SKRIPTA IZ DISKRETNE MATEMATIKE 1

školska godina 2023/24.

1 Iskazna logika

1.1 Iskazi, iskazne formule

Iskaz je rečenica koja ima tačno jedno od svojstava „biti tačan“ ili „biti netačan“. Za označavanje obično koristimo mala slova $p, q, r \ldots$ Od iskaza p, q, r koristeći tzv. logičke veznike *ne, i, ili, ako... onda, ako i samo ako* dobijamo složene iskaze.

- *Negacija* iskaza p je ne p. Označava se sa $\neg p$. Negacija tačnog iskaza je netačan iskaz i obrnuto.

  p: 3 deli 14. $\neg p$: 3 ne deli 14.

- *Konjunkcija* redom iskaza p i q je iskaz p i q. Označava se sa $p \wedge q$. Konjunkcija je tačan iskaz ako su p i q tačni iskazi, u ostalim slučajevima konjunkcija je netačan iskaz.

- *Disjunkcija* redom iskaza p i q je iskaz p ili q. Označava se sa $p \vee q$. Disjunkcija je netačan iskaz ako su p i q netačni iskazi, u ostalim slučajevima disjunkcija je tačan iskaz. Usvaja se da veznik ili nema isključni smisao.

- *Implikacija* redom iskaza p i q je iskaz ako p onda q. Označava se sa $p \Rightarrow q$. Implikacija je netačan iskaz ako je p tačan iskaz a q je netačan iskaz, u ostalim slučajevima je tačan. Kažemo da u implikaciji $p \Rightarrow q$, p je dovoljan uslov za q, a q je potreban uslov za p. Kažemo još da je p *antecedent*, a q *konsekvent*, kao i sledeće formulacije: iz p sledi q, p implicira q.

  Iskaz „Ako ovaj putnički avion poleti ka mesecu, taj avion će sleteti na mesec.“ je matematički gledano tačan iskaz, iako na prvi pogled deluje da nije.

- *Ekvivalencija* redom iskaza p i q je iskaz p ako i samo ako q. Označava se sa $p \Leftrightarrow q$. Ekvivalencija je tačan iskaz ako su p i q ili oba tačna ili oba netačna. U preostalim slučajevima ekvivalencija je netačan iskaz. Ekvivalencijom se u matematici često definišu novi termini, polazeći od već poznatih. Često umesto „ako i samo ako“ pišemo skraćeno „akko“.

Slova kojima se označavaju iskazi zovu se iskazna slova, a oznake logičkih veznika $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ zovu se *znaci logičkih operacija*. U nastavku dajemo kako se definišu precizno *iskazne formule*. Ovo je primer tzv. rekurzivne definicije.

1. Iskazna slova su iskazne formule.
2. Ako su A i B iskazne formule, onda su i $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$ iskazne formule.
3. Izraz je iskazna formula samo ako je formiran konačnim brojem primena pravila 1. i 2..

Po dogovoru se izostavljaju neke zagrade u iskaznim formulama kao što sledi

- Ne stavljaju se spoljne zagrade.
- Ako su $A_1, A_2, \ldots, A_n$ iskazne formule, onda se umesto $(\ldots((A_1 \wedge A_2) \wedge A_3) \wedge \cdots \wedge A_{n-1}) \wedge A_n$ piše $A_1 \wedge A_2 \wedge A_3 \cdots \wedge A_{n-1} \wedge A_n$ i slično za veznik $\vee$.
- Uvodi se dogovor o redosledu veznika prema kome su $\wedge$ i $\vee$ ispred $\Rightarrow$ i $\Leftrightarrow$. Na primer, umesto $p \Rightarrow (q \wedge r)$, pišemo $p \Rightarrow q \wedge r$.

Podniz iskazne formule je njena *potformula*, ako je i sam taj izraz iskazna formula. Definicija potformule se odnosi samo na iskaznu formulu kod koje nisu uklonjene zagrade. Na primer $q \wedge p$ jeste, a $p \Rightarrow q$ nije potformula formule $p \Rightarrow q \wedge p$.

- *Pitanje:* Ako je $A \wedge B$ iskazna formula, da li A i B moraju biti iskazne formule?

1.2 Iskazna algebra, interpretacija

Iskazna algebra je uređena šestorka $(\{\top, \bot\}, \neg, \wedge, \vee, \Rightarrow, \Leftrightarrow)$ čija je prva komponenta skup $\{\top, \bot\}$, druga komponenta je jedna unarna operacija, a ostale komponente su četiri binarne operacije, definisane redom sledećim tablicama:

	$\neg$	$\wedge$	$\top$	$\bot$	$\vee$	$\top$	$\bot$	$\Rightarrow$	$\top$	$\bot$	$\Leftrightarrow$	$\top$	$\bot$
$\top$	$\bot$	$\top$	$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$	$\bot$
$\bot$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\top$	$\bot$	$\bot$	$\top$

Navedene operacije označavaju se isto kao odgovarajući logički veznici, ali to nisu isti pojmovi. Znak $\wedge$ u iskaznoj formuli $p \wedge q$ je zamena za veznik, reč *i*, a oznaka u gornjoj tablici opisuje operaciju na skupu $\{\top, \bot\}$.

Neka je A iskazna formula. *Interpretacija* formule A je funkcija koja svakom iskaznom slovu iz A pridružuje elemenat skupa $\{\top, \bot\}$. Elemenat dodeljen iskaznom slovu je njegova (istinitosna) *vrednost*. Ako su svim slovima iz A dodeljene vrednosti, možemo definisati *vrednost iskazne formule A za datu interpretaciju*, u oznaci $v(A)$ na sledeći način:

1. Ako je formula iskazno slovo p, onda je $v(p)$ vrednost slova p.
2. Ako su $v(A)$ i $v(B)$ istinitosne vrednosti formula A i B, onda je
   - $v(\neg A) = \neg v(A)$
   - $v(A \wedge B) = v(A) \wedge v(B)$
   - $v(A \vee B) = v(A) \vee v(B)$
   - $v(A \Rightarrow B) = v(A) \Rightarrow v(B)$
   - $v(A \Leftrightarrow B) = v(A) \Leftrightarrow v(B)$

Ako je za neku interpretaciju vrednost formule $\top$, kažemo da je formula *tačna* u toj interpretacji, a ako joj je vrednost $\bot$, kažemo da je *netačna* u toj interpretaciji.

Da bi se odredile vrednosti formule za sve interpetacije, koristimo tablice istinitosti. Ako formula A sadrži n različitih iskaznih slova, tablica instinosti će imati 2^n redova.

1.3 Tautologije

Iskazna formula je *tautologija*, ako je tačna u svakoj interpretaciji. U njenoj tablici istinitosti poslednja kolona se sastoji samo od simbola $\top$. Neke poznate tautologije:

1. zakon isključenja trećeg: $p \vee \neg p$;
2. modus ponendo ponens: $p \wedge (p \Rightarrow q) \Rightarrow q$;

3. modus tollendo tollens: $\neg q \wedge (p \Rightarrow q) \Rightarrow \neg p$;
4. modus tollendo ponens: $\neg p \wedge (p \vee q) \Rightarrow q$;
5. zakon hipotetičkog silogizma: $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$;
6. zakon svođenja na apsurd: $p \Rightarrow (q \wedge \neg q) \Rightarrow \neg p$;
7. zakon pojednostavljivanja: $p \wedge q \Rightarrow p$;
8. zakon dvostruke negacije: $p \Leftrightarrow \neg\neg p$;
9. zakon kontrapozicije: $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$;
10. De Morganovi zakoni: $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$, $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$;
11. zakon za implikaciju: $(p \Rightarrow q) \Leftrightarrow \neg p \vee q$;
12. zakon za ekvivalenciju: $(p \Leftrightarrow q) \Leftrightarrow (p \Rightarrow q) \wedge (q \Rightarrow p)$;
13. zakoni komutativnosti: $\begin{cases} p \wedge q \Leftrightarrow q \wedge p; \\ p \vee q \Leftrightarrow q \vee p; \end{cases}$
14. zakoni asocijativnosti $\begin{cases} p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r; \\ p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r; \end{cases}$
15. zakoni distributivnosti: $\begin{cases} p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r); \\ p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r); \end{cases}$
16. zakoni idempotentnosti $\begin{cases} p \wedge p \Leftrightarrow p; \\ p \vee p \Leftrightarrow p; \end{cases}$
17. zakoni apsorpcije $\begin{cases} p \wedge (p \vee q) \Leftrightarrow p; \\ p \vee (p \wedge q) \Leftrightarrow p. \end{cases}$

Tautologije 8–17 se zovu tautološke ekvivalencije. Ponekad se koristi i oznaka $\sim$ ako je u pitanju tautološka ekvivalencija; recimo umesto $(p \Rightarrow q) \Leftrightarrow \neg p \vee q$ pišemo $p \Rightarrow q \sim \neg p \vee q$

1.4 Kanonske forme

Za proizvoljnu operaciju $f : \{\top, \bot\}^n \to \{\top, \bot\}$ možemo odrediti iskaznu formulu $A(p_1, \ldots, p_n)$ čija tablica istinitosti odgovara operaciji f. Zbog lakšeg zapisa koristićemo sledeću oznaku:

$$x^\alpha = \begin{cases} x, \alpha = \top \\ \neg x, \alpha = \bot \end{cases}$$

Teorema 1.1. *Ako je $f : \{\top, \bot\}^n \to \{\top, \bot\}$ proizvoljna n-arna operacija na skupu $\{\top, \bot\}$ koja nije konstantno jednaka $\bot$, onda*

$$f(x_1, \ldots, x_n) = \bigvee_{f(\alpha_1, \ldots, \alpha_n) = \top} x_1^{\alpha_1} \wedge \cdots \wedge x_n^{\alpha_n}. \tag{1}$$

Dokaz. S obzirom da $\bot \wedge v(A) = \bot$ i $\bot \vee v(A) = v(A)$ za bilo koju iskaznu formulu A, sledi da (1) možemo zapisati na sledeći način:

$$f(x_1, \ldots, x_n) = \bigvee_{(\alpha_1, \ldots, \alpha_n) \in \{\top, \bot\}^n} f(\alpha_1, \ldots, \alpha_n) \wedge x_1^{\alpha_1} \wedge \cdots \wedge x_n^{\alpha_n}. \tag{2}$$

tj. dovoljno je pokazati (2). Neka je $(b_1, \ldots, b_n) \in \{\top, \bot\}^n$ proizvoljno. Možemo primetiti da je $b_i^{\alpha_i} = \top$ ako i samo ako je $b_i = \alpha_i$, tj. $b_1^{\alpha_1} \wedge \cdots \wedge b_n^{\alpha_n} = \top$ ako i samo ako $\alpha_i = b_i$ za sve i. U svim ostalim slučajevima je vrednost tog izraza $\bot$. Sledi da je vrednost desne strane jednakosti (2)

$$\bot \vee \cdots \vee (f(b_1, \ldots, b_n) \wedge \top) \vee \cdots \vee \bot = f(b_1, \ldots, b_n).$$

■

Iskazna formula koja se u obliku (1) pridružuje funkciji f zove se *kanonska disjunktivna forma*.

Analogno možemo dokazati sledeće tvrđenje.

Teorema 1.2. *Ako je $f : \{\top, \bot\}^n \to \{\top, \bot\}$ proizvoljna n-arna operacija na skupu $\{\top, \bot\}$ koja nije konstantno jednaka $\top$, onda*

$$f(x_1, \ldots, x_n) = \bigwedge_{f(\alpha_1, \ldots, \alpha_n) = \bot} x_1^{\neg\alpha_1} \vee \cdots \vee x_n^{\neg\alpha_n}. \tag{3}$$

Iskazna formula koja se u obliku (3) pridružuje funkciji f zove se *kanonska konjunktivna forma*.

Zadaci iz iskazne logike

1. Da li su sledeće rečenice iskazi?

   a) Svaki broj deljiv sa 4 je paran.

   b) Ako je broj deljiv sa 3, deljiv je i sa 6.

   c) $2 + 3 = 5$.

   d) Ova rečenica nije tačna.

2. Koji od sledećih izraza su iskazne formule?

   a) $p \Rightarrow q$;

   b) $qp \vee \neg p \Rightarrow p$;

   c) $p \Rightarrow (q \Rightarrow (p \Rightarrow (p)))$;

   d) $\neg p \vee q \Leftrightarrow (q \wedge r \Rightarrow p$.

3. Za datu interpretaciju odrediti istinitosnu vrednost iskazne formule.

   a) $p \Leftrightarrow q \vee (q \Rightarrow p), \quad v(p) = \top$;

   b) $(p \wedge q) \vee r \Leftrightarrow \neg q \wedge r, \quad v(p) = v(q) = \top, v(r) = \bot$.

4. Šta se može reći o $v(q)$ ako je $v((p \Rightarrow (q \Rightarrow p)) \Rightarrow) = \top$ i $v(p) = \top$?

5. Odrediti istinitosnu vrednost iskazne formule u svim interpretacijama.

   a) $p \wedge q \Rightarrow (q \Rightarrow \neg p)$;

   b) $p \wedge \neg p \Rightarrow r \wedge q$.

6. Dokazati da je iskazna formula tautologija diskusijom po slovu.

   a) $p \Rightarrow (q \Rightarrow p)$;

   b) $p \vee q \Leftrightarrow ((p \Rightarrow q) \Rightarrow q)$.

7. Dokazati da je iskazna formula tautologija svođenjem na protivrečnost.

   a) $x \Rightarrow (\neg x \Rightarrow y)$;

   b) $(x \Rightarrow z) \Rightarrow ((y \Rightarrow z) \Rightarrow (x \vee y \Rightarrow z))$;

8. Naći formulu u kanonskoj konjunktivnoj formi i kanonskoj disjunktivnoj formi čija je istinitosna tablica:

p	q	r	F
$\top$	$\top$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\bot$
$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$	$\top$

9. Konstruisati iskaznu formulu $F(p, q, r)$ koja je tačna ako i samo ako tačno dve njene promenljive imaju vrednost $\top$.

10. Naći bar jednu iskaznu formulu $F(p, q, r)$ takvu da važe sledeća tri uslova:

    a) u svakoj interpretaciji u kojoj je $p \vee q \Rightarrow r$ tačno, tačno je i F;

    b) u interpretaciji u kojoj je F tačno, tačno je i $p \Rightarrow q \vee r$;

    c) u interpretaciji kada je $\neg p \wedge q \wedge \neg r$ tačno, tada je F netačno.

11. Naći iskaznu formulu $F(p, q, r)$ takvu da važi: formula $p \wedge F$ tautološki je ekvivalentna sa $p \wedge q$, a $p \vee F$ tautološki je ekvivalentna sa $p \vee r$.

12. Da li postoji iskazna formula $F(p, q, r)$ takva da je formula $(p \vee q \Rightarrow F) \Leftrightarrow (F \Rightarrow p \wedge r)$ tautologija?

13. *Generatorni skup* operacija iskazne algebre je skup operacija pomoću kojih se mogu izraziti sve ostale operacije iskazne algebre. *Baza* iskazne algebre je minimalni generatorni skup. Dokazati da je $\{\Rightarrow, \neg\}$ generatorni skup.

14. Dokazati da je $\{\Rightarrow, \not\Rightarrow\}$ generatorni skup gde je operacija $\not\Rightarrow$ data tabelom:

$\not\Rightarrow$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\bot$

15. Dokazati da ne postoji za svaku iskaznu formulu njoj ekvivalentna u kojoj su jedini veznici $\vee$ i $\Rightarrow$.

16. Dokazati da se $\Rightarrow$ ne može izraziti preko $\wedge$ i $\vee$.

17. Neka je $F(p_1, ..., p_n; \Rightarrow)$ formula koja od veznika sadrži samo $\Rightarrow$. Dokazati da postoji iskazno slovo $p_i, i \in \{1, 2, ..., n\}$ takvo da u svakoj interpretaciji važi: ako je $v(p_i) = \top$, onda je $v(F) = \top$.

