Osnovne algebarske strukture
4. Homomorfizmi grupa. Prstenovi i polja.

Borka Jadrijević

4.1 Homomorfizmi grupa

- U apstraktnoj teoriji grupa (ili grupoida, polugrupa, monoida) zanimaju nas samo ona svojstva koja su posljedica svojstava binarne operacije a ne ovise o prirodi elemenata ili o definiciji same operacije.
- Od ineresa imati neko "sredstvo" pomoću kojega ćemo te strukture uspoređivati. To sredstvo su preslikavanja koja poštuju danu strukturu.

Definicija 4.1 *Neka su* $(G, \cdot_G)$ *i* $(H, \cdot_H)$ *grupe. Preslikavanje* $f : G \longrightarrow H$ *je* ***homomorfzam grupe*** G *u grupu* H *ako je*

$$f(a \cdot_G b) = f(a) \cdot_H f(b)$$

za svaki izbor $a, b \in G$.

Definicija 4.2 *Neka je* $f : G \to H$ *homomorfizam grupe* G *u grupu* H.

- *Ako je* f *surjekcija onda ga nazivamo* ***epimorfizam****.*
- *Ako je* f *injekcija onda ga nazivamo* ***monomorfizam****.*
- *Ako je* f *bijekcija onda ga nazivamo* ***izomorfizam****.*

- *Homomorfzam $f : G \longrightarrow G$ se naziva **endomorfzam** grupe G. Bijektivni endomorfzam se naziva **automorfzam**.*

Napomena: Analogno kao kod grupa definiramo gornje pojmove i za druge strukture koje smo do sada definirali (grupoide, polugrupe, monoide).

Primjer 4.1

a) Neka su $(G, \cdot_G)$ i $(H, \cdot_H)$ grupe i e^* jedinica u H. Tada je preslikavanje $f : G \longrightarrow H$ dano sa

$$f(a) = e^* \text{ za sve } a \in G,$$

homomorfizam. Takav f se naziva **trivijalni** ili **nul-homomorfizam**;

b) Neka je $(G, \cdot)$ grupa i neka je $H < G$ podgrupa od G. Tada je inkluzija $i : H \longrightarrow G$, dana sa

$$i(a) = a \text{ za sve } a \in H,$$

homomorfizam (monomorfizam). Posebno, identiteta $i : G \longrightarrow G$ je homomorfizam.

c) Neka je $(G, \cdot_G) = (\mathbb{R}, +)$ i $(H, \cdot_H) = (\mathbb{R}^*, \cdot)$ i $f : \mathbb{R} \longrightarrow \mathbb{R}^*$ preslikavanje dano sa

$$f(x) = e^x \text{ za sve } x \in \mathbb{R}.$$

Tada je f homomorfizam grupa jer je

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$$

za sve $x, y \in \mathbb{R}$. Uočimo da je f monomorfizam.

d) Neka je $f : \mathbb{R} \longrightarrow S^1$ dano sa $f(x) = e^{2\pi x i}$. Tada je f homomorfizam grupa $(\mathbb{R}, +)$ i $(S^1, \cdot)$ koji se naziva **namatanje pravca na kružnicu**.

e) Neka je $(\overrightarrow{a_1}, \overrightarrow{a_2}, \overrightarrow{a_3})$ baza u V^3. Definiramo $f : V^3 \longrightarrow \mathbb{R}^3$ sa

$$f(\vec{a}) = f(\alpha_1 \overrightarrow{a_1} + \alpha_2 \overrightarrow{a_2} + \alpha_3 \overrightarrow{a_3}) = (\alpha_1, \alpha_2, \alpha_3,).$$

Tada je f dobro definirano i to je izomorfizam grupa $(V^3, +)$ i $(\mathbb{R}^3, +)$.

Propozicija 4.1 *Neka su G i H grupe s jedinicama e i e^*, redom. Ako je $f : G \to H$ homomorfizam, onda vrijedi:*

i) $f(e) = e^*$;

ii) $(f(a))^{-1} = f\left(a^{-1}\right)$.

