Linearna algebra

0. Osnovne algebarske strukture

Borka Jadrijević

LINEARNA ALGEBRA (za fizičare)

Sadržaj:

Literatura:

Udžbenici:

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

Zbirke zadataka:

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

Obveze:

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

Provjere znanja:

- *dva kolokvija (parcijalna ispita):*

- zadaci;
- oba pozitivna.

- *završni ispit:*

- pismeni ispit;
- usmeni ispit.

0.0 Uvod.

Algebra je jedna od osnovnih grana matematike. Ona se bavi algebarskim operacijama, tj. pučavanjem 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

- 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.

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

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

Definicija 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 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

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

Npr.

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

i

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

0.1 Binarna operacija. Grupoid.

Definicija 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 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 1:

a) 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: $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

b) 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;

c) Skup $\mathbb{N}$ uz standardno oduzimanje $\theta(a, b) = a - b$ nije grupoid, dok $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ to jesu;

d) Neka je S bilo koji skup i $\mathcal{P}(S) = \{A \,|A \subset S\}$ njegov partitivni skup. Tada je $\mathcal{P}(S)$, uz svaku od sljedećih operacija, grupoid:

$$\begin{aligned} \theta(A,B) &= A \cup B \\ \theta(A,B) &= A \cap B \\ \theta(A,B) &= A \setminus B \end{aligned}$$

e) 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 $\left(S^S, \circ\right)$ grupoid.

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

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

a u apstratktnim razmatranjima obično identificiramo

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

Primjer 2 Ako je G konačan skup i nema previše elemenata, tada se binarna operacija može zadati tablično (tablicom množenja). Npr. neka je $G=\{a,b,c,d\}$ i binarna operacija $\circ$ zadana tablično:

$*$	a	b	c	d
a	a	b	c	d
b	b	b	b	b
c	c	c	c	c
d	d	c	b	a

Uočimo: $a*a=a,\ d*c=b$, $c*d=c$, ...i $d*c\neq c*d$.

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

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

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

Primjer 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;
- Grupoidi $(\mathbb{Z}, -)$, $(\mathbb{Q}, -)$, $(\mathbb{R}, -)$, $(\mathbb{C}, -)$ nisu komutativni;
- Grupoidi (u Primjeru 1, d)) $(\mathcal{P}(S), \cup)$ i $(\mathcal{P}(S), \cap)$ su komutativni, dok $(\mathcal{P}(S), \setminus)$ to nije;
- Grupoid $\left(S^S, \circ\right)$ (u Primjeru 1, e)) i grupoid $(G, *)$ (u Primjeru 2) nije komutativan.

Definicija Neka je $(G, \circ)$ grupoid i $A \subseteq G$. Kažemo da je skup A **grupoid s obzirom na operaciju** $\circ$ **naslijeđenu iz** G ako za sve $a, b \in A$ vrijedi $a \circ b \in A$. Još kažemo da je A **zatvoren** s obzirom na operaciju $\circ$, odnosno da je $(A, \circ)$ **podgrupoid** od $(G, \circ)$.

Primjer 4

- Kako je $(\mathbb{Z}, +)$ grupoid i $\mathbb{N} \subset \mathbb{Z}$, tada $(\mathbb{N}, +)$ možemo smatrati grupoidom s obzirom na operaciju $+$ naslijeđenu iz $\mathbb{Z}$;
- 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 $\mathbb{R}$;

0.2 Polugrupa. Monoid

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

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

Napomena:

a) Iz zakona asocijacije slijedi

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

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

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

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

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

Primjer 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;

- Grupoidi (u Primjeru 1, d)) $(\mathcal{P}(S), \cup), (\mathcal{P}(S), \cap)$ su (komutativne) polugrupe dok $(\mathcal{P}(S), \setminus)$ nije polugrupa;

- Grupoid $\left(S^S, \circ\right)$ (u Primjeru 1, e)) je (nekomutativna) polugrupa;

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

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

Element e nazivamo **jedinica** ili **neutralni element** ili **jedinični element**.

Napomena: Ako je binarna operacija dodatno i komutativna onda govorimo o **komutativnom monoidu.**

Propozicija 1 Svaki monoid ima točno jedan jedinični element.

Primjer 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 (u Primjeru 1, d)) $(\mathcal{P}(S), \cup)$ ima neutralni element $\emptyset$, dok je u polugrupi $(\mathcal{P}(S), \cap)$ neutralni element S. Dakle, $(\mathcal{P}(S), \cup)$ i $(\mathcal{P}(S), \cap)$ su (komutativni) monoidi;

- Polugrupa $\left(S^S, \circ\right)$ (u Primjeru 1, e)) 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.

0.3 Grupa.

Definicija 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 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 $a \in G$;

iv) za svaki $a \in G$ postoji inverzni element a^{-1}, tj. element za kojeg vrijedi da je $aa^{-1} = a^{-1}a = e$;

Grupa $(G, \cdot)$ je **komutativna** ili **Abelova** ako dodatno vrijedi: $ab = ba$ za svaki izbor $a, b \in G$.

Propozicija 2 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 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 $a \in \mathbb{R} \setminus \{0\}$. 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?

- Komutativni monoidi $(\mathcal{P}(S), \cup)$ i $(\mathcal{P}(S), \cap)$ nisu grupe. Zašto?

