LINEARNA ALGEBRA

(za fizičare)

0. Pregled osnovnih algebarskih struktura - 1

Borka Jadrijević

Sadržaj:

Literatura:

Udžbenici:

1. K. Horvatić, *Linearna algebra*, Golden marketing - Tehnička knjiga, Zagreb, 2004. ;
2. S. Kurepa, *Uvod u linearnu algebru*, Školska knjiga, Zagreb, 1990.
3. N. Elezović, *Linearna algebra*, Element, Zagreb, 2001.

Zbirke zadataka:

1. N. Bakić, A. Milas, *Zbirka zadataka iz linearne algebre s rješenjima,* PMF–Matematički odjel, HMD, Zagreb, 1995.;
2. N. Elezović, A. Aglić, *Linearna algebra – zbirka zadataka*, Element, Zagreb, 2001.

Obveze:

- predavanja ($\geq 70\%$)
- vježbe ($\geq 70\%$)

Provjere znanja:

- *dva kolokvija:*
  - oba pozitivna
  - zadaci ($\geq 50\%$)
- *ispit:*
  - pismeni i usmeni.

Uvod

- Algebra je jedna od osnovnih grana matematike. Ona se bavi algebarskim operacijama, tj. pročuvanjem algebarskih struktura. Pritom, priroda samih elemenata skupa na kojemu se izvode spomenute algebarske operacije nije od primarne važnosti.
- Primarni je cilj proučavanje tih algebarskih operacija.
- Imamo dvije vrste algebarskih operacija, tzv. unutarnja množenja i vanjska množenja.

Definicija (0.1)

Neka je S neki neprazan skup. Svako preslikavanje $u : S \times S \longrightarrow S$,

$$(x, y) \in S \times S \longrightarrow u(x, y) := xy \in S$$

nazivamo **unutarnje množenje** *(ili* **binarna operacija***) na S.*

Definicija (0.1 - nastavak)

Neka je S neki neprazan skup i Ω neki drugi neprazan skup. Svako preslikavanje $v : \Omega \times S \longrightarrow S$,

$$(\alpha, x) \in \Omega \times S \longrightarrow v(\alpha, x) := \alpha y \in S$$

nazivamo **vanjsko množenje** *na S elementima iz Ω.*

Definicija (0.2)

Neka je S neki neprazan skup. **Algebarska struktura** *na S je skup S zajedno sa barem jednim unutarnjim množenjem i/ili bar jednim vanjskim množenjem koja zadovaoljavaju (neki) skup aksioma množenja.*

Najvažniji reprezentanti algebarskih struktura:

a) Strukture s unutarnjim množenjem/množenjima:

- Grupe (1 unutarnje množenje);
- Prsteni, polja (2 unutarnja množenja).

b) Strukture s barem jednim unutarnjim množenjem i barem jednim vanjskim množenjem:

- Vektorski prostori (1 unutarnje množenje i 1 vanjsko množenje);
- Algebre (2 unutarnja množenja i 1 vanjsko množenje);

Definicija (0.3)

Relacija ρ na skupu S *je svaki podskup Kartezijevog produkta* $S \times S$.*Neka je* $\rho \subset S \times S$ *relacija na* S. *Ako je* $(a, b) \in \rho$ *kažemo da je "a u relaciji* ρ *sa b" i pišemo* $a \rho b$.

Posebna svojstva relacija:

1. $(\forall a \in S)\ (a \rho a)$ (**refleksivnost**);
2. $(\forall a, b \in S)\ (a \rho b \Longrightarrow b \rho a)$ (**simetričnost**);
3. $(\forall a, b \in S)\ (a \rho b\ i\ b \rho a \Longrightarrow a = b)$ (**antisimetričnost**);
4. $(\forall a, b, c \in S)\ (a \rho b\ i\ b \rho c \Longrightarrow a \rho c)$ (**tranzitivnost**).
   Ako relacija ρ *ima svojstva 1., 2. i 4. kažemo da je* ρ **relacija ekvivalencije na** S *i obično je označujemo s* "$\sim$".

Neka je $\sim$ relacija ekvivalencije na S i $a \in S$.

Definiramo **klasu ekvivalencije** elementa a po relaciji $\sim$, u oznaci $[a]$, sa

$$[a] = \{x \in S \,|\, x \sim a\}.$$

Očito je $[a] \neq \emptyset$ i vrijedi:

Teorem (0.1)

Neka su a i b proizvoljni elementi iz S. Tada je $[a] \cap [b] = \emptyset$ *ili* $[a] = [b]$.

Dokaz:

Dakle, relacija ekvivalencije na nekom skupu određuje particiju tog skupa na disjunktne klase ekvivalencije.