2 Predikatska logika

2.1 Termi, formule

Cilj ove sekcije je da definišemo predikatske formule. Polazni simboli su:

- zagrade, zarez, tzv. pomoćni znaci;
- znaci konstante $a_1, a_2, a_3, \ldots$
- promenljive $x_1, x_2, x_3, \ldots$;
- funkcijski znaci $f_1^1, f_2^1, \ldots, f_1^2, \ldots, f_i^j \ldots$;
- relacijski znaci $R_1^1, R_2^1, \ldots, R_1^2, \ldots, R_i^j \ldots$;
- logički veznici $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ i oznake $\forall, \exists$.

Konstante su oznake za pojedinačne objekte. Na primer 0, 1, π, $\sqrt{2}$, $\top$, $\bot$, tačka A, prava p i slično. Zajednička imena za objekte iste vrste su *promenljive*. Gornji indeks u funkcijskom i relacijskom znaku označava njegovu arnost, a donji služi za razlikovanje znakova iste dužine. Neke unarne operacije na odgovarajućim domenima su recimo $\sqrt{}$, log , neke binarne operacije su $+, -$. Neke unarne relacije na odgovarajućim skupovima su „biti paran“, „biti prost“, neke binarne relacije su $\leqslant, \cong, |$. Ako je $P(x)$ zapis rečenice x ima svojtstvo P, onda se rečenica „Za svako x, x ima svojstvo P.“ označava sa $(\forall x)P(x)$. Oznaka $(\forall x)$ se zove *univerzalni kvantifikator*. Rečenica „Postoji x tako da x ima svojstvo P.“ označava se sa $(\exists x)P(x)$. Oznaka $(\exists x)$ se zove *egzistencijalni kvantifikator*. Kada se ističe skup na koji se odnosi formula, onda možemo na dva načina simbolički da zapišemo rečenicu. Na primer rečenicu „Svi prirodni brojevi su deljivi sa 1.“ možemo zapisati kao

$$(\forall x \in \mathbb{N})(1|x) \text{ ili } (\forall x)(x \in \mathbb{N} \Rightarrow 1|x);$$

A rečenicu „Postoji prirodan broj deljiv sa 2.“ možemo zapisati kao

$$(\exists x \in \mathbb{N})(2|x) \text{ ili } (\exists x)(x \in \mathbb{N} \wedge 2|x).$$

U nastavku prikazujemo kako se precizno definišu *termi*.

1. Promenljive i znaci konstanti su termi.
2. Ako je f_m^n funkcijski znak, a $t_1, \ldots, t_n$ termi, onda je i $f_m^n(t_1, \ldots, t_n)$ isto term.
3. Izraz je term samo ako je formiran konačnim brojem primena pravila 1. i 2..

Ako je R_i^n relacijski znak, a $t_1, \ldots, t_n$ termi, onda je $R_i^n(t_1, \ldots, t_n)$ *atomarna formula*.

Predikatske formule se definišu na sledeći način:

1. Svaka atomarna formula je predikatska formula.
2. Ako su $\mathcal{F}$ i $\mathcal{G}$ predikatske formule, a x promenljiva, onda su i $\neg\mathcal{F}$, $(\mathcal{F} \wedge \mathcal{G})$, $(\mathcal{F} \vee \mathcal{G})$, $(\mathcal{F} \Rightarrow \mathcal{G})$, $(\mathcal{F} \Leftrightarrow \mathcal{G})$, $((\forall x)\mathcal{F})$ i $((\exists x)\mathcal{F})$ predikatske formule.
3. Izraz je predikatska formula samo ako je formiran konačnim brojem primena pravila 1. i 2..

Potformula predikatske formule je podniz koji je i sam formula.

Oblast dejstva kvantifikatora $(\forall x)$ i $(\exists x)$ koji se pojavljuje u formuli je sam kvantifikator zajedno sa najmanjom potformulom koja neposredno sledi iza njega.

Pojavljivanje promenljive x u nekoj formuli je *vezano* ako se x javlja u oblasti dejstva nekog kvantifikatora, inače je *slobodno*.

Primer 2.1. *U sledećim formulama crvenom bojom su označena vezana, a zelenom bojom slobodna pojavljivanja promenljivih.*

- $(\forall x)\alpha(x) \Rightarrow (\exists y)\beta(x, y) \vee \gamma(y)$
- $(\forall x)(\alpha(x) \Rightarrow (\exists y)\beta(x, y) \vee \gamma(y))$
- $(\forall x)(\alpha(x) \Rightarrow (\exists y)(\beta(x, y) \vee \gamma(y)))$

Promenljiva x je *slobodna* ili *vezana* u formuli A ako u njoj ima redom slobodno ili vezano pojavljivanje.

2.2 Interpretacija

Interpretacija formule ili skupa formula je uređeni par $\mathcal{D} = (D, \phi)$, gde je D domen interpretacije a ϕ funkcija koja pridružuje

- svakoj konstanti fiksni element iz D;
- svakom funkcijskom simbolu dužine n neku n-arnu operaciju na D (tj. funkciju iz D^n u D);
- svakom relacijskom simbolu dužine n neku n-arnu relaciju na D (tj. podskup iz D^n).

Primer 2.2. *Neka je data formula* $R(y, f(x, a))$*, i neka je data interpretacija* $\mathcal{D} = (\mathbb{N}, \phi)$*, gde je* $\mathbb{N}$ *skup prirodnih brojeva, a* $\phi = \begin{pmatrix} a & f & R \\ 1 & + & > \end{pmatrix}$*. Tada gornja formula postaje rečenica „Prirodan broj* y *je veći od* $x{+}1$ *(*x *je takođe prirodan broj).“*

Neka je data formula $(\forall x)(R_1^2(x, a) \Rightarrow (\exists y)(R_1^2(f_1^2(x, y), a)))$ *i posmatrajmo interpretaciju* $\mathcal{D} = (\mathbb{R}, \phi)$*, tj. domen interpretacije skup realnih brojeva* $\mathbb{R}$*, a neka je* $\phi = \begin{pmatrix} a & f_1^2 & R_1^2 \\ 0 & \cdot & < \end{pmatrix}$*. Tada gornja formula postaje rečenica „Za svaki realan broj* x *manji od* 0 *postoji realan broj* y *takav da je proizvod* $x \cdot y$ *manji od* 0*.“*

Niz elemenata iz domena kojima zamenjujemo promenljive zove se *valuacija* domena D. Predikatska formula za datu valuaciju postaje tačan ili netačan iskaz nakon što se njene slobodne promenljive zamene odgovarajućim elementima valuacije. Prva formula iz prethodnog primera je tačna za valuaciju $(1, 3)$, ali nije tačna za valuaciju $(2, 3)$.

Kažemo da je formula $\mathcal{F}$ tačna u interpretaciji $\mathcal{D}$, ako je tačna za svaku valuaciju iz D. Formula je *zatvorena*, ako u njoj nema slobodnih promenljivih (kao druga formula iz prethodnog primera). Zatvorena formula je u svakoj interpretaciji tačna ili netačna rečenica, dakle iskaz, bez obzira na valuaciju. Ako je formula $\mathcal{F}$ tačna u interpretaciji $\mathcal{D}$, onda je $\mathcal{D}$ model formule $\mathcal{F}$. $\mathcal{D}$ je model za neki skup formula $\mathcal{S}$, ako je svaka formula iz $\mathcal{S}$ tačna u interpretaciji $\mathcal{D}$.

2.3 Valjane formule

Formula $\mathcal{F}$ je *valjana* ako je tačna u svakoj interpretaciji. To se označava na sledeći način: $\models \mathcal{F}$.

Teorema 2.3. *Ako su $\mathcal{F}$ i $\mathcal{G}$ proizvoljne predikatske formule, onda su sledeće formule valjane:*

1. $(\forall x)\mathcal{F} \Rightarrow (\exists x)\mathcal{F}$;
2. $(\forall x)(\forall y)\mathcal{F} \Leftrightarrow (\forall y)(\forall x)\mathcal{F}$;
3. $(\exists x)(\exists y)\mathcal{F} \Leftrightarrow (\exists y)(\exists x)\mathcal{F}$;
4. $(\exists x)(\forall y)\mathcal{F} \Rightarrow (\forall y)(\exists x)\mathcal{F}$;
5. $(\exists x)\neg\mathcal{F} \Leftrightarrow \neg(\forall x)\mathcal{F}$;
6. $(\forall x)\neg\mathcal{F} \Leftrightarrow \neg(\exists x)\mathcal{F}$;
7. $(\forall x)(\mathcal{F} \wedge \mathcal{G}) \Leftrightarrow (\forall x)\mathcal{F} \wedge (\forall x)\mathcal{G}$;
8. $(\exists x)(\mathcal{F} \wedge \mathcal{G}) \Rightarrow (\exists x)\mathcal{F} \wedge (\exists x)\mathcal{G}$;
9. $(\forall x)\mathcal{F} \vee (\forall x)\mathcal{G} \Rightarrow (\forall x)(\mathcal{F} \vee \mathcal{G})$;
10. $(\exists x)(\mathcal{F} \vee \mathcal{G}) \Leftrightarrow (\exists x)\mathcal{F} \vee (\exists x)\mathcal{G}$.

Dokaz.

1. Neka je $\mathcal{D}$ proizvoljna interpretacija i v proizvoljna valuacija domena D. Treba dokazati da važi sledeće tvrđenje: ako je $(\forall x)\mathcal{F}$ tačna za v, onda je i $(\exists x)\mathcal{F}$ tačna za valuaciju v. Ako je $(\forall x)\mathcal{F}$ tačna za v, onda je formula $\mathcal{F}$ tačna za sve valuacije koje se od v razlikuju najviše na mestu x-a. Jasno je da onda u tom domenu postoji elemenat b tako da je za valuaciju dobijenu iz v uvrštavanjem elementa b na mesto x-a formula $\mathcal{F}$ tačna. To znači da je za valuaciju v tačna formula $(\exists x)\mathcal{F}$.

2. Formula $(\forall x)(\forall y)\mathcal{F}$ je tačna na nekom domenu D u interpretaciji $\mathcal{D}$ i za valuaciju v ako i samo ako je formula $(\forall y)\mathcal{F}$ tačna za svaku valuaciju koja se od v razlikuje najviše na mestu x-a, ako i samo ako je formula $\mathcal{F}$ tačna za svaku valuaciju koja se od prethodne razlikuje najviše na mestu y-a, dakle koja se od valuacije v razlikuje najviše na mestima

x i y. Sa druge strane, kada se krene od formule $(\forall y)(\forall x)\mathcal{F}$, na sličan način se dobija da je ona tačna za valuaciju v ako i samo ako je formula $\mathcal{F}$ tačna za valuaciju koja se od v razlikuje na mestima y i x. Dakle, formule $(\forall x)(\forall y)\mathcal{F}$ i $(\forall y)(\forall x)\mathcal{F}$ su tačne uvek za iste valuacije, pa je ekvivalencija te dve formule valjana formula.

■

Da se pokaže kako obrnute implikacije u formulama 1,4,8,9 nisu tačne, dovoljno je naći kontraprimer.

1. Neka je domen $D = \{1, 2, 3\}$ i $\mathcal{F}$ atomarna formula koja predstavlja unarnu relaciju: x je u relaciji ako je manji od 2.

4. Neka je domen skup prirodnih brojeva, a $\mathcal{F}$ atomarna formula koja predstavlja binarnu relaciju $y \leqslant x$.

8-9. Neka je domen skup prirodnih brojeva, a $\mathcal{F}$ i $\mathcal{G}$ atomarne formule x je paran i x je neparan.

Izvod iskazne formule A je predikatska formula dobijena iz A zamenom svih iskaznih slova predikatskim formulama, pri čemu se isto slovo zamenjuje istom formulom.

Teorema 2.4. *Izvod tautologije je valjana formula.*

Dokaz. Neka su $p_1, \ldots, p_n$ sva iskazna slova koja se javljaju u tautologiji A i $\mathcal{F}$ predikatska formula dobijena iz A zamenom tih slova redom formulama $\mathcal{F}_1, \ldots, \mathcal{F}_n$. Neka je data interpretacija $\mathcal{D}$ formula $\mathcal{F}$ i neka je v jedna valuacija. Za tu valuaciju formule $\mathcal{F}_1, \ldots, \mathcal{F}_n$ postaju iskazi, njihove istinitosne vrednosti obrazuju n-torku simbola $\top, \bot$, pa kada se pridruže slovima $p_1, \ldots, p_n$, određuju jednu interpretaciju iskazne formule A. Pošto je A tautologija, ona je tačna u ovoj interpretaciji. Ovo važi za bilo koju valuaciju proizvoljne interpretacije formule $\mathcal{F}$, pa je ona valjana. ■

Teorema 2.5. *Formula $\mathcal{F}$ je tačna u interpetaciji $\mathcal{D}$ ako i samo ako je u toj interpretaciji tačna i formula $(\forall x_i)\mathcal{F}$.*

Zadaci iz predikatske logike

1. Ispitati tačnost formula:

   a) $\alpha^2(a * a, a)$

   b) $(\exists x)\alpha^2(x * x, a)$

   c) $(\forall x)(\exists y)\alpha^2(x * y, a)$

   u sledećim interpretacijama $(\alpha^2, *, a)$:

   - $\mathcal{D} = (\mathbb{N}, =, +, 1)$;
   - $\mathcal{D} = (\mathbb{N}, =, \cdot, 1)$;
   - $\mathcal{D} = (\mathbb{R}, =, +, 0)$.

2. Naći bar jedan model i kontramodel za svaku od formula (gde su $\alpha.\beta$ i γ relacijski znakovi).

   a) $(\forall x)(\exists z)\alpha(x, z)$;

   b) $(\forall x)(\forall y)(\forall z)(\alpha(x, y) \wedge \alpha(y, z) \Rightarrow \alpha(x, z))$;

   c) $(\forall x)(\gamma(x) \vee \beta(x)) \Rightarrow (\forall x)\gamma(x) \vee (\forall x)\beta(x)$.

3. Negirati sledeće formule.

   a) $(\forall x)(\rho(x) \Rightarrow (\exists y)\sigma(x, y))$;

   b) $(\forall x)(\exists y)(\varphi(x, y) \Leftrightarrow (\exists z)\varphi(f(x, y, z), z))$;

   c) $(\exists x)(\forall y)\varphi(x, y) \Rightarrow (\forall z)\varphi(z, z)$.

4. Dokazati:

   $$\models (\forall x)(P(x) \Rightarrow Q(x)) \wedge (\exists x)P(x) \Rightarrow (\exists x)Q(x)$$

   gde su P i Q relacijski znakovi.

5. Dokazati:

   $$\models (\forall x)(\exists y)(P(x) \Rightarrow Q(y)) \wedge (\exists x)P(x) \Rightarrow (\exists x)Q(x)$$

   gde su P i Q relacijski znakovi.

6. Dokazati:

   $$\models (\forall x)(\exists y)P(x,y) \wedge (\forall y)(\exists z)Q(y,z) \Rightarrow (\forall x)(\exists y)(\exists z)(P(x,y) \wedge Q(y,z))$$

   gde su P i Q relacijski znakovi.

7. Dokazati:

   $$\models \neg(\exists x)(M(x) \wedge \neg P(x)) \wedge (\exists x)(S(x) \wedge M(x)) \Rightarrow (\exists x)(S(x) \wedge P(x))$$

   gde su M, P i S relacijski znakovi.

8. Dokazati:

   $$\models (\forall x)(\exists y)P(x,y) \wedge (\forall x)(\forall y)(P(x,y) \wedge \neg Q(y,x) \Rightarrow P(y,x)) \\ \Rightarrow (\forall x)(\exists y)P(y,x) \vee (\exists x)(\exists y)Q(x,y)$$

   gde su P i Q relacijski znakovi.

