

Način dostupa
(URL): https://www.pmf.uns.ac.rs/studije/epubikacije /matinf/mudrinski_predavanja_iz_algebre.pdf. - Opis zasnovan na stanju na dan 30.3.2018. - Nasl. s naslovnog ekrana. - Bibliografija.

ISBN 978-86-7031-360-6

a) Алгебра
COBISS.SR-ID 322437127