Definicija (0.4)

Skup svih klasa ekvivalencije skupa S po relaciji ekvivalencije $\sim$ označujemo sa $S/\sim$ i nazivamo **kvocijentni skup** *(skupa S po $\sim$). Preslikavanje*

$$q : S \longrightarrow S/\sim$$

definirano sa

$$q(a) = [a]$$

naziva se **kvocijentno preslikavanje**. *To preslikavanje je surjektivno.*

Primjer (0.1)

Neka je $S = \mathbb{Z}$ *i* $m \in \mathbb{N}$. *Definirajmo relaciju* $\sim_m$ *na* $\mathbb{Z}$ *(kongruencija modulo m). Za* $a, b \in \mathbb{Z}$ *definiramo*

$$a \sim_m b \iff m \,|\, a - b \quad \text{(još pišemo i } a \equiv b \,(\mathrm{mod}\, m)\text{)}.$$

Ovo je relacija ekvivalencije i

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

Npr.

$$\mathbb{Z}/\sim_2 = \{[0],\ [1]\}$$

i

$$\mathbb{Z} = [0] \cup [1] = \{\ldots, -4, -2,\ 0,\ 2,\ 4, \ldots\} \cup \{\ldots, -3, -1,\ 1,\ 3, \ldots\}.$$

Kvocijentno preslikavanje $q : \mathbb{Z} \longrightarrow \mathbb{Z}/\sim_2$ *je dano sa*

$$q(\pm 2n) = [\pm 2n] = [0] \quad i \quad q(\pm(2n+1)) = [\pm(2n+1)] = [1].$$

0.1 Binarna operacija. Grupoid. Polugrupa. Monoid. Grupa.

Definition (0.5)

Neka je G neprazni skup. **Binarna operacija** (ili **unutarnje množenje**) na skupu G je svako preslikavanje $\theta : G \times G \longrightarrow G$. Dakle, binarna operacija svakom uređenom paru $(a, b) \in G \times G$ pridružuje točno jedan element

$$c = \theta(a, b) \in G$$

koji nazivamo **rezultat** binarne operacije na paru (a, b).

Definicija (0.6)

Binarnom operacijom θ na nepraznom skupu G zadana je algebarska struktura koju nazivamo **grupoid**. *Dakle,* **grupoid** *je uređeni par (G, θ) koji se sastoji od nepraznog skupa G i binarne operacije θ.*

Primjer (0.2)

1. *Neka je* $G = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *a binarana operacija definirana kao*

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

standardno zbrajanje.

Svi ovi skupovi su uz ovu binarnu operaciju grupoidi: $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

2. *Slično, skupovi* $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *su grupoidi su i uz binarnu operaciju standardnog množenja*

$$\theta(a, b) = a \cdot b.$$

Uočimo: npr. $(\mathbb{N}, +)$ *i* $(\mathbb{N}, \cdot)$ *su različiti grupoidi.*

Primjer (0.2 - nastavak)

3. *Neka je S bilo koji skup i $\mathcal{F}(S) = \{f \,|f : S \longrightarrow S\} := S^S$ (sva preslikavanja iz S u S). Na skupu S^S promatramo binarnu operaciju:*

$$\theta(f, g) = g \circ f$$

danu sa

$$(g \circ f)(x) = g(f(x)) \quad \text{za svaki } x \in S.$$

Onda je $(S^S, \circ)$ grupoid.

Napomena

Umjesto funkcijske vrijednosti $\theta(a, b)$, rezultat binarne operacije na paru (a, b) obično pišemo

$$a + b, \;\; a \cdot b, \;\; a \circ b, \;\; a * b, \ldots.$$

a u apstratktnim razmatranjima obično identificiramo

$$\theta(a, b) \equiv a \cdot b \equiv ab.$$

Definicija (0.7)

Neka je $(G, \cdot)$ grupoid i $a, b \in S$. Ako je $ab = ba$ onda kažemo da a i b **komutiraju**. *Nadalje, ako vrijedi*

$$ab = ba \quad \text{za sve } a, b \in G,$$

onda kažemo da je binarna operacija **komutativna**, *tj. da je $(G, \cdot)$* **komutativan** *ili* **Abelov grupoid**.

Primjer (0.3)

- *Grupoidi $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C}, \cdot)$ (uz standardno zbrajanje i množenje) su komutativni grupoidi;*
- *Grupoid $\left(S^S, \circ\right)$ (u Primjeru 0.2, 3.) nije komutativan.*

Definicija (0.8)

Neka je $(G, \cdot)$ grupoid i $A \subseteq G$. Kažemo da je skup A **grupoid s obzirom na operaciju $\cdot$ naslijeđenu iz G** *ako za sve $a, b \in A$ vrijedi $a \cdot b \in A$.*

Još kažemo da je A **zatvoren** *s obzirom na operaciju $\cdot$, odnosno da je $(A, \cdot)$* **podgrupoid** *od $(G, \cdot)$.*

Primjer (0.4)

- *Kako je $(\mathbb{Z}, +)$ grupoid i $\mathbb{N} \subset \mathbb{Z}$, tada $(\mathbb{N}, +)$ možemo smatrati grupoidom s obzirom na operaciju $+$ naslijeđenu iz $\mathbb{Z}$, tj. podgrupoidom od $(\mathbb{Z}, +)$.*
- *Kako je $(\mathbb{R}, \cdot)$ grupoid i $\mathbb{Q} \subset \mathbb{R}$, tada $(\mathbb{Q}, \cdot)$ možemo smatrati da je grupoidom s obzirom na operaciju $\cdot$ naslijeđenu iz $\mathbb{R}$, tj. podgrupoidom od $(\mathbb{R}, \cdot)$.*

