3. TEORIJA BROJEVA

3.1 Uvod

Aritmetika (računstvo) je grana matematike koja se bavi brojevima.

Danas je češći naziv za aritmetiku **teorija brojeva.**

Teorija brojeva (klasična) se bavi ponajprije prirodnim brojevima, te cijelim i racionalnim brojevima.

Algebarska teorija brojeva se bavi algebarskim brojevima, ali i apstraktnim matematičkim strukturama (ispreplitanje s algebrom).

- prvi aritmetički problemi zapisani su u starom Babilonu i Egiptu 2-3 tisuće godina prije Krista;

- važno:

  - ▲ otkriće iracionalnih brojeva, te osnovnih svojstva djeljivosti prirodnih brojeva (starogrčka matematika - prva znanja sadržana u Euklidovim *Elementima*);

  - ▲ otkriće dekadskog zapisa i nule (Indijci);

- ▲ znanja sintetizirana u europskoj srednjovjekovnoj i novovjekovnoj matematici;

- kraljica matematike (gotovo svi veliki matematičari su se bavili aritmetikom).

Neki najpoznatiji riješeni i neriješni problemi teorije brojeva:

- **Goldbachova slutnja**: svaki se paran broj $2n, 2n \geq 4$, može izraziti kao suma dva prim broja p i q, tj.

$$p + q = 2n.$$

Tvrdnja je još ne dokazana. (Nagrada 1.000.000 $)

- **10. Hilbertov problem** (**1900**): Postoji li algoritam za nalaženje rješenja Diofantske jednadžbe[1]?

Negativan odgovor dao je Matijaševič 1970.

---

[1] **Diofant** (grč. $\Delta\iota\acute{o}\varphi\alpha\upsilon\tau o\varsigma$; vjerojatno u 3. stoljeću Aleksandriji) veliki starogrčki matematičar.

Diofantska jednadžba - algebarska jednadžba s dvjema ili više nepoznanica s cjelobrojnim koeficijentima, kojoj se traže cjelobrojna ili racionalna rješenja.
Ime je dobila po Diofantu koji je prvi sustavno proučavao takve jednadžbe.

▲ **Pellova jednadžba**[2]**:** Najpoznatija Diofantska jednadžba oblika

$$x^2 - dy^2 = 1,$$

gdje je d prirodan broj koji nije kvadrat. Sva pozitivna (cijela) rješenja (x_n, y_n) ove jednadžbe dana su sa

$$x_n + \sqrt{d} y_n = \left(x_0 + \sqrt{d} y_0\right)^n,$$

gdje je (x_0, y_0) prvo ("najmanje") rješenje u prirodnim brojevima[3].

▲ **Fermatov zadnji (veliki) teorem:** Jednadžba

$$x^n + y^n = z^n,$$

gdje su x, y, z, n cijeli brojevi, nema rješenje za $n > 2$.

Teorem je konačno dokazao Andrew Wiles 1995.

---

[2] Ime jednadžbi je pogrešno dao Euler 1730. po engleskom matematičaru Johnu Pellu.

[3] Rješenje je navodno znao i Fermat (1657.), ali pripisuje se Wallisu i Brounckleru, iako je 500 godina prije riješio Bhāskara (12 st.). Postojanje najmanjeg rješenja je strogo dokazao Lagrange 1769.

▲ **Catalanova slutnja (1843):** Jedina rješenja jednadžbe

$$x^u - y^v = 1,$$

u prirodnim brojevima x, y, u, v su $3^2 - 2^3 = 1$.

Slutnju je konačno dokazao Mihăilescu 2003.[4]

■ **Teorem (Roth)**[5] Za realan algebarski broj α nejednadžba

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}},$$

gdje je $\varepsilon > 0$, ima konačno mnogo rješenja.

---

[4] Mihăilescu je dokazao da jednadžba

$$x^p - y^q = 1,$$

nema rješenja u ne-nul cijelim brojevima i prim brojevima p i q.
Ovo zajedno s rezultatima Lesbegua (1850) i Ko Chaoa (1865) dokazuje slutnju.

[5] Njemački matematičar Klaus Roth je za ovaj rezultat 1958. dobio Fieldsovu medalju.

3.2 Cijeli brojevi. Djeljivost.

Skup cijelih brojeva je skup

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}.$$

Definicija Neka su a i b cijeli brojevi. Kažemo da a *dijeli* b ako je $a \neq 0$ i postoji $k \in \mathbb{Z}$ tako da je $b = ak$. Pišemo $a\,|b$ i čitamo "a dijeli b". Broj a nazivamo *djelitelj* broja b, a broj b *višekratnik* broja a.

Propozicija 1 Relacija "biti djelitelj" ima sljedeća svojstva:

- refleksivnost: za svaki cijeli broj $a \neq 0$ vrijedi $a\,|a$;
- antisimetričnost: za svaka dva cijela broja a i b iz $a\,|b$ i $b\,|a$ slijedi $a = \pm b$. Ako su $a, b \in \mathbb{N}$, onda slijedi $a = b$;
- tranzitivnost: ako $a\,|b$ i $b\,|c$ onda $a\,|c$.