- Nekomutativni monoid $\left(S^S, \circ\right)$ (u Primjeru 1, e)) 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

$$f \circ f^{-1} = f^{-1} \circ f = e.$$

Neka je

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

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

- Neka je $P = \{p, n\} = \{\text{par, nepar}\}$. Provjerite je li skup P, uz operacije prirodnog zbrajanja $+$ i množenja $\cdot$ koje su dane s

$+$	p	n
p	p	n
n	n	p

i

$\cdot$	p	n
p	p	p
n	p	n

,

grupa? $(P, +)$ je komutativa grupa, dok je $(P, \cdot)$ komutativni monoid ali nije grupa.

Usporedite strukture sa skupom $\{0,1\}$ na kojem je definirano Booleovo zbrajanje i množenje.

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**.

Primjer 7 (nastavak) Skup $\mathbb{Z}_m = \{0,1,...,m-1\}$, $m \in \mathbb{N}$, uz zbrajanje $\bmod m$, je Abelova grupa. Npr. za $m=6$, imamo $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$. Neutralni element je 0 i

$$3+5 = 5+3 = 2$$

$$2+4 = 0 \Longrightarrow -2 = 4$$

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

Propozicija 3 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

$$\begin{aligned} ac &= bc \iff a = b \\ ca &= cb \iff a = b \end{aligned}$$

Definicija 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 4 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 $(ab)^n = a^n b^n$;

Napomena: 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: $na := a + ... + a$;
- 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 3 za aditivnu grupu glasi:

Propozicija 4' U svakoj grupi $(G, +)$ vrijede sljedeća pravila za sve $a \in G$ i $m, n \in \mathbb{Z}$.

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

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

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

Definicija 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 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 5 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.

Napomena: Svojstvo i) iz Propozicije 5 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 $a - b \in H$;

Definicija Neka je grupa $(G, \cdot)$ i $a \in G$. Skup

$$\left\{a^k : k \in \mathbb{Z}\right\}$$

je podgrupa od G. Oznaka

$$\langle a \rangle = \left\{a^k : k \in \mathbb{Z}\right\}.$$

Podgrupa $\langle a \rangle$ je najmanja podgrupa od G koja sadrži a. Podgrupu $\langle a \rangle$ nazivamo **podgrupom generiranom elementom** a, a element a **generator**.

Definicija 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 je a reda n, onda je inverz elementa a^k jednak a^{n-k}, jer je

$$\begin{aligned} a^k a^{n-k} &= a^{k+n-k} = a^n = e \\ a^{n-k} a^k &= a^{n-k+k} = a^n = e. \end{aligned}$$

Definicija Za grupu $(G, \cdot)$ kažemo da je **ciklička grupa** ako postoji element $a \in G$ tako da je $G = \langle a \rangle$, tj. svaki $b \in G$ možemo napisati kao

$$b = a^k$$

za neki $k \in \mathbb{Z}$. Tada kažemo da je G **ciklička grupa generirana elementom** a.
Ako je a konačnog reda n, onda je G reda n, tj.

$$G = \left\{e, a, a^2 ..., a^{n-1}\right\} .$$

Ako je $a^k \neq e$ za sve $k \in \mathbb{N}$, onda je G beskonačna **ciklička grupa**

$$G = \left\{..., a^{-2}, a^{-1}, e, a, a^2 ...\right\} .$$

Napomena: Svaka ciklička grupa je komutativna.

Teorem (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 $|G|$.

Primjer 8 Neka je

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\} = \{\cos x + i \sin x \mid x \in \mathbb{R}\} = \left\{e^{ix} \mid x \in \mathbb{R}\right\},$$

tada je $\left(S^1, \cdot\right)$ grupa s obzirom na operaciju standardnog množenja $\cdot$ naslijeđenu iz $\mathbb{C} \setminus \{0\} := \mathbb{C}^*$, tj. $S^1 < \mathbb{C}^*$. Grupu $\left(S^1, \cdot\right)$ nazivamo **grupa kružnice**.

Za dani $n \in \mathbb{N}$ promatrajmo jednadžbu $z^n - 1 = 0$ i skup

$$K_n = \left\{z \in \mathbb{C} \mid z^n = 1\right\}.$$

Rješenja jednadžbe $z^n - 1 = 0$ ima točno n različitih: $\xi_1 = 1, ..., \xi_n$ i nazivamo ih $n-$**ti korijeni iz jedinice.** Dakle,

$$K_n = \{\xi_1, ..., \xi_n\}.$$

Očito je $(K_n, \cdot)$ grupa s obzirom na operaciju standardnog množenja $\cdot$ naslijeđenu iz $\mathbb{C}^*$, tj. $K_n < \mathbb{C}^*$ i $(K_n, \cdot)$ je grupa reda n.

Svi elementi od K_n se mogu dobiti kao potencije jednog od njih, tzv. **primitivnog n-tog korijena iz jedinice.** Dakle, K_n je ciklička reda n. Općenito,

$$K_n = \left\{ \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \mid k = 0, 1, ..., n-1 \right\},$$

a generator je svaki $\xi_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$, za koji je $nzd\,(k, n) = 1$.
Npr.

$$K_2 = \{1, \ -1\}, \quad K_3 = \left\{ 1, \ -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \ -\frac{1}{2} - \frac{\sqrt{3}}{2}i \right\}, ...$$

Očito je

$$K_n < S^1 < \mathbb{C}^* \text{ za svaki } n \in \mathbb{N},$$

(uz standardno množenje).

Neka je $(G, \cdot)$ komutativna grupa i $H \leq G$. Tada na 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 - 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:

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

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

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

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

Primjer 9 Neka je $(G,+)=(\mathbb{Z},+)$, $m\in\mathbb{N}$ i $m\mathbb{Z}=\{mk\,|k\in\mathbb{Z}\}$. Tada je $m\mathbb{Z}\leq\mathbb{Z}$.

