

# Algebra 1

Vid Drobnič

# Kazalo

<b>1</b>	<b>Vektorji v trirazsežnem prostoru</b>	<b>3</b>
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
<b>2</b>	<b>Analitična geomterija v <math>\mathbb{R}^3</math></b>	<b>14</b>
2.1	Premica . . . . .	14
2.2	Ravnina . . . . .	15
2.3	Razdalja med mimobežnima premicama . . . . .	17
<b>3</b>	<b>Osnovne algebrske strukture</b>	<b>18</b>
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
<b>4</b>	<b>Vektorski prostori</b>	<b>42</b>
4.1	Nekaj osnovnih lastnosti vektorskih prostorov . . . . .	44
4.2	Vektorski podprostor . . . . .	44

4.3	Linearna ogrinjača . . . . .	46
4.4	Kvocietni vektorski prostor . . . . .	48
4.5	Linearne preslikave . . . . .	49
4.5.1	Slika in jedro linearnih preslikav . . . . .	50
4.6	Vektorski prostor linearnih preslikav . . . . .	52
4.7	Končno razsežni vektorski prostori . . . . .	54
4.8	Linearne preslikave na končno razsežnih V.P. . . . .	63
4.8.1	Poseben primer . . . . .	64
4.8.2	Splošna situacija . . . . .	67
4.8.3	Množenje matrik . . . . .	69
4.8.4	Poseben primer . . . . .	69
4.8.5	Rang linearne preslikave in matrike . . . . .	70
4.8.6	Sistemi linearnih enačb . . . . .	75
4.8.7	Gaussov algoritem za reševanje sistema . . . . .	77
4.8.8	Simultano reševanje sistemov z isto matriko koeficientov . . . . .	79
4.8.9	Sprememba baze . . . . .	79
4.8.10	Ekivalentnost matrik . . . . .	81
4.8.11	Podobnost matrik . . . . .	83
4.8.12	Diagonalne matrike in diagonalizacija . . . . .	84
4.8.13	Iskanje lastnih vrednosti in lastnih vektorjev . . . . .	86

# 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:<sup>1</sup>

- (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  $\alpha < 0$
- $|\alpha\vec{a}| = |\alpha||\vec{a}|$

---

<sup>1</sup>Dokaz 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  $\alpha$  in  $\beta$  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  $\alpha, \beta, \gamma$  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  $(\alpha, \beta, \gamma)$  je s točko  $R$  enolično določena.

$\alpha, \beta, \gamma$  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

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

$\varphi$  je bijekcija.

S  $\varphi$  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**<sup>2</sup> 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:

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

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

---

<sup>2</sup>Prej 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 orientacija  $(\vec{a}, \vec{b})$  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  $\vec{b}$   
 $\delta$  - 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

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

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

$$\vec{e} \perp \vec{c}$$

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

$$\vec{e} \cdot \vec{c} = 0$$

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

$$\beta = \lambda \vec{a}\vec{c}$$

$$\alpha = -\lambda \vec{b}\vec{c}$$

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

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

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) ( $\lambda$  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  $\Sigma$ , 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  $\Sigma$  določa enačba:

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

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

$$\begin{aligned}\vec{r}_0 &= (x_0, y_0, z_0) \\ \vec{r} &= (x, y, z) \\ \vec{n} &= (a, b, c)\end{aligned}$$

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  $\Sigma$  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  $\Sigma$  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  $\Sigma_1$ , ki jo tvorita ta dva vektorja. Nato naredimo ravnino  $\Sigma_2$  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  $\Sigma_1$  v  $\Sigma_2$  in dobimo premico  $p_1^*$ , ki se seka s premico  $p_2$  v točko  $S_2$ . Podobno lahko premaknemo premico  $p_2$  v ravnino  $\Sigma_1$  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.

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

(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  $\sim$ :

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

### 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  $\pi$  dobimo:

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

Pravimo, da je  $\pi$  *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  $\pi$  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  $j, k \in \{1, \dots, n\}, j \neq k$

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

$\tau$  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  $\pi$  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  $\pi$ , 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  $\pi$  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:

$$\pi \text{ je soda} \iff s(\pi) = 1$$

$$\pi \text{ je liha} \iff s(\pi) = -1$$

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

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

DOKAZ:

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

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

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

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

$\tau$  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  $\tau_i$  transpozicije.

Potem je  $\pi$  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  $A_n = \{\pi \in S_n : \pi \text{ soda}\}$ ,  $e \in A_n$

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

$\rho, \sigma$  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  $\tau_i$  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  $\tau$  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:

$$\begin{aligned} G/\sim &= \{[a] : a \in G\} \\ \forall a, b \in G : [a] + [b] &= [a + b] \end{aligned}$$

$(G/\sim, +)$  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:

$$\begin{aligned} G/H &= \{[q] : q \in G\} \\ [q] &= \{x \in G : x - q \in H\} = \{q + h : h \in H\} \end{aligned}$$

Uvedemo novi oznaki:

$$\begin{aligned} [q] &\equiv q + H \\ [0] &= H \end{aligned}$$

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:

$$\begin{aligned} [j] &\equiv j \\ \mathbb{Z}/n\mathbb{Z} &\equiv \mathbb{Z}_n \end{aligned}$$

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  $G_2$ <sup>3</sup>
- (3)  $\ker f = \{x \in G_1 : f(x) = e_2\}$  ( $e_2$  je enota grupe  $G_2$ ) je podgrupa v  $G_1$ <sup>4</sup>

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:

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

---

<sup>3</sup> $\text{im} f$  je slika (image) od  $f$

<sup>4</sup> $\ker f$  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 *zunanjo 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:

$$x = (x_1, x_2, \dots, x_n) \in \mathcal{O}^n (x_i \in \mathcal{O} \forall i)$$

$$y = (y_1, y_2, \dots, y_n) \in \mathcal{O}^n (y_i \in \mathcal{O} \forall i)$$

Operaciji definiramo sledeče:

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

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

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:

$$(\alpha f)(t) = \alpha f(t) \quad \forall t \in M (\alpha \in \mathbb{R})$$

$$(f + g)(t) = f(t) + g(t) \quad \forall t \in M$$

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

$V$  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:

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

TRDITEV: Vsota  $V_1 + V_2$  vektorskih podprostorov  $V_1$  in  $V_2$  je direktna natanko takrat, kadar je  $V_1 \cap V_2 = \{0\}$ .

DOKAZ:

( $\Rightarrow$ ) Naj bo vsota  $V_1 + V_2$  direktna ( $V_1 \oplus V_2$ ). Vzemimo  $x \in V_1 \cup V_2$ .

$$x = \underbrace{x}_{\in V_1} + \underbrace{0}_{\in V_2} = \underbrace{0}_{\in V_1} + \underbrace{x}_{\in V_2} \Rightarrow x = 0$$

$$\Rightarrow V_1 \cup V_2 = \{0\}$$



( $\Leftarrow$ ) Naj bo  $V_1 \cup V_2 = \{0\}$ .

$$\begin{aligned}
x &\in V_1 + V_2 \\
x &= x_1 + x_2, x_1 \in V_1, x_2 \in V_2 \\
x &= x'_1 + x'_2, x'_1 \in V_1, x'_2 \in V_2 \\
x_1 + x_2 &= x'_1 + x'_2 \\
\underbrace{x_1 - x'_1}_{\in V_1} &= \underbrace{x_2 - x'_2}_{\in V_2} = z
\end{aligned}$$

$$\Rightarrow z \in V_1 \cap V_2 = \{0\}$$

$$\Rightarrow x = 0 \Rightarrow$$

$$\Rightarrow x'_1 = x_1 \wedge x'_2 = x_2$$

$$V_1 \oplus V_2$$

□

## 4.4 Kvocientni vektorski prostor

Naj bo  $U$  vektorski prostor nad  $\mathcal{O}$ ,  $U \leq V$ . Definiramo:

$$v_1 \sim v_2 \iff v_1 - v_2 \in U$$

kjer je  $\sim$  ekvivalenčna relacija.  $U$  je Abelova podgrupa Abelove grupe  $V$ .  $V/U$  je torej Abelova grupa in velja:

$$\begin{aligned}
[x] + [y] &= [x + y] \forall x, y \in V \\
[z] &= z + U \forall z \in V
\end{aligned}$$

V  $V/U$  uvedemo množenje s skalarji:

$$\alpha[x] := [\alpha x], \alpha \in \mathcal{O}, x \in V$$

Definicija je dobra če velja:

$$\begin{aligned}
y \sim x &\Rightarrow \alpha x \sim \alpha y \\
y - x \in U &\Rightarrow \underbrace{\alpha y - \alpha x}_{\alpha(y-x)=z} \in U
\end{aligned}$$

Ker je  $U$  podprostor zaprt za množenje s skalarjem, vemo:

$$z \in U \Rightarrow \alpha z \in U \forall \alpha \in \mathcal{O}$$

□

Sledi, da je  $V/U$  vektorski prostor nad  $\mathcal{O}$ . Elementi so  $x + U, x \in V$ .

PRIMER:  $U$  premica skozi 0 v  $V = \mathbb{R}^3$ . Elementi  $V/U : x + U, x \in \mathbb{R}^3$  so premice vzporedne premici  $U$ .

## 4.5 Linearne preslikave

So neke vrste homomorfizmi vektorskih prostorov.

DEFINICIJA: Naj bosta  $V$  in  $U$  vektorska prostora nad istim  $\mathcal{O}$ . Preslikava  $\mathcal{A} : V \rightarrow U$  je *linear* (= homomorfizem vektorskih prostorov), kadar velja:

$$(1) \quad \mathcal{A}(x + y) = \mathcal{A}x + \mathcal{A}y \quad \forall x, y \in V$$

$$(2) \quad \mathcal{A}(\alpha x) = \alpha \mathcal{A}x \quad \forall \alpha \in \mathcal{O}, \forall x \in V$$

Pogoju (1) pravimo, da je  $\mathcal{A}$  *aditivna*, pogoju (2) pa pravimo, da je  $\mathcal{A}$  *homogena*.

**Nekaj lastnosti:**

- $\mathcal{A}0 = 0$  (pride iz Abelove grupe)
- $\mathcal{A}(-x) = -\mathcal{A}x$  (pride iz Abelove grupe)  $\forall x \in V$
- $\mathcal{A}(x - y) = \mathcal{A}x - \mathcal{A}y$   $\forall x, y \in V$

$$(3) \quad \mathcal{A}(\alpha x + \beta y) = \mathcal{A}(\alpha x) + \mathcal{A}(\beta y) = \alpha \mathcal{A}x + \beta \mathcal{A}y \quad \forall x, y \in V, \forall \alpha, \beta \in \mathcal{O}$$

$$\mathcal{A}(\alpha x + \beta y) = \alpha \mathcal{A}x + \beta \mathcal{A}y$$

Ta lastnost sledi iz pogojev (1) in (2). Iz te lastnosti lahko dobimo nazaj pogoj (1) in (2).

$$((1) \wedge (2)) \iff (3)$$

SPLOŠNO:

$$\mathcal{A}(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n) = \alpha_1 \mathcal{A}x_1 + \alpha_2 \mathcal{A}x_2 + \cdots + \alpha_n \mathcal{A}x_n$$

DEFINICIJA:  $\mathcal{A}V \rightarrow U$  je *izomorfizem* vektorskega prostora, kadar je  $\mathcal{A}$  bijektivna in sta  $\mathcal{A}$  in  $\mathcal{A}^{-1}$  linearni preslikavi. **Velja:** bijektivna linearna preslikava je izomorfizem vektorskega prostora.

