

Algebra 1

Vid Drobnič

Kazalo

1	Vektorji v trirazsežnem prostoru	3
1.1	Operacije z vektorji	4
1.2	Linearna neodvisnost	5
1.3	Skalarni produkt	9
1.4	Vektorski produkt	10
1.5	Mešani produkt	13
1.6	Dvojni vektorski produkt	14
2	Analitična geomterija v \mathbb{R}^3	14
2.1	Premica	14
2.2	Ravnina	15
2.3	Razdalja med mimobežnima premicama	17
3	Osnovne algebrske strukture	18
3.1	Preslikave in relacije	18
3.2	Operacije	22
3.3	Grupe	23
3.4	Abelove grupe	33
3.5	Homomorfizmi	37
3.6	Kolobar	40
4	Vektorski prostori	42
4.1	Nekaj osnovnih lastnosti vektorskih prostorov	44
4.2	Vektorski podprostor	44

4.3	Linearna ogrinjača	46
-----	------------------------------	----

1 Vektorji v trirazsežnem prostoru

\mathcal{P} - prostor

$T \in \mathcal{P}$ - točka

$A, B \in \mathcal{P}$

\overrightarrow{AB} - usmerjena daljica

FORMALNO: $\overrightarrow{AB} = (A, B) \in \mathcal{P} \times \mathcal{P}$ (urejen par)

Ekvivalentnost usmerjenih daljic:

$\overrightarrow{CD} \sim \overrightarrow{AB}$, kadar je \overrightarrow{AB} z vzporednim premikom mogoče premakniti v \overrightarrow{CD} .

- $|AB| = |CD|$ (dolžini daljic sta enaki)
- imata isto smer (če potegnemo premico čez izhodišča daljic (AC), morata biti točki B in D na istem "bregu" te premice)
- $AB \parallel CD$ (premici skozi točke sta vzporedni)

$$\overrightarrow{CD} \sim \overrightarrow{AB} \iff \overrightarrow{AB} \sim \overrightarrow{CD}$$

DEF: Vektor \vec{AB} je množica $\vec{AB} = \{\overrightarrow{XY} : \overrightarrow{XY} \sim \overrightarrow{AB}\}$ (usmerjene daljice ekvivalentne daljici \overrightarrow{AB})

- ničelni vektor: $\vec{AA} = \vec{0}$
- nasprotni vektor vektorja \vec{AB} je \vec{BA} ($\vec{BA} = -\vec{AB}$)

Dodatna oznaka: $\vec{a}, -\vec{a}$ nasprotni vektor

$V = \{\vec{v} : \vec{v} \text{ vektor}\}$ - vektorski prostor.

$O \in \mathcal{P}$; O fiksiramo (izberemo si neko točko v prostoru, ki jo fiksiramo)

$$f : \mathcal{P} \rightarrow V$$

$$f(T) = \vec{OT}$$

f je bijekcija (vsaki točki priredi natanko en vektor).

$$\vec{a} = \vec{OT}$$

1.1 Operacije z vektorji

Seštevanje:

$$\begin{aligned}\vec{a}, \vec{b} &\in V \\ \vec{a} &= \vec{AB}, \vec{b} = \vec{BC} \\ \vec{a} + \vec{b} &= \vec{AC} \\ \vec{AB} + \vec{BC} &= \vec{AC}\end{aligned}$$

LASTNOSTI:¹

- (1) $(\vec{a} + \vec{b}) + \vec{c} = \vec{a} + (\vec{b} + \vec{c})$ asociativnost
- (2) $\vec{a} + \vec{b} = \vec{b} + \vec{a}$ komutativnost
- (3) $\vec{a} + \vec{0} = \vec{a}$
- (4) $\vec{a} + (-\vec{a}) = \vec{0}$

Za lastnosti od (1) do (4) $(V, +)$ **Abelova grupa**.

Razliko dveh vektorjev definiramo tako:

$$\vec{a} - \vec{b} := \vec{a} + (-\vec{b})$$

Množenje s skalarjem

Skalar je realno število.

$$\vec{a}, \alpha \in \mathbb{R}$$

$\alpha\vec{a}$ je vektor.

- ima isto smer kot \vec{a} za $\alpha > 0$
- ima nasprotno smer kot \vec{a} za $\alpha < 0$
- $|\alpha\vec{a}| = |\alpha||\vec{a}|$

¹Dokaz lastnosti (1) in (2) s skico.

$$\vec{a} = \vec{OA} \neq \vec{0}$$

$$\alpha\vec{a} = \vec{OT}, O, A, T \text{ so na isti premici}$$

S tem uvedemo koordinatni sistem na premici OA .

LASTNOSTI:

$$(5) \quad \alpha(\beta\vec{a}) = (\alpha\beta)\vec{a}$$

$$(6) \quad (\alpha + \beta)\vec{a} = \alpha\vec{a} + \beta\vec{a}$$

$$(7) \quad \alpha(\vec{a} + \vec{b}) = \alpha\vec{a} + \alpha\vec{b}$$

$$(8) \quad 1 \cdot \vec{a} = \vec{a}$$

$V, +$ in množenje s skalaji je **vektorski prostor**: veljajo lastnosti od (1) do (8).

1.2 Linearna neodvisnost

$$\vec{a}, \vec{b} \in V$$

\vec{a}, \vec{b} sta linearno odvisna kadar je:

bodisi $\vec{b} = \alpha\vec{a}$ za ustrezen $\alpha \in \mathbb{R}$,

bodisi $\vec{a} = \beta\vec{b}$ za ustrezen $\beta \in \mathbb{R}$.

V nasprotnem primeru sta \vec{a} in \vec{b} linearno neodvisna.

$$\vec{a} = \vec{OA}, \vec{b} = \vec{OB}$$

1. \vec{OA} in \vec{OB} sta linearno odvisna $\Leftrightarrow O, A, B$ kolinearne (ležijo na isti premici).

2. \vec{a}, \vec{b} sta linearno neodvisna $\Leftrightarrow (\alpha\vec{a} + \beta\vec{b} = \vec{0} \Rightarrow \alpha = \beta = 0)$

Privzamemo da sta \vec{a}, \vec{b} linearno neodvisna:

$$\{T : \vec{OT} = \alpha\vec{a} + \beta\vec{b}, \alpha, \beta \in \mathbb{R}\} = \mathcal{R}$$

$\alpha\vec{a} + \beta\vec{b}$ - linearna kombinacija

\mathcal{R} - ravnina določena z O, A, B (z vektorji \vec{a}, \vec{b}) in točko O .

$$\vec{r} = \vec{OT}, T \in \mathcal{R}$$

$$\exists \alpha, \beta \in \mathbb{R} : \vec{r} = \alpha\vec{a} + \beta\vec{b}$$

Pri tem sta α in β enolično določena skalarja.

V \mathcal{R} smo z vektorjema \vec{a}, \vec{b} vpeljali koordinatni sistem.

$\vec{a}, \vec{b}, \vec{c} \in V$ so linearno odvisni, kadar je vsaj eden od njih linearna kombinacija drugih dveh.

npr: $\vec{c} = \alpha\vec{a} + \beta\vec{b}$

V nasprotnem primeru so $\vec{a}, \vec{b}, \vec{c}$ linearno neodvisni.

1. $\vec{a} = \vec{OA}, \vec{b} = \vec{OB}, \vec{c} = \vec{OC}$ so linearno odvisni $\Leftrightarrow O, A, B, C$ koplanarne (ležijo na isti ravnini)

2. $\vec{a}, \vec{b}, \vec{c}$ so linearno neodvisni $\Leftrightarrow (\alpha\vec{a} + \beta\vec{b} + \gamma\vec{c} = \vec{0} \Rightarrow \alpha = \beta = \gamma = 0)$

$\vec{a}, \vec{b}, \vec{c}$ linearno neodvisni

$$\vec{a} = \vec{OA}$$

$$\vec{b} = \vec{OB}$$

$$\vec{c} = \vec{OC}$$

$$V = \{\alpha\vec{a} + \beta\vec{b} + \gamma\vec{c} : \alpha, \beta, \gamma \in \mathbb{R}\}$$

$\alpha\vec{a} + \beta\vec{b} + \gamma\vec{c}$ je linearna kombinacija vektorjev $\vec{a}, \vec{b}, \vec{c}$.

V - množica vseh vektorjev prostora \mathcal{P}

$$\mathcal{P} = \{R \in \mathcal{P} : \vec{OR} = \alpha\vec{a} + \beta\vec{b} + \gamma\vec{c}, \alpha, \beta, \gamma \in \mathbb{R}\}$$

DODATEK: V zapisu vektorja $\vec{r} \in V$: $\vec{r} = \alpha\vec{a} + \beta\vec{b} + \gamma\vec{c}$, so koeficienti α, β, γ enolično določeni.

DOKAZ: Recimo, da lahko vektor \vec{r} izrazimo na 2 različna načina:

$$\begin{aligned}\vec{r} &= \alpha \vec{a} + \beta \vec{b} + \gamma \vec{c} \\ \vec{r} &= \alpha_1 \vec{a} + \beta_1 \vec{b} + \gamma_1 \vec{c} \\ \Rightarrow \alpha \vec{a} + \beta \vec{b} + \gamma \vec{c} &= \alpha_1 \vec{a} + \beta_1 \vec{b} + \gamma_1 \vec{c} \\ (\alpha - \alpha_1) \vec{a} + (\beta - \beta_1) \vec{b} + (\gamma - \gamma_1) \vec{c} &= \vec{0} \\ \vec{a}, \vec{b}, \vec{c} \text{ linearno neodvisni} &\Rightarrow \alpha - \alpha_1 = \beta - \beta_1 = \gamma - \gamma_1 = 0 \\ \alpha = \alpha_1, \beta = \beta_1, \gamma = \gamma_1\end{aligned}$$

$\{\vec{a}, \vec{b}, \vec{c}\}$ je **baza** vektorskega prostora V . $\vec{a}, \vec{b}, \vec{c}$ so linearno neodvisni.

$R \in \mathcal{P}$ (O - fiksirana točka) $\vec{OR} = \alpha \vec{a} + \beta \vec{b} + \gamma \vec{c}$

$$R \mapsto (\alpha, \beta, \gamma) \in \mathbb{R}^3 = \{(x, y, z) : x, y, z \in \mathbb{R}\}$$

Urejena trojica (α, β, γ) je s točko R enolično določena.

α, β, γ so koordinate točke R glede na koordinaten sistem, ki je določen z bazo $\{\vec{a}, \vec{b}, \vec{c}\}$ in točko O (izhodišče koordinatnega sistema).

Imena koordinat: abscisa, ordinata, aplikata

$$\begin{aligned}\varphi : V &\rightarrow \mathbb{R}^3 \\ \vec{r} &\mapsto (\alpha, \beta, \gamma); \vec{r} = \alpha \vec{a} + \beta \vec{b} + \gamma \vec{c}\end{aligned}$$

φ je bijekcija.