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): $[0],[1],...,[m-1]$. Prema tome to je grupa reda m. Tu 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.**

0.4 Homomorfizmi i izomorfizmi grupa

Definicija 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 10

a) 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

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

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

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

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

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

c) 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 homomorfizam jer je

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

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

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 $(S^1, \cdot)$.

Propozicija 6 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 7 Neka je $f : G \to H$ homomorfizam grupa.

i) Skup

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

je (normalna) 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 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 8 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:

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

Propozicija 9

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.

Napomena: Dvije grupe G i H su izomorfne ako postoji barem jedan izomorfizam $f : G \to H$.

Propozicija 10 Relacija $\simeq$ izomorfnosti među grupama je relacija ekvivalencije.

Napomena: Grupe G i H koje su međusobno izomorfne s motrišta teorije grupa ne razlikujemo, tj. smatramo da su jednake. 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 11

a) 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;

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, po Propoziciji 9, ii), također izomorfizam grupa $(\mathbb{R}^+, \cdot)$ i $(\mathbb{R}, +)$.

c) 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 $(S^1, \cdot)$ dan sa $f : \mathbb{R} \longrightarrow S^1$, $f(x) = e^{2\pi x i}$ epimorfizam, ali nije monomorfizam. Naime, ovdje je

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

Ovaj epimorfizam nazivamo **namatanje pravca na kružnicu.**

d) 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 $\mathbb{Z}/m\mathbb{Z}$.

0.5 Prsten. Integralna domena.

Definicija 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 12:

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

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

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;

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 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 $\bmod m$, je komutativni prsten s jedinicom kojeg nazivamo **prsten cijelih brojeva modulo** m.

Propozicija 11 U svakom prstenu P vrijedi:

i) $0 \cdot a = a \cdot 0 = 0$ za svaki $a \in P$;

ii) $a\,(-b) = (-a)\,b = -ab$ za sve $a, b \in P$;

iii) $(-a)\,(-b) = ab$ za sve $a, b \in P$;

Iz Propozicije 11, i) slijedi:

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

Definicija

- Za element $a \neq 0$ u komutativnom prstenu P kažemo da je **djelitelj nule** ako postoji $b \neq 0$ takav da je $ab = 0$. Onda je i b djelitelj 0.
- Komutativan prsten s jedinicom 1 koji nema djelitelja nule nazivamo **integralnom domenom**.

Propozicija 12 Ako je D integralna domena i $a \neq 0$, onda vrijedi pravilo lijevog i desnog skraćivanja, tj.

$$ab = ac \implies b = c$$
$$ba = ca \implies b = c$$

Primjer 13:

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

b) Neka je S bilo koji neprazni skup i $F{=}\mathbb{R}^S = \{f \,|\, f : S \longrightarrow \mathbb{R}\}$. Uz množenje i zbrajanje definirano kao u Primjeru 11, b), F komutativni prsten s jedinicom ali nije integralna domena. Npr. neka je $A \subset S$ i $B = S \setminus A$. Definirajmo

$$f(x) = \begin{cases} 0, & x \in A \\ 1, & x \in B \end{cases} \quad \text{i} \quad g(x) = \begin{cases} 1, & x \in A \\ 0, & x \in B \end{cases}.$$

Očito je $f \neq n$ i $g \neq n$ ali vrijedi

$$(f \cdot g)(x) := f(x) \cdot g(x) = 0 = n(x) \text{ za sve } x \in S,$$

tj. $f \cdot g = n$, pa su f i g djelitelji nule.

c) Skup $\mathbb{Z}_m = \{0, 1, ..., m-1\}$, $m \in \mathbb{N}$, uz zbrajanje i množenje $\bmod m$, je integralna domena ako i samo ako je m prost broj. Inače, prsten ima djelitelje nule.
Npr. za $m = 6$, u prstenu $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ elementi 2, 3 i 4 su djelitelji nule jer je

$$2 \cdot 3 = 0 \text{ i } 3 \cdot 4 = 0.$$

Definicija 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 Integralna domena 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:

polja $\subset$ integralne domene $\subset$ komutativni prstenovi $\subset$ prstenovi

Primjer 14:

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 (integralana domena) $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ 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:

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

0.6 Potprsteni i ideali.

Definicija 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 podprstena**: potprsten $\{0\}$ i potprsten P;

Propozicija 13 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 13, 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 15

- 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 (poddomena) 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 $\mathbb{Z}$.

Definicija Neka je $(P, +, \cdot)$ komutativni prsten. Potprsten A prstena P je **ideal**[1] od P ako vrijedi: $AP \subseteq A$, tj. ako je ispunjeno

$$ax \in A \text{ za svaki } a \in A \text{ i za svaki } x \in P.$$

Napomena

- U komutativnom prstenu P s jedinicom za ideal A vrijedi $1 \in A \Longrightarrow A = P$.

- Pravi ideal ne sadrži invertibilni element od P.

- U polju nema pravih ideala.

[1] Ideal se može definirati i u prstenu koji nije komutativan.

Primjer 16 $(\mathbb{Z}, +, \cdot)$ je komutativan prsten s jednicom. Tada je $m\mathbb{Z} = \{mk \,|k \in \mathbb{Z}\}$ potprsten od $\mathbb{Z}$ za svaki $m \in \mathbb{N}$. Kako je

$$ak \in m\mathbb{Z} \text{ za svaki } a \in m\mathbb{Z} \text{ i za svaki } k \in \mathbb{Z},$$

onda je $m\mathbb{Z}$ ideal od $\mathbb{Z}$.