Naj bo  $\mathcal{A} : V \rightarrow U$  linearna bijekcija.  $\mathcal{A}^{-1} : U \rightarrow V$  je linearna

Aditivnost sledi iz dejstva, da je  $\mathcal{A}$  izomorfizem Abelovih grup  $(V, +)$ ,  $(U, +)$ .

$$\mathcal{A}^{-1}(\alpha u) = \mathcal{A}^{-1}(\alpha \mathcal{A}v) = \mathcal{A}^{-1}(\mathcal{A}(\alpha v)) = \alpha v = \alpha \mathcal{A}^{-1}u$$

kjer upoštevamo, da  $\exists v \in V : u = \mathcal{A}v$  ( $v = \mathcal{A}^{-1}u$ )

$\Rightarrow \mathcal{A}^{-1}$  je homogena

□

PRIMERI:

(1)  $V = U = \mathbb{R}^3$

- $\mathcal{A} : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  pravokotna projekcija na ravnino skozi 0.
- $\mathcal{A} : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  zasuk za določen kot okrog dane osi skozi 0.

(2)  $\mathcal{A} : \mathbb{R}[x] \rightarrow \mathbb{R}[x]$ ,  $\mathcal{A}$  odvajanje.

(3)  $\mathcal{A} : \mathbb{R}[x] \rightarrow \mathbb{R}$ ,  $\mathcal{A}$  je določeno integriranje.

#### 4.5.1 Slika in jedro linearnih preslikav

DEFINICIJA: Naj bo  $\mathcal{A} : V \rightarrow U$  linearna preslikava. Definiramo:

- $\text{im}\mathcal{A} = \{\mathcal{A}x : x \in V\}$  slika preslikave  $\mathcal{A}$
- $\text{ker}\mathcal{A} = \{x \in V : \mathcal{A}x = 0\}$  jedro preslikave  $\mathcal{A}$

VELJA:  $\text{im}\mathcal{A} \leq U$  in  $\text{ker}\mathcal{A} \leq V$

DOKAZ: za  $\text{im}\mathcal{A}$ :  $u_1, u_2 \in \text{im}\mathcal{A} \Rightarrow \alpha_1 u_1 + \alpha_2 u_2 \in \text{im}\mathcal{A}$

$$\exists x_1, x_2 \in V : u_1 = \mathcal{A}x_1, u_2 = \mathcal{A}x_2$$

$$\alpha_1 u_1 + \alpha_2 u_2 = \alpha_1 \mathcal{A}x_1 + \alpha_2 \mathcal{A}x_2 = \mathcal{A}(\alpha_1 x_1 + \alpha_2 x_2) \in \text{im}\mathcal{A}$$

DEFINICIJA: Naj bo  $\mathcal{A} : V \rightarrow U$ . Velja:

(1)  $\mathcal{A}$  je surjektivna  $\iff \text{im}\mathcal{A} = U$

(2)  $\mathcal{A}$  je injektivna  $\iff \ker \mathcal{A} = \{0\}$

DOKAZ za (2):

( $\Rightarrow$ )  $\mathcal{A}$  je injektivna. Vemo  $\mathcal{A}0 = 0$ . Zanima nas, za katere  $x$  velja  $\mathcal{A}x = 0$ .  
 $\ker$  je injektivna je  $x = 0 \Rightarrow \ker \mathcal{A} = \{0\}$ .

( $\Leftarrow$ )  $\ker \mathcal{A} = \{0\}$  Naj bosta  $\mathcal{A}x = \mathcal{A}y$ ,  $x, y \in V$ .

$$\begin{aligned} &\Rightarrow \underbrace{\mathcal{A}x - \mathcal{A}y}_{\mathcal{A}(x-y)=0} = 0 \\ &\Rightarrow x - y \in \ker \mathcal{A} = \{0\} \\ &\Rightarrow x - y = 0 \Rightarrow x = y \end{aligned}$$

□

IZREK: Naj bo  $\mathcal{A} : V \rightarrow U$  linearna preslikava. Potem obstaja izomorfizem med vektorskima prostoroma  $V/\ker \mathcal{A}$  in  $\text{im}\mathcal{A}$ . Izomorfizem deluje s predpisom:

$$\hat{\mathcal{A}} : [x] \mapsto \mathcal{A}x$$

DOKAZ:

- Predpis je dober t.j.:  $[x] = [y] \Rightarrow \mathcal{A}x = \mathcal{A}y$ .

$$x \sim y \Rightarrow x - y \in \ker \mathcal{A} \Rightarrow \underbrace{\mathcal{A}(x - y)}_{\mathcal{A}x - \mathcal{A}y = 0} = 0 \Rightarrow \mathcal{A}x = \mathcal{A}y$$

- $\hat{\mathcal{A}}$  je linearna

$$\begin{aligned} \hat{\mathcal{A}}(\underbrace{\alpha[x]}_{[\alpha x]} + \underbrace{\beta[y]}_{[\beta y]}) &= \\ &= \hat{\mathcal{A}}(\alpha x + \beta y) = \mathcal{A}(\alpha x + \beta y) = \alpha \mathcal{A}x + \beta \mathcal{A}y = \\ &= \alpha \hat{\mathcal{A}}([x]) + \beta \hat{\mathcal{A}}([y]) \end{aligned}$$

- $\hat{\mathcal{A}}$  je surjektivna – sledi neposredno iz definicije  $\hat{\mathcal{A}}$

- $\hat{\mathcal{A}}$  je injektivna

$$\begin{aligned} \underbrace{\hat{\mathcal{A}}([x])}_{\mathcal{A}x} &= \underbrace{\hat{\mathcal{A}}([y])}_{\mathcal{A}y} \\ \Rightarrow \mathcal{A}(x - y) &= \mathcal{A}x - \mathcal{A}y = 0 \\ \Rightarrow x - y &\in \ker \mathcal{A} \Rightarrow \\ \Rightarrow x \sim y &\Rightarrow [x] = [y] \end{aligned}$$

$\Rightarrow \hat{\mathcal{A}}$  je linearne in bijektivna  $\Rightarrow \hat{\mathcal{A}} : V/\ker \mathcal{A} \rightarrow \text{im} \mathcal{A}$  je izomorfizem vektorskih prostorov.  $\square$

POSLEDICI: Naj bo  $\mathcal{A} : V \rightarrow U$  linearna preslikava

- (1) Če je  $\mathcal{A}$  surjektivna, je vektorski prostor  $V/\ker \mathcal{A}$  izomorfen  $U$ .
- (2) Če je  $\mathcal{A}$  injektivna, je vektorski prostor  $V$  izomorfen vektorskemu prostoru  $\text{im} \mathcal{A}$

$$\mathcal{A} \text{ injektivna} \Rightarrow \ker \mathcal{A} = \{0\} \Rightarrow V/\{0\} = V$$

## 4.6 Vektorski prostor linearnih preslikav

$V, U$  naj bosta vektorska prostora nad komutativnim obsegom  $\mathcal{O}$ .

$$\mathcal{L}(V, U) = \{\mathcal{A} : V \rightarrow U; \mathcal{A} \text{ je linearna}\}$$

Ničelna preslikava  $0$  je element te množice  $0 \in \mathcal{L}(V, U)$ .

V  $\mathcal{L}(V, U)$  uvedemo operavijo  $+$  (seštevanje) po točkah:

$$\begin{aligned} \mathcal{A}, \mathcal{B} &\in \mathcal{L}(V, U) \\ (\mathcal{A} + \mathcal{B})(x) &= \mathcal{A}x + \mathcal{B}x, \forall x \in V \end{aligned}$$

Velja  $\mathcal{A} + \mathcal{B} \in \mathcal{L}(V, U)$ . Preverimo homogenost (aditivnost za DN):

$$(\mathcal{A} + \mathcal{B})(\alpha x) = \alpha \mathcal{A}x + \alpha \mathcal{B}x = \alpha(\mathcal{A}x + \mathcal{B}x) = \alpha((\mathcal{A} + \mathcal{B})x)$$

VELJA:

- $(\mathcal{L}(V, U), +)$  je Abelova grupa

- 0 (ničelna preslikava) je ničelni element
- $\mathcal{A} \in \mathcal{L}(V, U); -\mathcal{A} = -\mathcal{A}x \forall x \in V$

$$\begin{aligned} (-\mathcal{A})x &= -\mathcal{A}x, \forall x \in V \\ (\mathcal{A} + (-\mathcal{A}))x &= \mathcal{A}x + (-\mathcal{A})x = \mathcal{A}x + (-\mathcal{A})x = 0(\in U), \forall x \in V \\ &\Rightarrow \mathcal{A} + (-\mathcal{A}) = 0 \end{aligned}$$

**Množenje s skalarji** definiramo po točkah:

$$\begin{aligned} (\alpha A)x &= \alpha(Ax), \forall x \in V, \alpha \in \mathcal{O} \\ \mathcal{A} \in \mathcal{L}(V, U) &\Rightarrow \alpha A \in \mathcal{L}(V, U) \end{aligned}$$

$\mathcal{L}(V, U)$  postane z obema operacijama vektorski prostor nad  $\mathcal{O}$ . **Poseben primer**  $U = V$

$\mathcal{L}(V, V) \equiv \mathcal{L}(V)$  – množica vseh endomorfizmov vektorskega prostora  $V$ . V množico  $\mathcal{L}(V)$  uvedemo že množenje (= komponiranje preslikav).

$$\begin{aligned} \mathcal{A}, \mathcal{B} &\in \mathcal{L}(V) \\ (\mathcal{AB})x &= A(Bx), \forall x \in V \end{aligned}$$

Množenje je operacija na  $\mathcal{L}(V) : \mathcal{A}, \mathcal{B} \in \mathcal{L}(V) \Rightarrow \mathcal{AB} \in \mathcal{L}(V)$ .

$(\mathcal{L}(V), \cdot)$  je polgrupa (množenje je asociativno) in velja

- $\mathcal{A}(\mathcal{B} + \mathcal{C}) = \mathcal{AB} + \mathcal{AC}$
- $(\mathcal{B} + \mathcal{C})\mathcal{A} = \mathcal{BA} + \mathcal{CA}$

$(\mathcal{L}(V), +, \cdot)$  je kolobar. Velja še:

$$(\alpha\mathcal{A})(\beta\mathcal{B}) = (\alpha\beta)(\mathcal{AB})$$

Pravimo, da je  $\mathcal{L}(V)$  *algebra* nad  $\mathcal{O}$ .