Primjer Ako su $a, b, c \in \mathbb{Z}$, onda iz $a\,|b$ i $a\,|c$ slijedi $a\,|(nb + mc)$ za bilo koja dva cijela broja m i n.

Definicija Ako su $a, b, d \in \mathbb{Z}$ takvi da je $d\,|a$ i $d\,|b$, onda d nazivamo *zajedničiki djelitelj* od a i b.

Ako je barem jedan od brojeva a i b različit od 0, onda postoji i najveći zajednički djelitelj kojeg nazivamo *najveća zajednička mjera (Nzm)* od a i b i označavamo sa $M(a, b)$ ili $Nzm(a, b)$.

Ako su brojevi a i b različiti od 0, onda najmanji prirodan broj čiji su a i b djelitelji nazivamo *najmanji zajednički višekratnik (nzv)* od a i b i označavamo sa $v(a, b)$ ili $nzv(a, b)$.

Primjer:

- $Nzm(a, b) > 0$;
- $Nzm(a, 0) = a$, za sve $a \in \mathbb{N}$;
- $Nzm(a, b) = Nzm(b, a) = Nzm(|a|\,, |b|)$
  $nzv(a, b) = nzv(b, a) = nzv(|a|\,, |b|)$
- Ako su $a, b \in \mathbb{N}$ onda je

$$Nzm(a, b) \leq \min\{a, b\} \leq \max\{a, b\} \leq nzv(a, b);$$

- Ako je $a \in \mathbb{N}$ i $b \in \mathbb{Z}$ onda

$$a\,|b \Longrightarrow Nzm(a, b) = a.$$

Napomena: Na sličan način možemo definirati, za bilo koji konačan skup cijelih brojeva $a_1,\ a_2, ..., a_n$, $Nzm(a_1, a_2, ..., a_n)$ i $nzv(a_1, a_2, ..., a_n)$.

Propozicija 2 Neka su $a_1, a_2, ..., a_r$ i $b_1, b_2, ..., b_s$ cijeli brojevi i neka je

$$a_1 + a_2 + ... + a_r = b_1 + b_2 + ... + b_s.$$

Ako su svi gornji brojevi djeljivi s $d \in \mathbb{N}$ osim jednog onda je i taj broj djeljiv s d.

Teorem 1 (o dijeljenju) Neka su dani $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ onda postoje jedinstveni cijeli brojevi q i r, $0 \leq r < b$, takvi da je

$$a = bq + r.$$

Broj q se naziva <u>*kvocijent*</u> pri dijeljenju a i b, a r <u>*ostatak*</u>.

Neka je $m \in \mathbb{N}$, Označimo

$$m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\}$$

skup svih višekratnika od m.

Propozicija 3 Neprazan podskup S skupa cijelih brojeva koji je zatvoren s obzirom na operaciju oduzimanja (tj. iz $a, b \in S$ slijedi $a - b \in S$) jednak je ili $\{0\}$ ili $m\mathbb{Z}$ za neki $m \in \mathbb{N}$.

3.3 Euklidov algoritam

Propozicija 4 Neka su $a, b, q, r \in \mathbb{Z}$ i $a = bq + r$. Onda je svaki zajednički djelitelj od a i b ujedno i zajednički djelitelj od b i r. Posebno vrijedi $Nzm(a, b) = Nzm(b, r)$.

Teorem 2 (Euklidov algoritam za nalaženje Nzm) Neka su dani $a \in \mathbb{Z}$ i $b \in \mathbb{N}$. Pretpostavimo da je uzastopnom primjenom Teorema1 dobiven niz jednakosti

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 < r_1 < b \\ b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \qquad \text{(*)} \\ &\vdots \\ r_{k-2} &= r_{k-1} q_k + r_k, \quad 0 < r_k < r_{k-1} \\ r_{k-1} &= r_k q_{k+1}. \end{aligned}$$

Tada je $Nzm(a, b) = r_k$, tj. $Nzm(a, b)$ jednako je posljednjem ostatku različitom od 0. Nadalje, postoje brojevi $s, t \in \mathbb{Z}$ takvi da je

$$Nzm(a, b) = r_k = sa + tb, \qquad \text{(**)}$$

tj. r_k se može izraziti kao linearna kombinacija od a i b.

Primjer Odredite $d = Nzm(252, 198)$ i prikažite d kao linearnu kombinaciju brojeva 252 i $198.$

Napomena

- U Euklidovom algoritmu smo pretpostavili da je $b > 0$ što nije bitno ograničenje jer je $Nzm(a, b) = Nzm(|a|, |b|);$

- ako su $a, b \in \mathbb{N}$ i $a < b$, onda u prvom koraku imamo $a = b \cdot 0 + a$, pa a i b zamijene mjesta.