Neka je $A \subset P$ je potprsten prstena $(P, +, \cdot)$. Tada je A podgrupa komutativne aditivne grupe $(P, +)$, pa je dobro definirana kvocijentna grupa

$$P/A = \{x + A \,|\, x \in P\}$$

i ona je komutativna.

Želimo P/A organizirati u prsten. Pretpostavimo dodatno da je A ideal od P. Tada definiramo množenje klasa sa

$$(x + A) \cdot (y + A) := xy + A.$$

Uz ovako definirano množenje P/A je komutativni prsten kojeg nazivamo **kvocijentni prsten prstena** P **po idealu** A. Ako je P prsten s jedinicom 1, tada je i P/A prsten s jedinicom a to je klasa $1 + A$.

Primjer 17 $(\mathbb{Z}, +, \cdot)$ je komutativan prsten s jednicom. Tada je $m\mathbb{Z} = \{mk \,|k \in \mathbb{Z}\}$ ideal od $\mathbb{Z}$ za svaki $m \in \mathbb{N}$, pa je

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

kvocijentni prsten prstena $\mathbb{Z}$ po idealu $m\mathbb{Z}$. Binarne operacije zbrajanja i množenja dane su sa

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

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

a jedinica je $1 + m\mathbb{Z}$.

0.7 Homomorfizmi i izomorfizmi prstenova

Definicija 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

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

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

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

Definicija 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 14 Relacija $\simeq$ izomorfnosti među prstenovima je relacija ekvivalencije.

Propozicija 15 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;

ii) Ako je P polje, onda je i S polje.

Propozicija 17 Neka je $f : P \to S$ homomorfizam prstenova.

i) Skup

$$J(f) = Ker(f) := \{x \in P : f(x) = 0_S\}$$

je ideal prstena P 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 potprsten prstena S.

Neka je $A \subset P$ je ideal prstena $(P, +, \cdot)$ i $P/A = \{x + A \mid x \in P\}$ kvocijentni prsten prstena P po idealu A. Tada je prirodna projekcija

$$p : P \longrightarrow P/A, \;\; p(a) = [a] = a + A$$

homomorfizam prstenova. Štoviše to je epimorfizam s jezgrom $Ker(p) = A$.

Primjer 17 $(\mathbb{Z}, +, \cdot)$ je komutativan prsten s jednicom i

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

kvocijentni prsten prstena $\mathbb{Z}$ po idealu $m\mathbb{Z}$. Tada je prirodna projekcija

$$p : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}, \;\; p(a) = a + m\mathbb{Z}$$

epimorfizam s jezgrom $Ker(p) = m\mathbb{Z}$.

Propozicija 18 Neka je $f : P \to S$ homomorfizam polja. Tada je

i) $f(1_P) = 1_S$;

ii) $f\left(a^{-1}\right) = f(a)^{-1}$ za svaki $a \in P, a \neq 0$.

Primjer 18 $(\mathbb{Z}_m, +, \cdot)$ 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

$$\begin{aligned}
(2 + 5\mathbb{Z}) \cdot (3 + 5\mathbb{Z}) &= (3 + 5\mathbb{Z}) \cdot (2 + 5\mathbb{Z}) = 6 + 5\mathbb{Z} = 1 + 5\mathbb{Z} \\
&\Longrightarrow (3 + 5\mathbb{Z})^{-1} = 2 + 5\mathbb{Z} \ \text{ i } \ (2 + 5\mathbb{Z})^{-1} = 3 + 5\mathbb{Z} \\
(1 + 5\mathbb{Z}) \cdot (1 + 5\mathbb{Z}) &= 1 + 5\mathbb{Z} \Longrightarrow (1 + 5\mathbb{Z})^{-1} = 1 + 5\mathbb{Z} \\
(4 + 5\mathbb{Z}) \cdot (4 + 5\mathbb{Z}) &= 16 + 5\mathbb{Z} = 1 + 5\mathbb{Z} \Longrightarrow (4 + 5\mathbb{Z})^{-1} = 4 + 5\mathbb{Z}
\end{aligned}$$

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.

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

0.8 Vektorski prostori

Osnovni model algebarske strukture koju nazivamo vektorski ili linerani prostor je V^3- skup klasa ekvivalencije orijentiranih dužina koje znamo zbrajati (unutarnje množenje - binarna operacija) i množiti s realnim brojem (vanjsko množenje) s tim da te operacije zadovoljavaju neka svojstva (aksiome).

Definicija Neka je $(V, +)$ Abelova grupa i $(F, +, \cdot)$ polje. Nadalje, neka je

$$h : F \times V \to V$$

preslikavanje kojeg nazivamo **vanjsko** ili **hibridno množenje**, i kratko označujemo sa $h(\alpha, a) = \alpha a$, koje ima ova svojstva:

i) **kvaziasocijativnost**, tj.

$$\alpha(\beta a) = (\alpha\beta) a, \quad \forall \alpha, \beta \in F, \ \forall a \in V;$$

ii) **posjedovanje jedinice**, tj.

$$1 \cdot a = a, \quad 1 \in F \ \text{ i } \ \forall a \in V;$$

iii) **distributivnost u odnosu na zbrajanje u** F, tj.

$$(\alpha + \beta)\, a = \alpha a + \beta a, \quad \forall \alpha, \beta \in F,\ \forall a \in V;$$

iv) **distributivnost u odnosu na zbrajanje u** V, tj.

$$\alpha\,(a + b) = \alpha a + \alpha b, \quad \forall \alpha \in F,\ \forall a, b \in V.$$

Tada uređenu trojku (V, F, h) nazivamo **linearni** ili **vektorski prostor nad poljem** F.