9. Dokazati:

   $$\models (\forall x)(\exists y)P(f(y,x,x),y) \wedge (\exists x)(\forall y)\neg P(x, f(y,x,y)) \\ \Rightarrow (\exists x)(\exists y)(\exists z)\neg(P(f(x,y,z),x) \Rightarrow P(y, f(z,z,z)))$$

   gde je P relacijski, a f funkcijski znak.

10. Dokazati:

    $$\not\models (\forall x)(A(x) \Rightarrow B(x)) \Rightarrow \neg((\exists x)A(x) \wedge (\exists x)\neg B(x))$$

    gde su A i B relacijski znakovi.

11. Dokazati:

    $$\not\models (\forall x)(\forall y)(R(x,y) \Rightarrow R(y,x)) \Rightarrow (\forall x)R(x,x) \vee (\forall x)(\forall y)(\forall z)(R(x,y) \wedge R(y,z) \Rightarrow R(x,z))$$

    gde je R relacijski znak.

12. Dokazati:

    $$\not\models (\forall x)R(x,x) \wedge (\forall x)(\forall y)(R(x,y) \Rightarrow R(y,x)) \Rightarrow (\forall x)(\forall y)(\forall z)(R(x,y) \wedge R(y,z) \Rightarrow R(x,z))$$

    gde je R relacijski znak.

13. Naći model za sledeći skup formula:

$$\{(\forall x)(\exists y)(R(x,y) \vee R(y,x)),(\forall x)\neg R(x,x),$$
$$(\exists x)(\forall y)\neg R(x,y),(\exists x)(\forall y)\neg R(y,x)\},$$

pri čemu je R relacijski znak.

14. Naći model za sledeći skup formula:

$$\{(\forall x)\neg R(x,x),(\forall x)(\exists y)R(x,y),{}^{(}\forall x)(\exists y)R(y,x),$$
$${}^{(}\exists x)(\exists y)(x \neq y \wedge \neg R(x,y) \wedge \neg R(y,x)),(\forall x)(\forall y)\neg(R(x,y) \wedge R(y,x))\},$$

pri čemu je R relacijski znak.

15. Dokazati:

$$\not\models (\forall x)(\forall y)R(f(x,y),y) \vee (\forall x)(\forall y)R(x,f(x,y))$$

gde je R relacijski, a f funkcijski znak.

16. Data je formula $(\forall x)(\alpha(x) \Rightarrow \alpha(f(x)))$ gde je α relacijski, a f funkcijski znak. Dokazati da formula nije valjana.

17. Dokazati:

$$\not\models (\exists x)(\exists y)R(x,y)\wedge(\forall x)(\forall y)(R(x,y) \Leftrightarrow (\exists z)(R(x,z)\wedge R(z,y))) \Rightarrow (\exists x)R(x,x)$$

gde je R relacijski znak.

3 Skupovi

3.1 Skup, podskup, prazan skup

Skup je osnovni pojam za koji se ne daje eksplicitna definicija. Skupovi imaju *elemente*, a osnovni odnos između njih i skupova je pripadanje. Da je a elemenat skupa A beleži se oznakom $a \in A$. Negacija ove formule beleži se sa $a \notin A$ i ona znači da a ne pripada skupu A. Ako je $P(x)$ formula sa slobodnom promenljivom x, onda oznaka $\{x : P(x)\}$ označava skup čiji elementi zadovoljavaju formulu $P(x)$.

Primer 3.1. *Oznaka* $\{x : x \in \mathbb{Z} \wedge x^2 = 1\}$ *određuje skup čiji su elementi brojevi* 1 *i* -1.

Za skupove A i B definiše se da su *jednaki*, u oznaci $A = B$, ako imaju iste elemente:

$$A = B \leftrightarrow (\forall x)(x \in A \Leftrightarrow x \in B).$$

Skup A je podskup skupa B, ako su svi elementi skupa A sadržani u skupu B:

$$A \subseteq B \leftrightarrow (\forall x)(x \in A \Rightarrow x \in B).$$

Napomena 3.2. *U prethodnim definicijama i u daljem tekstu znak* $\leftrightarrow$ *i tekst „ako i samo ako“ imaju isti smisao i ulogu.*

Teorema 3.3. *Za proizvoljne skupove* A, B, C *važi*

1. $A = A$;
2. $A = B \Rightarrow B = A$;
3. $A = B \wedge B = C \Rightarrow A = C$.

Dokaz.

1. Formula $x \in A \Leftrightarrow x \in A$ je izvod tautologije $p \Leftrightarrow p$, pa je na osnovu tvrđenja 2.5 formula $(\forall x)(x \in A \Leftrightarrow x \in A)$ valjana.
2. Sledi iz tautologije $(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$ i tvrđenja 2.5:

$$A = B \leftrightarrow (\forall x)(x \in A \Leftrightarrow x \in B) \leftrightarrow (\forall x)(x \in B \Leftrightarrow x \in A) \leftrightarrow B = A.$$

3. Tranzitivnost se pokazuje pomoću valjane formule 7. iz teoreme 2.3: $(A = B) \wedge (B = C) \leftrightarrow (\forall x)(x \in A \Leftrightarrow x \in B) \wedge (\forall x)(x \in B \Leftrightarrow x \in C) \leftrightarrow (\forall x)((x \in A \Leftrightarrow x \in B) \wedge (x \in B \Leftrightarrow x \in C))$, a odavde sledi $(\forall x)(x \in A \Leftrightarrow x \in C)$.

■

Teorema 3.4. *Za proizvoljne skupove A, B, C važi*

1. $A \subseteq A$;
2. $A \subseteq B \wedge B \subseteq A \Rightarrow A = B$;
3. $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$.

Ako je $B \subseteq A$ i $B \neq A$, kaže se da je B *pravi* podskup skupa A, u oznaci $B \subset A$.

Razlika skupova A i B je skup $A \backslash B$ koji se definiše sa

$$A \backslash B = \{x : x \in A \wedge x \notin B\}.$$

Teorema 3.5. *Neka su X i Y proizvoljni skupovi. Tada $X \backslash X = Y \backslash Y$.*

Dokaz. $x \in X \backslash X \leftrightarrow x \in X \wedge x \notin X \leftrightarrow x \in Y \wedge x \notin Y \leftrightarrow x \in Y \backslash Y$, na osnovu tautologije $p \wedge \neg p \Leftrightarrow q \wedge \neg q$. ■

Razlika $X \backslash X$ tako ne zavisi od skupa X. Zato definišemo *prazan skup*, u oznaci $\emptyset$. Po ovoj definiciji $x \in \emptyset \Leftrightarrow x \in X \wedge x \notin X$. Budući da je desna strana ekvivalencije kontradikcija, ni za jedno x ne važi $x \in \emptyset$. Prazan skup dakle nema elemenata.

Teorema 3.6. *Za svaki skup X važi $\emptyset \subseteq X$.*

3.2 Konstrukcije skupova

Presek skupova A i B je skup koji sadrži tačno one elemente koji se nalaze istovremeno u oba skupa:

$$A \cap B = \{x : x \in A \wedge x \in B\}.$$

Za skupove A i B čiji je presek prazan skup kaže se da su *disjunktni*.

Unija skupova A i B je skup koji sadrži sve elemente koji se nalaze bar u jednom od njih:

$$A \cup B = \{x : x \in A \vee x \in B\}.$$

Razlika skupova već je definisana. Specijalno, ako $B \subseteq A$, onda se razlika $A \backslash B$ zove komplement skupa B u odnosu na A i označava se sa $C_A(B)$. Često se posmatraju isključivo podskupovi nekog unapred datog skupa U, koji se zove *univerzalni skup*. Tada se za $B \subseteq U$, $C_U(B)$ označava sa $\overline{B}$ i zove se komplement skupa B:

$$\overline{B} = \{x : x \notin B\}.$$

Kolekcija svih podskupova proizvoljnog skupa A zove se *partitivni skup* skupa A, u oznaci $\mathcal{P}(A)$:

$$\mathcal{P}(A) = \{X : X \subseteq A\}.$$

Primer 3.7. $\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$, $\mathcal{P}(\emptyset) = \{\emptyset\}$.

Teorema 3.8. *Neka je A skup i $X, Y, Z \subseteq A$. Tada važi:*

1. $X \cap Y = Y \cap X$, $X \cup Y = Y \cup X$;
2. $X \cap (Y \cap Z) = (X \cap Y) \cap Z$, $X \cup (Y \cup Z) = (X \cup Y) \cup Z$;
3. $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$, $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$;
4. $X \cap X = X$, $X \cup X = X$;
5. $X \cap \overline{X} = \emptyset$, $X \cup \overline{X} = A$;
6. $X \cap A = X$, $X \cup \emptyset = X$.

Dokaz. Za vežbu. ■

Ako su A i B skupovi, onda se skup svih uređenih parova sa prvom koordinatom iz A, a drugom iz B zove *direktan proizvod* skupova A i B, u oznaci $A \times B$:

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}.$$

Primer 3.9. *Ako $A = \{0, 1\}$ i $B = \{a, b, c\}$, onda*

$$A \times B = \{(0, a), (0, b), (0, c), (1, a), (1, b), (1, c)\}$$

$$B \times A = \{(a, 0), (a, 1), (b, 0), (b, 1), (c, 0), (c, 1)\}.$$

Dakle, u opštem slučaju $A \times B \neq B \times A$.

Direktan proizvod n skupova $A_1, \ldots, A_n$, u oznaci $A_1 \times \cdots \times A_n$, je skup uređenih n-torki sa koordinatama iz odgovarajućih skupova:

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_i \in A_i, i = 1, \ldots, n\}$$

Zadaci iz skupova

1. Neka je A skup i $X, Y, Z \subset A$. Tada važi:
   a) $X \cap Y = Y \cap X, X \cup Y = Y \cup X$;
   b) $X \cap (Y \cap Z) = (X \cap Y) \cap Z, X \cup (Y \cup Z) = (X \cup Y) \cup Z$;
   c) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z), X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$;
   d) $X \cap X = X, X \cup X = X$;
   e) $X \cap \overline{X} = \emptyset, X \cup \overline{X} = A$;
   f) $X \cap A = X, X \cup \emptyset = X$;
   g) $(X \cap Y) \cup X = X, (X \cup Y) \cap X = X$.

2. Dokazati da za $A, B \subset U$ važi:
   a) $A \subset \emptyset \Leftrightarrow A = \emptyset$;
   b) $A \setminus B = A \cap \overline{B}$;
   c) $\overline{\overline{A}} = A$;
   d) $A \cap \emptyset = \emptyset$;
   e) $A \cup U = U$.

3. Dokazati da za proizvoljne skupove A i B važi:
   a) $A, B \subset A \cup B$;
   b) $A \cap B \subset A, B$.

4. Dokazati da za proizvoljne $A, B, C \subset U$ važi:
   a) $A \cup B \subset C \Leftrightarrow A \subset C \wedge B \subset C$;
   b) Ako je $A \subset B$, onda važi:
      i) $A \cap C \subset B \cap C$;

ii) $A \cup C \subset B \cup C$;
iii) $C \setminus B \subset C \setminus A$.

5. Dokazati da su sledeći uslovi ekvivalentni ako su A i B proizvoljni podskupovi skupa U.

   a) $A \subset B$;
   b) $A \cup B = B$;
   c) $A \cap B = A$;
   d) $A \cap \overline{B} = \emptyset$.

6. Dokazati da za proizvoljne skupove A, B, C važi:

   a) $\overline{A \cap B} = \overline{A} \cup \overline{B}, \overline{A \cup B} = \overline{A} \cap \overline{B}$;
   b) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;
   c) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
   d) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$.

7. Dokazati da za $A, B, C \subset U$ važi:

   a) $A \triangle A = \emptyset, A \triangle \emptyset = A, A \triangle U = \overline{A}$;
   b) $A \triangle B = B \triangle A$;
   c) $A \triangle B = (A \cup B) \setminus (A \cap B)$;
   d) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

8. Neka je $A = \{1, 2\}$. Odrediti $A \cap \mathcal{P}(A)$.

9. Neka je $A = \{1, \{1\}\}$. Odrediti $A \cap \mathcal{P}(A)$.

10. Naći skup A koji ima bar dva zajednička elementa sa skupom $\mathcal{P}(A)$.

11. Dokazati da za proizvoljne skupove E i F važi:

    a) $\mathcal{P}(E) \cap \mathcal{P}(F) = \mathcal{P}(E \cap F)$;
    b) $\mathcal{P}(E) \cup \mathcal{P}(F) \subset \mathcal{P}(E \cup F)$;
    c) $\mathcal{P}(E) \cup \mathcal{P}(F) \neq \mathcal{P}(E \cup F)$ u opštem slučaju.

12. Naći troelementni skup A koji ima bar dva zajednička elementa sa $\mathcal{P}(A)$.

13. Naći skup A koji ima neprazan presek sa $\mathcal{P}(\mathcal{P}(A))$.

4 Relacije

4.1 Osnovni pojmovi

Ako je A neprazan skup i n prirodan broj, onda je podskup ρ iz A^n *n-arna relacija* na A. Broj n je arnost relacije ρ. Relacije arnosti 1 su *unarne*, relacije arnosti dva su *binarne* relacije, a arnosti tri su *ternare* relacije. Za nas su najinteresantnije binearne relacije. Ako je $(x, y) \in \rho$, kažemo da je x u relaciji ρ sa y, to označavamo i na sledeći način: $x\rho y$.

Primer 4.1.

- *Skup* $\mathbb{P}$ *parnih brojeva je unarna relacija na skupu* $\mathbb{N}$.
- *Najpoznatije binarne relacije na skupu* $\mathbb{N}$ *su* $\leqslant$, $<$, $=$, $|\ldots$
- *Skup* $\{(x, y, z) : x^2 + y^2 = z^2\}$ *je ternarna relacija na* $\mathbb{R}$.

Nadalje, kad kažemo relacija, uvek mislimo na binarnu relaciju sem ako nije drugačije naglašeno.

Prazan skup kao podskup iz A^2 je *prazna relacija* na A. Ceo skup A^2 je puna relacija na A. Relacija $\triangle = \{(x, x) : x \in A\}$ zove se *dijagonalna relacija* na skupu A. Ako su ρ i θ relacije na A, onda je

- $\rho \cap \theta = \{(x, y) : (x, y) \in \rho \wedge (x, y) \in \theta\}$;
- $\rho \cup \theta = \{(x, y) : (x, y) \in \rho \vee (x, y) \in \theta\}$;
- $\overline{\rho} = \{(x, y) : (x, y) \notin \rho\}$;
- $\rho \subseteq \theta \Leftrightarrow ((x, y) \in \rho \Rightarrow (x, y) \in \theta)$;
- $\rho^{-1} = \{(y, x) : (x, y) \in \rho\}$.

Primer 4.2.

Na skupu $\mathbb{N}$ $\leqslant \cap \geqslant = \triangle$, $\leqslant \cup \geqslant = \mathbb{N}^2$;

Na skupu $\mathbb{N}$ $\overline{<} = \geqslant$, $<^{-1} = >$.

Na skupu $\mathbb{N}$ $\triangle \subseteq | \subseteq \leqslant$.

Kompozicija relacija ρ i θ na skupu A je relacija $\rho \circ \theta$ na A definisana na sledeći način:

$$\rho \circ \theta = \{(x, y) : (\exists z)((x, z) \in \rho \wedge (z, y) \in \theta)\}.$$

Primer 4.3. *Neka je* $A = \{a, b, c, d\}$ *i* $\rho = \{(a, b), (a, c), (a, d), (b, d)\}$ *i* $\theta = \{(b, a), (b, c), (d, c)\}$. *Tada*

$$\rho \circ \theta = \{(a, a), (a, c), (b, c)\};$$

$$\theta \circ \rho = \{(b, b), (b, c), (b, d)\}.$$

Dakle, u opštem slučaju kompozicija nije komutativna. Komutativnost važi samo u nekim specijalnim slučajevima.