DEFINICIJA:  $\mathcal{A}$  je *algebra* nad komutativnim obsegom  $\mathcal{O}$ , kadar je  $\mathcal{A}$  vektorski prostor nad  $\mathcal{O}$ , v katerem je dano množenje

$$\mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A} \quad ((a, b) \mapsto ab)$$

ki ustreza pogojem:

- $(\mathcal{A}, +, \cdot)$  je kolobar
- $(\alpha a)(\beta b) = (\alpha\beta)(ab) \quad \forall \alpha, \beta \in \mathcal{O}, \quad \forall a, b \in \mathcal{A}$

PRIMERI:

- (1)  $\mathcal{L}(V)$  je algebra
- (2)  $(\mathbb{R}^M) \equiv \mathcal{F}(M, \mathbb{R})$  za operacije definirane po točkah je algebra
- (3)  $\mathbb{R}[x]$  algebra polinomov z realnimi koeficienti, kjer so operacije definirane po točkah

$id_V \in \mathcal{L}(V)$  je enota algebre  $\mathcal{L}(V)$

$$id_V(x) = x \quad \forall x \in V$$

## 4.7 Končno razsežni vektorski prostori

DEFINICIJA: Naj bo  $V$  vektorski prostor nad  $\mathcal{O}$  in  $M \subseteq V$ .  $M$  je *ogrodje* vektorskega prostora  $V$ , kadar velja  $\text{Lin}M = V$

$M \neq \emptyset$  je ogrodje vektorskega prostora  $V$ , kadar za vsak  $x \in V$  velja

$$\exists v_1, \dots, v_m \in M, \alpha_1, \dots, \alpha_m \in \mathcal{O} : x = \alpha_1 v_1 + \dots + \alpha_m v_m$$

DEFINICIJA: Vektorski prostor  $V$  je *končno razsežen*, kadar ima kakšno končno ogrodje.

$$M = \{v_1, \dots, v_m\} \text{ ogrodje v.p. } V$$

$$x \in V \Rightarrow x = \alpha_1 v_1 + \dots + \alpha_m v_m, \quad \alpha_1, \dots, \alpha_m \in \mathcal{O}$$

Poglejmo si kako je z enolišnostjo zapisa. Naj bo

$$0 = 0v_1 + 0v_2 + \dots + 0v_m$$

$$0 = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m$$

Če je zapis enoličen, velja sklep

$$\alpha_1 v_1 + \dots + \alpha_m v_m = 0 \Rightarrow \alpha_1 = \dots = \alpha_m = 0$$

Poglejmo si še, kako je v obratno smer. Naj velja prejšnji sklep

$$\begin{aligned}x &= \alpha_1 v_1 + \cdots + \alpha_m v_m \\x &= \beta_1 v_1 + \cdots + \beta_m v_m \\ \Rightarrow (\alpha_1 - \beta_1)v_1 + \cdots + (\alpha_m - \beta_m)v_m &= 0 \\ \Rightarrow \alpha_1 - \beta_1 = \cdots = \alpha_m - \beta_m &= 0 \\ \Rightarrow \beta_j = \alpha_j \quad \forall j = 1, \dots, m\end{aligned}$$

Torej velja enoličnost zapisa.

DEFINICIJA: Vektorji  $v_1, \dots, v_m$  so *linearno neodvisni*, kadar velja sklep

$$\alpha_1 v_1 + \cdots + \alpha_m v_m = 0 \Rightarrow \alpha_1 = \cdots = \alpha_m = 0$$

Če je  $M = \{v_1, \dots, v_m\}$  ogrodje vektorskega prostora  $V$ , potem vsak  $x \in V$  lahko zapišemo v obliki  $x = \alpha_1 v_1 + \cdots + \alpha_m v_m$ , pri čemer so  $\alpha_1, \dots, \alpha_m$  enolično določeni z  $x$  natanko takrat, kadar so  $v_1, \dots, v_m$  linearno neodvisni.

Če so  $v_1, \dots, v_m$  linearno neodvisni, potem so različni ( $i \neq j \Rightarrow v_i \neq v_j$ ). Naj bo  $v_1 = v_2$ . Zapišemo lahko:

$$\underbrace{1}_{\neq 0} v_1 + \underbrace{(-1)}_{\neq 0} v_2 + 0v_3 + \cdots + 0v_m = 0$$

$\Rightarrow$  vektorji niso neodvisni.

DEFINICIJA: Naj bo  $M \subseteq V$ .  $M$  je linearno neodvisna, kadar je vsaka njena končna podmnožica linearno neodvisna.

DEFINICIJA: Naj bo  $M \subseteq V$ .  $M$  je *baza* vektorskega prostora  $V$ , kadar je linearno neodvisna in hkrati ogrodje vektorskega prostora  $V$ .

PRIMERI:

1) Baze v  $\mathbb{R}^3$  so oblike  $\{\vec{a}, \vec{b}, \vec{c}\}$ , kjer so  $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$  linearno neodvisni.

2)  $V = \mathcal{O}^n$

$$e_j(0, \dots, 0, \underbrace{1}_{j\text{-to mesto}}, 0, \dots, 0) \in \mathcal{O}^n$$

$\{e_1, e_2, \dots, e_n\}$  je *standardna baza*  $\mathcal{O}^n$ .

$$x = (\alpha_1, \dots, \alpha_n) \in \mathcal{O}^n \Rightarrow x = \alpha_1 e_1 + \cdots + \alpha_n e_n$$



3)  $V = \mathbb{R}[x]$

$$p(x) \in \mathbb{R}[x]$$

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$

Baza tega prostora je

$$\{p_j(x) = x^j : j = 0, 1, \dots\} = \{1, x, x^2, x^3, \dots\}$$

DEFINICIJA: Vektorji  $v_1, \dots, v_m$  so *linearno odvisni*, kadar niso linearno neodvisni.

Naj bodo  $v_1, \dots, v_m$  linearno odvisni ( $m > 1$ ). Potem obstajajo tudi skalarji  $\alpha_1, \dots, \alpha_m \in \mathcal{O}$ , da niso vsi enako 0, vendar pa je

$$\alpha_1 v_1 + \cdots + \alpha_m v_m = 0$$

Recimo, da  $\alpha_1 \neq 0$ , Potem je

$$v_1 = \underbrace{(-\alpha_1^{-1}\alpha_2)}_{\beta_2} v_2 + \cdots + \underbrace{(-\alpha_1^{-1}\alpha_m)}_{\beta_m} v_m$$

$v_1$  je linearna kombinacija elementov  $v_2, \dots, v_m$ .

Potem obstaja tak  $j \in \{2, \dots, m\}$ , da je  $v_j$  linearna kombinacija vektorjev

$$v_1, \dots, v_{j-1}, v_{j+1}, \dots, v_m$$

**Obratno:** Če velja prejšnja trditev, potem so  $v_1, \dots, v_m$  linearno odvisni

$$v_1 = \beta_2 v_2 + \cdots + \beta_m v_m$$

$$1v_1 + (-\beta_2)v_2 + \cdots + (-\beta_m)v_m = 0$$

TRDITEV: Naj bodo  $v_1, \dots, v_m$  linearno odvisni in  $v_1 \neq 0$ ,  $m > 1$ . Potem obstaja tak  $k > 1$ ,  $k \leq m$ , da je  $v_k$  linearna kombinacija vektorjev  $v_1, \dots, v_{k-1}$ .

DOKAZ: Naj bo  $\alpha_1 v_1 + \cdots + \alpha_m v_m = 0$ , pri čemer niso vsi  $\alpha_j = 0$ .

$$\exists \alpha_j \neq 0 : j > 1$$

$$k = \max\{j : \alpha_j \neq 0\} \quad (k > 1)$$

$$\Rightarrow v_k = \beta_1 v_1 + \cdots + \beta_{k-1} v_{k-1}$$

□

TRDITEV: Naj vektorji  $x_1, \dots, x_m$  tvorijo ogrodje vektorskega prostora  $V$ . Če obstaja  $j \in \{1, \dots, m\}$ , da je  $x_j$  linearna kombinacija vektorjev  $x_i, i \in \{1, \dots, m\} \setminus \{j\}$ , potem vektorji  $\{x_i : i \in \{1, \dots, m\} \setminus \{j\}\}$  sestavljajo ogrodje vektorskega prostora  $V$ .

DOKAZ: Smemo vzeti  $j = 1$ , ker lahko spremenimo indekse.

$$x_1 = \alpha_2 x_2 + \dots + \alpha_m x_m$$

$$v \in V$$

$$\begin{aligned} v &= \beta_1 x_1 + \dots + \beta_m x_m = \\ &= \beta_1 (\alpha_2 x_2 + \dots + \alpha_m x_m) + \beta_2 x_2 + \dots + \beta_m x_m = \\ &= (\beta_1 \alpha_2 + \beta_2) x_2 + \dots + (\beta_1 \alpha_m + \beta_m) x_m \end{aligned}$$

Torej  $x_2, \dots, x_m$  sestavljajo ogrodje vektorskega prostora  $V$ .

□

TRDITEV: Iz vsakega končnega ogrodja vektorskega prostora  $V \neq \{0\}$ , lahko izberemo bazo.

DOKAZ: Iz ogrodja postopoma odstanjujemo vektorje, ki so linearna kombinacija drugih. Na koncu ostane baza. (Predpostavimo lahko, da so vektorji v ogrodju različni).

POSLEDICA: Vsak netrivialen končno razsežen vektorski prostor ima bazo.

TRDITEV: Naj vektorji  $x_1 \dots x_m$  sestavljajo ogrodje vektorskega prostora  $V$ , vektorji  $y_1, \dots, y_n$  pa naj bodo linearno neodvisni. Potem je  $m \geq n$ .

DOKAZ: Predpostavimo, da je  $n > m$ . Imamo dve vrsti vektorjev:

$$x_1, \dots, x_m \quad y_1, \dots, y_n$$

Premaknemo  $y_1$  v bazo in dobimo

$$y_1, x_1, \dots, x_m$$

To je ogrodje, vektorji  $y_1, x_1, \dots, x_m$  pa so linearno odvisni. Torej obstaja tak vektor, ki je linearna kombinacija predhodnih. To je eden od vektorjev  $x_1, \dots, x_m$ . Tega odstranimo in ostane ogrodje

$$y_1, x'_1, \dots, x'_{m-1}$$

Postopem ponovimo še enkrat in dobimo

$$y_2, y_1, x'_1, \dots, x'_{m-1}$$

Ti vektorji sestavljajo ogrodje in so linearno odvisni. Odstranimo vektor, ki je linearna kombinacija predhodnih. To je eden od vektorjev  $x'_1, \dots, x'_{m-1}$ , ker so  $y_i$  linearno neodvisni. Dobimo ogrodje

$$y_2, y_1, x''_1, \dots, x''_{m-2}$$

Postopoma izpodrinemo vse  $x$ -e in dobimo ogrodje  $y_m, y_{m-1}, \dots, y_1$ . Zato je  $y_{m+1}$  linearna kombinacija vektorjev  $y_1, \dots, y_m$ .  $\rightarrow \leftarrow$  ( $y_1, \dots, y_n$  so linearno neodvisni).