Definicija (0.9)

Polugrupa *je grupoid* $(G, \cdot)$ *kod kojeg je operacija* $\cdot$ **asocijativna**, *tj. vrijedi:*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \text{za sve } a, b, c \in G.$$

Napomena

a) *Iz zakona asocijacije slijedi*

$$a\,(bc) = (ab)\,c := abc \quad \text{za sve } a, b, c \in G.$$

Ovo svojstvo vrijedi i za više od tri faktora. Npr.

$$(ab)\,cd = a\,(bc)\,d := ab\,(cd) := abcd \quad \text{za sve } a, b, c, d \in G.$$

b) *U polugrupi* $(G, \cdot)$ *ima smisla pojam potencije. Definiramo:*

$$a^1 := a, \ a^2 := aa \ \text{ i induktivno } a^{n+1} := a^n a \ \text{ za } n \in \mathbb{N}.$$

Vrijedi $a^m \cdot a^n = a^{m+n}$ *i* $(a^m)^n = a^{m \cdot n}$ *za sve* $m, n \in \mathbb{N}$.

Primjer (0.5)

- *Grupoidi* $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C}, \cdot)$ *(uz standardno zbrajanje i množenje) su (komutativne) polugrupe;*
- *Grupoid* $\left(S^S, \circ\right)$ *(u Primjeru 0.2, 3.) je (nekomutativna) polugrupa.*

Definicija (0.10)

Monoid *je polugrupa* $(G, \cdot)$ *u kojoj postoji element* $e \in G$ *takav da vrijedi:*

$$ea = ae = a, \quad \text{za sve } a \in G.$$

Element e *nazivamo* **jedinica** *ili* **neutralni element** *ili* **jedinični element**.
Ako je binarna operacija dodatno i komutativna onda govorimo o **komutativnom monoidu** .

Napomena

Svaki monoid ima točno jedan jedinični element.

Primjer (0.6)

- *U polugrupi* $(\mathbb{N}, +)$ *nema neutralnog elementa, dok je u* $(\mathbb{N}, \cdot)$ *to broj* 1*, pa je* $(\mathbb{N}, \cdot)$ *(komutativni) monoid.*
  Polugrupe $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ *imaju neutralni* $e = 0$*, pa su to (komutativni) monoidi. Slično,* $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ *su (komutativni) monoidi s neutralnim elementom* $e = 1$*;*
- *Polugrupa* $\left(S^S, \circ\right)$ *(u Primjeru 0.2, 3.) ima neutralni element i to je preslikavanje* $e : S \longrightarrow S$*, definirano sa* $e(x) = x$ *za sve* $x \in S$*. Dakle,* $\left(S^S, \circ\right)$ *je (nekomutativni) monoid.*

Definicija (0.11)

Grupa *je monoid* $(G, \cdot)$ *kod kojeg za svaki* $a \in G$ *postoji jedinstven* $a^{-1} \in G$ *sa svojstvom*

$$aa^{-1} = a^{-1}a = e.$$

Element a^{-1} *nazivamo* **inverz** *od* a*.*

Alternativno:

Definicija (0.11-a)

Uređeni par $(G, \cdot)$, gdje je G skup, $a \cdot$ binarna operacija na G, je **grupa** *ako su ispunjeni sljedeći uvjeti:*

i) *za sve $a, b \in G$ vrijedi $ab \in G$; (grupoidnost)*

ii) *za sve $a, b, c \in G$ vrijedi $a(bc) = (ab)c$; (asocijativnost)*

iii) *postoji jedinični element e, tj. postoji element za kojeg vrijedi $ea = ae = a$ za sve $a \in G$ (postojanje jediničnog elementa);*

iv) *za svaki $a \in G$ postoji inverzni element a^{-1}, tj. element za kojeg vrijedi da je $aa^{-1} = a^{-1}a = e$ (postojanje inverza);*
Grupa $(G, \cdot)$ je **komutativna** *ili* **Abelova grupa** *ako dodatno vrijedi: $ab = ba$ za svaki izbor $a, b \in G$.*

Napomena

Inverzni element a^{-1} od a u grupi G je jedinstven za svaki $a \in G$ i vrijedi $\left(a^{-1}\right)^{-1} = a$.

Primjer (0.7)

- $(\mathbb{Z}, +)$ *je komutativna grupa. Neutralni element je* 0*, dok je* $-a$ *inverz od* a*, jer vrijedi* $a + (-a) = 0$ *za svaki* $a \in \mathbb{Z}$.

  Slično, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ *su komutativne grupe. Napomena: Dakle, (standardno) oduzimanje je zbrajanje sa suprotnim elementom:* $a + (-b) := a - b$*;*

- $(\mathbb{R} \setminus \{0\}, \cdot)$ *je komutativna grupa. Neutralni element je* 1*, dok je* a^{-1} *inverz od* a*, jer vrijedi* $a \cdot a^{-1} = 1$ *za svaki* $a \in \mathbb{R} \setminus \{0\} := \mathbb{R}^*$.