Dokaz:

Propozicija 4.2 *Neka su G i H grupe i $f : G \to H$ homomorfizam. Tada vrijedi:*

i) *Ako je $G_0 < G$ podgrupa od G. Onda je slika $f(G_0) \subseteq H$ podgrupa od H;*

ii) *Ako je $H_0 < H$ podgrupa od H. Onda je praslika $f^{-1}(H_0) \subseteq G$ podgrupa od G.*

Dokaz:

Napomena: Općenito, ako je $f : G \to H$ preslikavanje, $G_0 \subseteq G$ i $H_0 \subseteq H$. Onda je:

$$f(G_0) = \{b \in H : (\exists a \in G_0)\ b = f(a)\} = \{f(a) : a \in G_0\}$$ - slika od G_0

$$f^{-1}(H_0) = \{a \in G : f(a) \in H_0\}$$ - praslika od H_0 (f^{-1} samo oznaka!!!)

Posebno: Ako je $f : G \to H$ homomorfizam grupa, onda je:

i) Skup

$$J(f) = Ker(f) := f^{-1}(\{e^*\}) = \{a \in G : f(a) = e^*\}$$

je podgrupa grupe G i naziva se **jezgra** homomorfizma f;

ii) Skup

$$S(f) = Im(f) := f(G) = \{y \in H : (\exists a \in G)\ y = f(a)\}$$

je podgrupa grupe H i naziva se **slika** homomorfizma f.

Primjer 4.2

- Neka je $f : \mathbb{R} \longrightarrow S^1$ dano sa $f(x) = e^{2\pi xi}$. Tada je f homomorfizam grupa iz $(\mathbb{R}, +)$ u $(S^1, \cdot)$ i

$$S(f) = S^1 \ \text{ i } \ J(f) = \mathbb{Z}.$$

- Skup $\{1,-1\}$, uz standardno množenje ima strukturu grupe. Onda je funkcija pariteta

$$sgn : S_n \to \{1,-1\}, \quad sgn(p) = (-1)^{I(p)},$$

homomorfizam simetrične grupe $(S_n, \circ)$ u grupu $(\{1,-1\}, \cdot)$. Ovdje je

$$S(sgn) = \{1,-1\} \quad \text{i} \quad J(sgn) = A_n.$$

Propozicija 4.3 *Neka su $f : G \to H$ i $g : H \to K$ homomorfizmi grupa. Onda je i kompozicija $h = g \circ f : G \to K$, homomorfizam grupa.*

Dokaz:

4.2 Izomorfizam grupa

Neka su G i H dane grupe. Kako smo već rekli, preslikavanje $f : G \to H$ nazivamo **izomorfizam** grupe G na grupu H ako je ono homomorfizam i bijekcija. Ako je $G = H$, izomorfizam f nazivamo **automorfizam**.

Propozicija 4.4 *Neka je $f : G \to H$ homomorfizam grupa. Onda je:*
i) *f epimorfizam, ako i samo ako je $S(f) = H$;*

ii) *f monomorfizam, ako i samo ako je $J(f) = \{e\}$.*

Dokaz:

Posljedica 4.1 *Homomorfizam $f : G \to H$ je izomorfizam grupa ako i samo ako je $S(f) = H$ i $J(f) = \{e\}$.*

Primjer 4.3

a) Neka je $f : \mathbb{R} \longrightarrow S^1$ dano sa $f(x) = e^{2\pi x i}$. Tada je f homomorfizam grupa $(\mathbb{R}, +)$ i $(S^1, \cdot)$ epimorfizam, ali nije monomorfizam. Naime, ovdje je

$$S(f) = S^1 \text{ i } J(f) = \mathbb{Z}.$$

b) Neka je $(G, \cdot_G) = (\mathbb{R}, +)$ i $(H, \cdot_H) = (\mathbb{R}^*, \cdot)$ i $f : \mathbb{R} \longrightarrow \mathbb{R}^*$ dano sa

$$f(x) = e^x \text{ za sve } x \in \mathbb{R}.$$

Tada je f monomorfizam jer je

$$J(f) = \{0\}.$$

Uočimo: f nije epimorfizam (pa onda ni izomorfizam) jer je

$$S(f) = \mathbb{R}^+ = (0, \infty) \neq \mathbb{R}^*.$$

Ako promijenimo (suzimo) kodomenu, tj. uzmemo $(H, \cdot_H) = (\mathbb{R}^+, \cdot)$ (podgrupa od $(\mathbb{R}^*, \cdot)$), f postaje epimorfizam tj. izomorfizam.