**Sklep:**  $m \geq n$  □

**Posledica:** Vse baze netrivialnega končno razsežnega vektorskoga prostora imajo enako elementov.

**DEFINICIJA:** Število elementov v bazi končno razsežnega vektorskega prostora imenujemo *razsežnost* ali *dimenzija* tega vektorskega prostora. **Oznaka:**  $\dim V$

**DOKAZ POSLEDICE:**  $V \neq \{0\}$ . Naj bosta

$$\begin{aligned} X &= \{x_1, \dots, x_m\} \\ Y &= \{y_1, \dots, y_n\} \end{aligned}$$

bazi vektorskega prostora  $V$  in velja  $x_i \neq x_j \forall i \neq j$  in  $y_i \neq y_j \forall i \neq j$ . Potem velja:

$X$  je ogrodje,  $Y$  niz linearno neodvisnih vektorjev  $\Rightarrow m \geq n$

$Y$  je ogrodje,  $X$  niz linearno neodvisnih vektorjev  $\Rightarrow n \geq m$

$\Rightarrow m = n$

**IZREK:** Naj bo  $V$   $n$ -razsežen vektorski prostor nad  $\mathcal{O}$  (komutativen),  $N \in \mathbb{N}$ . Potem je vektorski prostor  $V$  izomorfen vektorskemu prostoru  $\mathcal{O}^n$ .

**DOKAZ:** Naj bo  $\mathcal{V} = \{v_1, \dots, v_n\}$  baza  $V$  (*urejena*, t.j., določen vrstni red).

$$\begin{aligned} x \in V, x &\mapsto (\alpha_1, \dots, \alpha_n) \in \mathcal{O}^n \\ x &= \alpha_1 v_1 + \dots + \alpha_n v_n \end{aligned}$$

ker je  $\{v_1, \dots, v_n\}$  baza, so  $\alpha_1, \dots, \alpha_n$  enolično določeni. Zapišemo lahko preslikavo

$$\begin{aligned}\Phi_v : V &\rightarrow \mathcal{O}^n \\ \Phi_v(x) &= (\alpha_1, \dots, \alpha_n)\end{aligned}$$

$\Phi_v$  je odvisen od vrstnega reda baze in je izomorfen. Zapišemo lahko tudi preslikavo

$$\begin{aligned}\Psi_v : \mathcal{O}^n &\rightarrow V \\ \Psi_v(\alpha_1, \dots, \alpha_n) &= \alpha_1 v_1 + \dots + \alpha_n v_n\end{aligned}$$

$\Psi_v$  je inverz preslikave  $\Phi_v \Rightarrow \Psi_v, \Phi_v$  sta bijekciji. Zadoš'ca dokazati, da je  $\Psi$  linearna. Torej je potrebno dokazati homogenost in aditivnost. Oboje je očitno, zato nismo napisali dokaza. Lahko ga napišeš za vajo doma (ni težek, saj je očiten).

**IZREK:** Končno razsežna vektorska prostora nad istim obsegom sta izomorfna natanko takrat, kadar imata enako dimenzijo.

**DOKAZ:** Smemo privzeti, da sta  $V, U$  netrivialna. Kot se je izrazil profesor: „če sta  $V$  in  $U$  trivialna, je tudi dokaz trivialen.”

$(\Leftarrow)$   $\dim V = \dim U = n \Rightarrow$  obstajata izomorfizma  $\Phi, \Psi$ :

$$\begin{aligned}\Phi : V &\rightarrow \mathcal{O}^n \\ \Psi : \mathcal{O}^n &\rightarrow U\end{aligned}$$

$\Rightarrow \Psi\Phi : V \rightarrow U$  je izomorfizem

$(\Rightarrow)$  Naj bo  $F : V \rightarrow U$  izomorfizem vektorskih prostorov in  $\dim V = n, n \in \mathbb{N}$ , ter  $\{v_1, \dots, v_n\}$  baza  $V$ . Trdimo, da je  $\{F(v_1), \dots, F(v_n)\}$  baza  $U$ .

1. linearna neodvisnost

$$\begin{aligned}\alpha_1 F(v_1) + \dots + \alpha_n F(v_n) &= 0 \\ F(\alpha_1 v_1 + \dots + \alpha_n v_n) &= F(0) \\ \Rightarrow \alpha_1 v_1 + \dots + \alpha_n v_n &= 0 \Rightarrow \\ \Rightarrow \alpha_1 = \dots = \alpha_n &= 0\end{aligned}$$

2.  $\{F(v_1), \dots, F(v_n)\}$  je ogrodje

$$\begin{aligned}u \in U &\Rightarrow \exists v \in V : F(v) = u \\ v &= \beta_1 v_1 + \dots + \beta_n v_n \Rightarrow \\ \Rightarrow u = f(v) &= F(\beta_1 v_1 + \dots + \beta_n v_n) = \\ &= \beta_1 F(v_1) + \dots + \beta_n F(v_n)\end{aligned}$$

□

TRDITEV: Naj bo  $V \neq \{0\}$  končno razsežen vektorski prostor. Če so  $v_1, \dots, v_m \in V$  linearno neodvisni, obstaja baza  $V$ , ki vsebuje  $v_1, \dots, v_m$ .

DOKAZ:  $u_1, \dots, u_n$  naj tvorijo ogrodje  $V$ .

$\Rightarrow \{v_1, \dots, v_m, u_1, \dots, u_n\}$  je ogrodje  $V$ . Postopoma iz tega ogrodja odtranjamo vektorje, ki so linearna kombinacija vektorjev pred njimi. Vsi vektorji  $v_1, \dots, v_m$  ostanejo, ker so linearno neodvisni. Ostane nam baza, ki vsebuje  $\{v_1, \dots, v_m\}$ .

TRDITEV: Naj bo  $V$  končno razsežen vektorski prostor in  $U$  njegov vektorski podprostor. Potem je  $\dim U \leq \dim V$ , pri čemer velja enačaj le v primeru  $U = V$ .

DOKAZ:  $V \neq \{0\}, \dim V = n \in \mathbb{N}$ .

$U \subseteq V, U \neq \{0\}$

$u_1, \dots, u_m \in U$  linearno neodvisni v  $U$  ( $\Rightarrow$  v  $V$ ), zato je  $m \leq n$ . Naj bo  $m$  maksimalen. Trdimo, da je potem  $\{u_1, \dots, u_m\}$  baza  $U$ . Zadošča dokaz, da je  $\mathcal{U} = \{u_1, \dots, u_m\}$  ogrodje  $U$ .

Če  $\mathcal{U}$  ni ogrodje vektorskega prostora  $U$ , obstaja tak  $u \in U$  da  $u$  ni linearna kombinacija vektorjev  $u_1, \dots, u_m$  ( $u \notin \text{Lin}\mathcal{U}$ ). Potem so vektorji  $u_1, \dots, u_m, u$  linearno neodvisni, to pa je protislovje z maksimalnostjo števila  $m$ . Torej je  $\mathcal{U}$  ogrodje vektorskega prostora  $U$ , zato je baza  $U$  in  $\dim U = m (\leq n)$ . Če je  $\dim U = n$ , je  $U$  baza  $V$ , zato  $U = V$ .

□

TRDITEV: Naj bo  $V$  končno razsežen vektorski prostor in  $U$  njegov vektorski podprostor. Potem obstaja tak vektorski podprostor  $W \subset V$ , da velja  $V = U \oplus W$ .

DOKAZ:  $U = \{0\}, W = V$ . Bolj zanimivo je, če  $U \neq \{0\}, \{u_1, \dots, u_m\}$  baza  $U$ . Dopolnimo jo do baze  $V$

$$\{u_1, \dots, u_m, u_{m+1}, \dots, u_{m+k}\}$$

Postavimo  $W = \text{Lin}\{u_{m+1}, \dots, u_{m+k}\}$ . Če dopolnimo tako, da nič ne dopol-

nimo potem:

$$\begin{aligned} W &= \text{Lin}\{\} = \{0\} \\ U &= V \end{aligned}$$

Trdimo, da je  $V = U \oplus W$

$$\begin{aligned} v \in V \Rightarrow v &= \underbrace{\alpha_1 u_1 + \dots + \alpha_m u_m}_{x \in U} + \underbrace{\alpha_{m+1} u_{m+1} + \dots + \alpha_{m+k} u_{m+k}}_{y \in W} \\ v &= x + y, x \in U, y \in W \\ \Rightarrow V &= U + W \end{aligned}$$

$$U \cap W = \{0\}$$

$$\begin{aligned} z &\in U \cap W \\ z &= \beta_1 u_1 + \dots + \beta_m u_m = \beta_1 u_{m+1} + \dots + \beta_{m+k} u_{m+k} \\ \beta_1 u_1 + \dots + (-\beta_{m+k}) u_{m+k} &= 0 \\ \Rightarrow \beta_1 = \dots = \beta_{m+k} &= 0 \Rightarrow z = 0 \end{aligned}$$

$$\Rightarrow V = U \oplus W$$

□

Tej trditvi pravimo *trditev o eksistenci direktnega komplementa*.

TRDITEV: Naj bo  $V$  končno razsežen vektorski prostor in  $U, W$  njegova vektorska podprostora. Če je  $U \cap W = \{0\}$ , potem velja  $\dim U \oplus W = \dim U + \dim W$ .

DOKAZ:  $U, W$  sta netrivialna, drugače je očitno. Naj bosta

$$\begin{aligned} \{u_1, \dots, u_m\} &\text{ baza } U, \dim U = m \\ \{w_1, \dots, w_n\} &\text{ baza } W, \dim W = n \end{aligned}$$

Trdimo, da je  $\{u_1, \dots, u_m, w_1, \dots, w_n\}$  baza  $U \oplus W$ .