Napomena:

- Elemente od V nazivamo **vektorima**, posebno neutralni element (nulu) grupe $(V, +)$ nazivamo **nulvektor** i označavamo s Θ;

- Elemente od F nazivamo **skalarima**, a s 0 i 1 označavamo nulu i jedinicu polja $(F, +, \cdot)$, redom;

- Ako je $F = \mathbb{R}$ onda govorimo o **realnom vektorskom prostoru**, a ako je $F = \mathbb{C}$ onda govorimo o **kompleksnom vektorskom prostoru**;

Propozicija 19 U svakom vektorskom prostoru vrijedi:

a) $0a = \Theta$ za svaki $a \in V$.

b) $\alpha\Theta = \Theta$ za svaki $\alpha \in F$.

c) $\alpha a = \Theta$ ako i samo ako je $a = \Theta$ ili $\alpha = 0$.

Dokaz:

Primjer 19:

a) Skupovi V^1, V^2, V^3, $V^1(0)$, $V^2(0)$, $V^3(0)$ uz standardno zbrajanje vektora (radij vektora) i množenje vektora (radij vektora) sa skalarom vektorski prostori;

b) Skup $\mathbb{R}^n = \{(\alpha_1, \alpha_2, ..., \alpha_n) \,|\alpha_i \in \mathbb{R}\}$ uz standardno koordinatno zbrajanje i množenje s elementima iz polja $\mathbb{R}$

$$(\alpha_1, \alpha_2, ..., \alpha_n) + (\alpha_1', \alpha_2', ..., \alpha_n') := (\alpha_1 + \alpha_1', \alpha_2 + \alpha_2', ..., \alpha_n + \alpha_n')$$

$$\alpha(\alpha_1, \alpha_2, ..., \alpha_n) := (\alpha\alpha_1, \alpha\alpha_2, ..., \alpha\alpha_n)$$

za sve $(\alpha_1, \alpha_2, ..., \alpha_n)$, $(\alpha'_1, \alpha'_2, ..., \alpha'_n) \in \mathbb{R}^n$ i $\alpha \in \mathbb{R}$, vektorski prostor nad $\mathbb{R}$ kojeg nazivamo $n-$**dimenzionalni koordinatni prostor**.

Općenito, ako je F bilo koje polje (npr. $F = \mathbb{Q}$, $\mathbb{R}$ ili $\mathbb{C}$), onda je $F^n = \{(\alpha_1, \alpha_2, ..., \alpha_n) \,|\alpha_i \in F\}$ uz analogno definirane opercije zbrajanje vektora i množenje vektora sa skalarom vektorski prostor nad F. Specijalno, za $n = 1$, imamo da je svako polje vektorski prostor nad samim sobom (i nad svakim svojim potpoljem).

c) Neka je

$$P_n = \left\{p(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1x + a_0 \,|a_i \in \mathbb{R}\right\}$$

skup svih polinoma u jednoj varijabli x s realnim koeficijentima stupnja najviše $n-1$. Onda je P_n uz standardno zbrajanje i množenje s elementima iz polja $\mathbb{R}$

$$p(x) + q(x) =$$

$$= \left(a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1x + a_0\right) + \left(a'_{n-1}x^{n-1} + a'_{n-2}x^{n-2} + ... + a'_1x + a'_0\right)$$

$$:= \left(a_{n-1} + a'_{n-1}\right)x^{n-1} + \left(a_{n-2} + a'_{n-2}\right)x^{n-2} + ... + (a_1 + a'_1)x + (a_0 + a'_0)$$

$$\begin{aligned} \alpha p(x) &= \alpha\left(a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\ldots+a_1x+a_0\right) \\ &= \left(\alpha a_{n-1}\right)x^{n-1}+\left(\alpha a_{n-2}\right)x^{n-2}+\ldots+\left(\alpha a_1\right)x+\alpha a_0 \end{aligned}$$

za sve $p(x), q(x) \in P_n$ i $\alpha \in \mathbb{R}$, vektorski prostor. Isto vrijedi i za

$$P = \bigcup_{n=1}^{\infty} P_n = \left\{p(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0 \mid n \in \mathbb{N},\ a_i \in \mathbb{R}\right\}.$$

Analogno, imamo i za skup polinoma nad bilo kojim poljem F.

d) Neka je S bilo koji neprazni skup i F proizvoljno polje (npr. $\mathbb{R}$), tada je

$$F^S = \{f \mid f : S \longrightarrow F\}$$

tzv. **funkcijski vektorski prostor nad** F uz operacije

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

za sve $f, g \in F^S$ i $\alpha \in F$. Specijalno, $\mathbb{R}^{\mathbb{R}}$ je realni vektorski prostor.

0.9 Linearna zavisnost i nezavisnost

Definicija Neka je V vektorski prostor nad poljem F, $a_1, a_2, ..., a_n \in V$ i $\alpha_1, \alpha_2, ..., \alpha_n \in F$ proizvoljni vektori, odnosno skalari. Tada vektor

$$\alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_n a_n$$

nazivamo **linearna kombinacija vektora** $a_1, a_2, ..., a_n$ **s koeficijentima** $\alpha_1, \alpha_2, ..., \alpha_n$.