S φ prenesemo operaciji seštevanja vektorjev in množenja vektorjev s skalarji iz V v \mathbb{R}^3 .

$$\begin{aligned}\vec{r}_1, \vec{r}_2 &\in V \\ \vec{r}_1 &= \alpha_1 \vec{a} + \beta_1 \vec{b} + \gamma_1 \vec{c} \\ \vec{r}_2 &= \alpha_2 \vec{a} + \beta_2 \vec{b} + \gamma_2 \vec{c} \\ \varphi(\vec{r}_1) &= (\alpha_1, \beta_1, \gamma_1) \\ \varphi(\vec{r}_2) &= (\alpha_2, \beta_2, \gamma_2) \\ \vec{r}_1 + \vec{r}_2 &= (\alpha_1 + \alpha_2) \vec{a} + (\beta_1 + \beta_2) \vec{b} + (\gamma_1 + \gamma_2) \vec{c} \\ \varphi(\vec{r}_1 + \vec{r}_2) &= (\alpha_1 + \alpha_2, \beta_1 + \beta_2, \gamma_1 + \gamma_2)\end{aligned}$$

Torej velja:

$$(\alpha_1, \beta_1, \gamma_1) + (\alpha_2, \beta_2, \gamma_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2, \gamma_1 + \gamma_2)$$

seštevanje je definirano po komponentah.

Podobno velja za množenje s skalarji:

$$\lambda(\alpha, \beta, \gamma) = (\lambda\alpha, \lambda\beta, \lambda\gamma)$$

\mathbb{R}^3 je za te operaciji **vektorski prostor** (zadošča A1-A8).

$$\varphi(\vec{a}) = (1, 0, 0)$$

$$\varphi(\vec{b}) = (0, 1, 0)$$

$$\varphi(\vec{c}) = (0, 0, 1)$$

$$\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$$

je **standardna baza** vektorskega prostora \mathbb{R}^3 .

$$(\alpha, \beta, \gamma) = \alpha(1, 0, 0) + \beta(0, 1, 0) + \gamma(0, 0, 1)$$

OZNAKE:

$$\vec{i} = (1, 0, 0)$$

$$\vec{j} = (0, 1, 0)$$

$$\vec{k} = (0, 0, 1)$$

Dodatna zahteva za standardno bazo vektorskega prostora \mathbb{R}^3 : baza je **ortonormirana**, torej:

- $|\vec{i}| = |\vec{j}| = |\vec{k}| = 1$
- $\vec{i}, \vec{j}, \vec{k}$ so paroma pravokotni.

Opomba: Po dogovoru je trojica $(\vec{i}, \vec{j}, \vec{k})$ pozitivno orientirana (pri določanju orientacije si v 3D koordinatnem sistemu pomagamo z pravilom desnega vijaka).

1.3 Skalarni produkt

$$\vec{a}, \vec{b} \in V$$

Kot med njima je $\varphi, 0 \leq \varphi \leq \pi$

$$\text{DEFINICIJA } \vec{a} \cdot \vec{b} = |\vec{a}| \cdot |\vec{b}| \cos \varphi$$

V **identificiramo**² z \mathbb{R}^3 (glede na standardno bazo in dano izhodišče O).

$$O = (0, 0, 0)$$

$$\vec{i} = (1, 0, 0)$$

$$\vec{j} = (0, 1, 0)$$

$$\vec{k} = (0, 0, 1)$$

$$\vec{a} = (a_1, a_2, a_3) \in \mathbb{R}^3$$

$$\vec{b} = (b_1, b_2, b_3) \in \mathbb{R}^3$$

$$\vec{a} \cdot \vec{b} = ?$$

$$\vec{a} = (a_1, a_2, a_3) = \vec{OA}$$

$$|\vec{a}| = |OA| = \sqrt{a_1^2 + a_2^2 + a_3^2}$$

$$d(A, B) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2 + (a_3 - b_3)^2}$$

Kosinusni izrek:

$$(\vec{a} - \vec{b})^2 = |\vec{a}|^2 + |\vec{b}|^2 - 2|\vec{a}||\vec{b}| \cos \varphi$$

$$(a_1 - b_1)^2 + (a_2 - b_2)^2 + (a_3 - b_3)^2 = a_1^2 + a_2^2 + a_3^2 + b_1^2 + b_2^2 + b_3^2 - 2|\vec{a}||\vec{b}| \cos \varphi$$

$$\Rightarrow |\vec{a}||\vec{b}| \cos \varphi = a_1 b_1 + a_2 b_2 + a_3 b_3$$

$$\vec{a} \cdot \vec{b} = a_1 b_1 + a_2 b_2 + a_3 b_3$$

LASTNOSTI:

$$(1) \vec{a} \cdot \vec{a} = |\vec{a}|^2 \geq 0 \text{ (enačaj le za } \vec{a} = \vec{0})$$

$$(2) (\vec{a} + \vec{b}) \cdot \vec{c} = \vec{a} \cdot \vec{c} + \vec{b} \cdot \vec{c}$$

²Prej smo vse izpeljevali za splošen vektorski prostor, sedaj pa za V vzamemo \mathbb{R}^3 .

$$(3) \quad (\alpha \vec{a}) \vec{b} = \alpha(\vec{a} \vec{b})$$

$$(4) \quad \vec{a} \vec{b} = \vec{b} \vec{a}$$

$$\begin{aligned} \vec{a} \perp \vec{b} &\Leftrightarrow \varphi = \frac{\pi}{2}, \vec{a} \neq \vec{0}, \vec{b} \neq \vec{0} \\ \varphi = \frac{\pi}{2} &\Leftrightarrow \cos \varphi = 0 \quad (0 \leq \varphi \leq \pi) \\ \vec{a} \perp \vec{b} &\Leftrightarrow \vec{a} \cdot \vec{b} = 0 \end{aligned}$$

PRIMER:

$$\begin{aligned} \mathbb{R}^3 &\equiv \mathbb{R}^2 \times \{0\} \\ \vec{a} &= (a_1, a_2, 0) \\ \vec{a} \text{ v } \mathbb{R}^2 : \vec{a} &= (a_1, a_2) \\ \vec{a} \vec{b} &= a_1 b_1 + a_2 b_2 \end{aligned}$$

p - ploščina paralelograma

p si želimo izraziti z a_1, a_2, b_1, b_2

$$p = |\vec{a}| |\vec{b}| \sin \varphi$$

$$\begin{aligned} \vec{a}' &\perp \vec{a} \\ |\vec{a}'| &= |\vec{a}| \end{aligned}$$

\vec{a}, \vec{a}' pozitivno orientirana

$$\vec{a}' = (-a_2, a_1)$$

$\psi = \frac{\pi}{2} - \varphi$ ali $\varphi - \frac{\pi}{2}$ če je orienacija (\vec{a}, \vec{b}) pozitivna.

$$|\vec{a}| |\vec{b}| \sin \varphi = |\vec{a}| |\vec{b}| \cos \theta = \vec{a}' \vec{b} = (-a_2, a_1) \cdot (b_1, b_2) = a_1 b_2 - a_2 b_1$$

$p = a_1 b_2 - a_2 b_1$, če je orientacija \vec{a}, \vec{b} pozitivna, če pa je negativna velja:

$$p = -(a_1 b_2 - a_2 b_1)$$

1.4 Vektorski produkt

Vzamemo vektorja \vec{a}, \vec{b} iz prostora. Njun vektorski produkt označimo:

$$\vec{a} \times \vec{b}$$

- (1) $\vec{a} \times \vec{b}$ je pravokoten na \vec{a} in \vec{b} .
- (2) $|\vec{a} \times \vec{b}|$ je enaka ploščini paralelograma, ki ga določata \vec{a} in \vec{b} . (= 0, kadar sta \vec{a} in \vec{b} linearno odvisna)
- (3) Urejena trojica $(\vec{a}, \vec{b}, \vec{a} \times \vec{b})$ je pozitivno orientirana.

$$\begin{aligned}\vec{a} &= (a_1, a_2, a_3) \\ \vec{b} &= (b_1, b_2, b_3) \\ \vec{a} \times \vec{b} &= (x, y, z)\end{aligned}$$

$$\begin{aligned}\vec{k} &= (0, 0, 1) \\ z &= (\vec{a} \times \vec{b}) \cdot \vec{k} = \\ &= |\vec{a} \times \vec{b}| |\vec{k}| \cos \delta = \\ &= p \cos \delta\end{aligned}$$

p - ploščina paralelograma, ki ga določata vektorja \vec{a} in \vec{b}
 δ - kot med ravninama, ki ju določata osi (1),(2) in vektorja \vec{a}, \vec{b} .

$$\begin{aligned}\vec{a}' &= (a_1, a_2, 0) \\ \vec{b}' &= (b_1, b_2, 0) \\ p' &= \pm(a_1 b_2 - a_2 b_1)\end{aligned}$$

p' je ploščina paralelograma, ki ga določata pravokotni projekciji vektorjev \vec{a} in \vec{b} na ravnino (\vec{i}, \vec{j}) , tj. ploščina paralelograma, ki ga določata vektorja \vec{a}' in \vec{b}' .

p' ima predznak +, kadar sta \vec{a}' in \vec{b}' pozitivno orientirana, ter -, kadar sta negativno orientirana.

$$p' = \pm p \cos \delta$$

+ kadar: $0 \leq \delta \leq \frac{\pi}{2}$
 - kadar: $\frac{\pi}{2} \leq \delta \leq \pi$

$$z = \pm p' = a_1 b_2 - a_2 b_1$$

\pm se izniči, ker se predznak, ki nastane zaradi \cos in predznak, ki nastane pri izračunu ploščine paralelograma z vektorjema ujemata.

$$\begin{aligned}x &= a_2 b_3 - a_3 b_2 \\ y &= a_3 b_1 - a_1 b_3\end{aligned}$$

$$\vec{a} \times \vec{b} = (a_2b_3 - a_3b_2, a_3b_1 - a_1b_3, a_1b_2 - a_2b_1)$$

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \alpha\delta - \beta\gamma$$

determinanta (reda 2)

$$\vec{a} \times \vec{b} = \left(\begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}, \begin{vmatrix} a_3 & a_1 \\ b_3 & b_1 \end{vmatrix}, \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \right)$$

$$\begin{vmatrix} a_3 & a_1 \\ b_3 & b_1 \end{vmatrix} = - \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix}$$

$$\vec{a} \times \vec{b} = \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix} \vec{i} + \begin{vmatrix} a_3 & a_1 \\ b_3 & b_1 \end{vmatrix} \vec{j} + \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \vec{k}$$

$$\vec{a} \times \vec{b} = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}$$

Lastnosti:

- $(\alpha\vec{a}) \times \vec{b} = \alpha(\vec{a} \times \vec{b}), \forall \alpha \in \mathbb{R}$
- $(\vec{a} + \vec{b}) \times \vec{c} = \vec{a} \times \vec{c} + \vec{b} \times \vec{c}$
- $\vec{c} \times (\vec{a} + \vec{b}) = \vec{c} \times \vec{a} + \vec{c} \times \vec{b}$
- $\vec{a} \times \vec{b} = -\vec{b} \times \vec{a}$