  Slično, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ *su komutativne grupe.*

  Zašto $(\mathbb{R}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{C}, \cdot)$ *nisu grupe?*

- *Nekomutativni monoid* $\left(S^S, \circ\right)$ *nije grupa. U tom monoidu invertibilna su samo ona preslikavanja koja su bijekcije. Naime, jedino za bijekciju* $f : S \longrightarrow S$ *postoji inverzno preslikavanje*

$$f^{-1} : S \longrightarrow S,$$

  tj. ono za koje je vrijedi $f \circ f^{-1} = f^{-1} \circ f = e$.

Primjer (0.7 - nastavak)

Neka je

$$B(S) = \left\{ f \in S^S \mid f \text{ je bijekcija} \right\} \subset S^S.$$

Tada je $B(S)$ *s obzirom na operaciju komponiranja* $\circ$ *naslijeđenu iz* S^S, *(tj.* $(B(S), \circ)$*) (nekomutativna) grupa. Tu grupu nazivamo* **grupom permutacija** *od* S.

- *Skup* $\mathbb{Z}_m = \{0, 1, ..., m-1\}$, $m \in \mathbb{N}$, *uz zbrajanje* $\bmod m$, *je Abelova grupa* $(\mathbb{Z}_m, +_m)$. *Npr. za* $m = 6$, *imamo* $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. *Neutralni element je* 0 *i*

$$\begin{aligned} 3 +_6 5 &= 5 +_6 3 = 2 \\ 2 +_6 4 &= 0 \Longrightarrow -2 = 4 \end{aligned}$$

  Skup $\mathbb{Z}_m^* = \{1, ..., m-1\}$, $m \in \mathbb{N}$, *uz množenje* $\bmod m$, *je Abelova grupa* $(\mathbb{Z}_m, \cdot_m)$ *ako i samo ako je* m *prost. Inače je komutativni monoid.*

Napomena

- *Apstraktnu grupu $(G, \cdot)$ (neprecizno) nazivamo "multiplikativna" grupa, a binarnu operaciju $\cdot$ "množenje".*
- *U Abelovoj grupi binarnu operaciju obično zapisujemo aditivno, tj. ako grupu zadamo sa $(G, +)$ onda je nazivamo "aditivna" grupa i podrazumijevamo da je Abelova. Neutralni element aditivne grupe nazivamo* **nula** *(i označavamo sa 0), a inverzni element od a označavamo sa $-a$ (umjesto a^{-1}) i nazivamo* **suprotni element**.

Propozicija (0.1)

Neka je $(G, \cdot)$ grupa.

i) *(invertiranje produkta) Za sve $a, b \in G$ vrijedi*

$$(ab)^{-1} = b^{-1}a^{-1}.$$

ii) *(pravilo skraćivanja) Za sve $a, b, c \in G$ vrijedi*

$$ac = bc \iff a = b;$$
$$ca = cb \iff a = b.$$

Napomena

Ako je n prirodan broj onda se u grupi $(G, \cdot)$ definira potencija elementa $a \in G$ sa $a^n := a \cdot \ldots \cdot a$, $a^{-n} := \left(a^{-1}\right)^n$, $a^0 := e$.

Propozicija (0.2)

U svakoj grupi $(G, \cdot)$ vrijede sljedeća pravila potenciranja za sve $a \in G$ i $m, n \in \mathbb{Z}$.

i) $a^m a^n = a^n a^m = a^{m+n}$;

ii) $(a^m)^n = a^{m \cdot n}$;

iii) *ako je grupa komutativna, onda za sve $a, b \in G$ vrijedi $(ab)^n = a^n b^n$.*

Za nekomutativne grupe tvrdnja **iii)** *općenito ne vrijedi. Isto tako iz svojstva ii) slijedi: $a^{-n} = (a^n)^{-1}$.*

Napomena

- *Potenciji a^n u multiplikativnoj grupi odgovara u aditivnoj:* $na := a + \ldots + a$;
- *Potenciji a^{-n} u multiplikativnoj grupi odgovara u aditivnoj:* $(-n)\,a := n\,(-a) = -\,(na)\,;$
- *Potenciji $a^0 = e$ u multiplikativnoj grupi odgovara u aditivnoj:* $0a := \mathbf{0}$ *(oprez!)*;

Sada Propozicija 0.2 za aditivnu grupu glasi:

Propozicija (0.2')

i) $ma + na = (m + n)\,a$;

ii) $m\,(na) = (mn)\,a$;

iii) $n\,(a + b) = na + nb$ *(ako je* $(G, +)$ *komutativna).*

Definicija (0.12)

Ako je grupa $(G, \cdot)$ konačna, tj. ako skup G ima konačno elemenata, onda broj elemenata od G nazivamo **red grupe** *i označavamo sa $|G|$.*

Prema redu grupe dijelimo na **konačne** *i* **beskonačne** *.*

Definicija (0.13)