Definicija Neka je V vektorski prostor nad poljem F. Za konačan skup vektora $\{a_1, a_2, ..., a_n\} \subseteq V$ kažemo da je **linearno nezavisan** ako iz

$$\alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_n a_n = \Theta \tag{1}$$

slijedi $\alpha_1 = ... = \alpha_n = 0$. U protivnom kažemo da je skup vektora $\{a_1, a_2, ..., a_n\}$ **linearno zavisan.**

Napomena Iz gornje definicije slijedi da je skup vektora $\{a_1, a_2, ..., a_n\} \subset V$ linearno zavisan ako postoje skalari $\alpha_1, \alpha_2, ..., \alpha_n \in F$, od kojih je barem jedan različit od 0, tako da vrijedi (1).

Definicija Neka je V vektorski prostor nad poljem F i $S \subset V$ bilo koji skup vektora. Za S kažemo da je **linearno nezavisan** ako je svaki njegov konačan podskup linerano nezavisan. Za S kažemo da je **linearno zavisan** ako postoji barem jedan njegov konačan neprazan podskup koji je linearno zavisan. Smatramo da je prazan skup $\emptyset \subset V$ linearno nezavisan.

Napomena Iz gornjih definicijh slijedi da je linearna (ne)zavisnost svojstvo skupa vektora a ne pojedinog vektora.

Primjer 20

a) Neka je F polje. Vektori $e_1 = (1, 0, 0, ..., 0)$, $e_2 = (0, 1, 0..., 0)$, ..., $e_n = (0, 0, ...0, 1) \in F^n$ tvore linearno zavisan skup vektora vektorskog prostora F^n. Specijalno, za $F = \mathbb{R}$ i $n = 3$, nađite neki linearno zavisan skup vektora iz $\mathbb{R}^3$.

b) Neka je $P_n = \left\{ p(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1x + a_0 \,|a_i \in F \right\}$, gdje je F neko polje. Tada je skup

$$\left\{1, x, x^2, ..., x^k\right\},\ k \leq n-1$$

linearno zavisan skup vektora vektorskog prostora P_n. Isto tako skup

$$\left\{1, x, x^2, ..., x^k, ...\right\} \subset P,$$

gdje je $P = \bigcup_{n=1}^{\infty} P_n$, je (beskonačni) linearno nezavisan skup vektora (polinoma) iz P.

Specijalno, za $F = \mathbb{R}$, nađite neki linearno zavisan skup vektora iz P.

Propozicija 20 U svakom vektorskom prostoru V vrijedi:

a) Jednočlan podskup $\{a\} \subset V$ je linearno zavisan ako i samo ako je $a = \Theta$.

b) Podskup linearno nezavisnog skupa vektora je linearno nezavisan. Nadskup linearno zavisnog skupa vektora je linearno zavisan.

Dokaz:

Posljedica 2 Svaki skup vektora koji sadrži nulvektor je linearno zavisan.

Dokaz:

Propozicija 21 Skup vektora $S = \{a_1, a_2, ..., a_k\} \subset V$, $k > 1$, je linearno zavisan ako i samo ako se barem jedan od vektora iz S može prikazati kao linearna kombinacija preostalih vektora iz S.

Dokaz:

0.10 Skup izvodnica. Baza i dimenzija.

Definicija Neka je V vektorski prostor nad poljem F i $G \subset V$ njegov podskup. Kažemo da je G **skup izvodnica** ili **skup generatora** od V ako za svaki $a \in V$ postoji $k \in \mathbb{N}$ i vektori $a_1, a_2, ..., a_k \in G$ takvi da je

$$a = \alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_k a_k$$

za neke $\alpha_1, ..., \alpha_k \in F$. Kažemo da skup izvodnica **razapinje** ili **generira** vektorski prostor V.

Definicija Za vektorski prostor V kažemo da je **konačnodimenzionalan** ako sadrži barem jedan konačan skup izvodnica. U protivnom kažemo da je **beskonačnodimenzionalan.**

Mi ćemo se baviti samo konačnodimenzionalnim vektorskim prostorima.

Definicija Za podskup $B \subset V$ vektorskog prostora V kažemo da je **baza** od V ako je:

1) B skup izvodnica;

2) B je linearno nezavisan skup.

Primjer 21

a) Svaki skup od tri nekomplanarna vektora iz V^3 je baza od V^3.

b) Vektori $e_1 = (1, 0, 0, ..., 0)\,,\ e_2 = (0, 1, 0..., 0)\,, ..., e_n = (0, 0, ...0, 1) \in F^n$ su baza vektorskog prostora F^n.

c) $\{1, i\}$ je baza od vektorskog prostora $\mathbb{C}$ nad (pot)poljem $\mathbb{R}$.

d) Tada je skup $\left\{1, x, x^2, ..., x^{n-1}\right\}$je baza vektorskog prostora P_n. Isto tako skup

$$\left\{1, x, x^2, ..., x^k, ...\right\},$$

je baza vektorskog prostora $P = \bigcup_{n=1}^{\infty} P_n$.

Pitanje: Postoji li baza konačnodimenzionalnog vektorskog prostora?

Za odgovor na ovo pitanje ključne su sljedeće tvrdnje:

Lema 1 Neka je $G = \{a_1, ..., a_k, ..., a_n\}$ skup izvodnica vektorskog prostora V. Ako se $a_k \in G$ može prikazati kao linearna kombinacija preostalih vektora iz G onda je i $G \setminus \{a_k\}$ također skup izvodnica.

Dokaz:

Teorem 1 Neka je $G = \{a_1, ..., a_n\} \subset V$ skup izvodnica vektorskog prostora V. Tada G sadrži podskup koji je baza od V.

Dokaz:

Posljedica 3 Svaki netrivijalni (kon. dim.) vektorski prostor ima bazu.

Teorem 2 Svake dvije baze danog vektorskog prostora su ekvipotentne (jednakobrojne).