\vec{a}, \vec{b} linearno neodvisna $\Rightarrow \{\vec{a}, \vec{b}, \vec{a} \times \vec{b}\}$ je baza.

$$\vec{r} = \alpha\vec{a} + \beta\vec{b} + \gamma(\vec{a} \times \vec{b})$$

Poseben primer:

$$|\vec{a}| = |\vec{b}| = 1, \vec{a} \cdot \vec{b} = 0 (\vec{a} \perp \vec{b})$$

$\Rightarrow \{\vec{a}, \vec{b}, \vec{a} \times \vec{b}\}$ je ortonormirana baza.

$$\vec{r} = \alpha\vec{a} + \beta\vec{b} + \gamma(\vec{a} \times \vec{b}) / \cdot \vec{a} \text{ (ali } \vec{b}, \vec{c})$$

$$\vec{r} \cdot \vec{a} = \alpha$$

$$\vec{r} \cdot \vec{b} = \beta$$

$$\vec{r} \cdot (\vec{a} \times \vec{b}) = \gamma$$

$$\begin{aligned}
(|\vec{a} \times \vec{b}|)^2 &= (|\vec{a}||\vec{b}| \sin \varphi)^2 \\
(\vec{a} \cdot \vec{b})^2 &= (|\vec{a}||\vec{b}| \cos \varphi)^2 \\
\Rightarrow |\vec{a} \times \vec{b}|^2 + (\vec{a} \cdot \vec{b})^2 &= |\vec{a}|^2 \cdot |\vec{b}|^2
\end{aligned}$$

1.5 Mešani produkt

$$(\vec{a} \times \vec{b}) \cdot \vec{c}$$

Paralelepiped je prizma, ki ima za osnovno ploskev paralelogram. V - prostornina paralelepipeda

$$\begin{aligned}
P &= |\vec{a} \times \vec{b}| \\
V &= |\vec{a} \times \vec{b}| \cdot v \\
v &= \pm |\vec{c}| \cos \delta \\
V &= \pm |\vec{a} \times \vec{b}| |\vec{c}| \cos \delta = \\
&= \pm (\vec{a} \times \vec{b}) \cdot \vec{c} \\
(\vec{a} \times \vec{b}) \cdot \vec{c} &= \pm V
\end{aligned}$$

+: $(\vec{a}, \vec{b}, \vec{c})$ pozitivno orientirani

–: $(\vec{a}, \vec{b}, \vec{c})$ negativno orientirani $\vec{a}, \vec{b}, \vec{c}$ linearno odvisni $\Leftrightarrow (\vec{a} \times \vec{b}) \vec{c} = 0$.

Orientacija se pri cikličnih zamenjavah ohrani:

$$\begin{aligned}
(\vec{a} \times \vec{b}) \vec{c} &= (\vec{b} \times \vec{c}) \vec{a} = \vec{a} (\vec{b} \times \vec{c}) \\
(\vec{a} \times \vec{b}) \vec{c} &= \vec{a} (\vec{b} \times \vec{c}) = [\vec{a}, \vec{b}, \vec{c}]
\end{aligned}$$

$$\vec{a} = (a_1, a_2, a_3)$$

$$\vec{b} = (b_1, b_2, b_3)$$

$$\vec{c} = (c_1, c_2, c_3)$$

$$[\vec{a}, \vec{b}, \vec{c}] = \vec{a}(\vec{b} \times \vec{c}) = a_1 e_1 + a_2 e_2 + a_3 e_3 =$$

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} \equiv a_1 \begin{vmatrix} b_2 & b_3 \\ c_2 & c_3 \end{vmatrix} - a_2 \begin{vmatrix} b_1 & b_3 \\ c_1 & c_3 \end{vmatrix} + a_3 \begin{vmatrix} b_1 & b_2 \\ c_1 & c_2 \end{vmatrix}$$

$$[\vec{a}, \vec{b}, \vec{c}] = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$$

1.6 Dvojni vektorski produkt

$$(\vec{a} \times \vec{b}) \times \vec{c} = \vec{e} = ?$$

$$\begin{aligned}\vec{e} &\perp \vec{a} \times \vec{b} \\ \vec{e} &\perp \vec{c}\end{aligned}$$

\vec{a}, \vec{b} linearno neodvisna $\Rightarrow \vec{e} = \alpha \vec{a} + \beta \vec{b}$.
 $\vec{e} \cdot \vec{c} = 0$

$$\alpha(\vec{a}\vec{c}) + \beta(\vec{b}\vec{c}) = 0$$

$$\begin{aligned}\beta &= \lambda \vec{a}\vec{c} \\ \alpha &= -\lambda \vec{b}\vec{c}\end{aligned}$$

$$\begin{aligned}\vec{e} &= \lambda(\vec{b}\vec{c})\vec{a} + \lambda(\vec{a}\vec{c})\vec{b} \\ \vec{e} &= \lambda(-(\vec{b}\vec{c})\vec{a} + (\vec{a}\vec{c})\vec{b})\end{aligned}$$

Če razpišemo po komponentah dobimo $\lambda = 1$.

$$(\vec{a} \times \vec{b}) \times \vec{c} = -(\vec{b}\vec{c})\vec{a} + (\vec{a}\vec{c})\vec{b}$$

2 Analitična geometrija v \mathbb{R}^3

2.1 Premica

p podana s točko R_0 na njej in *smernim vektorjem* \vec{e} .

$$\vec{r}_0 = \vec{OR}_0 = (x_0, y_0, z_0)$$

$$R \in p$$

$$\vec{r} = \vec{OR} = (x, y, z)$$

Koordinatizirali smo premico.

$$\vec{R_0R} = \vec{r} - \vec{r}_0$$

$$\vec{r} = \vec{r}_0 + \lambda \vec{e}, \lambda \in \mathbb{R}$$

Enačba premice p (vektorska parametrična) (λ je parameter)

$$\vec{e} = (a, b, c)$$

$$x = x_0 + \lambda a$$

$$y = y_0 + \lambda b$$

$$z = z_0 + \lambda c$$

(Parametrična) enačba premice.

$$\frac{x - x_0}{a} = \frac{y - y_0}{b} = \frac{z - z_0}{c}$$

enačba premice (brez parametra)

$a = 0$?

$$\frac{x - x_0}{0} \equiv (x = x_0 \text{ ali } ax - x_0 = 0)$$

Podobno za $b = 0$ in $c = 0$.

$R_0 \vec{R}, \vec{e}$ linearno odvisna $\Leftrightarrow R \in p$

To je kadar: $R_0 \vec{R} \times \vec{e} = \vec{0} \Leftrightarrow (\vec{r} - \vec{r}_0) \times \vec{e} = \vec{e} \times (\vec{r} - \vec{r}_0) = \vec{0}$
(vektorska enačba premice)

Če imamo točko R_1 izven premice, je razdalja med premico p in to točko enaka:

$$\Delta = |\vec{r}_1 - \vec{r}_0| \sin \varphi$$

To enačbo lahko preoblikujemo da dobimo:

$$\Delta = \frac{|\vec{e} \times (\vec{r}_1 - \vec{r}_0)|}{|\vec{e}|}$$

To je posebej ugodno, kadar $|\vec{e}| = 1$, saj iz tega sledi $\Delta = |\vec{e} \times (\vec{r}_1 - \vec{r}_0)|$.

Razdaljo med točko in premico lahko zapišemo tudi kot: $\Delta = d(R_1, p)$.

2.2 Ravnina

Da določimo ravnino Σ , potrebujemo točko $R_0 \in \Sigma$ in vektor normale \vec{n} , kjer $\vec{n} \perp \Sigma$ in $\vec{n} \neq \vec{0}$.

Da določimo kdaj točka leži na ravnini zapišemo:

$$R \in \Sigma \Leftrightarrow \vec{r} - \vec{r}_0 \perp \vec{n} \Leftrightarrow \vec{n} \cdot (\vec{r} - \vec{r}_0) = 0$$

To pomeni da nam ravnino Σ določa enačba:

$$\vec{n} \cdot (\vec{r} - \vec{r}_0) = 0$$

Če zapišemo vektorje \vec{r}_0, \vec{r} in \vec{n} kot:

$$\vec{r}_0 = (x_0, y_0, z_0)$$

$$\vec{r} = (x, y, z)$$

$$\vec{n} = (a, b, c)$$

lahko zapišemo enačbo ravnine kot:

$$a(x - x_0) + b(y - y_0) + c(z - z_0) = 0$$

To enačbo lahko naprej pretvorimo v *implicitno obliko*:

$$ax + by + cz + d = 0$$

kjer je $d = -ax_0 - by_0 - cz_0$.

Če imamo podane točke R_0, R_1 in R_2 , lahko izračunamo vektor normale kot:

$$\vec{n} = (\vec{r}_1 - \vec{r}_0) \times (\vec{r}_2 - \vec{r}_0)$$

če to vstavimo v enačbo ravnine, dobimo da lahko ravnino Σ zapišemo kot:

$$((\vec{r}_1 - \vec{r}_0) \times (\vec{r}_2 - \vec{r}_0)) \cdot (\vec{r} - \vec{r}_0) = 0$$

Opazimo, da nam ta enačba predstavlja mešani produkt kar lahko zapišemo z determinanto reda 3:

$$\begin{vmatrix} x - x_0 & y - y_0 & z - z_0 \\ x_1 - x_0 & y_1 - y_0 & z_1 - z_0 \\ x_2 - x_0 & y_2 - y_0 & z_2 - z_0 \end{vmatrix} = 0$$

kjer je vektor \vec{r}_n zapisan kot: $\vec{r}_n = (x_n, y_n, z_n)$.

Če imamo točko R_1 , ki ni na ravnini, lahko zapišemo razdaljo te točke do ravnine kot:

$$\Delta = \pm |\vec{r}_1 - \vec{r}_0| \cos \varphi \quad (1)$$

To enačbo lahko s pomočjo enačbe ravnine preoblikujemo v:

$$\Delta = \frac{|\vec{n} \cdot (\vec{r}_1 - \vec{r}_0)|}{|\vec{n}|}$$

v števcu lahko uprabimo absolutno vrednost s katero se znebimo predznaka, ki se pojavi v (1), ker je razdalja vedno pozitivna.

Razdaljo med ravnino Σ in točko R_1 lahko zapišemo tudi kot:

$$\Delta = d(R_1, \Sigma)$$

Če si pomagamo z že izpeljano implicitno enačbo ravnine, se lahko znebimo vektorjev in dobimo naslednjo enačbo:

$$d(R_1, \Sigma) = \frac{|ax_1 + by_1 + cz_1 + d|}{\sqrt{a^2 + b^2 + c^2}}$$

kjer $\vec{OR}_1 = \vec{r}_1 = (x_1, y_1, z_1)$.