- Primijetimo da je

$$\left\lfloor \frac{a}{b} \right\rfloor = q_1, \quad \left\lfloor \frac{b}{r_1} \right\rfloor = q_2, \quad \left\lfloor \frac{r_1}{r_2} \right\rfloor = q_3 \ \ ...,$$

  gdje je $\lfloor x \rfloor$ *najveći cijeli dio* od x, tj. $\lfloor x \rfloor = q$ gdje je q najveći cijeli broj $\leq x.$

- Brojevi $s, t \in \mathbb{Z}$ u (**) nisu jednoznačno određeni, jer je npr.

$$Nzm(a, b) = sa + tb = (s + b)\,a + (t - a)\,b,$$

Posljedica 1 Neka su $a, b \in \mathbb{Z}$ i $d \in \mathbb{N}$ takvi da $d\,|a$ i $d\,|b$. Onda $d\,|Nzm(a, b)$.

Teorem 3 Ako je barem jedan od brojeva a, $b \in \mathbb{Z}$ različit od 0, onda je

$$Nzm(a,b) = \min\{sa+tb \,|\, s,t \in \mathbb{Z} \text{ i } sa+tb>0\}.$$

Definicija Kažemo da su cijeli brojevi a i b *relativno prosti*, ako je $Nzm(a,b)=1$.

Propozicija 5 Neka su $a,b,c \in \mathbb{Z}$ takvi da su a i b relativno prosti i $b\,|ac$, onda $b\,|c$.

Propozicija 6 Neka su $a,b \in \mathbb{Z}$ i $c \in \mathbb{N}$. Tada vrijedi:

i) $Nzm(ca,cb) = cNzm(a,b)$,

ii) ako $c\,|a$ i $c\,|b$, onda je $Nzm(\frac{a}{c},\frac{b}{c}) = \frac{1}{c}Nzm(a,b)$. Posebno, ako je $d = Nzm(a,b)$, onda su $\frac{a}{d}$ i $\frac{b}{d}$ relativno prosti.

Primjena gornjih rezultata:

Jednadžbu oblika

$$ax+by=c, \tag{1}$$

gdje su a,b,c zadani cijeli brojevi kojoj tražimo cjelobrojna rješenja x i y nazivamo *Diofantska jednadžba* prvog stupnja s dvije varijable.

Propozicija 7 Neka su $a, b, c \in \mathbb{Z}$ zadani cijeli brojevi. Diofantska jednadžba (1) ima rješenje onda i samo onda ako $Nzm(a, b)\,|c$.

3.4 Prosti brojevi. Osnovni teorem aritmetike.

Nadalje ćemo promatrati samo skup prirodnih brojeva $\mathbb{N}$. Djelitelje nekog broja $a \in \mathbb{N}$ gledat ćemo samo u skupu $\mathbb{N}$.

Definicija

- Svaki prirodan broj $a > 1$ ima uvijek dva djelitelja 1 i a i njih nazivamo *trivijalni djelitelji*.

- Za prirodan broj $p > 1$ kažemo da je *prost broj* (ili *prim broj*) ako ima samo trivijalne djelitelje.

- Prirodan broj $a > 1$ koji nije prost nazivamo *složen broj*.

Primjer Prvi prosti brojevi su: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...

Ako želimo naći sve proste projeve $\leq a$, koristimo jednostavni postupak kojeg nazivamo **Eratostenovo sito:**

- Ispišemo, po redu, sve prirodne brojeve od 1 do a;
- Križamo 1;
- Zaokružimo 2 (prost) i križamo sve višekratnike od 2;
- Prvi preostali 3 (prost) zaokružimo i križamo sve višekratnike od 3 (koji nisu već prekriženi);
- Prvi preostali 5 (prost) zaokružimo i križamo sve višekratnike od 5 (koji nisu već prekriženi);
- ....
- Algoritam završava u konačno koraka, a zaokruženi brojevi su prosti.

Primjer Nađimo sve proste brojeve ≤ 60 pomoću Eratostenovog sita.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Djelitelje od $a \in \mathbb{N}$ nazivamo još i *faktorima*., a prikaz $a = bc$ gdje su $b, c \in \mathbb{N}$ *faktorizacija* prirodnog broja a. Ako je djelitelj od b prost broj, nazivat ćemo ga *prostim djeliteljem* (ili prostim faktorom) od a.

Cilj nam je dokazati Osnovni teorem aritmetike.

Nekoliko pomoćnih tvrdnji:

Lema 1 Neka je prirodan broj $a > 1$ i neka je p najmanji djelitelj od a koji je veći od 1. Tada je p prost.

Lema 2 Neka je $a \in \mathbb{N}$. Za svaki prost broj p je ili $Nzm(p, a) = 1$ ili $p \,|a$.

Propozicija 8 Ako je p prost broj i $p \,|ab$, onda $p \,|a$ ili $p \,|b$.