Teorema 4.4. *Ako je* $\rho \subseteq A^2$, *onda je* $\rho \circ \triangle = \triangle \circ \rho = \rho$.

Dokaz. $(x, y) \in \rho \circ \triangle$ ako i samo ako $(\exists z)((x, z) \in \rho \wedge (z, y) \in \triangle)$. Ako postoji elemenat označen sa z, onda to može biti samo y, (jer $(z, y) \in \triangle$) i obratno, elemenat y garantuje postojanje traženog z. Zato je poslednja formula ekvivalentna sa $(x, y) \in \rho \wedge (y, y) \in \triangle$, odnosno $(x, y) \in \rho$. Sličan je dokaz i druge jednakosti. ■

Teorema 4.5. *Kompozicija relacija je asocijativna, tj. za* $\rho, \theta, \sigma \subseteq A^2$ *važi* $\rho \circ (\theta \circ \sigma) = (\rho \circ \theta) \circ \sigma$.

Teorema 4.6. *Za proizvolje relacija* ρ, θ, σ *na* A *važi:*

1. $\rho \circ (\theta \cup \sigma) = (\rho \circ \theta) \cup (\rho \circ \sigma)$; $(\rho \cup \theta) \circ \sigma = (\rho \circ \sigma) \cup (\theta \circ \sigma)$;
2. $\rho \circ (\theta \cap \sigma) \subseteq (\rho \circ \theta) \cap (\rho \circ \sigma)$; $(\rho \cap \theta) \circ \sigma \subseteq (\rho \circ \sigma) \cap (\theta \circ \sigma)$;
3. $(\rho \cup \theta)^{-1} = \rho^{-1} \cup \theta^{-1}$;
4. $(\rho \cap \theta)^{-1} = \rho^{-1} \cap \theta^{-1}$;
5. $(\rho \circ \theta)^{-1} = \theta^{-1} \circ \rho^{-1}$;
6. $(\rho^{-1})^{-1} = \rho$;
7. $(\overline{\rho})^{-1} = \overline{(\rho^{-1})}$.

Dokaz. Za vežbu. ■

Teorema 4.7. *Ako su* ρ, θ, σ *relacije na* A, *onda važi:* $\rho \subseteq \theta \Rightarrow \sigma \circ \rho \subseteq \sigma \circ \theta$ *i* $\rho \subseteq \theta \Rightarrow \rho \circ \sigma \subseteq \theta \circ \sigma$.

Dokaz. Za vežbu. ■

4.2 Relacija ekvivalencije i relacija poretka

Relacija ρ na skupu A je

- *refleksivna* ako i samo ako za sve $x \in A$ važi $(x, x) \in \rho$, odnosno ako i samo ako $\triangle \subseteq \rho$;
- *simetrična* ako i samo ako za sve $x, y \in A$ važi $(x, y) \in \rho \Rightarrow (y, x) \in \rho$, odnosno ako i samo ako $\rho \subseteq \rho^{-1}$;
- *tranzitivna* ako i samo ako za sve $x, y, z \in A$ važi $(x, y) \in \rho \wedge (y, z) \in \rho \Rightarrow (x, z) \in \rho$, odnosno ako i samo ako $\rho \circ \rho \subseteq \rho$.

Relacija ρ na A koja je refleksivna, simetrična i tranzitivna je *relacija ekvivalencije* na A.

Neka je ρ relacija ekvivalencije na A i $a \in A$. *Klasa ekvivalencije* za a je skup $[a]_\rho = \{x : a\rho x\}$ a skup $A/\rho = \{[x]_\rho : x \in A\}$ se zove *količnički skup*.

Teorema 4.8. *Neka je ρ proizvoljna relacija ekvivalencije na A i $x, y \in A$. Tada*

1. $[x]_\rho \neq \emptyset$;
2. $[x]_\rho \cap [y]_\rho \neq \emptyset \Rightarrow [x]_\rho = [y]_\rho$;
3. $\bigcup\{[x]_\rho : x \in A\} = A$.

Dokaz.

1. Za svako x iz A je zbog refleksivnosti $x\rho x$. Otuda bar $x \in [x]_\rho$.
2. Pretpostavimo da $z \in [x]_\rho \cap [y]_\rho$. Odatle $x\rho z$ i $y\rho z$. Koristeći to, kao i osobine relacije ekvivalencije, dokazujemo da su klase $[x]_\rho$ i $[y]_\rho$ jednake. Ako $u \in [x]_\rho$, onda $x\rho u$, odnosno $u\rho x$. Kako je $x\rho z$, sledi $u\rho z$, a zbog $z\rho y$ je $u\rho y$, odnosno $y\rho u$. Dakle, $u \in [y]_\rho$, tj. $[x]_\rho \subseteq [y]_\rho$. Analogno se pokazuje i obratna inkluzija, pa važi jednakost klasa.
3. Svaki $x \in A$ je u klasi $[x]_\rho$, zato je A podskup unije klasa, obrat je očigledan.

■

Kolekcija nepraznih, u parovima disjunktnih podskupova skupa A, čija je unija A, zove se *particija* (razbijanje) skupa A. Skupovi koji obrazuju particiju su njene *klase*. Količnički skup je tako jedna particija skupa A. Kaže se i da relacija ekvivalencije razbija skup na klase ekvivalencije.

Ne samo da klase ekvivalencije date relacije ekvivalencije obrazuju particiju, nego i obratno: particija na skupu A određuje relaciju ekvivalencije.

Teorema 4.9. *Neka je* Π *particija nepraznog skupa* A. *Definišemo na* A *relaciju* ρ_Π *na sledeći način:* $x\rho_\Pi y$ *ako i samo ako* x *i* y *pripadaju istoj klasi particije* Π. *Tada je* ρ_Π *relacija ekvivalencije na* A.

Dokaz. Sledi neposredno iz gornje definicije relacije ρ_Π. ■

Teorema 4.10. *Neka je* ρ *relacija ekvivalencije na* A, *a* ρ_1 *relacija ekvivalencije koja odgovara particiji* A/ρ. *Tada je* $\rho = \rho_1$. *Obratno, neka je* Π *particija skupa* A *i* ρ_Π *odgovarajuća relacija ekvivalencije. Tada* $A/\rho_\Pi = \Pi$.

Dokaz. Direktno iz definicije. ■

Relacija ρ na skupu A je *antisimetrična* ako i samo ako za sve $x, y \in A$ važi $(x, y) \in \rho \wedge (y, x) \in \rho \Rightarrow x = y$, odnosno ako i samo ako $\rho \cap \rho^{-1} \subseteq \triangle$.

Relacija ρ na A koja je refleksivna, antisimetrična i tranzitivna je *relacija poretka* na A. Ako je ρ relacija poretka na A, onda se kaže da je A *uređen* relacijom ρ. Uređeni par (A, ρ) tada se zove *uređeni skup*. Poredak ρ na A je *linearan* ako za sve $x, y \in A$ važi $x\rho y$ ili $y\rho x$.

Uređeni skupovi mogu se predstavljati dijagramima. Elementi skupa A predstavljaju se kao tačke u ravni i to tako da se $x\rho y$ obeležava spojnicom od x ka y, pri čemu je na crtežu x niže od y. Ne označava se $x\rho x$, niti $x\rho z$ ako postoje spojnice $x\rho y$ i $y\rho z$. Na sledećoj slici su dijagrami tri konačna uređena skupa. Prvi je linearno uređeni skup $(\{1, 2, 3, 4\}, \leqslant)$. Druga je kolekcija četiri podskupa skupa $\{a, b, c, d\}$ uređena inkluzijom. Treći je $(\{1, 2, 3, 4, 5, 6\}, |)$.

slika :)

Neka je (A, ρ) uređeni skup.

- Elemenat $a \in A$ je *minimalan*, ako ne postoji $x \in A$ tako da $x \neq a$ i $x\rho a$;
- Elemenat $a \in A$ je *maksimalan*, ako ne postoji $x \in A$ tako da $x \neq a$ i $a\rho x$;
- Elemenat $a \in A$ je *najmanji*, ako za sve $x \in A$ važi $a\rho x$;

- Elemenat $a \in A$ je *najveći*, ako za sve $x \in A$ važi $x \rho a$.

Primer 4.11. *U prvom uređenom skupu elemenat* 1 *je i minimalan i najmanji, a* 4 *i maksimalan i najveći. U drugom uređenom skupu elementi* $\{a\}$ *i* $\{b\}$ *su minimalni, a* $\{a, b, c\}$ *i* $\{a, b, d\}$ *maksimalni, najmanji i najveći elemenat ne postoji. U trećem uređenom skupu elemenat* 1 *je i minimalan i najmanji, elementi* 4, 5 *i* 6 *su maksimalni, a najveći ne postoji.*

Zadaci iz relacija

1. Dokazati da za proizvoljne relacije ρ, θ, σ na A važi:

   a) $\rho \circ (\theta \cup \sigma) = (\rho \circ \theta) \cup (\rho \circ \sigma)$; $(\rho \cup \theta) \circ \sigma = (\rho \circ \sigma) \cup (\theta \circ \sigma)$;

   b) $\rho \circ (\theta \cap \sigma) \subseteq (\rho \circ \theta) \cap (\rho \circ \sigma)$; $(\rho \cap \theta) \circ \sigma \subseteq (\rho \circ \sigma) \cap (\theta \circ \sigma)$;

   c) $(\rho \cup \theta)^{-1} = \rho^{-1} \cup \theta^{-1}$;

   d) $(\rho \cap \theta)^{-1} = \rho^{-1} \cap \theta^{-1}$;

   e) $(\rho \circ \theta)^{-1} = \theta^{-1} \circ \rho^{-1}$;

   f) $(\rho^{-1})^{-1} = \rho$;

   g) $(\overline{\rho})^{-1} = \overline{(\rho^{-1})}$.

2. Ako su ρ, θ, σ relacije na A, dokazati da važi: $\rho \subseteq \theta \Rightarrow \sigma \circ \rho \subseteq \sigma \circ \theta$ i $\rho \subseteq \theta \Rightarrow \rho \circ \sigma \subseteq \theta \circ \sigma$.

3. Odrediti da li su sledeće relacije na $A = \{1, 2, 3\}$ refleksivne, simetrične, anitisimetrične, tranzitivne:

   a) $\{(1, 1), (2, 2)\}$;

   b) $\{(1, 1), (1, 3)\}$;

   c) $\{(2, 2), (1, 3), (3, 1)\}$;

   d) $\{(1, 2), (1, 3)\}$;

   e) $\{(1, 1), (2, 2), (3, 3), (1, 3), (2, 3)\}$;

   f) $\{(1, 1), (2, 2), (3, 3)\}$.

4. Koje od sledećih relacija su relacije ekvivalencije:

   a) paralelnost pravih;

b) normalnost pravih;

c) podudarnost trouglova;

d) relacija $\equiv_m \subseteq \mathbb{N}^2$, $m \in \mathbb{N}$, gde $a \equiv_m b$ ako i samo ako $m \mid (a - b)$.

5. Data je relacija $\rho = \{(2,2),(2,3),(5,3)\}$ na skupu $A = \{1,2,3,4,5\}$.

   a) Odrediti najmanju relaciju ekvivalencije na A koja sadrži ρ i naći klase ekvivalencije;

   b) Odrediti najmanju relaciju poretka na A koja sadrži ρ i nacrtati odgovarajući Hase-dijagram.

6. Ako je $\mathbb{P}$ skup svih parnih brojeva, relacija $\sim$ na $\mathbb{Z}$ je definisana sa $x \sim y$ ako i samo ako je $x + y \in \mathbb{P}$. Da li je $\sim$ relacija ekvivalencije i ako jeste, šta su klase ekvivalencije?

7. Neka je ρ relacija ekvivalencije na skupu A, θ relacija ekvivalencije na B i τ relacija na $A \times B$ definisana sa $(x,y)\tau(u,v)$ ako i samo ako $x\rho u$ i $y\theta v$. Dokazati da je τ relacija ekvivalencije na $A \times B$.

8. Koja od navedenih relacija su parcijalna/linearna uređenja:

   a) $\leqslant$ na $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$;

   b) $\subseteq$ na $\mathcal{P}(A)$ za proizvoljno A;

   c) $\mid$ na $\mathbb{N}$, $\mathbb{Z}$.

9. Dokazati da svako parcijalno uređenje ima najviše po jedan najmanji i najveći elemenat.

10. Nacrtati Hase-dijagram za sledeće uređene skupove:

    a) $(\{1, 2, \ldots, 12\}, |)$;

    b) $(\mathbb{N}, \leqslant)$;

    c) $(P(A), \subseteq)$ za $A = \{a, b, c\}$.

11. Odrediti specijalne elemente za uređene skupove iz prethodnog zadatka.

5 Funkcije

5.1 Osnovni pojmovi

Neka su A i B proizvoljni neprazni skupovi. Tada se $f \subseteq A \times B$ zove *funkcija* iz A u B ako i samo ako za svako $x \in A$ postoji tačno jedno $y \in B$ tako da $(x, y) \in f$. $(x, y) \in f$ se beleži sa $f(x) = y$. Elemenat x je *original*, a y njegova *slika*. Skup A se zove *domen* funkcije f, a B *kodomen*. Skup

$$f(A) = \{y \in B : y = f(x), \text{za neko } x \in A\}$$

je podskup kodomena koji se zove *skup slika*. Da je f funkcija iz A u B označava se sa $f : A \to B$, a koristi se i oznaka $f : x \mapsto f(x)$. Funkcije $f \subseteq A \times B$ i $g \subseteq C \times D$ su jednake ako je $A = C$, $B = D$ i $f = g$. Ako je $f : A \to B$ i X neprazni podskup iz A, onda se definiše nova funkcija, čiji je domen X, u oznaci $f|_X : X \to B$, tako da je za $x \in X$ $f|_X(x) = f(x)$. $f|_X$ je *restrikcija* funkcije f na X.

Neka su dati skupovi A, B i C i funkcije $f : A \to B$ i $g : B \to C$. Uzastopnim primenom ovih funkcija dobija se *kompozicija* funkcija f i g u oznaci $g \circ f$. To je funkcija iz A u C definisana sa

$$g \circ f(x) = g(f(x)).$$

Funkcija $I_A : A \to A$ definisana sa $I_A(x) = x$ za sve $x \in A$ zove se *identička funkcija* ili identičko preslikavanje.

Teorema 5.1. *Neka je $f : A \to B$. Tada je $f \circ I_A = f$ i $I_B \circ f = f$.*

Dokaz. Domen funkcije $f \circ I_A$ je A, a kodomen B. Dalje, $f \circ I_A(x) = f(I_A(x)) = f(x)$. Dokaz druge jednakosti je sličan. ■

Teorema 5.2. *Neka je $f : A \to B$, $g : B \to C$ i $h : C \to D$. Tada je*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Dokaz. Domen obe funkcije $h \circ (g \circ f)$ i $(h \circ g) \circ f$ je A, a kodomen D. Dalje, za $x \in A$ $h \circ (g \circ f)(x) = h(g \circ f(x)) = h(g(f(x))$, i $(h \circ g) \circ f(x) = h \circ g(f(x))) = h(g(f(x)))$. ■

Funkcija $f : A \to B$ je *injektivna, injekcija, „1-1“* ako ispunjava uslov: iz $x_1 \neq x_2$ sledi $f(x_1) \neq f(x_2)$. Funkcija $f : A \to B$ je je *sirjektivna, sirjekcija, „na“* ako ispunjava uslov: za svako $y \in B$ postoji $x \in A$ tako da je $y = f(x)$. Funkcija $f : A \to B$ je *bijekcija* ako je istovremeno sirjekcija i injekcija.