2.3 Razdalja med mimobežnima premicama

p_1 : e_1 je smerni vektor; $R_1 \in p_1, r_1$

p_2 : e_2 je smerni vektor; $R_2 \in p_2, r_2$

Da sta premici mimobežni imamo dva pogoja:

- $\vec{e}_1 \times \vec{e}_2 \neq \vec{0} (p_1 \nparallel p_2)$
- $p_1 \cap p_2 = \emptyset$ (ne sekata se)

$$d(p_1, p_2) = \min\{d(T_1, T_2) : T_1 \in p_1, T_2 \in p_2\}$$

Z pomočjo skice in premisleka opazimo, da je najmanjša razdalja takrat, ko $S_1 S_2 \perp p_1, p_2$. To pomeni:

$$\begin{aligned} S_1 \vec{S}_2 &\perp \vec{e}_1, \vec{e}_2 \\ S_1 \vec{S}_2 &= \lambda \vec{e}_1 \times \vec{e}_2, \lambda \in \mathbb{R} \end{aligned}$$

Tu je spet v veliko pomoč skica. Ideja je, da z vzporednim premikom premaknemo vektor \vec{e}_2 v izhodišče vektorja \vec{e}_1 . S tem lahko naredimo ravnino Σ_1 , ki jo tvorita ta dva vektorja. Nato naredimo ravnino Σ_2 na podoben način – z vzporednim premikom premaknemo vektor \vec{e}_1 v izhodišče vektorja \vec{e}_2 . Velja $\Sigma_1 \parallel \Sigma_2$. Ker sta si ravnini vzporedni lahko premico p_1 z vzporednim premikom premaknemo iz Σ_1 v Σ_2 in dobimo premico p_1^* , ki se seka s premico p_2 v točko S_2 . Podobno lahko premaknemo premico p_2 v ravnino Σ_1 in dobimo točko S_1 kjer se sekata p_1 in p_2^* . Opazimo, da je daljica S_1S_2 pravokotna na premici p_1 in p_2 in je tudi najkrajša razdalja med tema premicama. To pomeni, da je dolžina daljice S_1S_2 razdalja med premicama p_1 in p_2 .

Z nadaljnim premislekom in zelo natančno narisano skico opazimo, da vektorji \vec{e}_1, \vec{e}_2 in $\vec{r}_1 - \vec{r}_2$ tvorijo paralelepiped, katerega višina je enaka daljici S_1S_2 . To pomeni, da lahko uporabimo naše znanje o mešanem produktu in naredimo naslednje:

$$\begin{aligned} V &= |[\vec{r}_1 - \vec{r}_2, \vec{e}_1, \vec{e}_2]| \\ V &= |\vec{e}_1 \times \vec{e}_2| \cdot \Delta \end{aligned}$$

kjer je $\Delta = |S_1S_2|$.

To lahko izenačimo in dobimo:

$$\Delta = \frac{|[\vec{r}_1 - \vec{r}_2, \vec{e}_1, \vec{e}_2]|}{|\vec{e}_1 \times \vec{e}_2|}$$

3 Osnovne algebrske strukture

3.1 Preslikave in relacije

A, B sta neprazni množici.

Preslikavo, ki slika iz A v B lahko zapišemo kot $f : A \rightarrow B$ ali $A \xrightarrow{f} B$.

$\forall x \in A$ predpis f določi natanko en element, ki je iz množice B . Množici A rečemo domena (včasih tudi definicijsko območje), množici B pa rečemo kodomena. $f(x)$ pravimo slika elementa x . ($x \mapsto f(x)$)

Zaloga (vrednosti) preslikave $f : A \rightarrow B$ je množica $\{f(x) : x \in A\} \subseteq B$.

$f : A \rightarrow B$ je *surjektivna* (surjekcija), kadar je njena zaloga B .

$$\forall y \in B \exists x \in A : y = f(x)$$

$f : A \rightarrow B$ je *injektivna* (injekcija), kadar velja sklep:

$$x_1, x_2 \in A, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

Za preverjanje uporabimo:

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2, x_1, x_2 \in A$$

$f : A \rightarrow B$ je *bijektivna* (bijekcija), kadar je injektivna in hkrati surjektivna. Če je $f : A \rightarrow B$ bijekcija, obstaja točno določena preslikava $g : B \rightarrow A$, da velja:

$$(\forall x \in A : g(f(x)) = x) \wedge (\forall y \in B : f(g(y)) = y)$$

Preslikavo $g : B \rightarrow A$ imenujemo *inverz* preslikave $f : A \rightarrow B$ in jo označimo z:

$$g = f^{-1}$$

Kompozitum preslikav $f : A \rightarrow B$ in $g : B \rightarrow C$ je:

$$\begin{aligned} g \circ f \text{ ali } gf \\ g \circ f : A \rightarrow C \\ (g \circ f)(x) = g(f(x)) \end{aligned}$$

za vsak $x \in A$.

Preslikavo $A \rightarrow A$ imenujemo *identična preslikava* ali *identiteta*:

$$\begin{aligned} id_A : A \rightarrow A \\ \forall x \in A : id_A(x) = x \end{aligned}$$

$$\begin{aligned} f : A \rightarrow B \text{ bijekcija} \\ g : B \rightarrow A \\ g \circ f = id_A \\ f \circ g = id_B \end{aligned}$$

$f : A \rightarrow B$ je bijekcija in $g : B \rightarrow A$ je inverzana preslikava $f \iff (g \circ f = id_A \wedge f \circ g = id_B)$

Graf preslikave $f : A \rightarrow B$ je množica:

$$G(f) = \{(x, f(x)) : x \in A\}$$

$$G(f) \subseteq A \times B$$

Relacija med elementi množice A in elementi množice B je podmnožica množice $A \times B$.

$R \subseteq A \times B$ (R je relacija)

$(x, y) \in R \equiv xRy$

Primeri kjer $A = B$ (relacija $R \subseteq A \times A$ je *binarna relacija* na množici A).

(1) $A = \mathbb{R}$

R relacija na \mathbb{R} : \leq

$$(x, y) \in R \subseteq \mathbb{R} \times \mathbb{R} \iff x \leq y$$

$$R = \leq$$

$$R = \{(x, y) \in \mathbb{R}^2 : x \leq y\}$$

(2) $A = \{p : p \text{ - premica v prostoru}\}$

R relacija vzporednosti

$$p, q \in A \quad pRq \equiv p \parallel q$$

(3) $M \neq \emptyset, \quad A = \mathcal{P}M$ R relacija *inkluzije* \subseteq

$$x, y \in A \quad (x \subseteq A, y \subseteq A)$$

$$xRy \equiv x \subseteq y$$

Definicije:

(1) Relacija R nad A je *refleksivna*, kadar velja xRx za vsak $x \in A$.

(2) Relacija R nad A je *tranzitivna*, kadar velja sklep:

$$(xRy \wedge yRz) \Rightarrow xRz$$

(3) Relacija R nad A je *antisimetrična*, kadar velja sklep:

$$(xRy \wedge yRx) \Rightarrow x = y$$

(4) Relacija R nad A je *simetrična*, kadar velja sklep:

$$xRy \Rightarrow yRx$$

(5) R je relacija *delne urejenosti*, kadar je refleksivna, antisimetrična in tranzitivna ($R \equiv \leq$).

(6) R je relacija *ekvivalence* (ali ekvivalenčna relacija), kadar je refleksivna, simetrična in tranzitivna ($R \equiv \sim$).

Naj bo A neprazna množica, \sim ekvivalenčna relacija na A in $a \in A$.

$$[a] = \{x \in A : x \sim a\}$$

$[a]$ je *ekvivalenčni razred* elementa a .

$$a \sim a \Rightarrow a \in [a]$$

a je predstavnik tega ekvivalenčnega razreda.

$$[a] = [b]?$$

Predpostavimo $b \sim a$ (zaradi simetričnosti sledi $a \sim b$).

$$x \in [a] \Rightarrow x \sim a \sim b \Rightarrow x \sim b \Rightarrow x \in [b]$$

Torej velja:

$$[a] \subseteq [b]$$

$$[b] \subseteq [a]$$

Zato $[a] = [b]$.

Velja tudi $[a] = [b] \Rightarrow a \sim b$

$$[a] = [b] \Rightarrow a \in [a] \Rightarrow a \in [b] \Rightarrow a \sim b$$

$$a \sim b \iff [a] = [b]$$

Naj velja $[a] \cap [b] \neq \emptyset$:

$$\begin{aligned} \exists c \in [a] \cap [b] \\ \Rightarrow c \sim a \wedge c \sim b \Rightarrow a \sim b \Rightarrow [a] = [b] \end{aligned}$$

$$\begin{aligned} [a] \cap [b] \neq \emptyset \Rightarrow [a] = [b] \\ [a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset \end{aligned}$$

$A/\sim = \{[a] : a \in A\}$ je *kvocientna* ali *faktorska* množica glede na ekvivalenčno relacijo \sim .

$A = \cup[a]$ pravimo *razčlenitev* A -ja.

Primeri:

(1) $A = \{\overrightarrow{MN} : M, N - \text{točki v prostoru}\}$

\overrightarrow{MN} je usmerjena daljica

$\overrightarrow{XY} \sim \overrightarrow{MN} \iff$ obstaja translacija, ki XY prenese v MN . \sim je ekvivalenčna relacija.

$$[\overrightarrow{MN}] = \{\overrightarrow{XY} : \overrightarrow{XY} \sim \overrightarrow{MN}\} = \overrightarrow{MN}$$

(2) $A = \mathbb{Z} \times \mathbb{N} = \{(m, n) : m \in \mathbb{Z}, n \in \mathbb{N}\}$

$$\sim : (m, n) \sim (p, q) \iff mq = np$$

\sim je ekvivalenčna relacija

$$A/\sim = \mathbb{Q}$$

$$[(m, n)] = \{(p, q) : (p, q) \sim (m, n)\}$$

3.2 Operacije

$$M \neq \emptyset$$

Operacija na M je preslikava $M \times M \rightarrow M, (a, b) \mapsto a \circ b$

$a \circ b$ je *kompozitum* elementov a in b .

PRIMERI:

1) $M = \mathbb{N}$ ali \mathbb{Z} ali \mathbb{Q} ali \mathbb{R} .

\circ je lahko $+$ ali \cdot .

2) $A \neq \emptyset$

$$M = \{f : A \rightarrow A\} \equiv F(A)$$

\circ je kompozitum preslikav

M z dano operacijo \circ je *grupoid* (M, \circ) .

Zapis operacije brez znaka $(a, b) \mapsto ab$ je *multiplikativen* zapis operacije.

Imamo grupoid (M, \sim, \circ) . Radi bi prenesli \circ v M/\sim .

Operacija \circ je usklajena z ekvivalenčno relacijo \sim , kadar velja sklep:

$$(m_1 \sim m \wedge n_1 \sim n) \Rightarrow m_1 \circ n_1 \sim m \circ n$$

kjer $m, n, m_1, n_1 \in M$.