Neka je $(G, \cdot)$ grupa i neka je $H \subseteq G$ neprazan podkup. Kažemo da je H **podgrupa** *grupe G ako je i sama grupa s obzirom na binarnu operaciju $\cdot$ naslijeđenu iz G. Pišemo $H \leq G$. Ako je $H \subset G$ pišemo $H < G$.*

Svaka grupa ima dvije **trivijalne podgrupe***: jediničnu podgrupu $\{e\}$ i podgrupu G.*

Propozicija (0.3)

Neka je $(G, \cdot)$ grupa i H neprazan podskup od G.

i) *H je podgrupa od G onda i samo onda ako za sve $a, b \in H$ vrijedi $ab^{-1} \in H$;*

ii) *Presjek dviju ili više podgrupa od G je opet podgrupa od G.*

Napomena

Svojstvo i) iz Propozicije 0.3 za aditivne grupe glasi:

Neka je $(G, +)$ grupa. H je podgrupa od G onda i samo onda ako za sve $a, b \in H$ vrijedi $a - b \in H$.

Napomena

Neka je grupa $(G, \cdot)$ i $a \in G$, $a \neq e$. Ako za neki prirodan broj n vrijedi $a^n = e$, onda najmanji takav n nazivamo **red elementa** *a. Ako takav n ne postoji kažemo da je element a* **beskonačnog reda**.

Teorem (0.1 - Lagrange)

Neka je $H \leq G$ i grupa G konačna.

i) *Red podgrupe $|H|$ je djelitelj od $|G|$;*

ii) *Za svaki $a \in G$, red od a je djelitelj od $|G|$.*

Neka je $(G, \cdot)$ komutativna grupa i $H \leq G$. Tada na skupu G možemo definirati relaciju $\sim$ stavljajući za $a, b \in G$

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

Relacija $\sim$ je relacija ekvivalencije. Dakle, relacija $\sim$ dijeli elemente od G u disjunktne skupove, tj. klase ekvivalencije u odnosu na $\sim$. Neka je za $a \in G$ sa

$$[a] = \{x \in G \,|\, x \sim a\}.$$

označena klasa ekvivalencije generirana sa a. Tada je

$$[a] = aH = \{ay \,|\, y \in H\}.$$

Kvocijentni skup $G/\sim$ označujemo sa

$$G/H = \{aH \,|\, a \in H\}.$$

Ovaj skup, uz prirodno množenje klasa kao binarnom operacijom

$$[a] \cdot [b] = (aH)(bH) = (ab)H$$

je grupa koju nazivamo **kvocijentna grupa (komutativne) grupe G po podgrupi H.**

Uz kvocijentnu grupu G/H prirodno povezujemo preslikavanje:

$$p : G \longrightarrow G/H$$

definirano sa

$$p(a) = [a] = aH$$

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

Napomena

Ako je komutativna grupa zapisana aditivno $(G, +)$, *onda imamo zapis:*

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

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

$$[a] + [b] = (a + H) + (b + H) = (a + b)\, H$$

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

Primjer (0.8)

Neka je $(G,+)=(\mathbb{Z},+)$, $m\in\mathbb{N}$ *i* $H=m\mathbb{Z}=\{mk\,|k\in\mathbb{Z}\}\subseteq\mathbb{Z}$.
Tada je $m\mathbb{Z}\leq\mathbb{Z}$, *a 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): $[0],[1],\ldots,[m-1]$. *Prema tome to je grupa reda m. Ovu grupu nazivamo* **grupom klasa ostataka modulo** *m. Prirodna projekcija je dana sa*

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

Imamo:

grupe $\subset$ **monoidi** $\subset$ **polugrupe** $\subset$ **grupoidi.**

0.2 Homomorfizmi i izomorfizmi grupa

Definicija (0.14)

Neka su $(G, \cdot_G)$ *i* $(H, \cdot_H)$ *grupe. Preslikavanje* $f : G \longrightarrow H$ *je* **homomorfzam grupa** *ako je ispunjeno:*

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

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

Primjer (0.9)

i) *Neka su* $(G, \cdot_G)$ *i* $(H, \cdot_H)$ *grupe i* e_2 *jedinica u* H. *Tada je preslikavanje* $f : G \longrightarrow H$ *dano sa*

$$f(a) = e_2 \quad \text{za sve } a \in G,$$

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

Primjer (0.9 - nastavak)

ii) *Neka je* $(H, \cdot)$ *grupa i neka je* $G \leq H$. *Tada je* **inkluzija** $i : G \longrightarrow H$, *dana sa*

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

homomorfizam. Posebno, identiteta $i : H \longrightarrow H$ *je homomorfizam.*

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

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

Tada je f *homomorfizam jer je*

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

za sve $x, y \in \mathbb{R}$.

Propozicija (0.4)

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

i) *Ako je e_1 jedinica u G, onda je $f(e_1) = e_2$ jedinica u H;*

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

Propozicija (0.5)

Neka je $f : G \to H$ homomorfizam grupa.

i) *Skup*

$$J(f) = Ker(f) := \{a \in G : f(a) = e\}$$

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

ii) **Slika** *homomorfizma f*

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

je podgrupa grupe H.