1. linearna neodvisnost

$$\begin{aligned} \alpha_1 u_1 + \dots + \alpha_m u_m + \beta_1 w_1 + \dots + \beta_n w_n &= 0 \\ z = \underbrace{\alpha_1 u_1 + \dots + \alpha_m u_m}_{\in U} &= \underbrace{(-\beta_1) w_1 + \dots + (-\beta_n) w_n}_{\in W} \\ z \in U \cap W = \{0\} &\Rightarrow z = 0 \\ \Rightarrow \alpha_1 = \dots = \alpha_m &= 0, \\ \beta_1 = \dots = \beta_n &= 0 \end{aligned}$$

(1)  $\Rightarrow u_1 \dots u_m, w_1 \dots w_n$  so različni

$$2. \text{Lin}\{u_1, \dots, u_m, w_1, \dots, w_n\} = U \oplus W$$

Očitno je, da je  $\text{Lin}\{u_1, \dots, u_m, w_1, \dots, w_n\} \subseteq U \oplus W$ . Dokazati je treba še obratno smer ( $\supseteq$ ).

$$\begin{aligned} x \in U \oplus W &\Rightarrow \\ \Rightarrow x = u + w, u \in U, w \in W \\ u &= \alpha_1 u_1 + \dots + \alpha_m u_m \\ w &= \beta_1 w_1 + \dots + \beta_n w_n \\ \Rightarrow x &= \alpha_1 u_1 + \dots + \alpha_m u_m + \beta_1 w_1 + \dots + \beta_n w_n \end{aligned}$$

$$(1), (2) \Rightarrow \dim U \oplus W = m + n = \dim U + \dim W$$

TRDITEV: Naj bo  $V$  končno razsežen vektorski prostor in  $U \leq V, W \leq V$ . Ptem velja enakost (= *dimeznisjska formula*):

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$$

OSNOVNA IDEJA DOKAZA: Vzamemo bazo vektorskega prostora  $U \cap W$ . V  $W$  najdemo vektorje s katerimi razširimo  $U \cap W$ . Linearno ogrinjačo teh vektorjev označimo z  $Z$ . Velja  $U + W = U \oplus Z$ .

$$\begin{aligned} \Rightarrow \dim(U + W) &= \dim U + \dim Z \text{ in} \\ W &= (U \cap W) \oplus Z \Rightarrow \dim W = \dim(U \cap W) + \dim Z \end{aligned}$$

Iz tega sledi zgornja formula.

TRDITEV: Naj bo  $V = U \oplus W, \dim V < \infty$ . Potem je vektorski prostor  $V/U$  izomorfen  $W$ , vektorski prsotor  $V/W$ , pa je izomorfen  $U$ .

DOKAZ:

$$\begin{aligned} f : W &\rightarrow V/U \\ f(w) &= [w] = w + U \end{aligned}$$

$f$  je linearna preslikava

$$f(w_1 + w_2) = [w_1 + w_2] = [w_1] + [w_2] = f(w_1) + f(w_2)$$

$\Rightarrow f$  je aditivna. Podobno dokažemo homogenost.

$f$  je injektivna

$$\begin{aligned}
 f(w_1) = f(w_2) &\Rightarrow \\
 \Rightarrow [w_1] = [w_2] &\Rightarrow \\
 \Rightarrow w_1 \sim w_2 &\Rightarrow \\
 \Rightarrow w_1 - w_2 \in U & \\
 w_1 - w_2 \in W & \\
 \Rightarrow w_1 - w_2 \in U \cap W = \{0\} &\Rightarrow w_1 - w_2 = 0 \\
 \Rightarrow w_1 = w_2 &
 \end{aligned}$$

$f$  je surjektivna:

$$\begin{aligned}
 [v] \in V/U, v \in V \\
 v = u + w, u \in U, w \in W
 \end{aligned}$$

$$f(w) = [v]$$

$$\begin{aligned}
 f(w) &= w \\
 v = u + w &\Rightarrow u = v - w \in U \Rightarrow w \sim v
 \end{aligned}$$

□

Naj bo  $V = V_1 \oplus V_2 \Rightarrow V/V_1 \cong V_2 \wedge V/V_2 \cong V_1$

TRDITEV: Naj bo  $V$  končno razsežen vektorski prostor in  $U$  njegov vektorski podprostor. Potem je

$$\dim V/U = \dim V - \dim U$$

DOKAZ: Poiščimo  $W \leq V$ , da je  $V = U \oplus W$ . Ker je  $V/U \cong W$ , velja  $\dim V/U = \dim W$ . Vemo:

$$\dim V = \dim U + \dim W$$

Zato je

$$\dim V/U = \dim V - \dim U$$

## 4.8 Linearne preslikave na končno razsežnih V. P.

Naj bosta  $V, U$  končno razsežna vektorska prostora nad  $\mathcal{O}$  in naj bo  $\mathcal{A} \in \mathcal{L}(V, U)$  linearna.



Naj bo  $\mathcal{V} = \{v_1, \dots, v_n\}$  baza  $V$ . Če poznamo slike  $\mathcal{A}v_1, \dots, \mathcal{A}v_n$ , poznamo  $\mathcal{A}$ :

$$\begin{aligned} x \in V, \quad \exists \alpha_1, \dots, \alpha_n \in \mathcal{O} : \\ x = \alpha_1 v_1 + \dots + \alpha_n v_n \\ \Rightarrow \mathcal{A}x = \mathcal{A}(\alpha_1 v_1 + \dots + \alpha_n v_n) = \alpha_1 \mathcal{A}v_1 + \dots + \alpha_n \mathcal{A}v_n \end{aligned}$$

#### 4.8.1 Poseben primer

$$\begin{aligned} V = \mathcal{O}^n, \quad U = \mathcal{O}^m \\ A = \mathcal{L}(\mathcal{O}^n, \mathcal{O}^m) \\ \{e_1, \dots, e_n\} \text{ standardna baza } \mathcal{O}^n \end{aligned}$$

$$e_j = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \end{bmatrix}$$

$$x \in \mathcal{O}^n, \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

Poznamo  $Ae_1, \dots, Ae_n \Rightarrow$  poznamo  $A$ .

$$\begin{aligned} Ae_j \in \mathcal{O}^m \\ Ae_j = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix} \in \mathcal{O}^m \end{aligned}$$

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} = m \times n \text{ matrika, ki predstavlja linearno preslikavo } A$$

$a_{ij}$  ( $1 \leq i \leq m, 1 \leq j \leq n$ ) je člen matrike  $A$ .  $a_{ij}$  leži v  $i$ -ti vrstici in  $j$ -tem stolpcu.

$$A^{(j)} = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix} = j\text{-ti stolpec matrike}$$

$$A_{(i)} = \begin{bmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{bmatrix}$$

$$A = [a_{ij}]$$

$$A : \mathcal{O}^n \rightarrow \mathcal{O}^m$$

$$x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \in \mathcal{O}^n$$

$$A = [a_{ij}]$$

$$Ax = y$$

$$y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{bmatrix}$$

$y$  izračunamo kot:

$$\begin{aligned} y = Ax &= A(x_1e_1 + x_2e_2 + \cdots + x_ne_n) = \\ &= x_1Ae_1 + x_2Ae_2 + \cdots + x_nAe_n = \\ &= x_1A^{(1)} + x_2A^{(2)} + \cdots + x_nA^{(n)} \\ \Rightarrow y_i &= x_1a_{i1} + x_2a_{i2} + \cdots + x_na_{in} = \\ &= \sum_{j=1}^n a_{ij}x_j, \quad i = 1, \dots, m \end{aligned}$$

PRIMER:  $A : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  zasuk za kot  $\varphi$  okrog  $z$ -osi. Kaj je matrika  $A$  in kam  $A$  preslika točko  $(1, 2, 3)$ ?

$$Ae_1 = A\vec{i} = A^{(1)}$$

$$Ae_2 = A\vec{j} = A^{(2)}$$

$$Ae_3 = A\vec{k} = A^{(3)}$$

$$\begin{aligned}
A^{(3)} &= A\vec{k} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \\
A^{(1)} &= A\vec{i} = \begin{bmatrix} \cos \varphi'' \sin \varphi \\ 0 \end{bmatrix} \\
A^{(2)} &= A\vec{j} = \begin{bmatrix} -\sin \varphi \\ \cos \varphi \\ 0 \end{bmatrix} \\
A &= \begin{bmatrix} \cos \varphi & -\sin \varphi & 0 \\ \sin \varphi & \cos \varphi & 0 \\ 0 & 0 & 1 \end{bmatrix}
\end{aligned}$$

Izračunajmo sliko točke  $(1, 2, 3)$ :

$$A \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} \cos \varphi - 2 \sin \varphi \\ \sin \varphi + 2 \cos \varphi \\ 3 \end{bmatrix}$$

$\mathcal{L}(\mathcal{O}^n, \mathcal{O}^m) \equiv \mathcal{O}^{m \times n}$  je množica vseh  $m \times n$  matrik s členi  $\mathcal{O}$ . Preslikave smo *identificirali* (poistovetili) z matrikami.

$\mathcal{L}(\mathcal{O}^n, \mathcal{O}^m)$  je vektorski prostor nad  $\mathcal{O}$ .  $\mathcal{O}^{m \times n}$  postane vektorski prostor nad  $\mathcal{O}$ .

Naj bosta  $A, B \in \mathcal{O}^{m \times n}$ .

$$\begin{aligned}
(A + B)x &= Ax + Bx \quad \forall x \in \mathcal{O}^n \\
(\underbrace{A + B}_{C \in \mathcal{O}^{m \times n}})e_j &= Ae_j + Be_j = A^{(j)} + B^{(j)}
\end{aligned}$$

$$\begin{aligned}
\Rightarrow C^{(j)} &= Ce_j = A^{(j)} + B^{(j)} \\
\Rightarrow c_{ij} &= a_{ij} + b_{ij} \quad \forall i, j
\end{aligned}$$

$\Rightarrow$  v  $\mathcal{O}^{m \times n}$  seštevamo po členih. Podobno je z množenjem s skalarji.

### 4.8.2 Splošna situacija

Naj bosta  $V, U$  vektorska prostora nad  $\mathcal{O}$ .

$$\dim V = n$$

$$\dim U = m$$

$$\mathcal{V} = \{v_1, \dots, v_n\} \text{ urejena baza } V$$

$$\mathcal{U} = \{u_1, \dots, u_m\} \text{ urejena baza } U$$

$\mathcal{A} = \mathcal{L}(V, U)$ ,  $\mathcal{A}$  poznamo, če poznamo slike  $\mathcal{A}v_j$ ,  $j = 1, \dots, n$ .

$$\Phi_{\mathcal{V}} : V \rightarrow \mathcal{O}^n \text{ izomorfizem}$$

$$v \in V$$

$$v = \alpha_1 v_1 + \dots + \alpha_n v_n$$

$$v \rightarrow (\alpha_1, \dots, \alpha_n) = \Phi_{\mathcal{V}}(v) = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$$

$$\Psi_{\mathcal{V}}(v_j) = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = e_j$$

Podobno velja za izomorfizem  $\Phi_{\mathcal{U}} : U \rightarrow \mathcal{O}^m$ .

$$\begin{array}{ccc} V & \xrightarrow{\mathcal{A}} & U \\ \Phi_{\mathcal{V}} \downarrow & & \downarrow \Phi_{\mathcal{U}} \\ \mathcal{O}^n & \xrightarrow{A} & \mathcal{O}^m \end{array}$$