Dokaz: Bez dokaza.

Definicija (Algebarska) dimenzija netrivijalnog vektorskog prostora V nad F, u oznaci $\dim V$ ili $\dim_F V$ je kardinalni broj neke baze prostora V. Dimenzija trivijalnog vektorskog prostora $\{\Theta\}$ je po dogovoru 0.

Primjer 22

- $\dim V^3 = 3, \quad \dim \mathbb{R}^2 = 2, \quad \dim \mathbb{R}^n = \dim F^n = 2, \quad \dim_{\mathbb{R}} \mathbb{C} = 2, \quad \dim_{\mathbb{C}} \mathbb{C} = 1,$ $\dim_F F = 1, \dim P_n = n, \quad \dim P = \aleph_0$ (alef nula).

Teorem 3 Neka je $S = \{a_1, ..., a_k\} \subset V$ linearno nezavisan skup vektora vektorskog prostora V. Tada je S podskup neke baze od V.

Dokaz (skica):

Napomena: Iz dokaza slijedi da proširenje skupa S do baze nije jednoznačno.

Posljedica 4 Neka je V $n-$dimenzionalan vektorski prostor. Tada je svaki linearno nezavisni podskup od n vektora iz V baza prostora V.

Dokaz:

Posljedica 5 Neka je V $n-$dimenzionalan vektorski prostor. Tada je svaki podskup od V koji sadrži više od n vektora linearno zavisan.

Dokaz:

Napomena: Dakle, maksimalan broj linearno nezavisnih vektora u nekom vektorskom prostoru jedanak je dimenziji tog prostora.

Još jedno svojstvo baze:

Teorem 4 Prikaz svakog vektora iz vektorskog prostora V kao linearne kombinacije vektora neke baze od V je jedinstven.

Dokaz:

0.11 Potprostor. Linearna ljuska.

Definicija Kažemo da je podskup $L \subset V$ vektorskog prostora V njegov **potprostor** ako je li i sam vektorski prostor s obzirom na operacije zbrajanja i množenja vektora sa sklararom naslijeđene iz V. Pišemo $L < V$.

Napomena: Svaki vektorski prostori V ima dva **trivijalna potprostora**: $\{\Theta\}$ i V. Ostale nazivamo **pravim** potprostorima.

Propozicija 22 Neprazan podskup $L \subset V$ vektorskog prostora V njegov potprostor ako i smo ako vrijedi:

1) $a + b \in L$ za sve $a, b \in L$;

2) $\alpha a \in L$ za sve $\alpha \in F$ i $a \in L$.

Posljedica 6 Neprazan podskup $L \subset V$ vektorskog prostora V njegov potprostor ako i smo ako vrijedi:

$$\alpha a + \beta b \in L \text{ za sve } \alpha, \beta \in F \text{ i } a, b \in L.$$

Primjer 23

a) $V^2 \subset V^3$ je potprostor od V^3;

b) Uz odgovarajući dogovor imamo $\mathbb{R} \subset \mathbb{R}^2 \subset ... \subset \mathbb{R}^n \subset ... \subset \mathbb{R}^\infty$, i svaki od ovih vektorskih prostora je potprostor sljedećeg;

c) Imamo $P_1 \subset P_2 \subset ... \subset P_n \subset ... \subset P$ (polinomi!), i svaki od ovih vektorskih prostora je potprostor sljedećeg.

Teorem 5 Ako je $L \subset V$ potprostor vektorskog prostora V, onda je $\dim L \leq \dim V$.

Dokaz (skica):

Definicija Neka je $S \subset V$ neprazan podskup vektorskog prostora V. Definiramo skup $[S]$ kao skup svih linearnih kombinacijh vektora iz S. Ako je $S = \emptyset$ definiramo $[S] = [\emptyset] = \{\Theta\}$.

Lako se pokaže da je $[S]$ potprostor od V za svaki podkup $S \subset V$. Ovaj vektorski prostor se naziva **linearna ljuska** ili **linearni omotač** skupa S i za njega je očito S skup izvodnica, a $[S]$ je najmanji potprostor vektorskog prostora V koji sadrži S.

0.12 Presjek i suma potprostora

Napomena: Presjek dva potprostora nikada nije prazan, on barem sadrži nulvektor Θ.

Propozicija 23 Neka su L i M potprostori vektorskog prostora V. Tada je i $L \cap M$ potprostor od V i to je najveći potprostor koji je sadržan i u L i u M.

Dokaz

Napomena: Slično se pokaže da je presjek bilo koje familije potprostora od V potprostor od V.

Unija dvaju vektorskih potprostora od V općenito nije potprostor od V.

Primjer: $\left[\left\{\vec{i}\right\}\right] \cup \left[\left\{\vec{j}\right\}\right] \not\leq V^3$.

Izmino, ako je $L \subset M$ te L i M potprostori od V, tada je $L \cup M = M < V$.

Zanima nas koji je to najmanji potprostori od V koji sadrži potprostore L i M.

Definicija Neka su L i M potprostori vektorskog prostora V. Tada sumu tih potprostora definiramo kao

$$L + M := [L \cup M]$$

i nazivamo je **suma potprostora** L i M.