Inverzno preslikavanje $f^{-1} : \mathbb{R}^+ \longrightarrow \mathbb{R}$, dano sa

$$f^{-1}(x) = \ln x \text{ za sve } x \in \mathbb{R}^+,$$

je također izomorfizam grupa $(\mathbb{R}^+, \cdot)$ i $(\mathbb{R}, +)$.

Propozicija 4.5 *Neka su $f : G \to H$ i $g : H \to K$ izomorfizmi grupa. Onda je i kompozicija $h = g \circ f : G \to K$ izomorfizam grupa.*
Dokaz:

Propozicija 4.6 *Neka je $f : G \to H$ izomorfizam grupa. Onda je $f^{-1} : G \to H$ također izomorfizam*.

Dokaz:

Definicija 4.3 *Neka su G i H dvije grupe. Kažemo da je grupa G izomorfna grupi H i pišemo $G \cong H$, ako postoji bar jedan izomorfizam $f : G \to H$.*

Teorem 4.1 *Relacija "biti izomorfan" je relacija ekvivalencije.*

Dokaz:

Uočimo: Iz gornjeg teorema slijedi da se sve grupe mogu razvrstati u međusobno disjunktne klase, tako da su u svakoj klasi sve međusobno izomorfne grupe.
Sve grupe unutar jedne klase su međusobno ekvipotentne i iste strukture, pa ih s apstraktnog gledišta smatramo **jednakima**. Stoga, možemo pisati $G = H$ umjesto $G \cong H$. Poistovjećivanje realizira izomomorfizam $f : G \to H$:

- $|G| = |H|$ (f je bijekcija);
- množi se na isti način: množenju $a \cdot_G b$ u G odgovara množenje $f(a) \cdot_H f(b)$ u H (ako su G i H konačne, tablica množenja je ista).

Primjer 4.4

- Sve grupe prvog reda (trivijalne grupe) su međusobno izomorfne.
- Sve grupe drugog reda su međusobno izomorfne, što poizlazi iz jedinstvene tablice množenja. Naime, neka je $G = \{a, b\}$, onda je tablica množenja

$*$	a	b
a	a	b
b	b	a

Primjer: grupe $(\mathbb{Z}_2, +_2)$ i $(\{1, -1\}, \cdot)$ su izomorfne.

- Sve grupe reda 3 su međusobno izomorfne, što poizlazi iz jedinstvene tablice množenja. Naime, neka je $G = \{a_0, a_1, a_2\}$ grupa, onda je tablica množenja

$\cdot$	a_0	a_1	a_2
a_0	a_0	a_1	a_2
a_1	a_1	a_2	a_0
a_2	a_2	a_0	a_1

.

Primjer: grupa $(\mathbb{Z}_3, +_3)$.

- Kod grupa reda 4 postoje dvije klase međusobno izomorfnih grupa. U jednoj klasi su grupe izomorfne s (ciličkom) grupom $(\mathbb{Z}_4, +_4)$, a u drugoj sve grupe izomorfne s $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, koja nije ciklička.

- $\mathbb{C} \cong \mathbb{R}^2$ jer je preslikavanje $f : \mathbb{C} \longrightarrow \mathbb{R}^2$ dano sa

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

izomorfizam.

- $\mathbb{Z} \cong m\mathbb{Z}$, $m \neq 0$, jer je preslikavanje $f : \mathbb{Z} \longrightarrow m\mathbb{Z}$ dano sa

$$f(k) = mk$$

izomorfizam. Ovo pokazuje da kod beskonačnih grupa, grupa i njena prava pogrupa mogu biti izomorfne (što nije slučaj kod konačnih grupa).