Teorema 5.3. *Neka je $f : A \to B$ i $g : B \to C$.*

1. *Ako su f i g injektivne, onda je i $g \circ f$ injektivna funkcija.*

2. *Ako su f i g sirjektivne, onda je i $g \circ f$ sirjektivna funkcija.*

Dokaz. 1. Neka $x_1 \neq x_2$. Tada, pošto je f injekcija sledi $f(x_1) \neq f(x_2)$. Iz ovoga sada, pošto je g injekcija sledi $g(f(x_1)) \neq g(f(x_2))$, pa je $g \circ f$ injektivna funkcija.

2. Neka je $z \in C$. Pošto je g sirjektivna funkcija postoji $y \in B$ tako da $g(y) = z$. Sada za $y \in B$ zbog sirjektivnosti funkcije f postoji $x \in A$ tako da $f(x) = y$, tj. sveukupno $g(f(x)) = z$ pa je $g \circ f$ sirjektivna funkcija.

■

Posledica 5.4. *Ako su $f : A \to B$ i $g : B \to C$ bijekcije, onda je i $g \circ f : A \to C$ bijekcija.*

Teorema 5.5. *Neka je $f : A \to B$ i $g : B \to C$.*

1. *Ako je $g \circ f$ injektivna funkcija, onda je i f injekcija.*

2. *Ako je $g \circ f$ sirjektivna funkcija, onda je i g sirjekcija.*

Dokaz. Za vežbu. ■

Teorema 5.6. *Neka je data funkcija $f : A \to B$. Postoji najviše jedna funkcija $g : B \to A$ takva da važi $g \circ f = I_A$ i $f \circ g = I_B$.*

Dokaz. Pretpostavimo suprotno, da postoje dve funkcije $g_1 : B \to A$ i $g_2 : B \to A$ sa navedenim osobinama, tj. takve da važi $g_1 \circ f = I_A$, $f \circ g_1 = I_B$, $g_2 \circ f = I_A$, $f \circ g_2 = I_B$. Tada prema teoremama 5.1 i 5.2 imamo

$$g_1 = g_1 \circ I_B = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = I_A \circ g_2 = g_2.$$

■

Na osnovu ovog tvrđenja uvodimo sledeću definiciju i novu oznaku. Neka je $f : A \to B$. Ako postoji funkcija $f^{-1} : B \to A$, sa osobinama $f^{-1} \circ f = I_A$ i $f \circ f^{-1} = I_B$, onda je f^{-1} *inverzna funkcija* funkcije f.

Teorema 5.7. *Funkcija f ima inverznu funkciju ako i samo ako je f bijekcija.*

Dokaz. Pretpostavimo da $f : A \to B$ ima inverznu funkciju f^{-1}. Dokazujemo da je f bijekcija. Iz $f^{-1} \circ f = I_A$ i $f \circ f^{-1} = I_B$ i činjenica da su I_A i I_B bijekcije, prema teoremi 5.5 sledi da je f bijekcija.

Obratno, pretpostavimo da je f bijekcija iz A u B. Definišemo funkciju $f^{-1} : B \to A$ na sledeći način. Za $y \in B$ $f^{-1}(y) = x$ ako i samo ako $f(x) = y$. Funkcija f^{-1} je dobro definisana jer je f injekcija i sirjekcija. Dokazujemo da f^{-1} ima svojstvo inverzne funkcije. Neka je $x \in A$. Tada je $f^{-1} \circ f(x) = f^{-1}(f(x)) = f^{-1}(y) = x = I_A(x)$, tj. $f^{-1} \circ f = I_A$. Ako je $y \in B$, onda je $f \circ f^{-1}(y) = f(f^{-1}(y)) = f(x) = y = I_B(y)$, tj. $f \circ f^{-1} = I_B$. ■

Teorema 5.8. *Neka je $f^{-1} : B \to A$ inverzna funkcija funkcije $f : A \to B$. Tada važi*

1. *f^{-1} je bijekcija;*
2. *$(f^{-1})^{-1} = f$*

Dokaz.

1. Kako je $f \circ f^{-1} = I_B$, a I_B injekcija, po teoremi 5.5 f^{-1} je injekcija. Slično, kako je $f^{-1} \circ f = I_A$, a I_A sirjekcija, opet po teoremi 5.5 f^{-1} je sirjekcija.

2. Kako je $f^{-1} : B \to A$ bijekcija, ima inverznu funkciju koja preslikava A u B. Iz jednakosti $f^{-1} \circ f = I_A$ i $f \circ f^{-1} = I_B$, kao i činjenice da je inverzna funkcija jedinstvena, sledi da je inverzna funkcija za f^{-1} upravo f.

■

Neka je f proizvoljna funkcija iz A u B. Definišemo na skupu A relaciju $\ker f$ na sledeći način: $x \ker f y$ ako i samo ako $f(x) = f(y)$. Relacija $\ker f$ zove se *jezgro* funkcije f.

Teorema 5.9. *Jezgro funkcije $f : A \to B$ je relacija ekvivalencije na skupu A.*

Dokaz. Dokaz sledi direktno iz definicije. ■

Kolekcija svih funkcija iz skupa A u skup B označava se sa B^A. Funkcija f iz $\mathbb{N}$ u A, gde je $\mathbb{N}$ skup prirodnih brojeva, a A proizvoljan neprazan skup zove se *niz*.

5.2 Ekvivalenti skupovi, kardinali

Skup A je ekvivalentan sa skupom B, u oznaci $A \sim B$ ako i samo ako postoji bijekcija $f : A \to B$.

Primer 5.10.

1. *Skupovi $\{1, 2, 3\}$ i $\{a, b, c\}$ jesu ekvivalentni, dok $\{1, 2\}$ i $\{a, b, c\}$ nisu, jer ne postoji nijedna bijekcija iz $\{1, 2\}$ u $\{a, b, c\}$.*

2. *Skup prirodnih brojeva $\mathbb{N}$ i skup svih parnih brojeva $\mathbb{N}_P$ su ekvivalentni, jedna bijekcija između njih je $f : \mathbb{N} \to \mathbb{N}_P$ data sa $f(n) = 2n$.*

3. *Intervali realnih brojeva $A = [0, 1]$ i $B = [5, 7]$ su ekvivalentni. Funkcija $f : A \to B$, data formulom $f(x) = 2x + 5$ je bijekcija iz A u B.*

Teorema 5.11. *Ako su A, B i C proizvoljni skupovi, onda važi:*

- *$A \sim A$;*
- *iz $A \sim B$ sledi $B \sim A$;*
- *ako je $A \sim B$ i $B \sim C$, onda je $A \sim C$.*

Dokaz. Direktno iz definicije. ■

Skup je *beskonačan* ako je ekvivalentan sa nekim svojim pravim podskupom. Skup koji nije beskonačan je *konačan*. Ako je skup ekvivalentan sa skupom prirodnih brojeva, onda je *prebrojiv*.

Teorema 5.12. *Skup celih brojeva $\mathbb{Z}$ je prebrojiv.*

Dokaz. Funkcija $f : \mathbb{Z} \to \mathbb{N}$ data sa

$$f(x) = \begin{cases} 2x + 1, \text{ ako je } x \geqslant 0; \\ -2x, \text{ ako je } x < 0. \end{cases}$$

je bijekcija. ■

Teorema 5.13. *Skup racionalnih brojeva $\mathbb{Q}$ je prebrojiv.*

Teorema 5.14. *Nijedan skup nije ekvivalentan sa svojim partitivnim skupom*

Dokaz. Pretpostavimo suprotno, tj. da za neki skup A postoji bijekcija f iz A u $\mathcal{P}(A)$. Uočimo skup

$$B = \{x \in A : x \notin f(x)\}.$$

B je podskup iz A. Po pretpostavci postoji $b \in A$ takav da je $f(b) = B$. Za b postoje dve mogućnosti: $b \in B$, ili $b \notin B$. Obe mogućnosti daju kontradikciju. ■

Teorema 5.15. *Skup realnih brojeva je ekvivalentan sa partitivnim skupom prirodnih brojeva.*

Skup realnih brojeva, dakle, nije prebrojiv, kažemo da je *neprebrojiv*.

Teorema 5.16. *Svi intervali realnih brojeva su međusobno ekvivalentni i ekvivalentni su sa celim skupom realnih brojeva.*

Dokaz. Za vežbu. ■

Svakom skupu A pridružuje se *kardinalni broj*, tako da važi A i B imaju isti kardinalni broj ako i samo ako $A \sim B$. Precizna definicija kardinalnog broja je van ovog kursa. Kardinalni broj konačnog skupa jednak je broju elemenata tog skupa. Kardinalni broj prebrojivog skupa je $\aleph_0$ (alef nula). Skupovi $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ dakle imaju kardinalni broj $\aleph_0$. Kardinalni broj skupa realnih brojeva $\mathbb{R}$ označava se sa c (kontinuum). Na osnovu teorema 5.14 i 5.15 sledi $\aleph_0 \neq c$.

Zadaci iz funkcija

1. Dopuniti sledeće skupove $f \subseteq A \times B$ do funkcije, ako je $A = \{1, 2, 3, 4\}$ i $B = \{1, 2, 3\}$, a zatim odrediti da li su injekcije, sirjekcije, bijekcije:

   a) $\{(1, 1), (2, 3), (3, 2)\}$;

   b) $\{(2, 1), (2, 2), (3, 3)\}$.

2. Ispitati da li su sledeće funkcije injekcije, sirjekcije, bijekcije:

   a) $f : \mathbb{R} \to \mathbb{R}$ definisana sa $f(x) = 2x - 1$;

b) $g : \mathbb{R} \to \mathbb{R}$ definisana sa $g(x) = x^2 - 5x - 10$;

c) $h : \mathbb{R} \to \mathbb{R}$ definisana sa $h(x) = x^3$;

d) $k : \mathbb{R} \to \mathbb{R}$ definisana sa $k(x) = \begin{cases} 3x + 2 & x \in \mathbb{Q} \\ x^3 & x \notin \mathbb{Q} \end{cases}$

3. Neka je $f : A \to B$ i $g : B \to C$. Dokazati:

   a) Ako je $g \circ f$ injektivna funkcija, onda je i f injektivna. Da li i g mora biti injektivna?

   b) Ako je $g \circ f$ sirjektivna funkcija, onda je i g sirjektivna. Da li i f mora biti sirjektivna?

4. Neka je $f : X \to Y$, $A, B \subseteq X$, $C, D \subseteq Y$. Tada važi:

   a) ako je $A \subseteq B$, onda $f(A) \subseteq f(B)$;

   b) ako je $C \subseteq D$, onda je $f^{-1}(C) \subseteq f^{-1}(D)$

   c) $f(A \cup B) = f(A) \cup f(B)$;

   d) $f(A \cap B) \subseteq f(A) \cap f(B)$;

   e) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$;

   f) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$;

   g) $A \subseteq f^{-1}(f(A))$;

   h) $f(f^{-1}(C)) \subseteq C$.

5. Odrediti $\ker f$ za $f : \mathbb{Z} \to \mathbb{Z}$ definisanu sa $f(x) = |x|$.

6. Data je funkcija $f : A \to B$. Dokazati da je f injekcija ako i samo ako $\ker f = \triangle_A$.

7. Dokazati da su svi intervali realnih brojeva međusobno ekvivalentni i da su ekvivalentni sa celim skupom realnih brojeva.

6 Grupe

6.1 Osnovni pojmovi

Ako je A neprazan skup i $n \in \mathbb{N}$, onda se funkcija $f : A^n \to A$ zove operacija na A.

Uređeni par $(G, \cdot)$, gde je G neprazan skup se zove *grupa*, ako

- $\cdot$ je binarna operacija na G;
- za sve $x, y, z \in G$ je ispunjeno $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
- postoji u G *neutralni elemenat* e tako da za svako $x \in G$ važi $x \cdot e = e \cdot x = x$;
- za svako $x \in G$ postoji *inverzni elemenat* $y \in G$, tako da je $x \cdot y = y \cdot x = e$, gde je e neutralni elemenat iz prethodne tačke.

Primer 6.1. $(\mathbb{Z}, +)$ *jeste grupa,* $(\mathbb{N}, +)$ *nije grupa jer (između ostalog) ne postoji u njoj neutralni elemenat,* $(\mathbb{N}_0, +)$ *nije grupa, jer sem* 0 *nijedan elemenat nema inverzni,* $(\mathbb{N}, -)$ *isto nije grupa jer (između ostalog)* $-$ *nije operacija na skupu* $\mathbb{N}$.

Ako u nekoj grupi $(G, \cdot)$ za sve $x, y \in G$ je ispunjeno $x \cdot y = y \cdot x$, onda kažemo da je $(G, \cdot)$ *Abelova grupa.*

Teorema 6.2.

1. *U svakoj grupi* $(G, \cdot)$ *neutralni elemenat je jedinstven.*
2. *U svakoj grupi* $(G, \cdot)$ *inverzni elemenat svakog elementa je jedinstven.*

Dokaz.

1. Pretpostavimo suprotno, da imamo bar dva neutralna elementa, neka su oni e_1 i e_2. Tada imamo $e_1 = e_1 \cdot e_2 = e_2$.
2. Opet pretpostavimo suprotno, neka elemenat x ima dva inverzna elementa y i z. Neka je e neutralni elemenat grupe G. Tada važi $y = y \cdot e = y \cdot (x \cdot z) = (y \cdot x) \cdot z = e \cdot z = z$.

■

Najčešće oznake za operacije u grupi su $\cdot$ i $+$. Prvo označavanje je *multiplikativno*, a drugo *aditivno*. U multiplikativnoj notaciji neutralni elemenat se često se označava sa 1, a inverzni za a sa a^{-1}, dok u aditivnoj notaciji neutralni elemenat se označava sa 0, a inverzni za a sa $-a$.

Iz jedinstvenosti inverznih elemenata i jednakosti $x \cdot x^{-1} = x^{-1} \cdot x = e$, sledi da je inverzni elemenat za x^{-1} je baš x. Drugim rečima, $(x^{-1})^{-1} = x$ za svako $x \in G$.

Teorema 6.3. *U svakoj grupi $(G, \cdot)$ za $a, b \in G$ jednačine $a \cdot x = b$ i $y \cdot a = b$ imaju jedinstvena rešenja po x odnosno y.*

Dokaz. Jedno rešenje jednačine $a \cdot x = b$ je $a^{-1} \cdot b$. Zaista, $a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = e \cdot b = b$. Označimo sa c elemenat $a^{-1} \cdot b$. Pretpostavimo da je i neko $d \in G$ rešenje, tj. da je $a \cdot d = b$. Tada je $d = e \cdot d = (a^{-1} \cdot a) \cdot d = a^{-1} \cdot (a \cdot d) = a^{-1} \cdot b = c$, pa je rešenje jedinstveno. ■

Ako je grupa konačna, onda se ova jedinstvenost rešenja gornjih jednačina prepoznaje u njenoj Kejlijevoj tablici: u svakoj vrsti i koloni, svaki elemenat grupe javlja se tačno jednom.

Posledica 6.4. *Za proizvoljne elemente a, b i c grupe $(G, \cdot)$ ispunjeno je*

iz $a \cdot c = b \cdot c$ sledi $a = b$;

iz $c \cdot a = c \cdot b$ sledi $a = b$.

Dokaz. Sledi neposredno iz jedinstvenosti rešenja jednačina navedenih u teoremi 6.3. ■

Za elemenat x grupe G kažemo da je *idempotentan* ako je ispunjeno $x \cdot x = x$. Važi sledeće.

Lema 6.5. *U grupi $(G, \cdot)$ jedini idempotentan elemenat je neutralni elemenat e.*

Dokaz. Lako se vidi da je e zaista idempotentan. S druge stane, ako je za neki elemenat x ispunjeno je $x \cdot x = x$, tada $x = x \cdot e = x \cdot (x \cdot x^{-1}) = (x \cdot x) \cdot x^{-1} = x \cdot x^{-1} = e$. ■

Ako je $(G, \cdot)$ grupa i H neprazni podskup iz G, onda je $(H, \cdot_1)$ *podgrupa* grupe G, ako je $(H, \cdot_1)$ grupa i $\cdot_1$ je restrikcija operacije $\cdot$ na skup $H \times H$. Uobičajeno je da se podgrupa grupe $(G, \cdot)$ označava sa $(H, \cdot)$, odnosno da operacija $\cdot$ i njena restrikcija imaju istu oznaku. Da je H podgrupa grupe G, označava se često i sa $H \leqslant G$.