PRIMER: $M = \mathbb{Z} \times \mathbb{N}$

\sim iz primera (2)

$$(p_1, q_1) \sim (p, q) \wedge (m_1, n_1) \sim (m, n) \Rightarrow (p_1, q_1) + (m_1, n_1) \sim (p, q) + (m, n) \\ (p, q) + (m, n) := (pn + mq, nq)$$

v $+$ iz $\mathbb{Z} \times \mathbb{N}$ lahko prenesemo na $\mathbb{Q} = (\mathbb{Z} \times \mathbb{N})/\sim$.

(M, \sim, \circ) , \sim in \circ usklajeni.

V M/\sim lahko uvedemo operacijo $\tilde{\circ}$ s predpisom:

$$[a] \tilde{\circ} [b] = [a \circ b]$$

Definicija je dobra zaradi uklajenosti operacije \circ z relacijo \sim :

$$[a_1] = [a] \text{ in } [b_1] = [b] \Rightarrow [a_1 \circ b_1] \sim [a \circ b]$$

3.3 Grupe

DEFINICIJE:

- (M, \circ) grupoid

$e \in M$ je *enota* ali *neutralni element* grupoida (M, \circ) kadar velja:

$$\forall a \in M : a \circ e = e \circ a = a$$

Če enota obstaja je ena sam

$e_1, e_2 \in M$ sta enoti. Sledi:

$$e_1 \circ e_2 = e_2$$

če upoštevamo da je e_1 enota,

$$e_1 \circ e_2 = e_1$$

če upoštevamo da je e_2 enota

$$\Rightarrow e_1 = e_2$$

□

- Grupoid (M, \circ) je *polgrupa*, kadar je opracije \circ *asociativna*:

$$\forall a, b, c \in M : (a \circ b) \circ c = a \circ (b \circ c)$$

V polgrupi oklepaji niso potrebni: $a \circ b \circ c$.

- Naj bo (M, \circ) polgrupa z enoto e .

Element $b \in M$ je *inverz* elementa $a \in M$, kadar velja:

$$a \circ b = b \circ a = e$$

Kadar ima element $a \in M$ inverz, pravimo, da je a *invertabilen* ali *obrnljiv*.

Če ima $a \in M$ inverz, je ta en sam

b_1, b_2 inverza elementa a .

$$a \circ b_1 = b_1 \circ a = e$$

$$a \circ b_2 = b_2 \circ a = e$$

$$\Rightarrow b_1 = b_1 \circ e = b_1 \circ (a \circ b_2) = (b_1 \circ a) \circ b_2 = e \circ b_2 = b_2$$

□

Če je $a \in M$ obrnljiv, njegov inverz zaznamujemo (v splošnem) z a^{-1} .

$$a \circ a^{-1} = a^{-1} \circ a = e$$

- Polgrupa z enoto, v kateri je vsak element obrnljiv se imenuje *grupa*.

Z multiplikativnim zapisom: (G, \circ) je grupa, kadar velja:

$$(1) \quad \forall a, b, c \in G : (ab)c = a(bc)$$

$$(2) \quad \exists e \in G \forall a \in G : ae = ea = a$$

$$(3) \quad \forall a \in G \exists b \in G : ab = ba = e$$

- (M, \circ) grupoid je *komutativen*, kadar velja:

$$\forall a, b \in M : a \circ b = b \circ a$$

PRIMERI:

(1) $(\mathbb{N}, +)$ polgrupa brez enote (če $0 \notin \mathbb{N}$).

(2) (\mathbb{N}, \cdot) polgrupa z enoto 1

(3) $(\mathbb{Z}, +)$ grupa

(4) (\mathbb{Z}, \cdot) polgrupa z enoto 1

(5) $A \neq \emptyset, M = F(A) = \{f : A \rightarrow A\}$

operacija: komponiranje preslikave

(M, \circ) je polgrupa z enoto $e = id$

(6) $M = S(A) = \{f : A \mapsto A, f \text{ je bijekcija}\}$

(M, \circ) je grupa

Prejšen primer lahko nekoliko spremenimo in dobimo:

$$A = \{1, 2, \dots, n\}$$

$$S(A) \equiv S_n$$

S_n je *simetrična grupa*.

$$\pi \in S_n$$

$$\pi : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$$

Če preslikamo vse elemente s preslikavo π dobimo:

$$\{\pi(1), \pi(2), \dots, \pi(n)\} = \{1, 2, \dots, n\}$$

Pravimo, da je π *permutacija* in jo zapišemo kot:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

Zapis $\pi(k)$ je rahlitvno dolg, zato ga skrajšamo na:

$$\pi(k) = i_k$$

S tem lahk permutacijo π zapišemo kot:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

Zelo lahko je izplejati, da S_n ima $n!$ elementov.

Ker so permutacije elementi grupe, ki ima za operacijo komponiranje preslikav (kompozitum), lahko z njimi računamo. Poglejmo si primer:

$$\begin{aligned} \rho &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\ \sigma &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \end{aligned}$$

kjer $\rho, \sigma \in S_3$

$$\begin{aligned} \rho\sigma &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ \sigma\rho &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \end{aligned}$$

Opazimo, da $\rho\sigma \neq \sigma\rho$.

Poglejmo si, kako lahko v grupi krajšamo. Naj bo (G, \cdot) grupa.

$$\begin{aligned} ab &= ac \\ a^{-1}(ab) &= a^{-1}(ac) \\ (a^{-1}a)b &= (a^{-1}a)c \\ eb &= ec \\ b &= c \end{aligned}$$

Pozorni moramo biti na vrstni red, ker v grupi ni obvezno da velja komutativnost. Pri tem primeru smo na obeh straneh enačbe a imeli na levi strani.

Analogno bi lahko pravilo krajšanja izpeljali, če bi bil a na desni strani, vendar ne če je na eni strani enačbe desni, na drugi pa levi člen. To pomeni da v grupi vlejajo naslednje trditve:

$$ab = ac \Rightarrow b = c$$

$$ab = ca \nRightarrow b = c$$

$$b \neq c \Rightarrow ab \neq ac$$

GRUPA S TREMI ELEMENTI JE SAMO ENA

Naj bo G grupa s tremi elementi.

$$G = \{e, a, b\}$$

kjer je e enota.

Zapišimo naslednjo tabelo:

	e	a	b
e			
a			
b			

Prva vrstica in prvi stolpec sta trivialna, saj imamo na eni strani enoto. Tabelo lahko dopolnimo in dobimo:

	e	a	b
e	e	a	b
a	a		
b	b		

Potrebujemo premisliti drugo vrstico. Vemo že, da $ae = a$, potrebujemo pa se odločiti, kaj bomo zapisali pri aa in pri ab .

Zgoraj smo zapisali pravilo, ki nam pravi naslednje: $b \neq c \Rightarrow ab \neq ac$. V grupi so trije različni elementi, to pomeni: $e \neq a \neq b \Rightarrow ae \neq aa \neq ab$. Drugače povedano, v vsaki vrstici bo vsak element nastopil natanko enkrat in tudi v vsakem stolpcu bo vsak element nastopil natanko enkrat. To si lahko predstavljamo kot nekakšen sudoku.

Če se vrnemo na prejšnji problem - odločitev kaj je aa in kaj ab . Sedaj vemo da imamo dve možnosti:

1) $ab = b \Rightarrow a = e \rightarrow \leftarrow$ ni možno, ker bi potem a bil enota, vemo pa da mora biti različen od enote.

2) $ab = e$

Torej se odločimo da bo veljalo $ab = e$. Za aa nam torej ostane samo ena možnost, to je: $aa = b$. Tabelo lahko še nekoliko dopolnimo:

	e	a	b
e	e	a	b
a	a	b	e
b	b		

Za izpolniti nam ostane samo še ba in bb . Zapisali smo že, da se mora v vsaki vrstici vsak element nahajati natanko enkrat. Torej lahko samo dopolnimo tabelo do konca in dobimo:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Definirajmo potence. To bomo naredili podobno kot pri analizi. Za pozitivne cele eksponente torej velja:

$$\begin{aligned} aa &= a^2 \\ aaa &= a^3 \\ \underbrace{aa \dots a}_n &= a^n \end{aligned}$$

Za negativne cele eksponente velja podobno:

$$\begin{aligned} a^{-1}a^{-1} &= a^{-2} \\ a^{-1}a^{-1}a^{-1} &= a^{-3} \\ \underbrace{a^{-1}a^{-1} \dots a^{-1}}_n &= a^{-n} \end{aligned}$$

Definirati moramo še a^0 . To naredimo na sledeč način:

$$a^0 \equiv e$$

Sedaj lahko zapišemo G kot $G = \{e, a, a^2\}$. Vemo tudi, da $a^3 = e$.

Primer take je grupe je podmnožica kompleksnih števil kjer je opracija množenje:

$$\begin{aligned} G &\subseteq \mathbb{C} \\ G &= \{1, a, a^2\} \\ a &= -\frac{1}{2} + \frac{\sqrt{3}}{2}i \end{aligned}$$

Za katerikoli n obstaja grupa. Zgornji grupi G pravimo tudi *ciklična grupa*.

DEFINICIJA transpozicije:

Naj bosta $j, k \in \{1, \dots, n\}, j \neq k$

$$\begin{aligned} \tau &\in S_n \\ \tau(j) &= k \\ \tau(k) &= j \\ \tau(i) &= i \forall i \in \{1, \dots, n\} \setminus \{j, k\} \end{aligned}$$

τ je *transpozicija*.

Vsaka permutacija je kompozitum samih transpozicij.

PRIMER:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

Lahko si naredimo diagram, kjer v vsakem koraku premaknemo en element na pravo mesto. Začnemo z 1, nato 2 in tako naprej. Nato samo komponiramo transpozicije, ki smo jih uporabili. Skica takega postopka je v zvezku. Če je ni, potem lahko poizkusiš izumiti toplo vodo, lahko pa vprašaš kakšnega študenta, ki je bolj priden od tebe in ima to skico v zvezku. Torej lahko permutacijo π zapišemo kot kompozitum transpozicij na naslednj način:

$$\pi = (4, 5)(2, 4)(1, 3)$$

Strategija velja v vsaki simetrični grupi S_n . Zelo lahko je opzaiti, da lahko vsako permutacijo zapišemo kot kompozitum največ $n - 1$ transpozicij.