4.3 Normalne podgrupe

Definicija 4.4 *Neka je $N < G$ podgrupa grupe G. Kažemo da je N* ***normalna podgrupa*** *od G i pišemo $N \lhd G$, ako je*

$$x^{-1}Nx \subset N, \tag{1}$$

za svaki $x \in G$, gdje je $x^{-1}Nx = \left\{x^{-1}nx : n \in N\right\}$.

Vidimo da će N biti normalna podgrupa onda i samo onda ako je

$$x^{-1}nx \in N$$

za svaki $x \in G$ i $n \in N$.

Definicijski uvjet (1) može se napisati i drugačije. Neka je $y = x^{-1}$. Onda je iz (1)

$$y^{-1}Ny \subset N \quad \Longrightarrow \quad N \subset yNy^{-1}.$$

Kako je

$$yNy^{-1} = x^{-1}Nx,$$

imamo

$$x^{-1}Nx \subset N \quad \text{i} \quad N \subset x^{-1}Nx \quad \Longrightarrow \quad N = x^{-1}Nx$$

Dakle, podgrupa $N < G$ grupe G je normalna ako je

$$N = x^{-1}Nx,$$

ili u simetričnoj formi, ako je

$$xN = Nx \tag{2}$$

za svaki $x \in G$.

Napomena:

- Uvjet (2) ne znači da element x komutira sa svakim elementom iz N.
- U komutativnoj grupi svaka podgrupa je normalna.

Svaka grupa G uvijek ima dvije trivijalne normalne podgrupe, to su $\{e\}$ i G. Ako G nema normalnih podgrupa osim trivijalnih $\{e\}$ i G, onda kažemo da je **jednostavna** ili **prosta**.

Primjer 4.5 U grupi S_3, alternirajuća podgrupa

$$A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

je normalna podgrupa od S_3 (provjerite!) dok

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

to nije. Npr. imamo

$$qpq^{-1} = \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}}_{q \in S_3} \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}}_{p \in H} \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}_{q^{-1} \in S_3} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin H.$$

Propozicija 4.7 *Neka su $M, N \lhd G$. Tada je i $M \cap N$ normalna podgrupa od G .*

Dokaz:

Napomena: Slično se pokazuje da je presjek bilo kojeg broja normalnih podgrupa od G, normalna podgrupa od G.

Propozicija 4.8 *Neka je $f : G \longrightarrow H$ epimorfizam grupa i $N \lhd G$ normalna podgrupa od G. Onda je i $f(N) \subset H$ normalna podgrupa od H.*

Dokaz:

Propozicija 4.9 *Neka je $f : G \longrightarrow H$ homomorfizam grupa i $M \lhd H$ normalna podgrupa od G. Onda je i $f^{-1}(M) \subset G$ normalna podgrupa od G.*

Dokaz:

Posljedica 4.2 *Neka je $f : G \longrightarrow H$ homomorfizam grupa. Onda je jezgra $J(f)$ normalna podgrupa od G.*

4.4 Susjedne klase. Lijevi i desni kvocijentni skup.

Neka je $H < G$ podgrupa od G. Onda na G možemo definirati relaciju $\sim$ stavljajući

$$a \sim b \quad \Longleftrightarrow \quad a^{-1}b \in H.$$

Propozicija 4.10 *Relacija $\sim$ je relacija ekvivalencije na G.*

Dokaz:

Neka je za $a \in G$ s $[a] = \{x \in G : x \sim a\}$ označena klasa ekvivalencije generirana s a.

Propozicija 4.11 *Za svaki* $a \in G$ *je*

$$[a] = aH = \{ay : y \in H\}$$

Dokaz:

Posljedica 4.3 *Neka su* $a, b \in G$ *proizvoljni elementi. Tada je*

i) $aH = bH$ *ako je* $a \sim b$;

ii) $aH \cap bH = \emptyset$ *ako je* $a \nsim b$.