Definicija (0.15)

Neka je $f : G \to H$ homomorfizam grupa.

- *Ako je homomorfizam f surjekcija onda ga nazivamo* **epimorfizam**.
- *Ako je homomorfizam f injekcija onda ga nazivamo* **monomorfizam**.
- *Ako je homomorfizam f bijekcija onda ga nazivamo* **izomorfizam grupa**. *U tom slučaju kažemo da je grupa G* **izomorfna** *grupi H i pišemo $G \simeq H$.*
- *Homomorfzam $\varphi : G \longrightarrow G$ se naziva* **endomorfzam** *grupe G. Bijektivni endomorfzam se naziva* **automorfzam** .

Napomena

Monomorfizam $f : G \to H$ nazivamo još i **ulaganje** *G u H, jer je*

$$G \simeq S(f) \leq H.$$

Propozicija (0.6)

Neka je $f : G \to H$ homomorfizam grupa.

i) *f je epimorfizmi grupa ako i samo ako je $S(f) = H$.*

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

Napomena

Da bi pokazali da je $f : G \to H$ izomorfizam grupa treba pokazati:

1. *f je homomorfizam;*
2. *$J(f) := \{e_G\}$;*
3. *f je surjekcija, tj. $S(f) = H$.*

Propozicija (0.7)

i) *Ako su $f : G \to H$ i $g : H \to K$ homomorfizmi (izomomorfizmi) grupa, onda je i $g \circ f : G \to K$ homomorfizam (izomomorfizam) grupa.*

ii) *Ako je $f : G \to H$ izomomorfizam grupa, onda je i $f^{-1} : H \to G$ izomomorfizam grupa.*

Korolar (0.1)

Relacija $\simeq$ izomorfnosti među grupama je relacija ekvivalencije.

Napomena

- *Dvije grupe G i H su izomorfne ako postoji barem jedan izomorfizam $f : G \to H$.*
- *Grupe G i H koje su međusobno izomorfne s motrišta teorije grupa ne razlikujemo, tj. smatramo da su jednake.*

Napomena (- nastavak)

Poistovjećivanje realizira izomomorfizam $f : G \to H$:

1. $|G| = |H|$ *(f je bijekcija);*
2. *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 (0.10)

1. *Neka je $(H, \cdot)$ grupa i neka je $G \leq H$. Tada je inkluzija $i : G \longrightarrow H$, monomorfizam. Posebno, identiteta $i : H \longrightarrow H$ je izomomorfizam;*
2. *Za svaki $m \in \mathbb{N}$, skup $\mathbb{Z}_m = \{0, 1, ..., m-1\}$ uz zbrajanje $\bmod m$, je Abelova grupa. Tada je grupa $\mathbb{Z}_m$ izomorfna kvocijentnoj grupi $\mathbb{Z}/m\mathbb{Z}$.*

Primjer (0.10 - nastavak)

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

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

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*

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

je, po Propoziciji 0.7, ii), također izomorfizam grupa $(\mathbb{R}^+, \cdot)$ *i* $(\mathbb{R}, +)$.

0.3 Prsten. Polje.

Definicija (0.16)

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. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, *za svaki izbor* $a, b, c \in P$ *(asocijativnost);*
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);*

Prsten $(P, +, \cdot)$ je **komutativan** *ako dodatno vrijedi:*

5. $a \cdot b = b \cdot a$, *za svaki izbor* $a, b \in P$.

$(P, +, \cdot)$ *je* **prsten s jedinicom** *ako postoji element* $1_P \in P$ *takav da vrijedi* $1_P \cdot a = a \cdot 1_P = a$, *za svaki izbor* $a \in P$.

Napomena

- *S 0_P označavamo neutralni element grupe $(P,+)$, a s $-a$ označujemo inverzni (suprotni) element od a u $(P,+)$.*
- *Ako je u prstenu s jedinicom $1_P = 0_P$, tada je $P = \{0_P\}$* **trivijalni prsten.**
- *Dogovorno je $\cdot$ "jače" od $+$ po snazi vezivanja. Npr. imamo*

$$ab + ac := (a \cdot b) + (a \cdot c), \quad \text{a ne} \quad a \cdot (b + a) \cdot c.$$

Primjer (0.11)

1. *Skupovi $P = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, uz standardno zbrajanje i množenje, su prstenovi i to komutativni prstenovi s jedinicom;*
2. *Za svaki $m \in \mathbb{N}$, skup $\mathbb{Z}_m = \{0, 1, ..., m-1\}$ uz zbrajanje i množenje $\bmod m$, je komutativni prsten s jedinicom kojeg nazivamo* **prsten cijelih brojeva modulo** *m.*

Primjer (0.11 - nastavak)

3. *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

$$(f+g)(x) := f(x)+g(x) \quad i \quad (f \cdot g)(x) := f(x) \cdot g(x) \;\; za\ sve\ x \in S$$

F 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** ;

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

Propozicija (0.8)

U svakom prstenu P vrijedi:

1. $0 \cdot a = a \cdot 0 = 0$ *za svaki* $a \in P$;
2. $a(-b) = (-a)\, b = -ab$ *za sve* $a, b \in P$;
3. $(-a)(-b) = ab$ *za sve* $a, b \in P$;

Iz Propozicije 0.8, i) slijedi:

Korolar (0.2)

Ako je P prsten s jedinicom i ima barem dva elementa (tj. nije nul-prsten), onda je $0 \neq 1$.