Posljedica 2 Ako je p prost broj i $p \,|a_1 a_2 ... a_n$, onda postoji barem jedan a_i takav da $p \,|a_i$.

Teorem 4 (Osnovni teorem aritmetike) Faktorizacija svakog prirodanog broja $a > 1$ na proste faktore je jedinstvena do na poredak prostih faktora. (Ili za svaki prirodan broja $a > 1$ postoji jedinstven rastav

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k},$$

gdje su $p_1 < p_2 < ... < p_k$ svi različiti prosti faktori od a. Broj $\alpha_i \in \mathbb{N}$ nazivamo *kratnošću* prostog broja p_i.)

Posljedica 3 Ukupan broj različitih djelitelja prirodnog broja $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$ rastavljenog na proste faktore je

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) ... (\alpha_k + 1)$$

Teorem 5 (Euklid) Skup svih prostih brojeva je beskonačan.

Propozicija 9 Neka su $a, b \in \mathbb{N}$ tada vrijedi

$$nzv(a, b) = \frac{ab}{Nzm(a, b)}$$

Napomena:

- Za $a, b \in \mathbb{Z}$ i $a, b \neq 0$ imamo

$$nzv(a, b) = \frac{|ab|}{Nzm(a, b)};$$

- Tvrdnja Propozicije 8 ne vrijedi za više od dva broja;

- Dokaz prethodne propozicije daje nam još jedan način traženja $Nzm(a, b)$. Međutim ovaj način je puno složeniji nego Euklidov algoritam.

Propozicija 10 Neka su $a, b, c \in \mathbb{N}$. Ako $a\,|c$ i $b\,|c$ onda $nzv(a, b)\,|c$. Posebno, ako su a i b relativno prosti onda $ab\,|c$.

Propozicija 11 Neka su $a_1, a_2, ..., a_n \in \mathbb{Z}$ i barem jedan je različit od 0. Definirajmo niz

$$\begin{aligned} d_2 &= Nzm(a_1, a_2),\ d_3 = Nzm(d_2, a_3), ... \\ d_n &= Nzm(d_{n-1}, a_n). \end{aligned}$$

Tada je $Nzm(a_1, a_2, ..., a_n) = d_n$.

Neka su $a_1, a_2, ..., a_n \in \mathbb{Z}$ i svi različiti od 0. Definirajmo niz

$$\begin{aligned} m_2 &= nzv(a_1, a_2),\ m_3 = nzv(m_2, a_3), ... \\ m_n &= nzv(m_{n-1}, a_n). \end{aligned}$$

Tada je $nzv(a_1, a_2, ..., a_n) = m_n$.

3.5 Kongruencije

Definicija Ako prirodan broj n dijeli razliku $a - b$, onda kažemo da je a *kongruentno* b *modulo* n i pišemo $a \equiv b (\mathrm{mod}\, n)$. U protivnom, kažemo da a nije kongruentno b modulo n i pišemo $a \not\equiv b (\mathrm{mod}\, n)$.

Propozicija 12 Relacija "biti kongruentan modulo n" je relacija ekvivalencije na skupu $\mathbb{Z}$.

Propozicija 13 Neka su a, b, c, d cijeli brojevi:

i) Ako je $a \equiv b (\mathrm{mod}\, n)$ i $c \equiv d (\mathrm{mod}\, n)$, onda je $a \pm c \equiv b \pm d (\mathrm{mod}\, n)$ i $ac \equiv bd (\mathrm{mod}\, n)$;

ii) Ako je $a \equiv b (\mathrm{mod}\, n)$, $d \in \mathbb{N}$ i $d \mid n$, onda je $a \equiv b (\mathrm{mod}\, d)$;

iii) Ako je $a \equiv b (\mathrm{mod}\, n)$, onda je $ac \equiv bc (\mathrm{mod}\, nc)$ za svaki $c \in \mathbb{N}$.

Posljedica 4 Neka su a, b, k, l cijeli brojevi i neka je $a \equiv b (\mathrm{mod}\, n)$, onda vrijedi:

i) $a \pm nk \equiv b \pm nl \ (\mathrm{mod}\, n)$;

ii) $ak \equiv bk (\mathrm{mod}\, n)$;

iii) Ako je $a^m \equiv b^m (\mathrm{mod}\, n)$ za svaki $m \in \mathbb{N}$.

Propozicija 14 Neka su a, b, $c \in \mathbb{Z}$ tada vrijedi: $ca \equiv cb (\mathrm{mod}\, n)$ ako i samo ako $a \equiv b (\mathrm{mod}\, \frac{n}{Nzm(c,n)})$. Specijalno, ako je $ca \equiv cb (\mathrm{mod}\, n)$ i $Nzm\,(c, n) = 1$, onda je $a \equiv b (\mathrm{mod}\, n)$.