Definirajmo inverzijo. Naj bo

$$\begin{aligned} \pi &= \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix} \in S_n \\ 1 &\leq j < k \leq n \end{aligned}$$

DEFINICIJA: Par (j, k) tvori *inverzijo* v permutaciji π , kadar v vrstici i_1, i_2, \dots, i_n k nastopa pred j (z leve proti desni). Drugače povedano: indeks mesta elementa i_k je manjši od indeksa elementa i_j .

$$\text{inv}\pi = \text{število inverzij v } \pi$$

PRIMER:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

Inverzije v π so:

$$\begin{aligned} &(1, 3), (1, 5) \\ &(2, 3), (2, 5) \\ &(4, 5) \end{aligned}$$

$$\text{inv}\pi = 5$$

Definirajmo naslednjo funkcijo:

$$s(\pi) = (-1)^{\text{inv}\pi} = \begin{cases} 1 & \pi \text{ ima sodo inverzij} \\ -1 & \pi \text{ ima liho inverzij} \end{cases}$$

Pravimo da:

$$\begin{aligned} \pi \text{ je soda} &\iff s(\pi) = 1 \\ \pi \text{ je liha} &\iff s(\pi) = -1 \end{aligned}$$

TRDITEV: Naj bo $\tau \in S_n$ transpozicija. Potem $\forall \rho \in S_n$ velja:

$$s(\tau\rho) = -s(\rho)$$

DOKAZ:

$$\rho = \begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}$$

$$1) \quad \tau = (i_k, i_{k+1})$$

$$\begin{aligned} \text{inv}(\tau\rho) &= \text{inv}(\rho) \pm 1 \\ \Rightarrow s(\tau\rho) &= -s(\rho) \end{aligned}$$

$$2) \quad \tau(i_k, i_{k+p}), p > 1$$

τ dosežemo s produktom transpozicij podobni tisti v primeru (1). To pomeni, da najprej element i_k premikamo v desno proti i_{k+p} , vsakič za

eno mesto, nato pa še element i_{k+p} premikamo nazaj na prvotno mesto elementa i_k . Če znamo vsaj malo algoritmov, se lahko spomnimo na bubble sort. Za ostale, ki ne znajo algoritmov pa obstaja skica, ki se žal ponovno nahaja samo v zvezku in domišljiji bralca.

Torej potrebujemo p transpozicij, da premakno element i_k na mesto elementa i_{k+p} . V tem trenutku, je i_{k+p} , že premaknjen eno mesto proti ciljni poziciji, zato potrebujemo samo še $p - 1$ transpozicij, da ga damo na mesto elementa i_k . Torej je skupno število potrebnih transpozicij:

$$p + p - 1 = 2p - 1$$

Vemo, da se na vsakem koraku predznak permutacije zamenja, zato velja:

$$s(\tau\rho) = (-1)^{2p-1}s(\rho) = -s(\rho)$$

saj je $2p - 1$ liho število. □

IZREK: Naj bo $\pi \in S_n$ in naj velja:

$$\pi = \tau_1 \tau_2 \dots \tau_k$$

kjer so τ_i transpozicije.

Potem je π soda (oziroma liha) natanko takrat, kadar je število k sodo (oziroma liho).

DOKAZ: $s(e) = 1$ kjer je $e = id_{\{1, \dots, n\}}$ enota grupa S_n . Z uporabo prejšnje trditve lahko naredimo naslednje:

$$\begin{aligned} s(\pi) &= s(\underbrace{\tau_1}_{\tau} \underbrace{\tau_2 \dots \tau_k}_{\rho} e) = \\ &= (-1)s(\tau_2 \dots \tau_k e) = (-1)^2 s(\tau_3 \dots \tau_k e) = \dots \\ &= (-1)^k s(e) = (-1)^k \end{aligned}$$

Naj bo $A_n = \{\pi \in S_n : \pi \text{ soda}\}$, $e \in A_n$

$$(1) \quad \rho, \sigma \in A_n \Rightarrow \rho\sigma \in A_n$$

ρ, σ zapišemo kot produkt samih transpozicij. Nato uporabimo prejšnji izrek.

Opomba: to velja samo za sode permutacije. Produkt 2 lihih permutacij je soda permutacija.

$$(2) \rho \in A_n \Rightarrow \rho^{-1} \in A_n$$

$$\begin{aligned}\rho &= \tau_1 \tau_2 \dots \tau_{k-1} \tau_k \\ \rho^{-1} &= \tau_k \tau_{k-1} \dots \tau_2 \tau_1\end{aligned}$$

kjer τ_i transpozicija in k je sodo.

$$\rho \rho^{-1} = \tau_k \tau_{k-1} \dots \tau_2 \tau_1 \tau_1 \tau_2 \dots \tau_{k-1} \tau_k$$

Ker je S_n grupa velja asociativnost, torej lahko začnemo v sredini: $\tau_1 \tau_1 = e$, nato $\tau_2 \tau_2 = e$ in tako naprej.

$A_n \subseteq S_n, e \in A_n$. Torej je A_n zaprta za množenje in zaprta za invertiranje. Zato je A_n grupa. Pravimo ji *alternirajoča grupa*.

Naj bo τ transpozicija, $\rho \in A_n \Rightarrow \tau \rho$ je liha

Naj bosta $\rho_1 \rho_2 \in A_n, \rho_1 \neq \rho_2$. Sledi $\tau \rho_1 \neq \tau \rho_2$.

$n > 1$ število lihih permutacij je enako številu sodih permutacij. Torej ima A_n $\frac{n!}{2}$ elementov.

DEFINIRAJMO podgrupo:

Naj bo (G, \cdot) grupa in $H \subseteq G, H \neq \emptyset$. H naj izpolnjuje pogoja:

$$(1) a, b \in H \Rightarrow ab \in H$$

Temu pravimo *zaprtost za množenje*

$$(2) a \in H \Rightarrow a^{-1} \in H$$

Temu pravimo *zaprtost za invertiranje*

Potem je H za operacijo iz G grupa.

$$\begin{aligned}a \in H &\stackrel{(2)}{\Rightarrow} a^{-1} \in H \\ a, a^{-1} \in H &\stackrel{(1)}{\Rightarrow} e = aa^{-1} \in H\end{aligned}$$

e enota grupa G leži v H in je enota v H . Pravimo, da je H *podgrupa* grupe G .

PRIMERI:

- (1) A_n je podgrupa S_n
- (2) G grupa, G je podgrupa v G .
 $\{e\}$ je *trivialna podgrupa* G
- (3) (G, \cdot) je grupa

$$\begin{aligned}
 a &\in G \\
 H &= \{a^m; m \in \mathbb{Z}\} \\
 H &= \{\dots, a^{-2}, a^{-1}, e, a, a^2, a^3, \dots\}
 \end{aligned}$$

H je najmanjša podgrupa grupe G , ki vsebuje a .

$$H \equiv \langle a \rangle$$

Recimo, da velja $a^{m_1} = a^{m_2}$ za celi števili $m_1 < m_2$.

$$\begin{aligned}
 a^m a^{-m_1} &= a^{m_2} a^{-m_1} = a^{m_2 - m_1} \\
 k &= m_2 - m_1 \in \mathbb{N}, k \geq 1 \\
 \exists k \in \mathbb{N} : a^k &= e
 \end{aligned}$$

Naj bo $k \in \mathbb{N}$ najmanjše naravno število, ki izpolnjuje pogoj $a^k = e$. Pona-
 vljal se bo vzorec:

$$e, a, a^2, \dots, a^{k-1}$$

in veja:

$$\begin{aligned}
 a^{k+1} &= a^k a = a \\
 a^{k+2} &= a^k a^2 = a^2
 \end{aligned}$$

$$H = \{e, a, a^2, \dots, a^{k-1}\}$$

H ima k elementov. Pravimo, da je H *ciklična grupa reda* k .

3.4 Ablove grupe

Pravimo jim tudi *komutativne grupe*.

$(G, +)$ je grupa in je komutativna:

$$\forall a, b \in G : a + b = b + a$$

PRIMERI: $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$

Naj bo (G, \cdot) grupa (ne nujno komutativna).

$$a \in G, \langle a \rangle = \{a^m : m \in \mathbb{Z}\}$$

$\langle a \rangle$ je abelova grupa:

$$a^i a^j = a^{i+j} = a^j a^i$$

Oznake v abelovi grupi:

- 0 -enota Abelove grupe
- $-a$ nasprotni element od a
- $\underbrace{a + a + \dots + a}_{n, n \in \mathbb{N}} \equiv na, n \in \mathbb{N}$
- $(-n)a \equiv -(na) = \underbrace{(-a) + (-a) + \dots + (-a)}_n, n \in \mathbb{N}$
- $0a \equiv 0$

Opomba: na levi strani je 0 število 0, na desni pa je enota grupe

- $a, b \in GG$

$$a - b \equiv a + (-b)$$

Naj bo $(G, +)$ Abelova grupa in $H \subseteq G, H \neq \emptyset, H$ podgrupa

$$(1) \ a, b \in H \Rightarrow a + b \in H$$

$$(2) \ a \in H \Rightarrow -a \in H$$

$$(1) \ \& \ (2) \iff (a, b \in H \Rightarrow a - b \in H)$$

PRIMER: $(G, +) = (\mathbb{Z}, +)$, $+$ je običajno seštevanje.

$$n \in \mathbb{N}$$

$$H = \{kn : k \in \mathbb{Z}\} = \{m \in \mathbb{Z} : n|m\}$$

H je podgrupa grupe $(\mathbb{Z}, +)$ in je množica večkratnikov n . Pišemo:

$$H \equiv n\mathbb{Z}$$

Naj bo $(G, +)$ Abelova grupa, $H \subseteq G$, H podgrupa.

$$a, b \in G : a \sim b \stackrel{\text{def}}{\iff} a - b \in H$$

\sim je ekvivalenčna relacija

(1) *refleksivnost*: $\forall a \in G : a \sim a$

$$a \sim a \iff \underbrace{a - a}_{\text{enota } H} \in H$$

(2) *simetričnost* $a \sim b \Rightarrow b \sim a$

$$a \sim b \Rightarrow a - b \in H \Rightarrow b - a = -(a - b) \in H$$

Dokazati je potrebno korak $b - a = -(a - b)$:

$$(b - a) + (a - b) = b + (-a) + a + (-b) = 0$$

(3) *tranzitivnost* $a \sim b \wedge b \sim c \Rightarrow a \sim c$

$$a - b \in H$$

$$b - c \in H$$

Po definiciji $a, b \in H : a + b \in H$, torej v našem primeru:

$$(a - b) + (b - c) = b - c \in H \Rightarrow a \sim c$$

□

Seštevanje in ekvivalenčna relacija \sim sta usklajeni: $x \sim a, y \sim b \Rightarrow x + y \sim a + b$

$$x - a \in H$$

$$y - b \in H$$

Po definiciji relacije potrebuje veljati: $(x + y) - (a + b) \in H$

$$(x + y) - (a + b) = \underbrace{x - a}_{\in H} + \underbrace{y - b}_{\in H} \in H$$

□

Zato lahko operacijo $+$ prenesemo na kvocientno množico:

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

$$\forall a, b \in G : [a] + [b] = [a + b]$$

$(G/\sim, +)$ je Abelova grupa

Opomba: $+$ je operacija med ekvivalenčnimi razredi in je različna od operacije med elementi

OZNAKA: G/H (namesto G/\sim , ker \sim definiramo s pomočjo H)

Komutativnost in asociativnost se hitro preveri. Za enoto vzamemo $[0]$. Nasprotni element definiramo kot $-[a] = [-a]$