Definicija (0.17)

Za element $a \in P$ prstena s jedinicom $(P, +, \cdot)$ kažemo da je **invertibilan s lijeva (s desna)** *ako postoji $b \in P$ takav da je $ba = 1$ ($ab = 1$). Za element koji je invertibilan s lijeva i s desna kažemo da je* **invertibilan** .

Napomena

Svi invertibilni elementi u prstenu s jedinicom $(P, +, \cdot)$ tvore grupu u odnosu na množenje.

Definicija (0.18)

Komutativni prsten s jedinicom F u kojem je skup $F^* = F \setminus \{0\}$ grupa s obzirom na množenje nazivamo **polje**.

Napomena

Dakle, polje je integralana domena u kojoj svaki element $\neq 0$ ima multiplikativni inverz.

Imamo:

$$\textbf{polja} \subset \textbf{komutativni prstenovi} \subset \textbf{prstenovi}$$

Primjer (0.12)

1. *Skupovi* $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, *uz standardno zbrajanje i množenje, su polja;*
2. *Skup* $\mathbb{Z}$ *uz standardno zbrajanje i množenje, nije polje jer elementi različiti od* ± 1 *nemaju multiplikativan inverz.;*
3. *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.*

Primjer (0.12 - nastavak)

Imamo:

$$\begin{aligned} 2\cdot 3 &= 3\cdot 2 = 1 \Longrightarrow 2^{-1} = 3 \ \ i \ \ 3^{-1} = 2 \\ 1\cdot 1 &= 1\cdot 1 = 1 \Longrightarrow 1^{-1} = 1 \\ 4\cdot 4 &= 4\cdot 4 = 1 \Longrightarrow 4^{-1} = 4 \end{aligned}$$

Definicija (0.19)

Za S kažemo da je **potprsten** *prstena $(P, +, \cdot)$ ako je $S \subseteq P$ i S je prsten s obzirom na operacije naslijeđene iz P.*

Napomena

Svaki prsten $(P, +, \cdot)$ ima dva **trivijalna potprstena***: potprsten $\{0\}$ i potprsten P.*

Propozicija (0.9)

Neka je $(P, +, \cdot)$ prsten i A neprazan podskup od P.

i) *A je potprsten od P onda i samo onda ako za sve $a, b \in H$ vrijedi $a - b \in A$ i $ab \in A$;*

ii) *Presjek dviju ili više potprstena od P je opet potprsten od P.*

Napomena

- *Iz Propozicije 0.9, i) vidimo da je neprazan podskup $A \subseteq P$ potprsten prstena P ako i samo ako je podgrupa aditivne grupe od P (tj. od $(P, +)$) i ako je A zatvoren s obzirom na množenje.*
- *Na analogan način se definira pojam potpolja.*

Primjer (0.13)

- *Kako je* $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, *uz standardno zbrajanje i množenje,* $\mathbb{Q}$ *i* $\mathbb{R}$ *su potpolja od* $\mathbb{C}$. *Isto tako* $\mathbb{Q}$ *je potpolje od* $\mathbb{R}$, *ali* $\mathbb{Z}$ *nije potpolje od* $\mathbb{Q}$ *(ni od* $\mathbb{R}$ *ni od* $\mathbb{C}$*) nego potprsten od* $\mathbb{Q}$, $\mathbb{R}$ *odnosno* $\mathbb{C}$;
- $(\mathbb{Z}, +, \cdot)$ *je komutativan prsten s jednicom. Neka je* $m \in \mathbb{N}$ *i* $m\mathbb{Z} = \{mk \,|k \in \mathbb{Z}\}$. *Tada je* $m\mathbb{Z}$ *potprsten od* $\mathbb{Z}$.

0.4 Homomorfizmi i izomorfizmi prstenova (polja)

Definicija (0.20)

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

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

Napomena

Budući je $f : P \to S$ *i homomorfizam Abelovih grupa* $(P, +_P)$ *i* $(S, +_S)$ *onda je*

$$f(0_P) = 0_S \quad i \quad f(-a) = -f(a).$$

Definicija (0.21)

Neka je $f : P \to S$ *homomorfizam prstenova.*

- *Ako je* $f : P \to S$ *bijekcija onda* f *nazivamo* **izomorfizam prstenova** *i pišemo* $P \simeq S$;
- *Ako je* $f : P \to S$ *surjekcija onda* f *nazivamo* **epimorfizam prstenova** ;
- *Ako je* $f : P \to S$ *injekcija onda* f *nazivamo* **monomorfizam prstenova** ;
- *Izmomorfizam* $f : P \to P$ *nazivamo* **automorfizam** *prstena* P.