Slika 1: Diagram preslikave

Diagram *komutira*  $\Phi_{\mathcal{U}}\mathcal{A} = A\Phi_{\mathcal{V}}$

$$(\Phi_{\mathcal{U}}\mathcal{A})v_j = (A\Phi_{\mathcal{V}})v_j = Ae_j = A^{(j)}$$

$$(\Phi_{\mathcal{U}}\mathcal{A})v_j = \Phi_{\mathcal{U}}(\mathcal{A}v_j) = \Phi_{\mathcal{U}}(\alpha_1 u_1 + \cdots + \alpha_m u_m) = \alpha_1 e_1 + \cdots + \alpha_m e_m = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{bmatrix}$$

$$\mathcal{A}v_j = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_m u_m$$

$$\Rightarrow A^{(j)} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{bmatrix} \Rightarrow \alpha_i = a_{ij} \quad \forall i, j$$

$$\mathcal{A}v_j = a_{1j}u_1 + a_{2j}u_2 + \cdots + a_{mj}u_m$$

Linearni preslikavi  $\mathcal{A} \in \mathcal{L}(V, U)$  priredimo (glede na bazi  $\mathcal{U}, \mathcal{V}$ ) matriko  $A \in \mathcal{O}^{m \times n}$ .

$$F : \mathcal{L}(V, U) \rightarrow \mathcal{O}^{m \times n}$$

$$\mathcal{A} \mapsto A = F(\mathcal{A})$$

$$F(\mathcal{A}) = \Phi_{\mathcal{U}}\mathcal{A}(\Phi_{\mathcal{V}})^{-1}$$

$F$  je izomorfizem med  $\mathcal{L}(V, U)$  in  $\mathcal{O}^{m \times n}$

- aditivnost in homogenost sta očitni
- iz diagrama hitro dobimo inverz  $F^{-1} = (\Phi_{\mathcal{U}})^{-1} A \Phi_{\mathcal{V}}$

$$\dim \mathcal{L}(V, U) = \dim \mathcal{O}^{m \times n} = ?$$

Standardna baza  $\mathcal{O}^{m \times n}$  je sestavljena iz *elementarnih matrik*. V elementarni matriki se nahaja ena 1, ostali členi so 0.

$$E_{pq} = [e_{ij}] \quad i = 1, \dots, m \quad j = 1, \dots, n$$

$$e_{ij} = \begin{cases} 1 & i = p \wedge j = q \\ 0 & \text{sicer} \end{cases}$$

### 4.8.3 Množenje matrik

Naj bodo  $U, V$  in  $W$  vektorski prostori, linearna preslikava  $\mathcal{B} : W \rightarrow V$ ,  $\mathcal{A} : V \rightarrow U$  in  $\mathcal{C} : W \rightarrow U$ , t.j.:  $\mathcal{C} = \mathcal{A}\mathcal{B}$ .

$\mathcal{U}$  je urejena baza v.p.  $U$ ,  $\mathcal{V}$  urejena baza  $V$ ,  $\mathcal{W}$ , pa urejena baza  $W$ .

Poznamo  $\Phi_{\mathcal{V}} : V \rightarrow \mathcal{O}^n$ ,  $\Phi_{\mathcal{U}} : U \rightarrow \mathcal{O}^m$  in  $\Phi_{\mathcal{W}} : W \rightarrow \mathcal{O}^p$ . in poznamo preslikavi  $A : \mathcal{O}^n \rightarrow \mathcal{O}^m$ , ter  $B : \mathcal{O}^p \rightarrow \mathcal{O}^n$ . Zanima nas  $C = AB$ .

$$\begin{aligned} A &= [a_{ij}] \in \mathcal{O}^{m \times n} \\ B &= [b_{ij}] \in \mathcal{O}^{n \times p} \\ C &= [c_{ij}] \in \mathcal{O}^{m \times p} \end{aligned}$$

$$\begin{aligned} C &= AB \\ C^{(j)} &= Ce_j = (AB)e_j = A(Be_j) = AB^{(j)} \Rightarrow \\ C^{(j)} &= AB^{(j)} \quad \forall j \\ \Rightarrow C_{ij} &= A_{(i)}B^{(j)} \\ C_{ij} &= \sum_{k=1}^n a_{ik}b_{kj} \end{aligned}$$

### 4.8.4 Poseben primer

Naj bo  $U = V = W$ , in  $m = n = p$ .

$$A, B \in \mathcal{O}^{n \times n} \Rightarrow C = AB \in \mathcal{O}^{n \times n}$$

$\mathcal{L}(\mathcal{O}^n) \equiv \mathcal{O}^{n \times n}$  je *algebra kvadratnih matrik*. Naj bodo baze  $U, V, W$  enake, to je  $\mathcal{U} = \mathcal{V} = \mathcal{W}$ . Skonstruiramo preslikavo

$$\begin{aligned} F : \mathcal{L}(V) &\rightarrow \mathcal{L}(\mathcal{O}^n) \equiv \mathcal{O}^{n \times n} \\ \mathcal{A} &\mapsto A \\ F(\mathcal{A}) &= \Phi_{\mathcal{V}} \mathcal{A} \Phi_{\mathcal{V}}^{-1} \end{aligned}$$

**Vemo:**  $F$  je izomorfizem vektorskih prostorov  $\mathcal{L}(V)$  in  $\mathcal{O}^{n \times n}$ .

**TRDITEV:**  $F$  je izomorfizem med algebrama  $\mathcal{L}(V)$  in  $\mathcal{O}^{n \times n}$ .

**DOKAZ:** Zadošča ugotoviti, da  $F$  ohranja množenje  $F(\mathcal{A}\mathcal{B}) = F(\mathcal{A})F(\mathcal{B})$

$$F(\mathcal{AB}) = \Phi_V(\mathcal{AB})\Phi_V^{-1}$$

$$F(\mathcal{A})F(\mathcal{B}) = \Phi_V\mathcal{A}\Phi_V^{-1}\Phi_V\mathcal{B}\Phi_V^{-1} = \Phi_V\mathcal{AB}\Phi_V^{-1}$$

□

$id_V$  je enota algebre  $\mathcal{L}(V)$ .  $F(id_V)$  je enota algebre  $\mathcal{O}^{n \times n}$

$$F(id_V) = id_{\mathcal{O}^{n \times n}} = I$$

$I$  je *enotska* (ali identična) matrika. Velja:

$$I^{(j)} = Ie_j = e_j$$

torej

$$I = [e_1, e_1, \dots, e_n]$$

Zapišemo lahko tudi kot

$$I = [\delta_{ij}] \quad i, j = 1, \dots, n$$

kjer je  $\delta_{ij}$  *Kroneckerjeva delta*, za katero velja predpis

$$\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & \text{sicer} \end{cases}$$

DEFINICIJA: Naj bo  $\mathcal{A} \in \mathcal{L}(V)$  bijekcija ( $\exists \mathcal{B} \in \mathcal{L}(V) : \mathcal{AB} = \mathcal{BA} = id_V$ ). Pravimo, da je  $F(\mathcal{A}) = A$  *obrnljiva*:

$$\exists B \in \mathcal{O}^{n \times n} : AB = BA = I$$

$A$  obrnljiva  $\Rightarrow B$  je enolično določena. Označimo:

$$B = A^{-1}$$

#### 4.8.5 Rang linearne preslikave in matrike

Naj bosta  $V, U$  končno razsežna vektorska prostora nad  $\mathcal{O}$  in  $\mathcal{A} \in \mathcal{L}(V, U)$ .

IZREK: Za  $\mathcal{A}$  velja formula

$$\dim(\text{im } \mathcal{A}) + \dim(\ker \mathcal{A}) = \dim V \quad (2)$$

DOKAZ: Vemo, da sta vektorska prostora  $V_{\ker \mathcal{A}}$  in  $\operatorname{im} \mathcal{A}$  izomorfna. Zato je  $\dim V / \ker \mathcal{A} = \dim(\operatorname{im} \mathcal{A})$ . Vemo  $\dim V / \ker \mathcal{A} = \dim V - \dim(\ker \mathcal{A})$ .  $\Rightarrow 2$ .

□

DEFINICIJA: Rang preslikave  $\mathcal{A}$  je  $\dim(\operatorname{im} \mathcal{A})$ . Oznaka  $\operatorname{rang} \mathcal{A} = \dim(\operatorname{im} \mathcal{A})$ .

TRDITEV:  $\mathcal{A} = \mathcal{L}(V, U)$

1.  $\mathcal{A}$  je injektivna  $\iff \operatorname{rang} \mathcal{A} = \dim V$
2.  $\mathcal{A}$  je surjektivna  $\iff \operatorname{rang} \mathcal{A} = \dim U$
3.  $\mathcal{A}$  je bijektivna  $\iff \dim V = \dim U = \operatorname{rang} \mathcal{A}$

DOKAZ:

1. vemo:  $\mathcal{A}$  injektivna  $\iff \ker \mathcal{A} = \{0\}$

$$\ker \mathcal{A} = \{0\} \iff \dim(\ker \mathcal{A}) = 0$$

2. vemo:  $\mathcal{A}$  surjektivna  $\iff \operatorname{im} \mathcal{A} = U$

$$\operatorname{im} \mathcal{A} = U \iff \underbrace{\dim(\operatorname{im} \mathcal{A})}_{\operatorname{rang} \mathcal{A}} = \dim U$$

3. kombiniramo 1 in 2.

TRDITEV: Za  $\mathcal{A} \in \mathcal{L}(V)$  so ekvivalentne naslednje izjave:

1.  $\mathcal{A}$  je bijekcija
2.  $\mathcal{A}$  je surjekcija
3.  $\mathcal{A}$  je injekcija
4.  $\operatorname{rang} \mathcal{A} = \dim V$

DOKAZ:  $U = V$  v prejšnji trditvi  $\Rightarrow$

$$\Rightarrow [(1) \iff (4), (2) \iff (4), (3) \iff (4)]$$



POSLEDICA: Matrika  $A \in \mathcal{O}^{n \times n}$  je obrnljiva natanko takrat, kadar je  $\text{rang } A = n$ .

DOKAZ: V prejšnji trditvi vzamemo  $V = \mathcal{O}^n$  in  $A$  razumemo kot endomorfizem vektorskih prostorov  $\mathcal{O}^n$ .

$A$  obrnljiva  $\iff A$  bijekcija, t.j.: (1)  $\iff$  (4) po prejšnji trditvi.

TRDITEV: Naj bo  $\mathcal{A} \in \mathcal{L}(V, U)$  in  $A$  matrika, ki pripada  $\mathcal{A}$  glede na dai baz  $\mathcal{V} \in V, \mathcal{U} \in U$ . Potem velja:

$$\text{rang } \mathcal{A} = \text{rang } A$$

DOKAZ: Narišemo si diagram in opazimo, da komutira.

$$\begin{aligned} \Phi_{\mathcal{U}} \mathcal{A} &= A \Phi_{\mathcal{V}} \\ (\underbrace{\Phi_{\mathcal{U}} \mathcal{A}}_{\text{im } \mathcal{A}}) V &= (A \underbrace{\Phi_{\mathcal{V}}}_{\mathcal{O}^n}) V \Rightarrow \\ &\Rightarrow \Phi_{\mathcal{U}}(\text{im } \mathcal{A}) = \text{im } A \end{aligned}$$

$\Phi_{\mathcal{U}}$  je izomorfizem, zato je

$$\begin{aligned} \dim(\text{im } \mathcal{A}) &= \dim(\text{im } A) \\ \text{rang } \mathcal{A} &= \text{rang } A \end{aligned}$$

Naj bo  $A \in \mathcal{O}^{m \times n} \equiv \mathcal{L}(\mathcal{O}^n, \mathcal{O}^m)$ . Velja

$$\begin{aligned} \text{im } A &= \{Ax : x \in \mathcal{O}^n\} = \\ &= \{A(x_1 e_1 + \dots + x_n e_n) : x \in \mathcal{O}^n\} = \\ &= \{x_1 A e_1 + \dots + x_n A e_n\} = \\ &= \{x_1 A^{(1)} + \dots + x_n A^{(n)} : x_j \in \mathcal{O}^{\forall j}\} = \\ &= \text{Lin}\{A^{(1)}, \dots, A^{(n)}\} \end{aligned}$$

TRDITEV: Stolpci matrike  $A$  tvorijo ogrodje vektorskega prostora  $\text{im } A$ .