Teorema 6.6. *Za podgrupu H grupe $(G, \cdot)$ ispunjeno je:*

1. *neutralni elemenat u H poklapa se sa neutralnim elementom iz G;*
2. *ako je $a \in H$, onda se inverzni elemenat za a u H poklapa sa inverznim elementom za a u G.*

Dokaz.

1. $(H, \cdot)$ je grupa, pa ona ima neutralni elemenat e_1, za koji važi $e_1 \cdot e_1 = e_1$. Kako je $e_1 \in G$, a u grupi je samo neutralni elemenat idempotentan (teorema 6.5), sledi $e_1 = e$.
2. Neka je a^{-1} inverzni elemenat za a u G. Zbog jedinstvenosti inverznih elemenata u G, samo je a^{-1} rešenje jednačine $a \cdot x = e$ i $x \cdot a = e$, pa je dokazan i ovaj deo.

■

Teorema 6.7. *Neprazan podskup H, grupe $(G, \cdot)$ je njena podgrupa, ako i samo ako su ispunjena sledeća dva uslova:*

a) Ako $a, b \in H$, onda $a \cdot b \in H$.

b) Ako $a \in H$, onda $a^{-1} \in H$.

Dokaz. Neka je H podgrupa u G. Uslov a) važi jer je operacija u podgrupi restrikcija operacije u grupi. b) je ispunjeno na osnovu teoreme 6.6.

Obratno, pretpostavimo da je za neprazni podskup H iz G ispunjeno a) i b). Iz a) sledi da je restrikcija operacije $\cdot$ iz G na uređene parove iz H operacija na H. Dokazujemo da neutralni elemenat e pripada H. Kako je H neprazan, postoji $a \in H$. Prema b) $a^{-1} \in H$, odakle, prema a) $a \cdot a^{-1} = e \in H$. Asocijativnost se prenosi na podskup, pa je $(H, \cdot)$ grupa. ■

Gornja karakterizacija podgrupe može se formulisati kao jedinstveni uslov:

Teorema 6.8. *Neprazan podskup H grupe G je njena podgrupa ako i samo ako iz $a, b \in H$ sledi $a \cdot b^{-1} \in H$.*

Dokaz. Ako je H podgrupa i $a, b \in H$, onda na osnovu dela b) prethodnog tvrđenja, $b^{-1} \in H$, a prema a), $a \cdot b^{-1} \in H$.

Obratno, pretpostavimo da uslov tvrđenja važi. Tada za neko $a \in H$ (H je neprazan), $e = a \cdot a^{-1} \in H$. Tada iz $a \in H$ sledi $e \cdot a^{-1} = a^{-1} \in H$. Ispunjen je uslov b) iz prethodne teoreme. Dokazujemo da važi i uslov a). Neka je $a, b \in H$. Tada $b^{-1} \in H$ i odatle $a \cdot (b^{-1})^{-1} = a \cdot b \in H$. Na osnovu prethodne teoreme, H je podgrupa grupe G. ■

U svakoj grupi $(G, \cdot)$ podgrupe su bar $\{e\}$ i sama grupa G, to su *trivijalne podgrupe*.

6.2 Simetrična i ciklična grupa

Sve bijekcije $A \to A$ na nekom nepraznom skupu A obrazuju grupu u odnosu na kompoziciju funkcija. Naime, kompozicija dve bijekcije je takođe bijekcija, kompozicija funkcija je asocijativna, neutralni elemenat je identička funkcija, a inverzni elemenat za f je f^{-1}. Ako skup A ima n elemenata, ova grupa se označava sa S_n i zove se *simetrična grupa* S_n. Primetimo da grupa S_n ima $n!$ elemenata.

Neka su $(G, \cdot)$ i $(H, *)$ dve grupe. Funkcija $f : G \to H$ je *homomorfizam* grupe G u grupu H, ako za sve $x, y \in G$ važi

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

Poslednju jednakost još formulišemo kao saglasnost funkcije f sa operacijama u G i H. Homomorfizam $f : G \to H$ koji je i bijekcija zove se *izomorfizam* grupe G na grupu H. Za grupe G i H kažemo da su izomorfni ako postoji izomorfizam iz G u H. Ako je G izomorfan sa H, pišemo $G \cong H$, odnosno $(G, \cdot) \cong (H, *)$.

Teorema 6.9. *Svaka konačna grupa G reda n izomorfna je sa nekom podgrupom simetrične grupe S_n*

Dokaz. Svaki elemenat a grupe G definiše jednu bijekciju na skupu elemenata te grupe; to je funkcije $\pi_a : x \mapsto ax$. Zaista, ako je $x \neq y$, onda je na osnovu posledice 6.4 $ax \neq ay$, pa je π_a injekcija. Ako je $y \in G$, onda je za $x = a^{-1}y$,

$\pi_a(x) = \pi_a(a^{-1}y) = aa^{-1}y = y$, pa je π_a sirjekcija. Za svako $a \in G$, π_a je tako jedna bijekcija, tj. permutacija skupa G.

Neka je $\Pi_G = \{\pi_a : a \in G\}$. Pokazujemo dve stvari:

1. Π_G u odnosu na kompoziciju je podgrupa grupe S_n.

2. Grupa G izomorfna je sa grupom Π_G.

1. $\pi_a \circ \pi_b = \pi_{ab} \in \Pi_G$, jer je za $x \in G$, $\pi_a \circ \pi_b(x) = \pi_a(\pi_b(x)) = \pi_a(bx) = abx = \pi_{ab}(x)$. Za $x \in G$, $\pi_a \circ \pi_{a^{-1}}(x) = \pi_a(\pi_{a^{-1}}(x)) = \pi_a(a^{-1}x) = aa^{-1}x = x$, pa je $\pi_{a^{-1}}$ inverzna permutacija za π_a i ona pripada skupu Π_G (primetimo da je neutralni elemenat permutacija π_e, za koju je $\pi_e(x) = ex = x$).

   Prema teoremi 6.7, Π_G je podgrupa grupe S_n.

2. Preslikavanje $F : a \mapsto \pi_a$ je bijekcija iz G na Π_G. Zaista, iz $a \neq b$ sledi $ax \neq bx$ (zbog kancelacije), pa je $\pi_a \neq \pi_b$, tj. F je injekcija. Sirjektivnost je očigledna, na π_a se preslikava elemenat a. S obzirom da je $F(ab) = \pi_{ab} = \pi_a \circ \pi_b = F(a) \circ F(b)$, F je izomorfizam.

■

Za $n \in \mathbb{N}$, n-ti stepen elemenata a, u oznaci a^n, je $a \cdot a \cdot \cdots \cdot a$, gde se a ponavlja n puta. Ako je a elemenat grupe $(G, \cdot)$, onda se još definiše $a^0 = e$ i $a^{-n} = (a^{-1})^n$. Skup svih stepena elementa a grupe G označavamo sa $\langle a \rangle$.

Teorema 6.10. *Ako je G grupa, onda je $\langle a \rangle$ podgrupa.*

Dokaz. $\langle a \rangle$ je neprazan podskup iz G, jer sadrži bar a^1 tj. a. Dalje, po definiciji stepena je $a^m \cdot a^n = a^{m+n}$, a inverzni elemenat za a^n je a^{-n}. Prema teoremi 6.7 $\langle a \rangle$ je podgrupa grupe G. ■

Ako je $G = \langle a \rangle$ za neko a, grupa G je *ciklična*.

6.3 Lagranžova teorema, normalne podgrupe

Teorema 6.11. *Ako je H podgrupa grupe G, onda je relacija δ_H na G, definisana sa*

$$a\delta_H b \text{ ako i samo ako } ab^{-1} \in H$$

relacija ekvivalencije.

Dokaz. Za svako $a \in G$, ispunjeno je $a\delta_H a$, jer je $aa^{-1} = e \in H$. Ako je $a\delta_H b$, onda je $ab^{-1} \in H$, pa je i $(ab^{-1})^{-1} \in H$. Kako je $(ab^{-1})^{-1} = ba^{-1}$, sledi $b\delta_H a$. Ako je $a\delta_H b$ i $b\delta_H c$, onda je $ab^{-1} \in H$ i $bc^{-1} \in H$. Odatle je $(ab^{-1})(bc^{-1}) = a(bb^{-1})c = ac^{-1} \in H$, pa važi $a\delta_H c$. ■

Klase ekvivalencije relacije δ_H se mogu opisati na sledeći način.

Ako je H podgrupa grupe G i $a \in G$, onda se skup

$$Ha = \{ha : h \in H\}$$

zove *desna klasa razlaganja* grupe G po podgrupi H, za $a \in G$, ili kraće, desni *koset*.

Desne klase obrazuju particiju grupe G, to sledi iz naredne teoreme.

Teorema 6.12. *Ako je H podgrupa grupe G i Ha desna klasa elementa a, onda je za svako $x \in G$ ispunjeno*

$$x \in Ha \text{ ako i samo ako } x\delta_H a.$$

Dokaz. Ako $x \in Ha$, onda je $x = ha$ za neko $h \in H$, pa je $xa^{-1} = (ha)a^{-1} = h(aa^{-1}) = h$, tj. $xa^{-1} \in H$, odakle $x\delta_H a$. Obratno, ako je $x\delta_H a$, onda je $xa^{-1} \in H$, pa je $xa^{-1} = h$ za neko $h \in H$, odnosno $xa^{-1}a = ha$, tj. $x = ha$, i najzad $x \in Ha$. ■

Zato važi $a\delta_H b$ ako i samo ako $Ha = Hb$. Drugim rečima, klase ekvivalencije relacije δ_H poklapaju se sa desnim klasama po H: $Ha = [a]_{\delta_H}$.

Analogno se za datu podgrupu H definiše relacija λ_H:

$$a\lambda_H b \text{ ako i samo ako } a^{-1}b \in H,$$

a takođe i *leva klasa* aH za $a \in G$:

$$aH = \{ah : h \in H\}.$$

Slično kao gore, važi $a\lambda_H b$ ako i samo ako $aH = bH$, a to znači da se klase ekvivalencije relacije λ_H poklapaju sa levim klasama po H.

Lema 6.13. *Ako je H podgrupa grupe G i $a \in G$, onda je preslikavanje $\sigma_a : h \mapsto ha$ bijekcija iz H na desnu klasu Ha.*

Dokaz. Ako su h_1 i h_2 elementi podgrupe H i $a \in G$, onda iz $h_1 a = h_2 a$ sledi $h_1 = h_2$, na osnovu zakona kancelacije. Zato je σ_a injekcija. Za $ha \in Ha$ jasno je da važi $\sigma_a(h) = ha$, tj. σ_a je i sirjekcija. ■

Sledi značajno svojstvo konačnih grupa, tzv. *Lagranžova teorema.*

Teorema 6.14. *Red konačne grupe deljiv je redom svake njene podgrupe.*

Dokaz. Neka je n red grupe, a m red podgrupe H. Desne klase po H obrazuju particiju skupa G. Grupa je konačnog reda, pa i klasa ima konačno mnogo, tj. $G = H \cup H_{a_1} \cup \cdots \cup Ha_{k-1}$, gde su $a_1, \ldots, a_{k-1}$ neki različiti elementi iz G. Na osnovu prethodne leme, svaka klasa ima isti broj elemenata kao H. Zato $n = k \cdot m$, pa m deli n. ■

Red elemenata a u grupi G definiše se kao red podgrupe $\langle a \rangle$ generisane sa a. Odavde neposredno sledi sledeće svojstvo.

Posledica 6.15. *U grupi konačnog reda red elemenata je delilac reda grupe.*

U opštem slučaju $Ha \neq aH$, tj. desna i leva klasa po podgrupi H za isti elemenat se razlikuju. Podgrupa H grupe G je *normalna*, ako za svako $a \in G$ važi jednakost $Ha = aH$. Da je H normalna podgrupa grupe G označava se sa $H \lhd G$.

Zadaci iz grupa

1. Proveriti da li je grupa:

   a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R} \setminus \{0\}, +)$, $(\mathbb{R}, +)$;

   b) $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$;

   c) Skup svih bijekcija na nepraznom skupu S u odnosu na $\circ$;

   d) Klajnova grupa;

   e) $(\mathcal{P}(S), \triangle)$;

   f) $(\mathbb{Z}_{/\equiv_m}, +_m)$.

2. Dokazati da za svako $n \in \mathbb{N}$ postoji grupa reda n.

3. Ako su $\mathbb{G} = (G, \cdot)$ i $\mathbb{H} = (H, *)$ grupe , onda je i $\mathbb{G} \times \mathbb{H} = (G \times H, \otimes)$ grupa, pri čemu je operacija $\otimes$ definisana sa:

$$(a, b) \otimes (c, d) := (a \cdot c, b * d).$$

4. Neka je $(G, \cdot)$ grupa. Dokazati da za sve $x, y \in G$ važi

$$x^{-1}yx = y^{-1} \wedge y^{-1}xy = x^{-1} \Rightarrow x^4 = y^4 = e.$$

5. Naći sve podgrupe Klajnove grupe.

6. Dokazati da je presek dve podgrupe grupe $\mathbb{G}$ takođe podgrupa od $\mathbb{G}$.

7. Dokazati da je $\mathbb{H} \cup \mathbb{K}$ podgrupa grupe $\mathbb{G}$, gde su $\mathbb{H}$ i $\mathbb{K}$ podgrupe od $\mathbb{G}$, ako i samo ako je $H \subseteq K$ ili $K \subseteq H$.

8. Razložiti sledeće permutacije iz S_4 na disjunktne cikluse:

   a) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$;

   b) $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$;

   c) $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$;

   d) $\delta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$;

   e) $\varepsilon = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$.

9. U $\mathbb{S}_8$ izračunati $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 4 & 2 & 7 & 5 & 6 & 1 \end{pmatrix}^{111}$.

10. Naći σ ako je:

    a) $(1\ 3\ 4)\sigma(3\ 4\ 1) = (2\ 3\ 4)$ u $\mathbb{S}_4$;

    b) $(5\ 1\ 3)^{10}(2\ 3\ 4\ 6)^{10}\sigma^{-1}((1\ 2\ 3)(3\ 6\ 7))^{-1} = id$ u $\mathbb{S}_7$.

11. Dokazati da je red elemenata a u grupi $(G, \cdot)$ najmanji prirodan broj k za koji je $a^k = e$ ili je beskonačnog reda ako takav broj ne postoji.

12. Dokazati da je grupa reda n ciklična ako i samo ako postoji elemenat reda n.

13. Svake dve ciklične grupe istog reda su izomorfne. Dokazati.

14. Svaka podgrupa H Abelove grupe G je normalna podgrupa od G.

15. Naći sve normalne podgrupe grupe $(\mathbb{Z}_{15}, +_{15})$.

16. Neka je $H \leqslant G$. Tada je $H \lhd G$ ako i samo ako za svako $g \in G$ i svako $h \in H$ važi $g^{-1}hg \in H$.

17. Dokazati da je $Z(\mathbb{G}) = \{x \in G : (\forall g \in G)(gx = xg)\}$ (centar grupe $\mathbb{G}$) normalna podgrupa grupe $\mathbb{G} = (G, \cdot)$.