Skupove aH, za $a \in G$ nazivamo **lijeve susjedne klase** podgrupe H u grupi G. Skup svih različitih lijevih susjednih klasa

$$Q = \{aH : a \in G\}$$

nazivamo **lijevi kvocijentni skup** grupe G po podgrupi H i označavamo $Q = G/H$.

Analogno, na G možemo definirati relaciju $\sim$ stavljajući

$$a \sim b \quad \Longleftrightarrow \quad ab^{-1} \in H.$$

Ovo je također relacija ekvivalencije čije su klase

$$[a] = Ha = \{ya : y \in H\}$$

a nazivamo **desne susjedne klase** podgrupe H u grupi G. Skup svih različitih desnih susjednih klasa

$$H\backslash G = \{aH : a \in G\}$$

nazivamo **desni kvocijentni skup** grupe G po podgrupi H.

Napomena:

- Općenito je $G/H \neq H\backslash G$.
- Posebno $aH \neq Ha$, jer H ne mora biti normalna podgrupa.

Propozicija 4.13 *Skupovi $G/H \neq H\backslash G$ su ekvipotentni.*

Dokaz:

Taj zajednički kardinalni broj kvocijentnih skupova naziva se **indeks podgrupe** H u grupi G i označava $[G : H]$. Ako je taj broj konačan, kažemo da je H podgrupa **konačnog indeksa** $k = [G : H]$.

Propozicija 4.12 *Neka je G konačna grupa reda m i H neka njezina podgrupa reda n. Tada za svaki element $a \in G$ lijeva susjedna klasa aH (desna susjedna klasa Ha) ima točno n elemenata.*

Dokaz:

Uočimo: Ako je G konačna grupa reda m i H njezina podgrupa reda n. Kako su susjedne klase aH disjunktne i svaka ima točno n elemenata, onda je

$$k = [G : H] = \frac{m}{n}.$$

		G
n	n	n
n	H	n
n	n	n

Dakle, $\frac{m}{n} \in \mathbb{N}$. Iz ovoga neposredno slijedi:

Posljedica 4.4 (Lagrange) *Red grupe je višekratnik reda svake njezine podgrupe.*

Uočimo: Iz gornje tvrdnje slijedi:

- Ako je G konačna grupa, za svaki $a \in G$, red od a je djelitelj od $|G|$;
- Ako je red grupe prost broj, ta grupa ne može imati pravih podgrupa. Primjer $(\mathbb{Z}_3, +_3)$, $(\mathbb{Z}_5, +_5)$, ..., nemaju pravih podgrupa.
- Obrat Lagrangeova teorema, općenito nije točan. Naime, ako je G grupa reda m i n djelitelj od m, tada ne mora postojati podgrupa reda n. Npr. može se pokazati da grupa A_4, koja je reda 12, nema podgrupe reda 6.

Primjer 4.6 Lijevi i desni kvocijentni skup grupe

$$S_3 = \left\{ p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\right.$$
$$\left. p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

po podgrupi

$$H = \left\{ p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

su redom

$$S_3/H = \{p_1H,\ p_2H,\ p_4H\} = \{H,\ p_2H,\ p_4H\}$$

$$H\backslash S_3 = \{Hp_1,\ Hp_2,\ Hp_3\} = \{H,\ Hp_2,\ Hp_5\}\,.$$

Uočimo da je $S_3/H \neq H\backslash S_3$ jer je

$$p_2H = \{p_2, p_5\}\,, \quad p_4H = \{p_4, p_6\}\,, \quad Hp_2 = \{p_2, p_4\}\,, \quad Hp_5 = \{p_5, p_6\}\,.$$

Ovdje je

$$[S_3 : H] = \frac{|S_3|}{|H|} = \frac{6}{2} = 3.$$

4.4 Kvocijentna grupa.

Zapis aH ili Ha je kraći zapis umnoška podskupova od G, tj. elemenata partitivnog skupa $\mathcal{P}(G)$, induciranog množenjem u grupi G.