POSLEDICA: Rang matrike  $A$  je največje število linearno neodvisnih stolpcev te matrike.

Operacije na matrkah, ki ohranjujejo rang:

S1) med sabo zamenjamo dva stolpca

S2) stolpec pomnožimo z neničelnim skalarjem

S3) Stolpci prištejemo večkratnik kakšnega drugega stolpca

V1, V2, V3 so analogne operacije na vrsticah.

TRDITEV: S1, S2, S3 in V1, V2, V3 ohranjajo rang.

DOKAZ:

S1) očitno

S2) Dokazati moramo, da velja

$$L1 = \text{Lin}\{\alpha A^{(1)}, A^{(2)}, \dots, A^{(n)}\} = \text{Lin}\{A^{(1)}, A^{(2)}, \dots, A^{(n)}\} = L2$$

Torej morajo biti vsi vektorji, ki so linearne kombinacije vektorjev L1 tudi linearne kombinacije vektorjev L2 in obratno. Zadošča

$$A^{(1)} = \alpha^{-1}(\alpha A^{(1)})$$

To velja, ker  $\alpha \neq 0$ . Torej lahko vsak vektor, ki je zapisan z linearno kombinacijo L1 pretvorimo v linearno kombinacijo vektorjev L2 in obratno, zato se ohranja slika preslikave  $A$  in posledično tudi rang.

S3) Dokazati moramo

$$\text{Lin}\{A^{(1)} + \alpha A^{(2)}, A^{(2)}, \dots, A^{(n)}\} = \text{Lin}\{A^{(2)}, A^{(2)}, \dots, A^{(n)}\}$$

Velja podoben razmislek kot pri S2, zato zadošča

$$A^{(1)} = (A^{(1)} + \alpha A^{(2)}) + (-\alpha)A^{(2)}$$

V1, V2, V3 ohranjajo ker  $A$

$$x \in \ker A \iff Ax = 0 \iff A_i x = 0, \quad i = 1, \dots, m$$

V1) očitno iz zgornje enakosti

V2)

$$A \rightarrow \begin{bmatrix} \alpha A_{(1)} \\ A_{(2)} \\ \vdots \\ A_{(m)} \end{bmatrix}$$

Pokazati moramo, da  $\alpha A_{(1)}x = 0 \quad \forall x \in \mathcal{O}^n$ . Ker  $\alpha \neq 0$ , velja

$$\alpha A_{(1)}x = 0 \iff A_{(1)}x = 0$$

Torej operacija ohranja ker  $A$ .

V3)

$$A \rightarrow \begin{bmatrix} A_{(1)} + \alpha A_{(2)} \\ A_{(2)} \\ \vdots \\ A_{(m)} \end{bmatrix}$$

Pokazati moramo

$$\left\{ \begin{array}{l} (A_{(1)} + \alpha A_{(2)})x = 0 \\ A_{(2)}x = 0 \\ \dots \\ A_{(n)}x = 0 \end{array} \right\} \iff \left\{ \begin{array}{l} A_{(1)}x = 0 \\ A_{(2)}x = 0 \\ \dots \\ A_{(n)}x = 0 \end{array} \right\}$$

( $\Leftarrow$ ) očitno

( $\Rightarrow$ ) vemo  $(A_{(1)} + \alpha A_{(2)})x = 0$ . Dokazati moramo, da je  $A_{(1)}x = 0$ .

$$\begin{aligned} (A_{(1)} + \alpha A_{(2)})x &= 0 \\ A_{(1)}x + \underbrace{\alpha A_{(2)}x}_0 &= 0 \\ \Rightarrow A_{(1)}x &= 0 \end{aligned}$$

Ker se ohranja jedro, se ohranja rang ( $= n - \dim(\ker A)$ ).

TRDITEV: Naj bo  $A \in \mathcal{O}^{m \times n}$ . Z uporabo operacij S1 - S3, V1 - V3 lahko postopoma pridemo iz matrike  $A$ , do matrike  $A_0$  oblike

$$A_0 = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \end{bmatrix} \in \mathcal{O}^{m \times n}$$

Kjer je rang  $A$  število stolpcev z eno enico. Natančna shema postopka je v zvezku.

PRIMER

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 0 \\ 2 & 3 & 4 & 5 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & -4 & -8 & -12 \\ 0 & -1 & -2 & -3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = A_0$$

Torej je rang  $A = \text{rang } A_0 = 2$ .

POSLEDICA Rang matrike je enak rangu njene *transponirane*.

$$\text{rang } A = \text{rang } A^T$$

Če je  $A = [a_{ij}] \in \mathcal{O}^{m \times n}$ , transponiranko  $B = A^\top$ , t.j.:  $B = [b_{ij}] \in \mathcal{O}^{n \times m}$  tvorimo na nasleden način:

$$b_{ij} = a_{ji} \quad \forall i, j$$

DOKAZ: Očitno je, da če na matriki  $A$  izvedemo operaijo  $Si$ , se bo ta pretvorila v  $Vi$  na matriki  $A^\top$ . Analogno za operacije  $Vi$ .

POSLEDICA: Največje število linearno neodvisnih stolpcev matrike je enako največjemu številu njenih linearno neodvisnih vrstic.

#### 4.8.6 Sistemi linearnih enačb

Naj bo

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

sistem linearnih enačb. Zapišemo lahko  $A \in \mathcal{O}^{m \times n}$ ,  $A = [a_{ij}]$ . Za  $b$  lahko zapišemo

$$b \in \mathcal{O}^m, \quad b = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

Podobno lahko  $x$  zapišemo kot

$$x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \mathcal{O}^n$$

Iščemo  $x \in \mathcal{O}^n$ , da bo veljalo

$$Ax = b$$

Če gledamo na  $A$  kot na preslikavo, velja  $A \in \mathcal{L}(\mathcal{O}^n, \mathcal{O}^m)$ . Naj bo  $\mathcal{R}$  množica vseh rešitev sistema  $Ax = b$ , t.j.:

$$\mathcal{R} = \{x \in \mathcal{O}^n : Ax = b\}$$

$[A|b] \in \mathcal{O}^{m \times (n+1)}$  je *razširjena matrika* sistema  $Ax = b$ .

Če je  $b = 0$ , potem imamo *homogen sistem*  $Ax = 0$ , potem

$$\mathcal{R} = \ker A$$

Če je  $b \neq 0$ , imamo *nehomogen sistem*  $Ax = b$ . Sistem je *protisloven*, kadar je  $\mathcal{R} = \emptyset$ , sicer pa je *neprotisloven*. Naj bo sistem  $Ax = b$  neprotisloven in  $w$  ena od rešitev ( $w \in \mathcal{R}$ ). Pravimo, da je  $w$  *partikularna rešitev*.

Naj bo

$$\begin{aligned} Aw = b, \quad x \in \mathcal{R} &\Rightarrow Ax = b \\ \Rightarrow A(x - w) &= \underbrace{Ax}_b - \underbrace{Aw}_b = 0 \Rightarrow x - w \in \ker A \\ &\Rightarrow x \in w + \ker A \end{aligned}$$

Torej velja  $\mathcal{R} \subseteq w + \ker A$ .

Naj bo  $x \in w + \ker A$ . Potem je  $x = w + y, y \in \ker A$ .

$$\Rightarrow Ax = A(w + y) = \underbrace{Aw}_b + \underbrace{Ay}_0 = b \Rightarrow x \in \mathcal{R}$$

Torej velja  $w + \ker A \subset \mathcal{R}$

Iz (1)&(2) sledi

$$\mathcal{R} = w + \ker A$$

TRDITEV: Če je  $w$  partikularna rešitev sistema  $Ax = b$ , je

$$\mathcal{R} = w + \ker A$$

IZREK (Kronecker, Capelli):  $\mathcal{R} \neq \emptyset$  natanko takrat, kadar je

$$\text{rang}[A|b] = \text{rang}[A]$$

DOKAZ:  $\mathcal{R} \neq \emptyset \iff b \in \text{im} A$  ( $\ker Ax = b$  pomeni, da je  $b \in \text{im} A$ )

$$\text{im}[A|b] = \text{Lin}\{A^{(1)}, \dots, A^{(n)}, b\}$$

$$\text{im} A = \text{Lin}\{A^{(1)}, \dots, A^{(n)}\}$$

$$\dim(\text{im}[A|b]) = \dim(\text{im} A) \iff \text{im} A = \text{im}[A|b] \iff b \in \text{im} A$$

$\ker \text{im} A \subseteq \text{im}[A|b]$ , preveriti je treba še  $\text{im}[A|b] \subseteq \text{im} A \iff b \in \text{im} A$ .

#### 4.8.7 Gaussov algoritem za reševanje sistema

Dovoljene operacije so V1 - V3 in S1. S1 je dovoljena operacija samo za prvih  $n$  stolpcev in paziti je treba, da med seboj ustrezno zamenjamo spremenljivke. S temi operacijami bo množica rešitev ostala ista.