7 Prsteni i polja

7.1 Prsteni

Uređeni par $(G, \cdot)$, gde je G neprazan skup se zove *polugrupa*, ako

- $\cdot$ je binarna operacija na G;
- za sve $x, y, z \in G$ je ispunjeno $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

Prsten je operacijska struktura $(R, +, \cdot)$ sa dve binarne operacije, za koju važi

- $(R, +)$ je Abelova grupa;
- $(R, \cdot)$ je polugrupa;
- ispunjeni su sledeći distributivni zakoni: za sve $x, y, z \in R$

$$x \cdot (y + z) = x \cdot y + x \cdot z \text{ i } (x + y) \cdot z = x \cdot z + y \cdot z.$$

Po dogovoru u grupi $(R, +)$ neutralni elemenat obeležavamo sa 0, a inverzni za x sa $-x$. $+$ se naziva prva operacija, a $\cdot$ druga, i $\cdot$ ima prednost u odnosu na $+$ kad se gleda redosled operacija.

Primer 7.1. *Osnovni primer prstena od koga potiče i označavanje operacija u samoj definiciji, jeste struktura* $(\mathbb{Z}, +, \cdot)$ *celih brojeva u odnosu na sabiranje i množenje. Isto tako i racionalni, zatim realni i kompleksni, redom obrazuju prstene u odnosu na sabiranje i množenje. Ovi brojevi zadovoljavaju dodatna svojstva, pa ih razmotrimo kasnije u okviru bogatijih algebarskih struktura.*

Za prsten se kaže da je sa *jedinicom* ako u njemu postoji neutralni elemenat u odnosu na drugu operaciju. Taj neutralni elemenat obično označavamo sa 1. Prsten je *komutativan*, ako je druga operacija komutativna.

Elemenat $a \neq 0$ prstena R je *delitelj nule* ako postoji $b \neq 0$, tako da je $a \cdot b = 0$ ili $b \cdot a = 0$. Kažemo da je prsten *bez delitelja nule* ako za sve $x, y \in R$ iz $x \cdot y = 0$ sledi $x = 0$ ili $y = 0$.

Primer 7.2. *U prstenu* $(\mathbb{Z}_6, +_6, \cdot_6)$ *elemenat* $\overline{3}$ *je delitelj nule, jer* $\overline{3} \cdot \overline{2} = \overline{0}$.

Ako su a i b iz R, onda a *deli* b, kaže se i da je a *delitelj* elementa b, u oznaci $a \mid b$, ako postoji $c \in R$ tako da je $a \cdot c = b$.

Teorema 7.3. *U prstenu* R *za proizvoljne* x, y *važi:*

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

Dokaz.

1. $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$. Kako je 0 jedini idempotentni elemenat u grupi $(R, +)$, sledi $x \cdot 0 = 0$. Druga jednakost dokazuje se analogno.
2. $x \cdot y + (-x) \cdot y = (x + (-x)) \cdot y = 0 \cdot y = 0$; odavde je $(-x) \cdot y$ inverzni elemenat za $x \cdot y$, tj. $(-x) \cdot y = -(x \cdot y)$. Slično se dokazuje i druga jednakost.
3. Prema prethodnom delu $(-x) \cdot (-y) = -(x \cdot (-y)) = -(-(x \cdot y)) = x \cdot y$.

■

Teorema 7.4. *Neka je* R *prsten sa jedinicom. Tada važi:*

1. *jedinica prstena je jedinstvena;*
2. *ako* R *ima bar dva elementa, onda je* $1 \neq 0$.

Dokaz.

1. Pretpostavimo suprotno: neka su 1_1 i 1_2 dve jedinice. Tada je $1_1 = 1_1 \cdot 1_2 = 1_2$.
2. U protivnom, iz $1 = 0$ sledi $x = x \cdot 1 = x \cdot 0 = 0$, za svako x iz R.

■

Podskup P prstena $(R, +, \cdot)$ je *potprsten* u R, ako je P i sam prsten u odnosu na restrikcije operacija iz R.

Primer 7.5.

a) Trivijalno, $\{0\}$ *i* R *su potprsteni svakog prstena* R*.*

b) Parni brojevi obrazuju potprsten prstena celih brojeva.

c) Prsten celih je potprsten prstena racionalnih brojeva, a oba su potprsteni prstena realnih brojeva.

Teorema 7.6. *Neprazan podskup* P *prstena* R *je potprsten ako je ispunjeno: za sve* $x, y \in P$

1. $x + (-y) \in P$*;*
2. $x \cdot y \in P$*.*

Dokaz. Uslov 1) je zahtev da $(P, +)$ bude podgrupa aditivne grupe $(R, +)$, a ako važi uslov 2), onda je $\cdot$ operacija na P. $(P, \cdot)$ je polugrupa, jer se asocijativnost prenosi na R. Slično i distributivni zakoni važe na P, jer su ispunjeni na R. ■

Potprsten I prstena R je *ideal* ako važi

a) za sve $a \in I$ i $x \in R$, $ax \in I$ i $xa \in I$.

Ekvivalentno, neprazni podskup I prstena R je njegov ideal, ako i samo ako je ispunjeno uslov a) i

b) za sve $x, y \in I$ $x - y \in I$.

Primer 7.7.

a) U prstenu $(\mathbb{Z}, +, \cdot)$*, za proizvoljan broj* $a \in \mathbb{Z}$*, skup* $\{ax : x \in \mathbb{Z}\}$ *je ideal.*

b) $\{0\}$ *je ideal u svakom prstenu.*

Neka su $(R, +, \cdot)$ i $(P, +, \cdot)$ dva prstena. Funkcija $f : R \to P$ je *homomorfizam prstena*, ako za sve $x, y \in R$ važi:

1. $f(x + y) = f(x) + f(y)$;
2. $f(x \cdot y) = f(x) \cdot f(y)$.

7.2 Polja

Komutativan prsten sa jedinicom bez delitelja nule zove se *integralni domen.*

Primer 7.8.

a) Prsten celih brojeva je jedan integralni domen, jer proizvod brojeva različitih od nule nikad nije 0*.*

b) Skup $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ *je u odnosu na sabiranje i množenje integralni domen.*

Polje je komutativan prsten $(P, +, \cdot)$ sa jedinicom u kome je $(P \setminus \{0\}, \cdot)$ grupa.

Primer 7.9. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ *i* $(\mathbb{C}, +, \cdot)$ *su polja kao i* $(\mathbb{Z}_2, +_2, \cdot_2)$.

Teorema 7.10. *Svako polje je integralni domen.*

Dokaz. Direktno iz definicije. ■

Zadaci iz prstena i polja

1. Proveriti da li je prsten:

   a) $(\mathbb{Z}, +, \cdot)$;

   b) $(\{2k : k \in \mathbb{Z}\}, +, \cdot)$;

   c) $(\mathbb{Q}, +, \cdot)$;

   d) $(\mathbb{R}, +, \cdot)$;

   e) $(\mathbb{Z}_m, +_m, \cdot_m)$.

2. Dokazati da $(\mathbb{Z}_3, +_3, \cdot_3)$ nema netrivijalnih potprstena.

3. Naći sve potprstene i ideale od $(\mathbb{Z}_4, +_4, \cdot_4)$.

4. Neka je f homomorfizam prstena $(R, +, \cdot)$ u njega samog. Dokazati da je
$$S = \{x \in R : f(x) = x\}$$
domen potprstena od $(R, +, \cdot)$.

5. Ako su $\mathbb{I}$ i $\mathbb{J}$ ideali prstena $\mathbb{P}$, dokazati:

a) $\mathbb{I} \cap \mathbb{J} \triangleleft \mathbb{P}$;

b) $I + J = \{i + j : i \in I, j \in J\}$ je domen najmanjeg ideala koji sadri $I \cup J$.

Karakteristika prstena $\mathbb{R}$ je najmanji prirodan broj n takav da za sve $x \in R$ važi $n \cdot x + x + x + \cdots + x = 0$. Ako takav broj ne postoji, onda je karakteristika 0 (oznaka: Char($\mathbb{R}$)).

6. Ako je Char($\mathbb{R}$) prost broj p i $\mathbb{R}$ komutativan prsten, dokazati da za $x, y \in R$ važi $(x + y)^p = x^p + y^p$.

7. Karakteristika konačnog polja je uvek prost broj. Dokazati.

8 Polinomi

8.1 Prsten polinoma

Neka je $(R, +, \cdot)$ prsten. *Polinom* nad R u oznaci $p(x)$ je izraz

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

gde su $a_0, a_1, \ldots, a_n$ iz R i zovu se *koeficijenti*; pri tome je $a_n \neq 0$. x je promenljiva, a broj $n \in \{0, 1, 2 \ldots\}$ je *stepen polinoma*. Izrazi $a_i x^i$ su *članovi* polinoma, a među njima je $a_n x^n$ *vodeći član*. Polinom $0 \cdot x^n + \cdots + 0 \cdot x + 0$ nema definisan stepen, a zove se *nula-polinom*. Označavamo sa 0. Dva polinoma po x nad istim prstenom su jednaka ako su im jednaki koeficijenti uz odgovarajuće stepene promenljive x. Skup svih polinoma po x nad datim prstenom R označava se sa $R[x]$. Na tom skupu definišu se operacije sabiranja $(+)$ i množenja $(\cdot)$, na sledeći način. Neka je

$$p(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} + a_m x^m \text{ i}$$

$$q(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} + b_n x^n,$$

gde je $m \leqslant n$. Tada po definiciji

$$\begin{aligned} p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + b_{m+1}x^{m+1} + \ldots \\ + b_{n-1}x^{n-1} + b_n x^n; \end{aligned}$$

$$\begin{aligned} p(x) \cdot q(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots \\ + (a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \cdots + a_k b_0)x^k + \cdots + a_m b_n x^{m+n}. \end{aligned}$$

Teorema 8.1. *Ako je $R[x]$ skup svih polinoma po x nad prstenom R, onda je struktura $(R[x], +, \cdot)$ isto prsten. Taj prsten je*
-komutativan;
-sa jedinicom,
-bez delitelja nule,
ako i R poseduje odgovarajuće svojstvo.

Dokaz. Iz samih definicija operacija neposredno slede uslovi kojima se definiše prsten. Jasno je da su obe operacije asocijativne, kao i da važi distributivnost; ta svojstva proizilaze iz analognih na prstenu R. Polinom 0 je neutralni elemenat za sabiranje, a suprotni polinom za $p(x)$ je $-p(x) = -a_0 - a_1x - \cdots - a_{n-1}x^{n-1} - a_nx^n$.

Iz definicije množenja dalje sledi da se komutativnost ove operacije prenosi sa R na $R[x]$, kao i da je jedinica iz R (ako postoji) neutralni elemenat za množenje u $R[x]$.

Ako u R nema delitelja nule i $p(x)$, $q(x)$ su ne-nula polinomi, onda ni polinom $p(x)q(x)$ nije nula polinom. Zaista, ako su $p(x)$ i $q(x)$ redom stepena m i n, onda su odgovarajući koeficijenti a_m i b_n različiti od nule. Zato proizvod a_mb_n nije nula, pa je stepen polinoma $p(x)q(x)$ broj $m + n$. ■

S obzirom da su elementi prstena R polinomi nultog stepena, sledi da je prsten R potprsten u $R[x]$.

Ako za $b \in R$ važi $p(b) = 0$, onda je b *nula* polinoma $p(x)$.

Navodimo jedan kriterijum za određivanje racionalnih nula polinoma sa celobrojnim koeficijentima.

Teorema 8.2. *Ako je razlomak $\frac{p}{q}$, gde su p i q uzajamno prosti, nula polinoma*

$$p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0, \;\; a_i \in \mathbb{Z}, \;\; a_0a_n \neq 0,$$

onda $p \mid a_0$ i $q \mid a_n$.

Dokaz. Ako je razlomak $\frac{p}{q}$ nula gornjeg polinoma, onda je

$$a_n(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0 / \cdot q^{n-1},$$

$$a_n\frac{p^n}{q} + a_{n-1}p^{n-1} + \cdot + a_1q^{n-2}p + a_0q^{n-1} = 0 / \cdot \frac{q}{p},$$

$$a_np^{n-1} + a_{n-1}p^{n-2}q + \cdots + a_1q^{n-1} + a_0\frac{q^n}{p} = 0.$$

Brojevi p i q su uzajamno prosti po pretpostavci. Zato iz dve poslednje jednakosti sledi redom $q \mid a_n$, odnosno $p \mid a_0$. ■

8.2 Polinomi nad proizvoljnim poljem

Teorema 8.3. *Neka su $f(x)$ i $g(x)$ polinomi nad poljem P, pri čemu $g(x)$ nije nula polinom. Tada nad P postoje jedinstveni polinomi $q(x)$ i $r(x)$ tako da je ispunjeno*

$$f(x) = g(x)q(x) + r(x);$$

pri tome je ili $r(x) = 0$ ili je stepen polinoma $r(x)$ manji od stepena polinoma $g(x)$.

Dokaz. Ako je $f(x)$ nula polinom, ili ako je stepen polinoma $f(x)$ manji od stepena polinoma $g(x)$, onda je tvrđenje o postojanju polinoma $q(x)$ i $r(x)$ tačno, jer

$$f(x) = g(x) \cdot 0 + f(x),$$

pa ulogu polinoma $q(x)$ i $r(x)$ igraju redom 0 i $f(x)$.

Neka je dakle stepen m polinoma $f(x) = a_m x^m + \cdots + a_1 x + a_0$ veći od ili jednak sa stepenom n polinoma $g(x) = b_n x^n + \cdots + b_1 x + b_0$. Tada je stepen polinoma

$$r_1(x) = f(x) - \frac{a_m}{b_n} x^{m-n} g(x)$$

manji od m jer se od $f(x)$ oduzima vodeći član $a_m x^m$. Zato je ispunjena jednakost

$$f(x) = g(x)q_1(x) + r_1(x),$$

gde je $q_1(x) = \frac{a_m}{b_n} x^{m-n}$, a stepen polinoma $r_1(x)$ manji je od stepena polinoma $f(x)$. Ako je manji i od n dokaz je gotov, a ako nije, na analogan način pokazuje se da važi

$$r_1(x) = g(x)q_2(x) + r_2(x),$$

gde je stepen polinoma $r_2(x)$ manji od stepena polinoma $r_1(x)$.

Nastavljanjem ovog deljenja dobija se niz polinoma $r_1(x)$, $r_2(x), \ldots$ sa opadajućim stepenima, sve do nekog $r_k(x)$, čiji je stepen manji od stepena polinoma $g(x)$. Pri tome je

$$r_{k-1}(x) = g(x)q_k(x) + r_k(x).$$

Iz prethodnih jednakosti sledi

$$f(x) = g(x)(q_1(x) + \cdots + q_k(x)) + r_k(x)$$

pa ako je $q(x) = q_1(x) + \cdots + q_k(x)$ i $r(x) = r_k(x)$, dokaz prvog dela je gotov. Zaista, stepen polinoma $r(x) = r_k(x)$ je manji od stepena polinoma $g(x)$ ili je $r(x) = 0$.

Još treba dokazati jedinstvenost polinoma $q(x)$ i $r(x)$. Pretpostavimo da je

$$f(x) = g(x)q(x) + r(x) \quad \text{i} \quad f(x) = g(x)q'(x) + r'(x),$$

pri čemu je stepen polinoma $r(x)$ i $r'(x)$ manji od stepena polinoma $g(x)$. Sledi

$$g(x)q(x) + r(x) = g(x)q'(x) + r'(x),$$

pa je

$$g(x)(q(x) - q'(x)) = r'(x) - r(x).$$

Stepen polinoma $r'(x) - r(x)$ je ili 0 ili je manji od stepena polinoma $g(x)$. Sledi da polinom $q(x) - q'(x)$ mora biti nula polinom jer bi u protivnom stepen polinoma na levoj strani jednakosti bio veći od ili jednak sa stepenom polinoma $g(x)$. Dakle, $q(x) = q'(x)$, a odatle $r(x) = r'(x)$. ■

Ako je kao gore $f(x) = g(x)q(x) + r(x)$ i stepen polinoma $r(x)$ manji je od stepena polinoma $g(x)$ ili je 0, onda je $q(x)$ *količnik*, a $r(x)$ *ostatak* pri deljenju $f(x)$ sa $g(x)$.