Neka je G grupa i $\mathcal{P}(G)$ partitivni skup od G. Defniramo

$$AB = \{ab : a \in A, b \in B\} \subseteq G,$$

pa je $AB \in \mathcal{P}(G)$ za svake $A, B \in \mathcal{P}(G)$. Zapravo, $\mathcal{P}(G)$, uz ovo množenje, ima strukturu nekomutativnog monoida s jedinicom $\{e\}$.

Za danu podgrupu $H < G$ grupe G na lijevom, odnosno desnom kvocijentnom skupu željeli bismo uvesti strukturu grupe s obzirom na gore definirano množenje skupova.

To općenito nije moguće, jer npr. za klase $[a], [b] \in G/H$ imamo

$$[a][b] = (aH)(bH) = (\{a\} H)(\{b\} H) \in \mathcal{P}(G)$$

ali to općenito nije skup oblika xH za neki $x \in G$. Dakle, skupovi G/H i $H\backslash G$ općenito nisu zatvoreni s obzirom na množenje u $\mathcal{P}(G)$.

Ako pretpostavimo da je $H = N$ normalna podgrupa od G, onda je

$$aN = Na, \quad \text{za svaki } a \in G,$$

što pokazuje da se lijeve susjedne klase podudaraju s desnima i, odatle,

$$G/N = N\backslash G$$

tj. lijevi je kvocijent jednak desnom, pa govorimo jednostavno o **kvocijentnom skupu**

$$G/N = \{[a] = aN : a \in G\}$$

grupe G po normalnoj podgrupi N.

Sada je i množenje klasa dobro definirana binarna operacija, jer za $[a], [b] \in G/N$ vrijedi

$$[a][b] = (aN)(bN) = a(Nb)N = a(bN)N = (ab)(NN) = (ab)N = [ab] \in G/N.$$

Teorem 4.1 *Neka je $N \lhd G$ normalna podgrupa od G. Onda je kvocijentni skup G/N grupa, uz prirodno množenje klasa kao binarnu operaciju.*

Dokaz:

- Grupa G/N naziva se **kvocijentna grupa** ili **faktorska grupa** grupe G po normalnoj podgrupi N.
- U slučaju kad je grupa G/N konačna, njezin se red očito podudara s indeksom podgrupe N u grupi G. Primijetimo još da je $G/N \subseteq \mathcal{P}(G)$ podgrupa monoida $\mathcal{P}(G)$.
- Ako je G komutativna, onda je i G/N komutativana, jer imamo

  $$[a][b] = [ab] = [ba] = [b][a].$$

  Obrat međutim, ne vrijedi općenito. Na primjer, za bilo koju grupu G kvocijentna grupa $G/G = \{G\}$ je trivijalna grupa, dakle Abelova.

Uz kvocijentnu grupu G/N prirodno povezujemo preslikavanje definirano sa

$$p : G \longrightarrow G/N, \quad p(a) = [a] = aN \quad \text{za svaki } a \in G,$$

koje nazivamo **prirodna projekcija** grupe G na kvocijentnu grupu G/N.

Propozicija 4.13 *Prirodna projekcija je epimorfizam s jezgrom* $J(p) = N$.

Dokaz:

Napomena: Ako je (komutativna) grupa zapisana aditivno $(G, +)$ i $N \lhd G$, onda imamo zapis:

$$a \sim b \iff a - b \in N.$$

$$[a] = a + N = \{a + y \,|y \in N\} \quad \text{i} \quad G/N = \{a + N \,|a \in N\}$$

$$[a] + [b] = (a + N) + (b + N) = (a + b) + N$$

$$p : G \longrightarrow G/N, \quad p(a) = [a] = a + N$$

Primjer 4.7 Neka je $(G,+) = (\mathbb{Z},+)$, $m \in \mathbb{N}$ i $m\mathbb{Z} = \{mk \,|k \in \mathbb{Z}\} \subseteq \mathbb{Z}$. Tada je $N = m\mathbb{Z} \lhd \mathbb{Z}$ normalna podgrupa od $\mathbb{Z}$ (jer je $\mathbb{Z}$ komutativna grupa).