Naj bo $(G, +)$ Abelova grupa in H njena podgrupa. Velja:

$$G/H = \{[q] : q \in G\}$$

$$[q] = \{x \in G : x - q \in H\} = \{q + h : h \in H\}$$

Uvedemo novi oznaki:

$$[q] \equiv q + H$$

$$[0] = H$$

PRIMER: $G = \mathbb{Z}$ z običajnim seštevanjem. Naj bo $n \in \mathbb{N}$; $H = n\mathbb{Z}$ podgrupa \mathbb{Z} . Ekvivalenčni razred torej zaznamujemo kot:

$$[m] = m + n\mathbb{Z}$$

Če si narišemo skico za npr. $n = 4$ opazimo, da je $[0] = [4]$ Torej je kvocientna grupa:

$$\mathbb{Z}/4\mathbb{Z} = \{[0], [1], [2], [3]\}$$

V splošnem zapišemo:

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}$$

To da je m v nekem ekvivalenčnem razredu, lahko povemo kot:

$$m \in [j], j \in 0, 1, \dots, n \iff m \text{ pri deljenju z } n \text{ da ostanek } j$$

Običajno skrajšamo zapis in pišemo:

$$[j] \equiv j$$

$$\mathbb{Z}/n\mathbb{Z} \equiv \mathbb{Z}_n$$

Pravimo, da je \mathbb{Z}_n grupa ostankov pri deljenju z n . To lahko narišemo v tabelo. Poglejmo si, kako bi izgledala tabela za grupo

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

Tabela 1: Tabela za \mathbb{Z}_4

+	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

3.5 Homomorfizmi

DEFINICIJA: Naj bosta $(G_1, \circ), (G_2, \circ)$ grupoida. Preslikava $f : G_1 \rightarrow G_2$ je *homomorfizem*, kadar velja:

$$\forall x, y \in G_1 : f(x \circ y) = f(x) \circ f(y)$$

Z besedami: “Slika kompozituma je kompozitum slik”.

Če je $G_2 = G_1$ in $f : G_1 \rightarrow G_2$ homomorfizem, potem je f *endomorfizem*.

DEFINICIJA: Preslikava $f : G_1 \rightarrow G_2$ je *izomorfizem*, kadar je f bijektivna in sta f ter f^{-1} homomorfizma.

TRDITEV: Bijektven homomorfizem je izomorfizem.

DOKAZ: Naj bo $f : G_1 \rightarrow G_2$ bijektiven homomorfizem, kjer sta G_1 in G_2 grupoida. Trdimo, da je $f^{-1} : G_2 \rightarrow G_1$ homomorfizem. Naj bosta $u, v \in G_2$. Ker je f surjektivna velja: $u = f(x)$ in $v = f(y)$. Torej lahko zapišemo:

$$f^{-1}(u \circ v) = f^{-1}(f(x) \circ f(y)) = f^{-1}(f(x \circ y)) = x \circ y = f^{-1}(u) \circ f^{-1}(v)$$

Zadnji enačaj velja, ker je f injektivna. □

PRIMERI:

(1) $f : \mathbb{Z} \rightarrow G$, (G, \circ) grupa, $a \in G$. Predpis f definiramo kot $f(m) = a^m$.

f je homomorfizem med grupama $(\mathbb{Z}, +)$ in (G, \circ)

$$f(m_1 + m_2) = a^{m_1+m_2} = a^{m_1}a^{m_2} = f(m_1)f(m_2)$$

G nadomestimo s podgrupo $\langle a \rangle = \{a^m, m \in \mathbb{Z}\}$ in ohranimo isti predpis:

$$f : \mathbb{Z} \rightarrow \langle a \rangle$$

f je surjektiven homomorfizem.

Opazimo, da je f izomorfizem natanko takrat, ko $\langle a \rangle$ ni končna:

$$a^{m_1} = a^{m_2} \Rightarrow m_1 = m_2$$

(2) $f : \mathbb{Z}_n \rightarrow C_n$ kjer:

$$C_n = \{z \in \mathbb{C} : z^n = 1\}$$

imamo $(C_n, \circ), (\mathbb{Z}_n, +)$. Predpis od f definiramo kot:

$$f(j) = z_0^j, z_0 = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

f je homomorfizem

$$f(j+k) = z_0^{j+k} = z_0^j z_0^k = f(j)f(k)$$

f je surjekcija in injekcija $\Rightarrow f$ je izomorfizem.

(3) $(\mathbb{R}, +), (\mathbb{R}^+, \circ)$, kjer:

$$\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$$

$$f : (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \circ)$$

$$\mathbb{R} \rightarrow \mathbb{R}^+$$

Predpis definiramo kot:

$$f(x) = 2^x$$

f je homomorfizem

$$f(x+y) = 2^{x+y} = 2^x 2^y = f(x)f(y)$$

f je bijekcija z inverzom:

$$f^{-1}(x) = \log_2 x$$

Torej je f izomorfizem.

TRDITEV: Kompozitum (dveh) homomorfizmov je homomorfizem. Kompozitum izomorfizmov je izomorfizem.

DOKAZ:

$$\begin{aligned}(f \circ g)(x \circ y) &= \\ &= f(g(x \circ y)) = f(g(x) \circ g(y)) = f(g(x)) \circ f(g(y)) = \\ &= (f \circ g)(x) \circ (f \circ g)(y)\end{aligned}$$

Naj bosta G_1, G_2 grupi z multiplikativnim zapisom in $f : G_1 \rightarrow G_2$ homomorfizem. Potem velja:

- (1) f enoto grupe G_1 preslika v enoto grupe G_2
- (2) $\text{im} f = \{f(x) : x \in G_1\}$ (zaloga vrednosti) je podgrupa v G_2 ³
- (3) $\ker f = \{x \in G_1 : f(x) = e_2\}$ (e_2 je enota grupe G_2) je podgrupa v G_1 ⁴

DOKAZ: e_1 enota G_1 , e_2 enota G_2

- (1) $f(e_1) = f(e_2)$

$$f(e_1) = f(e_1 e_1) = f(e_1) f(e_1)$$

Označimo

$$f(e_1) = x \in G_2$$

Dobili smo:

$$\begin{aligned}x &= xx \\ xx^{-1} &= (xx)x^{-1} = x(xx^{-1})\end{aligned}$$

Torej:

$$e_2 = x$$

Sklep: $f(e_1) = e_2$

□

- (2) $\text{im} f$ je podgrupa G_2

Naj bosta $u, v \in \text{im} f$. Velja:

$$\exists x, y \in G_1 : u = f(x), v = f(y)$$

³ $\text{im} f$ je slika (image) od f

⁴ $\ker f$ je jedro (kernel) od f

Velja:

$$uv = f(x)f(y) = f(xy)$$

Torej $uv \in \text{im} f$.

Podgrupa potrebuje tudi zaprtost za invertiranje:

$$\underline{u \in \text{im} f \Rightarrow u^{-1} \in \text{im} f}$$

$$u = f(x) \Rightarrow f(x^{-1}) = u^{-1}$$

To je potrebno še dokazati in naj bi bilo doma za vajo. Iz tega sledi:

$$u^{-1} \in \text{im} f$$

3.6 Kolobar

DEFINICIJA: Kolobar je množica K skupaj z operacijama $+$ in \cdot na K . ($+$ je seštevanje, \cdot je množenje), kadar je $(K, +)$ Abelova grupa, (K, \cdot) je podgrupa. Operaciji povezujeta distributivnostna zakona:

$$a(b + c) = ab + ac$$

$$(b + c)a = ba + ca$$

PRIMERI:

(1) Številski kolobarji $(+, \cdot)$ običajni operaciji

$$(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$$

(2) $\mathbb{Z}_n, n \in \mathbb{N}$ Kolobar ostankov pri deljenju z n

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$$

Množenje definiramo podobno kot seštevanje:

$$i, j \in \mathbb{Z}_n; ij = k - \text{ostanek pri deljenju običajnega produkta } ij \text{ z } n$$

Primer množenja v \mathbb{Z}_6 :

$$3 \cdot 5 = 3$$

$$3 \cdot 4 = 0$$

(3) $K = \mathbb{R}^2$

$$\oplus (x, y) + (u, v) = (x + u, y + v)$$

$$\odot (x, y) \cdot (u, v) = (xu, yv)$$

$(\mathbb{R}^2, +, \cdot)$ je kolobar.

(4) $K = \mathbb{R}^3$

$$\oplus (x, y, z) + (u, v, w) = (x + u, y + v, z + w)$$

$$\odot (x, y, z) \cdot (u, v, w) = (xu, xv + yw, zw)$$

$(\mathbb{R}^3, +, \cdot)$ je kolobar.

(5) $M \neq \emptyset, K = \{f : M \rightarrow R\} = \mathbb{R}^M$

$$\oplus (f + g)(x) = f(x) + g(x) \forall x \in M (f, g \in K)$$

$$\odot (f \cdot g)(x) = f(x) \cdot g(x) \forall x \in M (f, g \in K)$$

Opomba: Pravimo, da operaciji definiramo po točkah.

K je *kolobar z enoto* (ali enico) e , kadar je e enota za množenje.

$$\forall a \in K : ea = ae = a$$

K je *komutativen kolobar*, kadar je množenje komutativno.

$$\forall a, b \in K : ab = ba$$

PRIMERI: (nanašajo se na primere za kolobarje)

	ima enoto	komutativen
1	✓	✓
2	✓	✓
3	✗	✗
4	✗	✓
5	✓	✓

DEFINICIJA: Naj bo $(K, +, \cdot)$ kolobar in $a, b \in K \setminus \{0\}$. Če velja $ab = 0$, sta a in b *delitelja nič*. Pravimo, da je a *levi delitelj nič* in b *desni delitelj nič*.

DEFINICIJA: Kolobar z enoto (enko) 1 je *obseg*, kadar je $1 \neq 0$ in vsak $a \in K \setminus \{0\}$ obrnljiv (v polgrupi (K, \cdot)). S simbolnim zapisom je to:

$$\forall a \in K \setminus \{0\} \exists b \in K : ab = ba = 1$$

Posledica je, da je $(K \setminus \{0\}, +, \cdot)$ grupa.

PRIMERI:

- (1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ za običajna $+$ in \cdot .
- (2) \mathbb{Z}_n je obseg, kadar je n praštevilo.

Naj bo \mathcal{O} obseg in $a, b, c \in \mathcal{O}$. Linearne enačbe lahko rešujemo na naslednji način:

$$ax + b = c$$

predpostavimo $a \neq 0 \Rightarrow \exists a^{-1}$

$$\begin{aligned} ax &= c - b \\ a^{-1}ax &= a^{-1}(c - b) \\ x &= a^{-1}(c - b) \end{aligned}$$

Ker komutativnost ni obvezna, moramo biti pozorni iz katere smeri pomnožimo enačbo z a^{-1} .