Primjer 23

$$\left[\left\{\vec{i},\vec{j}\right\}\right]+\left[\left\{\vec{k}\right\}\right]=V^3 \quad \text{ili} \quad \left[\left\{\vec{i},\vec{j}\right\}\right]+\left[\left\{\vec{j},\vec{k}\right\}\right]=V^3$$

Općenito: $+_\alpha L_\alpha := [\cup_\alpha L]$

Propozicija 24 Neka su L i M potprostori vektorskog prostora V. Tada je

$$L+M=\{a+b : a\in L \text{ i } b\in M\}.$$

Dokaz

Teorem 6 Neka su L i M potprostori vektorskog prostora V. Tada je

$$\dim(L+M)=\dim(L)+\dim(M)-\dim(L\cap M).$$

Dokaz (skica)

Primjer 24

$$\left[\left\{\vec{i},\vec{j}\right\}\right]+\left[\left\{\vec{j},\vec{k}\right\}\right]=V^3$$

$$\Longrightarrow \quad \dim\left(\left[\left\{\vec{i},\vec{j}\right\}\right]+\left[\left\{\vec{j},\vec{k}\right\}\right]\right)$$

$$=\dim\left(\left[\left\{\vec{i},\vec{j}\right\}\right])+\dim(\left[\left\{\vec{j},\vec{k}\right\}\right])-\dim(\left[\left\{\vec{j}\right\}\right])=2+2-1=3=\dim\left(V^3\right)$$

Definicija Neka su L i M potprostori vektorskog prostora V. Za sumu $L+M$ potprostora L i M kažemo da je **direktna suma** ako je $L\cap M=\{\Theta\}$. Oznaka $L\oplus M$.

Propozicija 25 Neka su L i M potprostori vektorskog prostora V. Suma $L+M$ je direktna ako i samo ako svaki vektor $x\in L+M$ ima jedinstven prikaz u obliku

$$x=a+b,\ \ a\in L,\ \ b\in M.$$

Dokaz

Propozicija 26 Neka su L i M potprostori vektorskog prostora V. Suma $L + M$ je direktna ako i samo vrijedi

$$\dim(L + M) = \dim(L) + \dim(M).$$

Dokaz Direktno iz Teorema 6.

Posljedica 7 Ako je suma $L + M$ je direktna, onda je unija baza od L i M jedna baza od $L + M = L \oplus M$.

Dokaz Iz skice dokaza Teorema 6.

Neka su L i M potprostori vektorskog prostora V. Ako je $L \oplus M = V$, onda L i M nazivamo **direktnim sumandima** prostora V i kažemo da se prostor V može rastaviti u direktnu sumu potprostora L i M.

Teorem 7 Neka je $L < V$ bilo koji potprostor vektorskog prostora V. Tada postoji potprostor $M < V$ takav da je $V = L \oplus M$.

Dokaz

Potprostor M iz prethodnog teorema nazivamo **direktnim komplementom** potprostora L. Iz konstrukcije je jasno da on nije jednoznačno određen. Npr.

$$V^3 = \left[\left\{\vec{i}, \vec{j}\right\}\right] \oplus \left[\left\{\vec{k}\right\}\right] \quad \text{i} \quad V^3 = \left[\left\{\vec{i}, \vec{j}\right\}\right] \oplus \left[\left\{\vec{i} + \vec{k}\right\}\right]$$

0.13 Kvocijentni prostor

Neka je V vektorski prostor nad F i $L < V$ potprostor od V. Tada je $(L, +)$ podgrupa Abelove (aditivne) grupe $(V, +)$, pa je dobro definirana kvocijentna grupa

$$V/L = \{a + L \mid a \in V\}$$

i ona je komutativna. Prisjetimo se, u ovoj grupi binarana operacija je dana sa

$$(a + L) + (b + L) = (a + b) + L$$

i neutralni elemet je $\Theta + L = L$. Ako još definiramo $h : F \times V/L \to V/L$ kao

$$h(\alpha, a + L) = \alpha(a + L) = \alpha a + L, \quad \text{za sve } \alpha \in F,$$

tada se pokazuje da je V/L vektorski prostor nad F i taj vektorski prostor nazivamo **kvocijentni prostor** prostora V po potprostoru L.

Elemente od V/L nazivamo **linearnim mnogostrukostima** u V.

Npr. $a+L$ je linearna mnogostrukost generirana elementom a "paralelana" potprostoru L. Još kažemo da je ta mnogostrukost dobivena "translacijom potprostora L za vektor a". Motivacija potječe iz $V^3 : V^3$ je disjunktna unija mnogostrukosti paralelnih prostoru L.

Teorem 8 Neka je V konačnodimenzionalni vektorski prostor nad F i neka je $L < V$ njegov potprostor. Tada vrijedi

$$\dim(V/L) = \dim(V) - \dim(L).$$

Dokaz

Dimenziju prostora V/L nazivamo **kodimenzijom** potprostora L u prostoru V.

0.13 Algebre

Definicija Neka je $(V, +)$ vektorski prostor nad poljem F. Neka je na V definirano i drugo unutrašnje množenje

$$\cdot \ : V \times V \to V$$

koje ima ova svojstva:

i) **kvaziasocijativnost**, tj.

$$(\alpha a)\, b = \alpha\, (ab) = a\, (\alpha b)\,, \quad \forall \alpha \in F,\ \forall a, b \in V;$$

ii) **distributivnost**

$$\begin{aligned} a\,(b+c) &= ab + ac, \quad \forall a, b, c \in V; \\ (a+b)\,c &= ac + bc, \quad \forall a, b, c \in V \end{aligned}$$

Tada V nazivamo **algebrom** nad poljem F.

Primjer

1. V^3 - **klasična algebra vektora** (uz vektorski produkt vektora). To je algebra koja je antikomutativna, neasocijativna i nema jedinicu.

2. $Hom_F V$ - **linearna algebra** (linearni operatori na vektorskom prostoru V). To je algebra koja je nekomutativna, asocijativna i ima jedinicu.