Kvocijentna grupa

$$\mathbb{Z}/m\mathbb{Z} = \{[k] \mid k \in \mathbb{Z}\} = \{k + m\mathbb{Z} \mid k \in \mathbb{Z}\}$$

očito ima m elemenata (različitih klasa), pa je

$$\mathbb{Z}/m\mathbb{Z} = \{[0], \ [1], ..., [m-1]\}.$$

Dakle, to je grupa reda m. Tu grupu nazivamo **grupom klasa ostataka modulo** m jer su svakoj klasi svi elementi (cijeli brojevi) iz $\mathbb{Z}$ koji imaju isti ostatak pri dijeljenju s m.

Prirodna projekcija grupe $\mathbb{Z}$ na $\mathbb{Z}/m\mathbb{Z}$ je dana sa

$$p : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}, \quad p(k) = [k] = k + m\mathbb{Z}, \quad \text{za svaki } k \in \mathbb{Z}.$$

Ovo je epimorfizam s jezgrom $J(p) = m\mathbb{Z}$.

Primjer 4.8 Grupe $(\mathbb{Z}_m, +_m)$ i $(\mathbb{Z}/m\mathbb{Z}, +)$ su izomorfne, jer je preslikavanje dano sa

$$f : \mathbb{Z}_m \longrightarrow \mathbb{Z}/m\mathbb{Z}, \quad f(k) = k + m\mathbb{Z} \quad \text{za svaki } k \in \mathbb{Z}_m$$

izomorfizam grupa. Dakle, $\mathbb{Z}_m \simeq \mathbb{Z}/m\mathbb{Z}$.

4.5 Prstenovi. Polja.

Definicija 4.5 *Uređenu trojku $(P, +, \cdot)$ koja se sastoji od nepraznog skupa P i dvije binarne operacije "$+$" i "$\cdot$" nazivamo **prstenom** ako je ispunjeno:*

(1) $(P, +)$ *je Abelova grupa;*

(2) $(P, \cdot)$ *je polugrupa, tj. vrijedi* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *za svaki izbor* $a, b, c \in P$*;*

(3) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *za svaki izbor* $a, b, c \in P$ *(lijeva distributivnost);*

(4) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ *za svaki izbor* $a, b, c \in P$ *(desna distributivnost).*

Grupu $(P, +)$ nazivamo **aditivna grupa prstena** P, a polugrupu $(P, \cdot)$ **multiplikativna polugrupa** prstena P. Neutralni element aditivne grupe nazivamo **nula prstena** P i označavamo ga standardno s 0.

Za prsten $(P, +, \cdot)$ kažemo da je **komutativan** ako dodatno vrijedi da je operacija množenja "$\cdot$" komutativna.

Ako je multiplikativna polugrupa $(P, \cdot)$ prstena monoid, kažemo da je $(P, +, \cdot)$ **prsten s jedinicom**. Jedinstveni neutralni element tog monoida nazivamo onda **jedinica prstena** P, i standardno označavamo s 1.

Uočimo: Prsten nije struktura koja je inducirana s dvije neovisne binarne operacije, nego te operacije moraju biti međusobno usklađene, povezane zakonom distribucije.

Primjer 4.9:

a) Skupovi $P = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, uz standardno zbrajanje i množenje, su prstenovi i to komutativni prstenovi s jedinicom;

b) Neka je S bilo koji neprazni skup i

$$F{=}\mathbb{R}^S = \{f \,|\, f : S \longrightarrow \mathbb{R}\}$$

(sve realne funkcije definirane na S). Onda je uz operacije dane s

$$(f+g)(x) := f(x) + g(x) \qquad (f \cdot g)(x) := f(x) \cdot g(x) \text{ za sve } x \in S,$$