Napomena: Propozicije 13 i 14, te Posljedica 4 govore nam koje su operacije s kongruencijama dozvoljene a koje ne:

- Dozvoljeno je: zbrajati, oduzimati, množiti (potencirati);
- Nije dozvoljeno: općenito dijeliti (osim ako je djelitelj c relativno prost s n);
- Primijetimo da za svaki $y \in \mathbb{Z}$ postoji točno jedan $x_j \in \{0, 1, ..., n - 1\}$ takav da je $y \equiv x_j (\mathrm{mod}\, n)$.

3.6 Möbiusova funkcija i formula inverzije

Definicija *Möbiusova funkcija* $\mu : \mathbb{N} \to \mathbb{R}$ je funkcija koja prirodnom broju n, s rastavom na proste faktore $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$, pridružuje vrijednost

$$\mu(n) = \begin{cases} (-1)^k, & \text{ako je } \alpha_1 = ... = \alpha_k = 1 \\ 0, & \text{inače.} \end{cases}$$

Još definiramo $\mu(1) = 1$.

Propozicija 15 Za svaki prirodan broj $n > 1$ vrijedi

$$\sum_{d|n} \mu(d) = 0,$$

(zbraja se po pozitivnim djeliteljima d).

Teorem 6 (teorem inverzije) Ako su zadane dvije funkcije $f, g : \mathbb{N} \to \mathbb{R}$ i ako za svaki $n \in \mathbb{N}$ vrijedi

$$f(n) = \sum_{d|n} g(d)$$

onda je

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

i obratno.

3.7 Eulerova funkcija

Definicija Neka je $\varphi(n)$ broj svih prirodnih brojeva $< n$ za koje vrijedi da su relativno prosti sa n. Definiramo $\varphi(1) = 1$. Na taj način je definirana funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ koju nazivamo Eulerova funkcija.

Dakle, $\varphi(n)$ je broj brojeva u nizu $1, 2, ..., n$ koji su relativno prosti sa n.

Za Eulerovu funkciju vrijedi:

- $\sum\limits_{d|n} \varphi(d) = n$ (Gaussova formula).
- Za $Nzm(a, n) = 1$ vrijedi $a^{\varphi(n)} \equiv 1 \pmod{n}$ (Eulerova kongruencija).
- Za p prost vrijedi $\varphi(p) = p - 1$;
- Ako je p prost i $p \nmid a$ onda je $a^{p-1} \equiv 1 \pmod{p}$ i $a^p \equiv a \pmod{p}$ (Mali Fermatov teorem).

Teorem 7 Za svaki prirodan broj $n > 1$ vrijedi

$$\varphi(n) = n \prod_{\substack{p|n \\ p-prost}} \left(1 - \frac{1}{p}\right),$$

tj. ako je $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$ (rastav na proste faktore) onda je

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right).$$

Posljedica 5 Eulerova funkcija ima svojstvo multiplikativnosti, tj.

$$\varphi(mn) = \varphi(m) \cdot \varphi(n)$$

za sve relativno proste m, n.

4. BINARNE RELACIJE

4.1 Relacije. Relacije ekvivalencije.

Definicija *Binarna relacija na skupu X* je bilo koji neprazan podskup $\rho \subseteq X \times X$. Kažemo da je x *u relaciji* ρ s y (ili x i y su u relaciji ρ) ako je $(x, y) \in \rho$. Pišemo $x\rho y$.

Napomena:

- binarna relacija - odnos između dva elementa (važno koji je prvi a koji drugi);
- x i y su *neusporedivi (po ρ)* ako nije $x\rho y$ ni $y\rho x$.

Definicija Za binarnu relaciju ρ na skupu X kažemo da je:

i) *refleksivna* ako vrijedi $(\forall x \in X)\ x\rho x$;

ii) *simetrična* ako vrijedi $(\forall x, y \in X)\ (x\rho y \Longrightarrow y\rho x)$;

iii) *antisimetrična* ako vrijedi

$$(\forall x, y \in X)\,(x\rho y\ \wedge\ y\rho x \Longrightarrow x = y)\,;$$

iv) *tranzitivna* ako vrijedi

$$(\forall x, y, z \in X)\,(x\rho y\ \wedge\ y\rho z \Longrightarrow x\rho z)\,.$$

Napomena: Za binarnu relaciju ρ na skupu X kažemo da je *funkcija* ako *za svaki* $x \in X$ postoji *točno jedan* $y \in X$ tako da je $x\rho y$, tj.

$$(\forall x \in X)\,(x\rho y_1 \ \wedge \ x\rho y_2 \Longrightarrow y_1 = y_2)$$

Oznaka: $f : X \to X$, $y = f(x)$.
Obratno, svaka funkcija $f : X \to X$ određuje relaciju ρ. Definiramo

$$x\rho y \Longleftrightarrow y = f(x).$$

Definicija Za binarnu relaciju ρ na skupu X kažemo da je *relacija ekvivalencije* ako je refleksivna, simetrična i tranzitivna.