DEFINICIJA: Naj bosta K_1 in K_2 kolobarja. Preslikava $f : K_1 \rightarrow K_2$ je homomorfizem kolobarjev, kadar za vse $a, b \in K_1$ velja:

$$\begin{aligned} f(a + b) &= f(a) + f(b) \\ f(ab) &= f(a)f(b) \end{aligned}$$

Če je $f : K_1 \rightarrow K_2$ bijektiven homomorfizem kolobarjev, je $f^{-1} : K_2 \rightarrow K_1$ homomorfizem kolobarjev. V tem primeru je f izomorfizem med kolobarjema K_1 in K_2 .

4 Vektorski prostori

DEFINICIJA: *Vektorski prostor* na obsegu \mathcal{O} je Abelova grupa $(V, +)$ skupaj z *zunanjjo operacijo*

$$\begin{aligned} \mathcal{O} \times V &\rightarrow V \\ (\alpha, v) &\mapsto \alpha v \end{aligned}$$

ki ustreza naslednjim pogojem:

1. $(\alpha + \beta)v = \alpha v + \beta v$ $\forall \alpha, \beta \in \mathcal{O}, \forall v \in V$
2. $\alpha(u + v) = \alpha u + \alpha v$ $\forall \alpha \in \mathcal{O}, \forall u, v \in V$
3. $\alpha(\beta v) = (\alpha\beta)v$ $\forall \alpha, \beta \in \mathcal{O}, \forall v \in V$
4. $1v = v$ $\forall v \in V$

Elemente iz \mathcal{O} imenujemo *skalarji*, elemente iz V imenujemo *vektorji*, zunanjo operacijo pa imenujemo *množenje z skalarji*.

PRIMER:

- (1) $V = \mathbb{R}^3, \mathcal{O} = \mathbb{R}$ običajen trirazsežen vektorski prostor
- (2) $V = \mathcal{O}^n, \mathcal{O}$ - obseg

Naj bosta x in y naslednja vektorja:

$$\begin{aligned} x &= (x_1, x_2, \dots, x_n) \in \mathcal{O}^n (x_i \in \mathcal{O} \forall i) \\ y &= (y_1, y_2, \dots, y_n) \in \mathcal{O}^n (y_i \in \mathcal{O} \forall i) \end{aligned}$$

Operaciji definiramo sledeče:

$$\begin{aligned} x + y &= (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n) \in \mathcal{O}^n \\ \alpha x &= (\alpha x_1, \alpha x_2, \dots, \alpha x_n) \in \mathcal{O}^n \end{aligned}$$

Za ti dve operaciji je \mathcal{O}^n vektorski prostor na obsegom \mathcal{O} . Ničelni element je

$$0 = (0, 0, \dots, 0) \in \mathcal{O}^n$$

Nasprotni element je:

$$-(x_1, x_2, \dots, x_n) = (-x_1, -x_2, \dots, -x_n) \in \mathcal{O}^n$$

- (3) $M \neq \emptyset \quad \mathcal{F}(M, \mathbb{R}) \equiv \mathbb{R}^M = \{f : M \rightarrow \mathbb{R}\}$

Operaciji definiramo po točkah:

$$\begin{aligned} (\alpha f)(t) &= \alpha f(t) & \forall t \in M (\alpha \in \mathbb{R}) \\ (f + g)(t) &= f(t) + g(t) & \forall t \in M \end{aligned}$$

$$V = \mathbb{R}^M, \mathcal{O} = \mathbb{R}$$

V je vektorski prostor nad \mathbb{R} .

4.1 Nekaj osnovnih lastnosti vektorskih prostorov

Naj bo V vektorski prostor nad \mathcal{O} . Velja:

$$(1) \quad 0v = 0 \qquad \qquad \qquad \forall v \in V$$

$$(2) \quad \alpha 0 = 0 \qquad \qquad \qquad \forall \alpha \in \mathcal{O}$$

$$(3) \quad \alpha v = 0 \Rightarrow (\alpha = 0 \vee v = 0)$$

$$(4) \quad (-1)v = -v \qquad \qquad \qquad \forall v \in V$$

DOKAZ:

(1)

$$\begin{aligned} 0v = x \in V &\Rightarrow \\ x + x &= 0v + 0v = (0 + 0)v = 0v = x \\ &\Rightarrow x + x = x \Rightarrow x = 0 \\ &\Rightarrow 0v = 0 \end{aligned}$$

(2) Podoben dokaz kot za (1).

(3) $\alpha v = 0$. Če $\alpha = 0$ optem velja (2). Drugače:

$$\begin{aligned} \alpha \neq 0 &\Rightarrow \exists \alpha^{-1} \in \mathcal{O} \Rightarrow \\ &\Rightarrow \alpha^{-1}(\alpha v) = \alpha^{-1}0 = 0 \\ &\quad \underbrace{(\alpha^{-1}\alpha)}_1 v = 1v = v \\ &\Rightarrow v = 0 \end{aligned}$$

(4)

$$(-1)v + v = (-1)v + 1v = (-1 + 1)v = 0v = 0$$

4.2 Vektorski podprostor

DEFINICIJA: Naj bo V vektorski prostor nad \mathcal{O} in $U \subseteq V, U \neq \emptyset$. U je vektorski poprostor vektorskega prostora V , kadar velja:

$$(1) \ x, y \in U \Rightarrow x + y \in U$$

$$(2) \ x \in U \Rightarrow \alpha x \in U \qquad \forall \alpha \in \mathcal{O}$$

Obe zahtevi lahko združimo v eno:

$$(1) \wedge (2) \iff (x, y \in U \Rightarrow \forall \alpha, \beta \in U : \alpha x + \beta y \in U)$$

$(U, +)$ je podgrupa grupe $(V, +)$.

PRIMERI:

$$(1) \ V = \mathbb{R}^3, \ U \text{ je ravnina skozi } 0 \text{ v } \mathbb{R}^3$$

$$(2)$$

$$\begin{aligned} V &= \mathbb{R}^3 \\ U &= \mathbb{R}[x] \end{aligned}$$

$$(3)$$

$$\begin{aligned} V &= \mathbb{R}[x] \\ U &= \mathbb{R}_m[x] = \{p(x) \in \mathbb{R}[x] : \text{stp}(x) \leq m\} \end{aligned}$$

Če je V vektorski prostor nad \mathcal{O} in $U \subseteq V$ podprostor, uporabljamo oznako:

$$U \leq V$$

Vsak podprostor vsebuje ničlo:

$$x \in U \Rightarrow 0x = 0 \in U$$

Nasprotni element je element podprostora:

$$x, y \in U \Rightarrow x - y = x + (-1) \in U$$

Ker velja $\alpha x \in U$ in $\beta y \in U$, lahko zapišemo:

$$\alpha x + \beta y \in U$$

Zapišemo lahko:

$$x_1, x_2, \dots, x_k \in U \Rightarrow \underbrace{\alpha x_1 + \alpha x_2 + \dots + \alpha x_k}_{\text{linearna kombinacija vektorjev } x_1, \dots, x_k} \in U$$

4.3 Linearna ogrinjača

DEFINICIJA: Naj bo $M \in V, M \neq \emptyset$. *Linearno ogrinjača množice* M je

$$\text{Lin}M = \{\alpha_1 x_1 + \dots + \alpha_k x_k : x_1, \dots, x_k \in M, \alpha_1, \dots, \alpha_k \in \mathcal{O}, k \in \mathbb{N}\}$$

Velja:

$$M \subseteq U \leq V \Rightarrow \text{Lin}M \subseteq U$$

LinM je vektorski podprostor vektorskega prostora V ($\text{Lin}M \leq V$)

- Zaprtost za seštevanje:

$$\alpha_1 x_1 + \dots + \alpha_k x_k \in \text{Lin}M$$

$$\beta_1 x_1 + \dots + \beta_n y_n \in \text{Lin}M$$

Opazimo, da so po definiciji $\text{Lin}M$ posamečni členi $\alpha_1 x_1, \dots, \alpha_k x_k \in \text{Lin}M$ in $\beta_1 y_1, \dots, \beta_n y_n \in \text{Lin}M$, torej je tudi vsota vseh členov $\in \text{Lin}M$.

- Zaprtost za množenje s skalarjem:

$$\begin{aligned} \beta(\alpha_1 x_1 + \dots + \alpha_k x_k) &= (\beta \alpha_1) x_1 + \dots + (\beta \alpha_k) x_k \in \text{Lin}M \\ x_1, \dots, x_k &\in M \end{aligned}$$

□

Iz tega sledi, da je $\text{Lin}M$ najmanjši vektorski podprostor, ki vsebuje M . Simbolno za malo naprednejše:

$$M \subseteq U \leq V \Rightarrow \text{Lin}M \subseteq U$$

Za prazno množico velja:

$$\text{Lin}\emptyset = \{0\}$$

Poglejmo si, kako je s preseki in unijami. Za preseke velja:

$$V_i \leq V \forall i \in I \Rightarrow \bigcap_{i \in I} V_i \leq V$$

To je očitno. Zaprtost za seštevanje velja, ker če sta neka dva vektorja x, y v $\bigcap_{i \in I} V_i$, potem se nahajata v vseh V_i . Ker so V_i vektorski podprostori, v njih tudi velja zaprtost za seštevanje. Zato je vsota $x + y$ tudi v vseh V_i ,

torej je tudi v $\bigcap_{i \in I} V_i$. Podobno lahko naredimo za zaprtost za množenje s skalarjem.

Malo več je za videti pri uniji. $V_1, V_2 \leq V \Rightarrow \text{Lin}(V_1 \cup V_2)$ je najmanjši vektorski podprostor, ki vsebuje V_1 in V_2 . Primer na katerem se lahko predstavljamo, sta dve premici. Unija dveh premic, ki se sekata ni vektorski podprostor, zato okoli naredimo linearno ogrinjačo. Poglejmo si eno zanimivost:

$$x \in \text{Lin}(V_1 \cup V_2)$$

$$x = \underbrace{\alpha_1 x_1 + \dots + \alpha_k x_k}_{\in V_1} + \underbrace{\beta_1 y_1 + \dots + \beta_n y_n}_{\in V_2} = u + v$$

Torej velja:

$$x \in \text{Lin}(V_1 \cup V_2) \iff x = u + v, u \in V_1, v \in V_2$$

Zapišemo:

$$V_1 + V_2 = \{u + v : u \in V_1, v \in V_2\}$$

Torej velja:

$$\text{Lin}(V_1 \cup V_2) = V_1 + V_2$$

Analogno naredimo za več sumandov:

$$\text{Lin}(V_1 \cup V_2 \cup \dots \cup V_k) = V_1 + V_2 + \dots + V_k$$

$$V_i \leq V \forall i$$

$$V_1 + \dots + V_k = \{x_1 + \dots + x_k : x_i \in V_i \forall i\}$$

DEFINICIJA: $V_1 + \dots + V_k$ je *prema* ali *direktna*, kadar za vsak $x \in V_1 + \dots + V_k$ obstajajo in so z x enolično določeni taki vektorji $x_i \in V_i (i = 1, \dots, k)$, da je $x = x_1 + \dots + x_k$. Ozaničimo:

$$V_1 \oplus \dots \oplus V_k$$