F je komutativni prsten s jedinicom, gdje je jedinica konstantna funkcija $e : S \longrightarrow \mathbb{R}$ dana sa $e(x) = 1$ za sve $x \in S$.
Nula u ovom prstenu je konstantna funkcija $n : S \longrightarrow \mathbb{R}$ dana sa $n(x) = 0$ za sve $x \in S$. Ovaj prsten nazivamo **prsten realnih funkcija na skupu** S;

c) Neka je P skup svih polinoma u jednoj varijabli x s realnim (ili kompleksnim) koeficijentima. Onda je P uz standardno zbrajanje i množenje polinoma komutativni prsten s jedinicom, tzv. **prsten polinoma**.

d) Za svaki $m \in \mathbb{N}$, skup $\mathbb{Z}_m = \{0, 1, ..., m-1\}$ uz zbrajanje i množenje modulo m, je komutativni prsten s jedinicom kojeg nazivamo **prsten cijelih brojeva modulo** m.

Definicija 4.6 *Komutativan prsten s jedinicom* $(F, +, \cdot)$, *nazivamo* ***polje*** *ako je svaki svaki element iz* F, *koji je različit od nule, invertibilan, tj. ako su svi elementi iz* $F^* = F \backslash \{0\}$ *invertibilni.*

Primjer 4.10:

a) Skupovi $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, uz standardno zbrajanje i množenje, su polja;

b) Skup $\mathbb{Z}$ uz standardno zbrajanje i množenje, nije polje jer elementi različiti od ± 1 nemaju multiplikativan inverz;

c) Skup $\mathbb{Z}_m = \{0, 1, ..., m-1\}$, $m \in \mathbb{N}$, uz zbrajanje i množenje $\bmod m$, je polje ako i samo ako je m prost broj.

Npr. za $m = 6$ (složen), prsten $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ nije polje jer svi elementi različiti od nule nemaju multiplikativni inverz. Npr. 2, 3 i 4 nemaju multiplikativni inverz dok 1 i 5 imaju:

$$1 \cdot 1 = 1 \cdot 1 = 1 \Longrightarrow 1^{-1} = 1$$
$$5 \cdot 5 = 5 \cdot 5 = 1 \Longrightarrow 5^{-1} = 5$$

Npr. za $m = 5$ (prost), prsten $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ je polje jer svi elementi različiti od nule imaju multiplikativni inverz. Imamo:

$$2 \cdot 3 = 3 \cdot 2 = 1 \Longrightarrow 2^{-1} = 3 \text{ i } 3^{-1} = 2$$
$$1 \cdot 1 = 1 \cdot 1 = 1 \Longrightarrow 1^{-1} = 1$$
$$4 \cdot 4 = 4 \cdot 4 = 1 \Longrightarrow 4^{-1} = 4$$

Npr. za $m = 7$ (prost), prsten $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ je polje jer svi elementi različiti od nule imaju multiplikativni inverz. Imamo:

$$2 \cdot 4 = 4 \cdot 2 = 1 \Longrightarrow 2^{-1} = 4 \text{ i } 4^{-1} = 2$$
$$3 \cdot 5 = 5 \cdot 3 = 1 \Longrightarrow 3^{-1} = 5 \text{ i } 5^{-1} = 3$$
$$1 \cdot 1 = 1 \cdot 1 = 1 \Longrightarrow 1^{-1} = 1$$
$$6 \cdot 6 = 6 \cdot 6 = 1 \Longrightarrow 6^{-1} = 6$$

Definicija 4.7 Neka su $(P, +_P, \cdot_P)$ i $(S, +_S, \cdot_S)$ dva prstena (polja). Preslikavanje $f : P \to S$ nazivamo **homomorfizam prstenova** (**polja**) ako za sve $a, b \in P$ vrijedi

$$f(a +_P b) = f(a) +_S f(b) \quad \text{i} \quad f(a \cdot_P b) = f(a) \cdot_S f(b).$$

Napomena: Uočimo da je $f : P \to S$ homomorfizam Abelovih grupa $(P, +_P)$ i $(S, +_S)$ i homomorfizam polugrupa (monoida) $(P, \cdot_P)$ i $(S, \cdot_S)$.

Napomena: Na analogan način kao kod grupa se definiraju pojmovi: **epimorfizam, monomorfizam, izomorfizam, automorfizma prstenova (polja)**.