4.2 Particija skupa. Razredi (klase) ekvivalencije.

Definicija Kažemo da obitelj podskupova $\{A_i\}_{i\in I}$ od X čini *particiju* (rastav) skupa X ako vrijedi:

i) $X = \bigcup\limits_{i\in I} A_i$, tj. obitelj skupova $\{A_i\}_{i\in I}$ je *pokrivač* od X;

ii) $A_i \cap A_j = \emptyset$ za sve $i, j \in I$, $i \neq j$, tj. skupovi iz $\{A_i\}_{i\in I}$ su međusobno disjunktni.

Često se particijom skupa X smatramo prikaz

$$X = \bigcup_{i \in I} A_i = \bigoplus_{i \in I} A_i$$

kao disjunktne unije podskupova.

Definicija Neka je ρ relacija ekvivalencije na skupu X. *Razred (klasa) ekvivalencije* $[x]$ elementa $x \in X$ je skup svih elemenata iz X koji su u relaciji ρ s x. Dakle,

$$[x] = \{y \in X : x\rho y\} \subseteq X.$$

Napomena:

- $x \in [x]$ jer je $x\rho x$;
- Element $y \in [x]$ se naziva *reprezentant* razreda (klase) $[x]$.

Teorem 1 Neka je ρ relacija ekvivalencije na skupu X. Onda za sve $x, y \in X$ vrijedi ili $[x] = [y]$ ili $[x] \cap [y] = \emptyset$. Pritom je $x\rho y$ ako i samo ako je $[x] = [y]$.

Uočimo: Ako je ρ relacija ekvivalencije na skupu X, onda je obitelj svih klasa ekvivalencije $[x]$ particija od X, tj.

$$X = \bigcup_{x \in X} [x] = \bigoplus_{x \in X} [x]$$

Teorem 2 Neka je $\{A_i\}_{i \in I}$ particija skupa X. Definirajmo relaciju ρ na skupu X tako da je $x \rho y$ onda i samo onda ako je y element istog skupa iz particije kao i x. Onda je ρ relacija ekvivalencije ρ na skupu X, a klase ekvivalencije se podudaraju sa A_i.

Definicija Neka je ρ relacija ekvivalencije na skupu X, onda skup svih klasa ekvivalencije nazivamo *kvocijentni skup* s obzirom na relaciju ρ i označavamo

$$X/\rho = \{[x]\}_{x \in X}.$$

Dakle, kvocijentni skup je particija od X s obzirom na relaciju ρ.

Propozicija 1 Kvocijentni skup na skupu svih cijelih brojeva po relaciji "biti kongruentan modulo n" ($\equiv \pmod n$) jednak je

$$\mathbb{Z}/_{\equiv} = \{[0], \ [1], ..., [n-1]\}$$

($n-$člani skup).

Taj skup se naziva *kvocijentni skup ostataka modulo n*, ili skup ostataka pri dijeljenju s n. Razredi ekvivalencije su:

$$[0] = \{qn : q \in \mathbb{Z}\} = n\mathbb{Z}$$

$$[1] = \{qn + 1 : q \in \mathbb{Z}\} = n\mathbb{Z}+1$$

$$\vdots$$

$$[n-1] = \{qn + (n-1) : q \in \mathbb{Z}\} = n\mathbb{Z}+(n-1).$$

Neka je ρ relacija ekvivalencije na skupu X i H bilo koji skup. Ako je $f : X \to H$ neka funkcija, pitanje je je li funkcija

$$\hat{f} : X/\rho \to H, \quad \hat{f}([x]) = f(x)$$

dobro definirana?

Odgovor: Da bi $\hat{f}$ bila dobro definirana mora biti

$$f(x) = f(y) \quad \text{za } x\rho y,$$

tj. f mora biti na svakom razredu ekvivalencije konstantna. Tada $\hat{f}$ ne ovisi o izboru reprezentanta iz razreda ekvivalencije $[x]$.

4.3 Relacija poretka

Definicija Za binarnu relaciju ρ na skupu X kažemo da je *relacija parcijalnog (djelomičnog) poretka* ako je refleksivna, antisimetrična i tranzitivna.

Napomena:

- Jedina binarna relacija ρ na skupu X koja je istodobno i relacija ekvivalencije i relacija parcijalnog poretka (simetrična i antisimetrična) je relacija jednakosti $" = "$;

- Skup X na kojem je zadana relacija parcijalnog poretka, oznaka $\leq$, kraće označavamo $(X, \leq)$ i kažemo da je X parcijalno poredan skup;

- Ako je $(X, \leq)$ parcijalno poredan skup, onda definiramo, za $x, y \in X$, $x < y$ ako je $x \leq y$ i $x \neq y$. Tada $(X, <)$ nije parcijalno poredan skup (relacija $<$ nije ni refleksivna ni antisimetrična).

Definicija Neka je $(X, \leq)$ parcijalno poredan skup i $S \subseteq X$.