Napomena

Na analogan način se definiraju pojmovi: **homomorfizam, izomorfizam, epimorfizam, monomorfizam, automorfizma polja**.

Propozicija (0.10)

Relacija $\simeq$ izomorfnosti među prstenovima je relacija ekvivalencije.

Propozicija (0.11)

Neka su prstenovi P i S izomorfni, tj. neka postoji izomorfizam prstenova $f : P \to S$. Tada vrijedi:

i) *Ako je 1_P jedinica u P, onda je $f(1_P) = 1_S$ jedinica u S;*

ii) *Ako je P komutativan prsten, onda je i S komutativan prsten;*

iii) *Ako je P polje, onda je i S polje i vrijedi $f\left(a^{-1}\right) = f(a)^{-1}$ za svaki $a \in P$, $a \neq 0$.*

Primjer (0.14)

$(\mathbb{Z}, +, \cdot)$ je komutativan prsten s jednicom. Tada je $m\mathbb{Z} = \{mk \,|k \in \mathbb{Z}\}$ potprsten od $\mathbb{Z}$ za svaki $m \in \mathbb{N}$, pa je

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

kvocijentna grupa grupe $(\mathbb{Z}, +)$ po podgrupi $(m\mathbb{Z}, +)$. Želimo $\mathbb{Z}/m\mathbb{Z}$ organizirati u prsten. Kako je $ax \in m\mathbb{Z}$ za svaki $a \in m\mathbb{Z}$ i za svaki $x \in \mathbb{Z}$ ($m\mathbb{Z}$ je ideal od $\mathbb{Z}$!), tada je dobro definiramo množenje klasa sa

$$(x + m\mathbb{Z}) \cdot (y + m\mathbb{Z}) := xy + m\mathbb{Z}.$$

Sada je, uz binarne operacije zbrajanja i množenja dane sa

$$(k + m\mathbb{Z}) + (l + m\mathbb{Z}) = (k + l) + m\mathbb{Z},$$

$$(k + m\mathbb{Z}) \cdot (l + m\mathbb{Z}) = kl + m\mathbb{Z},$$

$(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ je komutativan prsten s jednicom $1 + m\mathbb{Z}$.

Primjer (0.15 - nastavak)

$(\mathbb{Z}_m, +, \cdot)$ i $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ su komutativni prstenovi s jednicom. Preslikavanje dano sa

$$f : \mathbb{Z}_m \longrightarrow \mathbb{Z}/m\mathbb{Z} \quad \text{dano sa} \quad f(a) = a + m\mathbb{Z}$$

je izomorfizam prstenova, tj. $\mathbb{Z}_m \simeq \mathbb{Z}/m\mathbb{Z}$. Ako je $m = p$ prost broj, tada su $\mathbb{Z}_m$ i $\mathbb{Z}/m\mathbb{Z}$ polja pa je to izomorfizam polja.Npr. $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ je polje jer svi elementi različiti od nule imaju multiplikativni inverz:

$$1^{-1} = 1,\ 2^{-1} = 3,\ 3^{-1} = 2,\ 4^{-1} = 4.$$

Isto tako $\mathbb{Z}/5\mathbb{Z}$ je polje jer svi elementi različiti od nule imaju multiplikativni inverz:

$$(2 + 5\mathbb{Z}) \cdot (3 + 5\mathbb{Z}) = (3 + 5\mathbb{Z}) \cdot (2 + 5\mathbb{Z}) = 6 + 5\mathbb{Z} = 1 + 5\mathbb{Z}$$

$$\Longrightarrow (3 + 5\mathbb{Z})^{-1} = 2 + 5\mathbb{Z} \quad i \quad (2 + 5\mathbb{Z})^{-1} = 3 + 5\mathbb{Z}$$

Primjer (0.15 - nastavak)

Slično:

$$(1+5\mathbb{Z})\cdot(1+5\mathbb{Z}) = 1+5\mathbb{Z} \Longrightarrow (1+5\mathbb{Z})^{-1} = 1+5\mathbb{Z}$$

$$(4+5\mathbb{Z})\cdot(4+5\mathbb{Z}) = 16+5\mathbb{Z} = 1+5\mathbb{Z} \Longrightarrow (4+5\mathbb{Z})^{-1} = 4+5\mathbb{Z}$$

Neka je $f : \mathbb{Z}_5 \to \mathbb{Z}/5\mathbb{Z}$ *dano sa*

$$f(a) = a+5\mathbb{Z}.$$

Tada je f *izomorfizam polja. Imamo npr.*

$$\begin{aligned} f(0) &= 0+5\mathbb{Z} = 5\mathbb{Z} \quad (f(0_P) = 0_S) \\ f(1) &= 1+5\mathbb{Z} \quad (f(1_P) = 1_S) \\ f\left(3^{-1}\right) &= f(2) = 2+5\mathbb{Z} = (3+5\mathbb{Z})^{-1} = f(3)^{-1} \end{aligned}$$