S obzirom da je $P[x]$ prsten, kaže se da je polinom $f(x)$ *deljiv* polinomom $g(x)$ ako postoji polinom $q(x)$, tako da je $f(x) = g(x)q(x)$. Ako je pri tome $f(x)$ stepena n, onda je stepen polinoma $g(x)$ manji od ili jednak sa n; ako su istog stepena, $q(x)$ je stepena 0.

Sledi tzv. *Bezuov* stav.

Teorema 8.4. *Neka je $a \in P$. U prstenu $P[x]$ ostatak pri deljenju polinoma $p(x)$ polinomom $(x - a)$ je $p(a)$.*

Dokaz. Na osnovu prethodne teoreme ispunjeno je $p(x) = (x-a)q(x)+r$, gde je ostatak r elemenat polja P, jer njegov stepen mora biti manji od stepena polinoma $(x - a)$, tj. od 1. Sledi $p(a) = (a - a)q(x) + r$, odnosno $p(a) = r$. Zato je

$$p(x) = (x - a)q(x) + p(a).$$

■

Posledica 8.5. *Za $a \in P$, polinom $p(x) \in P[x]$ deljiv je sa $(x - a)$ ako i samo ako je $p(a) = 0$.*

Drugim rečima, $a \in P$ je nula polinoma $p(x) \in P[x]$ ako i samo ako je za neki polinom $q(x)$ ispunjeno

$$p(x) = (x - a)q(x).$$

Ako je polinom $p(x)$ iz prstena $P[x]$ deljiv sa $(x - a)^k$, gde je $a \in P$, a $k > 1$, onda je *a višestruka* nula polinoma $p(x)$. Ako uz to polinom nije deljiv sa $(x - a)^{k+1}$, onda je *višestrukost* te nule k.

Tvrđenje koje sledi formuliše se kao *Osnovni stav algebre.*

Teorema 8.6. *Svaki polinom iz $\mathbb{C}[x]$ koji nije nultog stepena ima bar jednu nulu u polju $\mathbb{C}$.*

Posledica 8.7. *Svaki polinom $p(x) = a_n x^n + \cdots + a_1 x + a_0$ nad poljem $\mathbb{C}$ ima tačno n nula u tom polju; pri tome se svaka nula broji onoliko puta kolika je njena višestrukost. Ako su $z_1, \ldots, z_n$ nule tog polinoma, onda $p(x) = a_n(x - z_1)(x - z_2)\ldots(x - z_n)$.*

Na kraju navodimo još jednu teoremu.

Teorema 8.8. *Neka je dat polinom $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ sa realnim koeficijentima. Ako je $\omega \in \mathbb{C}$ nula tog polinoma, onda je i $\overline{\omega}$ takođe njegova nula.*

Zadaci iz polinoma

1. Faktorisati:

   a) $6x^5 - 19x^4 - 3x^3 + 17x^2 - 9x + 36$ nad $\mathbb{R}$ i nad $\mathbb{C}$;

   b) $x^4 + x^2 + 1$ nad $\mathbb{R}$ i nad $\mathbb{C}$;

   c) $x^4 + 1$ nad $\mathbb{R}$.

2. Neka je $p(x)$ polinom koji pri deljenju sa $x - 1$ daje ostatak 1, a pri deljenju sa $x - 2$ ostatak 3. Naći ostatak pri deljenju tog polinoma sa $(x - 1)(x - 2)$.

3. Dokazati da je a višestruka nula polinoma $p(x)$ ako i samo ako važi $p(a) = p'(a) = 0$.

4. Za koje vrednosti parametra a polinom $p(x) = x^5 - 5x - a$ ima višestruku nulu?

5. Naći zbir koeficijenata uz članove sa neparnim stepenima polinoma $(x^5 + x - 1)^{2023}$.

6. Naći sve vrednosti realnog parametra a tako da nule α, β i γ polinoma $p(x) = x^3 - 6x^2 + ax + a$ zadovoljavaju jednakost $(\alpha - 3)^2 + (\beta - 3)^2 + (\gamma - 3)^2 + \alpha\beta\gamma = 0$.

7. Neka su x_1 i x_2 nule polinoma $x^2 - 2023x + 1$. Dokazati da je $x_1^n + x_2^n$ prirodan broj za sve $n \in \mathbb{N}$.

8. Da li postoji polinom $p(x)$ sa celobrojnim koeficijentima tako da je $p(5) = 4$ i $p(3) = 1$?

9. Odrediti koeficijente a i b tako da polinom $p(x) = ax^{n+1} + bx^n + 1$, $n \in \mathbb{N}$, bude deljiv sa $(x - 1)^2$.

10. Polinom $p(x) = x^4 - 3x^3 - 6x^2 + ax + b$ ima trostruku nulu. Odrediti a, b i nule tog polinoma.

9 Elementi teorije brojeva

9.1 Osnovne osobine

Teorema 9.1. *Za svaka dva cela broja a i b, gde $b > 0$, postoji jedinstveni par celih brojeva q i r tako da bude ispunjeno $a = bq + r$ i $0 \leqslant r < b$.*

Dokaz. Za $a = 0$ je $0 = b \cdot 0 + 0$ i tvrđenje važi.

Neka je a prirodan broj. Da postoji bar jedan par brojeva q i r sa navedenim svojstvom dokazujemo indukcijom po a. Ako je $a = 1$ i $b = 1$, imamo $1 = b \cdot 1 + 0$, a ako je $a = 1$ i $b > 1$, onda je $1 = b \cdot 0 + 1$, pa tvrđenje važi. Ako je dalje $a = bq + r$ za neke q, r, $0 \leqslant r < b$, onda je $a + 1 = bq + r + 1$ i $0 < r + 1 \leqslant b$. Ako $r + 1 < b$, traženi brojevi su q i $r + 1$, a ako je $r + 1 = b$, onda je $(a + 1) = b(q + 1)$ pa uslov ispunjavaju brojevi $q + 1$ i 0.

Neka je sada $a < 0$, u kom slučaju $-a > 0$. po prvom delu dokaza, za $-a$ i b postoje brojevi q_1 i r_1, takvi da je $-a = bq_1 + r_1$ i $0 \leqslant r_1 < b$. Za $r_1 = 0$. tvrđenje važi ybog $a = b(-q_1) + 0$, a za $r_1 > 0$ je $a = b(-q_1 - 1) + b - r_1$, pri čemu je $0 < b - r_1 < b$. Brojevi $-q - 1$ i $b - r_1$ ispunjavaju uslove.

Dokazujemo jedinstvenost brojeva q i r, za date a i b. Pretpostavimo da postoje dva takva para *tj.* da je $a = bq + r$, $0 \leqslant r < b$, i $a = bq_1 + r_1$, $0 \leqslant r_1 < b$. Ako je $r \neq r_1$ i, recimo, $r > r_1$, onda je $r - r_1 = b(q_1 - q)$ i $0 < r - r_1 < b$. Sledi $q_1 - q > 0$ tj. $q_1 - q \geqslant 1$. Ali tada je $r - r_1 \geqslant b$, što protivreči upravo pokazanom $r - r_1 < b$. Slično se pokazuje da ne može biti $r_1 > r$, pa ostaje $r_1 = r$. Sledi direktno da je $q_1 = q$. ■

Ako je $a = bq + r$, onda je q *količnik*, a r *ostatak* u deljenju a sa b. Ako je $r = 0$, broj a je *deljiv* brojem b, odnosno b je delitelj (delilac) broja a, a a je *sadržalac* broja b. Primetimo da se pojam delitelja na isti način definiše na svakom komutativnom prstenu.

U skladu sa ovim, na skupu celih $\mathbb{Z}$ celih brojeva posmatra se relacija deljivosti:

$$x \mid y \text{ ako i samo ako } (\exists z)(x \cdot z = y).$$

Na skupu $\mathbb{N}$ je ova relacija poredak, ali na $\mathbb{Z}$ nije, jer nije antisimetrična.

Teorema 9.2. *Za proizvoljne cele brojeve x, y, z, u, v ispunjeno je:*

1. $x \mid x$;

2. $x \mid 0$;

3. $1 \mid x$, $(-1) \mid x$;

4. *ako* $x \mid y$ *i* $y \mid z$, *onda* $x \mid z$;

5. *ako* $x \mid y$, *onda* $x \mid yz$;

6. *ako* $x \mid y$ *i* $x \mid z$, *onda* $x \mid (y+z)$ *i* $x \mid (y-z)$;

7. *ako* $x \mid y$, *onda* $xz \mid yz$;

8. *ako je* $x \neq 0$, *onda iz* $xy \mid xz$ *sledi* $y \mid z$;

9. *ako* $x \mid y$ *i* $u \mid v$, *onda* $xu \mid yv$;

10. *ako* $x \mid y$ *i* $x \mid z$, *onda* $x \mid (uy + vz)$.

Dokaz.

1. Važi zbog $x = x \cdot 1$.

2. $x \cdot 0 = 0$.

3. $x = 1 \cdot x$ i $x = (-1) \cdot (-x)$.

4. Iz $y = kx$ i $z = ly$ sledi $z = (kl)x$.

5. Važi $y = kx$, pa je $yz = x(kz)$, odnosno $x \mid yz$.

6. Važi $y = xu$ i $z = xv$ za neke $u, v \in \mathbb{Z}$. Odatle $y + z = x(u + v)$, pa $x \mid (y + z)$; slično za razliku.

7. Iz $x \mid y$ sledi da postoji t, takav da $xt = y$, pa je i $(xz)t = yz$, tj. $xy \mid yz$.

8. Postoji t, tako da $xyt = xz$, pa prema zakonu kancelacije sledi $yt = z$, odnosno $y \mid t$.

9. Ako postoje z i t, takvi da je $xz = y$ i $ut = v$, tada je $(xu)(zt) = yv$, pa $xu \mid yv$.

10. Iz $xp = y$ i $xq = z$, sledi $xpu = yu$ i $xqv = vz$, pa $x(pu+qv) = yu+vz$, odnosno $x \mid yu + vz$.

■

Prirodan broj p je *prost* ako nije jednak jedinici i delitelji su mu samo 1 i p. Prirodan broj koji je različit od 1, i nije prost, jeste *složen*.

9.2 NZD, NZS i Osnovni stav aritmetike

Za pozitivne cele brojeve a i b definiše *najveći zajednički delitelj*, kao pozitivan broj c u oznaci $c = \text{NZD}(a, b)$, na sledeći način: $c \mid a$ i $c \mid b$, a ako $d \mid a$ i $d \mid b$ za neko $d \in \mathbb{Z}$, onda $d \mid c$.

Teorema 9.3. *Najveći zajednički delitelj postoji za bilo koja dva prirodna broja, i on je jedinstven.*

Za pozitivne cele brojeve a i b definiše *najmanji zajednički sadržalac*, kao pozitivan broj c u oznaci $c = \text{NZS}(a, b)$, na sledeći način: $a \mid c$ i $b \mid c$, a ako $a \mid d$ i $b \mid d$ za neko $d \in \mathbb{Z}$, onda $c \mid d$.

Teorema 9.4. *Najmanji zajednički sadržalac postoji za bilo koja dva prirodna broja, i on je jedinstven.*

Sledeća lema će biti potrebna za nastavak, a jeste generalno korisna.

Lema 9.5. *Neka je p prost broj, a a i b prirodni brojevi. Ako $p \mid ab$, onda $p \mid a$ ili $p \mid b$.*

Sledi tvrđenje poznato kao *Osnovni stav artimetike.*

Teorema 9.6. *Za svaki prirodan broj a važi: $a = 1$, ili je a predstavljiv kao proizvod prostih brojeva. Predstavljanje je jedinstveno do na poredak faktora.*

Dokaz. Neka je a prirodan broj. Indukcijom po a dokazujemo da postoji predstavljanje preko prostih faktora. Ako je $a = 1$, ovo tvrđenje važi. Pretpostavimo da je ono tačno za sve prirodne brojeve manje od a i dokažimo da tada važi i za a. Ako je a prost broj, tvrđenje važi, a ako je složen, može se predstaviti kao proizvod $a = b \cdot c$, gde su b i c prirodni brojevi veći od 1, a manji od a. Po indukcijskoj pretpostavci $b = p_1 p_2 \dots p_m$, $c = q_1 q_2 \dots q_n$, gde su p_i, q_j prosti brojevi. Tada je traženo predstavljanje dato sa $a = p_1 p_2 \dots p_m q_1 q_2 \dots q_n$.

Dokažimo jedinstvenost predstavljanja. Ponovo koristimo indukciju po a. Za $a = 1$, jedinstvenost je ispunjena. Neka ona važi za sve brojeve manje od a. Pretpostavimo da za a postoje dva takva predstvaljanja: $a = p_1 p_2 \dots p_m =$

$q_1 q_2 \dots q_n$. S obzirom da $p_1 \mid q_1 q_2 \dots q_n$, p_1 deli bar jedan od brojeva q_i, b. u. o. $p_1 \mid q_1$, uz odgovarajuću prenumeraciju indeksa. Budući da su p_1 i q_1 prosti brojevi, sledi $p_1 = q_1$, pa se gornja jednakost može skratiti: $b = p_2 \dots p_m = q_2 \dots q_n$. Broj b je manji od a, pa se po indukcijskoj pretpostavci jednoznačno predstavlja. To znači da je $m = n$ i $p_2 = q_2, \dots, p_n = q_n$. Odatle se i a jednoznačno predstavlja kao proizvod faktora. ■

Gornje predstvaljanje može se označiti sa $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, pri čemu su $p_1, \dots, p_k$ različiti prosti brojevi, a $\alpha_1, \dots, \alpha_k$ prirodni brojevi. Ovo se naziva *kanonički oblik* prirodnog broja a. Na primer, $4212 = 2^2 \cdot 3^4 \cdot 13$.

Zadaci iz brojeva

1. Dokazati:

   a) broj je deljiv sa 2 akko mu je poslednja cifra deljiva sa 2;

   b) broj je deljiv sa 3 akko mu je zbir cifara deljiv sa 3;

   c) broj je deljiv sa 4 akko mu je dvocifreni završetak deljiv sa 4;

   d) broj je deljiv sa 5 akko se završava sa 5 ili 0;

   e) broj je deljiv sa 8 akko mu je trocifreni završetak deljiv sa 8;

   f) broj je deljiv sa 9 akko mu je zbir cifara deljiv sa 9;

   g) broj je deljiv sa 11 akko mu je razlika zbira cifara na parnim i neparnim mestima deljiva sa 11.

2. Ispitati koji brojevi od 2 do 11, osim 7, dele broj 64770325196.

3. Naći ostatak pri deljenju broja 222^{555} brojem 11.

4. Dokazati da je broj $3^{105} + 4^{105}$ deljiv sa 13.

5. Naći ostatak pri deljenju broja 536^{324} brojem 7.

6. Naći NZD$(2002, 2022)$ koristeći Euklidov algoritam.

7. Ako je NZD$(a, b) = 1$, onda postoje $x, y \in \mathbb{Z}$ takvi da je $ax + by = 1$. Dokazati.

8. Ako je NZD$(a, b) = d$, tada linearna Diofantova jednačina $ax + by = c$ ima rešenje u skupu $\mathbb{Z}$ ako i samo ako $d|c$. Dokazati.

9. Ako je (x_0, y_0) jedno rešenje linearne Diofantove jednačine $ax + by = c$, gde $\text{NZD}(a, b) = 1$, onda se sva rešenja mogu dobiti pomoću formula:

$$x = x_0 + bt, \quad y = y_0 - at, \quad t \in \mathbb{Z}.$$

10. Rešiti sledeće linearne Diofantove jednačine:

    a) $5x + 7y = 1$;

    b) $7x + 29y = 4$;

    c) $3004x + 2014y = 7$;

    d) $3004x + 2014y = 6$.