- Kažemo da je $m \in X \;\; (M \in X)$ **donja** (*gornja*) **međa skupa** S ako je

$$(\forall s \in S)\,(m \leq s) \qquad (\;(\forall s \in S)\,(s \leq M)\;)$$

- Za skup S kažemo da je **omeđen odozdol** (*odozgor*) ako ima barem jednu donju (gornju) među.

- Kažemo da je $m^* \in X \;\; (M^* \in X)$, ako postoji, **infinum** (*suprenum*) **skupa** S, i označavamo $\inf S$ ($\sup S$) ako vrijedi:
  - $m^* = \inf S$ ($M^* = \sup S$) je donja (*gornja*) međa od S;
  - za svaku donju (gornju) među m (M) vrijedi $m \leq \inf S$ ($\sup S \leq M$).

- Ako vrijedi da je $\inf S \in S$ ($\sup S \in S$) onda $\inf S$ ($\sup S$) nazivamo **minimum** (*maksimum*) **skupa** S, i označavamo $\min S$ ($\max S$).

Definicija Neka je $(X, \leq)$ parcijalno poredan skup. Za $(X, \leq)$ kažemo da je <u>*totalno poredan skup*</u> ako za sve $x, y \in X$ vrijedi $x \leq y$ ili $y \leq x$, tj. svaka dva elementa su usporediva.

Definicija Neka je $(X, \leq)$ totalno poredan skup. Za $(X, \leq)$ kažemo da je <u>*dobro poredan skup ili lanac*</u>,ako svaki njegov neprazan podskup ima minimalni element.

Definicija Neka su $(X_1, \leq_1)$ i $(X_2, \leq_2)$ dva parcijalno poredana skupa. <u>*Kartezijev produkt parcijalno poredanih skupova*</u> definiramo kao $(X_1 \times X_2, \ \leq)$. Pritom za (a_1, a_2), $(b_1, b_2) \in X_1 \times X_2$, definiramo $(a_1, a_2) \leq (b_1, b_2)$ ako je $a_1 \leq_1 b_1$ i $a_2 \leq_2 b_2$.

Napomena:

- Slično se definira za Kartezijev produkt više parcijalno poredanih skupova;

- Neka su $(X_1, \leq_1)$ i $(X_2, \leq_2)$ dva totalno poredana skupa, $(X_1 \times X_2, \ \leq)$ ne mora biti totalno poredan.

Definicija Neka su $(X_1, \leq_1)$ i $(X_2, \leq_2)$ dva parcijalno poredana skupa. Na Kartezijevom produktu $X_1 \times X_2$ definiramo tzv. relaciju *leksikografskog poredaka* $\leq_L$. Pritom za (a_1, a_2), $(b_1, b_2) \in X_1 \times X_2$, definiramo $(a_1, a_2) \leq_L (b_1, b_2)$ ako je ispunjen jedan od dva sljedeća uvjeta:

- $a_1 <_1 b_1$ (a_2, b_2 bilo kakvi);

- $a_1 = b_1$ i $a_2 \leq_2 b_2$.

$(X_1 \times X_2, \ \leq_L)$ je parcijalno poredan skup.

Napomena:

- Slično se definira za Kartezijev produkt više parcijalno poredanih skupova;

- Neka su $(X_1, \leq_1)$ i $(X_2, \leq_2)$ dva totalno poredana skupa, tada je $(X_1 \times X_2, \ \leq_L)$ totalno poredan.

4.4 Hasseov dijagam relacije poretka

Neka je X konačan skup i ρ relacija na X. Tada relaciju ρ možemo predočiti dijagramom kojeg nazivamo *usmjereni graf.*

- Svaki element skupa reprezentira (označena) točka koju nazivamo *čvor* ili *vrh*.

- Ako je $a\rho b$, tada dva čvora označena s a i b povežemo strelicom od a do b. Tu strelicu nazivamo *usmjereni brid*. Ako je $a\rho b$ i $b\rho a$ onda imamo dva usmjerena brida između a i b, pa, zbog jednostavnosti, a i b povezujemo jednom dvostranom strelicom.

- Ako je $a\rho a$ usmjereni brid između a i a se naziva *petlja*.

Neka je X konačan skup i ρ ($\leq$) relacija parcijalnog poretka na $X.$ Tada relaciju $\leq$ možemo predočiti jednostavnijom (zornijom) vrstom dijagrama kojeg nazivamo *Hasseov dijagam.*

- Svaki element skupa reprezentira (označena) točka koju nazivamo *čvor* ili *vrh*..

- Ispuštamo petlje, jer je relacija refleksivna.

- Ako je $a < b$ i između njih ne postoji niti jedan $c \in X$, tj. iz $a \leq c \leq b$ slijedi $a = c$ ili $b = c$, onda čvor koji pripada b satavljamo iznad čvora koji pripada a i spajamo ih crtom (a ne strelicom od a do b).

- Usmjereni brid koji je imliciran tranzitivnošću ne crtamo.

Definicija Kažemo da je parcijalno poredan skup $(X, \leq_1)$ *izomorfan* parcijalno poredanom skupu $(Y, \leq_2)$ ako postoji bijekcija $f : X \to Y$ koja čuva poredak, tj. tako da vrijedi

$$(\forall x, y \in X) \quad (x \leq_1 y \Longrightarrow f(x) \leq_2 f(y))$$

4.5 Mreže

Definicija Parcijalno poredan skup $(X, \leq)$ naziva se *mreža* ako za svaki par elemenata a, $b \in X$ postoji $\sup\{a, b\}$ i $\inf\{a, b\}$. Na taj način možemo uvesti dvije binarne operacije u parcijalno poredan skup X :

$$a + b = \sup\{a, b\}\,, \qquad a \cdot b = \inf\{a, b\}$$

Napomena: Ovo znači da u mreži svaki dvočlan podskup ima infinum (suprenum), a to znači i svaki konačan podskup.

Definicija Parcijalno poredan skup $(X, \leq)$ naziva se *potpuna mreža* ako za svaki njegov podskup (konačan ili beskonačan) ima infinum i suprenum. Svaka potpuna mreža onda ima $\inf X$, koji nazivamo *nula* i $\sup X$ koji nazivamo *jedinica.*

Teorem 3 Za operacije $+$ i $\cdot$ na mreži $(X, \leq)$ vrijede svojstva:

1. komutativnost: $a + b = b + a, \qquad a \cdot b = b \cdot a;$

2. asocijativnost:

$$(a + b) + c = a + (b + c)\,,$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)\,;$$

3. apsortivnost ili svojstvo upijanja:

$a \cdot (a + c) = a, a + (a \cdot c) = a$

4. idempotentnost zbrajanja i množenja:

$a + a = a, \qquad a \cdot a = a;$

5. $a + 0 = a, \quad a \cdot 1 = a;$

Napomena: distributivnost općenito ne vrijedi.

Definicija Za mrežu $(X, \leq)$ kažemo da je *distributivna mreža* ako u njoj vrijedi zakon distribucije, tj. za svaki a, $b \in X$ vrijedi $a\,(b + c) = ab + ac$.

Definicija Za element $\bar{a}$ u mreži $(X, \leq)$ kažemo da je *komplement* elementa a ako je $a + \bar{a} = 1, \quad a \cdot \bar{a} = 0$. Ako svaki element ima komplement kažemo da je $(X, \leq)$ *komplementarna mreža.*

Napomena: U distributivnoj mreži komplementiranje je jednoznačno (dokaz -sami).

Napomena: Ovo znači da je distributivna i komplementarna potpuna mreža X Booleova algebra $(X, +, \cdot, ^{-}, 0, 1)$. Vrijedi i obrat.

4.5 Skupovni prikaz konačnih Booleovih algebri

Definicija Neka je $(B, +, \cdot, ^{-}, 0, 1)$ Booleova algebra. Za $a, b \in B$ kažemo da je $a \leq b$ ako je $ab = a$.

Propozicija 2 Neka su a, b, c, d bilo koji elementi Booleove algebre B. Relacija $\leq$ ima sljedeća svojstva:

i) $(B, \leq)$ je parcijalno poredan skup;

ii) $a \leq b$ onda i samo onda ako je $a + b = b$;

iii) ako je $a \leq b$ i $c \leq d$ onda je $ac \leq bd$;

iv) $ab = \inf\{a, b\}$, $a + b = \sup\{a, b\}$;

v) $a \leq b$ onda i samo onda ako je $\bar{b} \leq \bar{a}$.

Definicija Element $a \neq 0$ u Booleovoj algebri B naziva se *atom* Booleove algebre ako iz $x \leq a$ slijedi $x = 0$ ili $x = a$.

Napomena: Svaka konačna Booleova algebra ima neprazan skup atoma.

Lema 1 Neka je B konačna Booleova algebra. Za svaki $x \neq 0$ u B postoji atom a takav da je $a \leq x$.
Lema 2 Ako je atom a atom takav da je $a \leq x$, onda je $a \not\leq \bar{x}$, i obratno.

Teorem 4 Neka je $(B, +, \cdot, ^-, 0, 1)$ konačna Booleova algebra i A pripadni skup svih atoma. Onda je Booleova algebra B izomorfna s algebrom skupova 2^A.

Korolar 1 Svaka konačna Booleova algebra ima 2^n elemenata, pri čemu je n broj atoma od B. Svake dvije konačne Booleove algebre s istim brojem elemenata međusobno su izomorfne.

Teorem 5 (Stone) Svaka beskonačna Booleova algebra B je izomorfna nekoj podalgebri algebre skupova 2^X za neki skup X. Preciznije, postoji neki skup X i podskup B' partitivnog skupa 2^X takav da je $(B', \cup, \cap, ^-)$ algebra koja je izomorfna sa B.