Skica poteka je v zvezku. Na začetku leta sem opozoril, da tu ne bo skic. Če si pričakoval spremembo toplo priporočam da znizaš pričakovanja. Ko pridemo do končne matrike, katere skica nje je v prej omenjenem zvezku, velja

$$\begin{aligned} Ax = b &\iff \\ 1x_{i1} + 0x_{i2} + \cdots + 0x_{ir} + *x_{ir+1} + \cdots + *x_{in} &= * \\ 0x_{i1} + 1x_{i2} + \cdots + 0x_{ir} + *x_{ir+1} + \cdots + *x_{in} &= * \\ &\vdots \\ 0x_{i1} + 0x_{i2} + \cdots + 1x_{ir} + *x_{ir+1} + \cdots + *x_{in} &= * \\ 0x_{i1} + 0x_{i2} + \cdots + 0x_{ir} + 0x_{ir+1} + \cdots + 0x_{in} &= \delta \end{aligned}$$

Če je  $\delta = 1$ , je sistem protisloven, če pa je  $\delta = 0$ , ima sistem  $n - r$  parametrično družino rešitev. Parametri so

$$\begin{aligned} x_{ir+1} &= \alpha_1 \\ &\vdots \\ x_{in} &= \alpha_{n-r} \end{aligned}$$

rešitve enačbe pa so

$$\begin{aligned} x_{i1} &= * + *\alpha_1 + \cdots + *\alpha_{n-r} \\ x_{i2} &= * + *\alpha_1 + \cdots + *\alpha_{n-r} \\ &\vdots \\ x_{ir} &= * + *\alpha_1 + \cdots + *\alpha_{n-r} \end{aligned}$$

PRIMER: Obravnavaj sistem linearnih enačb:

$$\begin{aligned} x_1 + 2x_2 + 3x_3 + 4x_4 &= 1 \\ 5x_1 + 4x_2 + 3x_3 + 2x_4 &= -1 \\ 3x_1 + 4x_2 + 5x_3 + 6x_4 &= p \end{aligned}$$

glede na realen parameter  $p$ .

$$\begin{aligned} \left[ \begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1 \\ 5 & 4 & 3 & 2 & -1 \\ 3 & 4 & 5 & 6 & p \end{array} \right] &\rightarrow \left[ \begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1 \\ 0 & -6 & -12 & -18 & -6 \\ 0 & -2 & -4 & -6 & p-3 \end{array} \right] \rightarrow \left[ \begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1 \\ 0 & 1 & 2 & 3 & 1 \\ 0 & -2 & -4 & -6 & p-3 \end{array} \right] \rightarrow \\ &\left[ \begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1 \\ 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 0 & 0 & p-1 \end{array} \right] \rightarrow \left[ \begin{array}{cccc|c} 1 & 0 & -1 & -2 & -1 \\ 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 0 & 0 & p-1 \end{array} \right] \end{aligned}$$

Sistem je neprotisloven natanko takrat, kadar je  $p - 1 = 0$ , torej  $p = 1$ .

$$\begin{aligned} x_1 - x_3 - 2x_4 &= -1 \\ x_2 + 2x_3 + 3x_4 &= 1 \\ x_3 &= \alpha_1 \\ x_4 &= \alpha_2 \end{aligned}$$

Za  $p = 1$  torej velja:

$$\begin{aligned} x_1 &= -1 + \alpha_1 + 2\alpha_2 \\ x_2 &= 1 - 2\alpha_1 - 3\alpha_2 \\ x_3 &= \alpha_1 \\ x_4 &= \alpha_2 \end{aligned}$$

kjer sta  $\alpha_1$  in  $\alpha_2$  realna parametra.

V resnici rešujemo sistem  $Ax = b$ , kjer je  $x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$

Spomnimo se, da za množico rešitev  $R$  velja  $R = w + \ker A$ , kjer je  $w$  partikularna rešitev. Torej velja

$$\begin{aligned} x \in R &\iff x = \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} 1 \\ -2 \\ 1 \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 2 \\ -3 \\ 0 \\ 1 \end{bmatrix} \\ R &= \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \text{Lin} \left\{ \begin{bmatrix} 1 \\ -2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ -3 \\ 0 \\ 1 \end{bmatrix} \right\} \end{aligned}$$

$$\Rightarrow \begin{bmatrix} 1 \\ -2 \\ 1 \\ 0 \end{bmatrix} \text{ in } \begin{bmatrix} 2 \\ -3 \\ 0 \\ 1 \end{bmatrix} \text{ tvorita bazo jedra } \ker A.$$

#### 4.8.8 Simultano reševanje sistemov z isto matriko koeficientov

$$AX^{(1)} = B^{(1)}$$

$$AX^{(2)} = B^{(2)}$$

$$\dots$$

$$AX^{(p)} = B^{(p)}$$

Zapišemo lahko

$$X = \begin{bmatrix} X^{(1)} & \dots & X^{(p)} \end{bmatrix} \in \mathcal{O}^{n \times p}$$

$$B = \begin{bmatrix} B^{(1)} & \dots & B^{(p)} \end{bmatrix} \in \mathcal{O}^{m \times p}$$

Torej rešujemo sistem  $AX = B$ .

Z Gaussom dobimo  $\begin{bmatrix} A & | & B \end{bmatrix} \rightarrow \begin{bmatrix} A' & | & B' \end{bmatrix}$ .

POSEBEN PRIMER:

$A \in \mathcal{O}^{n \times n}$ ,  $A$  obrnljiva ( $\Rightarrow \text{rang } A = n$ ).

$$A' = I.$$

$$AX = B \iff IX = B' \Rightarrow B' = X = A^{-1}B$$

$$B' = A^{-1}B$$

Vzamemo  $B = I$ , dobimo  $B' = A^{-1}$ .

$$\begin{bmatrix} A & | & I \end{bmatrix} \rightarrow \begin{bmatrix} I & | & A^{-1} \end{bmatrix}$$

#### 4.8.9 Sprememba baze

$V$  v.p. nad  $\mathcal{O}$ .

$\mathcal{V} = \{v_1, \dots, v_n\}$  urejena baza



$\mathcal{V}' = \{v'_1, \dots, v'_n\}$  urejena baza

$$v'_j = p_{1j}v_1 + p_{2j}v_2 + \dots + p_{nj}v_n$$

$$P = [p_{ij}] \quad i, j = 1, \dots, n \quad \in \mathcal{O}^{n \times n}$$

$P$  je prehodna matrika med  $\mathcal{V}$  in  $\mathcal{V}'$ .

Skica, ki naj bi bila v zvezku zelo pomaga pri naslednjem sklepu

$$P = \Phi_{\mathcal{V}}(\Phi'_{\mathcal{V}})^{-1}$$

$$id_V v'_j = v'_j = p_{1j}v_1 + \dots + p_{nj}v_n$$

POSEBEN PRIMER:

$$V = \mathcal{O}^n$$

$\mathcal{V} = \{e_1, e_2, \dots, e_n\}$  standardna baza

$P$  - prehodna matrika

$$\Rightarrow v'_j = p_{1j}e_1 + p_{2j}e_2 + \dots + p_{nj}e_n = \begin{bmatrix} p_{1j} \\ p_{2j} \\ \vdots \\ p_{nj} \end{bmatrix} = P^{(j)}$$

$$\Rightarrow \mathcal{V}' = \{P^{(1)}, P^{(2)}, \dots, P^{(n)}\}$$

Naj bo  $\mathcal{A} \in \mathcal{L}(V, U)$  in naj bosta  $\mathcal{V}, \mathcal{V}'$  bazi  $V$  in  $\mathcal{U}, \mathcal{U}'$  bazi  $U$ . Naj  $A \in \mathcal{O}^{m \times n}$  pripada  $\mathcal{A}$  glede na  $\mathcal{V}, \mathcal{U}$  in naj  $\mathcal{A}' \in \mathcal{O}^{m \times n}$  pripada  $\mathcal{A}$  glede na  $\mathcal{V}', \mathcal{U}'$ .

$P$  naj bo prehodna matrika med  $\mathcal{V}$  in  $\mathcal{V}'$ ,  $Q$  pa naj bo prehodna matrika med  $\mathcal{U}$  in  $\mathcal{U}'$ .

$$P \in \mathcal{O}^{n \times n}, \quad Q \in \mathcal{O}^{m \times m}$$

Zanima nas zveza med  $A'$  in  $A$ .

V zvezku na tem mestu stoji (ali pa leži, odvisno v kakšni poziciji bereš zvezek) en velik diagram, ki komutira. Iz tega diagrama razberemo

$$A' = Q^{-1}AP$$

POSEBEN PRIMER:

$\mathcal{A} = A$ ,  $\mathcal{V}, \mathcal{U}$  standardni bazi v  $V = \mathcal{O}^n$  in  $U = \mathcal{O}^m$

$\Rightarrow A' = Q^{-1}AP$  je matrika, ki pripada  $A$  glede na urejeni bazi  $\mathcal{V}' = \{P^{(1)}, \dots, P^{(n)}\}$  in  $\mathcal{U} = \{Q^{(1)}, \dots, Q^{(m)}\}$

#### 4.8.10 Ekivalentnost matrik

Naj bosta  $A, B \in \mathcal{O}^{m \times n}$

DEFINICIJA:  $B$  je *ekvivalentna*  $A$  ( $B \sim A$ ), kadar obstajata taki obrnljivi matriki  $P, Q$ , da velja

$$B = Q^{-1}AP$$

$\sim$  je ekvivalenčna relacija:

- $A \sim A$  (refleksivnost) (za  $Q, P$  vzamemo  $I$ )
- $A \sim B \Rightarrow B \sim A$  (simetričnost) ( $B = Q^{-1}AP \Rightarrow A = \underbrace{QBP^{-1}}_{(Q^{-1})^{-1}B(P^{-1})}$ )
- $A \sim B \wedge B \sim C \Rightarrow A \sim C$  (tranzitivnost) (dokaz za DN)

TRDITEV: Naj bo  $\mathcal{A} \in \mathcal{L}(V, U)$ . Potem obstajata v  $V$  in  $U$  taki urejeni bazi, da ima matrika, ki pripada  $\mathcal{A}$  v teh dveh bazah obliko

$$A_0 = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \end{bmatrix}$$

kjer je  $r = \text{rang } \mathcal{A}$ .

DOKAZ: Iščemo bazi  $\{v_1, \dots, v_n\}$  v  $V$  in  $\{u_1, \dots, u_n\}$  v  $U$ , tako da bo veljalo:

$$\begin{aligned} \mathcal{A}v_1 &= u_1 \\ \mathcal{A}v_2 &= u_2 \\ &\dots \\ \mathcal{A}v_r &= u_r \\ \mathcal{A}v_{r+1} &= 0 \\ &\dots \\ \mathcal{A}v_n &= 0 \end{aligned}$$

V  $\text{im } \mathcal{A}$  izberemo bazo  $\{u_1, \dots, u_r\}$ . Izberemo še praslke teh elementov  $\{v_1, \dots, v_r\} \in V$ . Velja  $\mathcal{A}v_j = u_j$  za  $j = 1, \dots, r$ .

Razširimo  $\{u_1, \dots, u_r\}$  do baze  $\{u_1, \dots, u_r, \dots, u_m\}$  v. p.  $U$ .

Spomnimo se:  $\dim(\ker \mathcal{A}) = n - \dim(\operatorname{im} \mathcal{A}) = n - r$ .

Izberemo bazo  $\ker \mathcal{A} : \underbrace{\{v_{r+1}, \dots, v_n\}}_{n-r \text{ vektorjev}}$ .

Trdimo, da je  $\{v_1, \dots, v_n\}$  baza  $V$ . Zadošča ugotoviti, da so ti vektorji linearno neodvisni (ker je  $\dim V = n$ ).

$$\begin{aligned} \alpha_1 v_1 + \dots + \alpha_r v_r + \alpha_{r+1} v_{r+1} + \dots + \alpha_n v_n &= 0 \\ \alpha_1 \underbrace{\mathcal{A}v_1}_{u_1} + \dots + \alpha_r \underbrace{\mathcal{A}v_r}_{u_r} + \alpha_{r+1} \underbrace{\mathcal{A}v_{r+1}}_0 + \dots + \alpha_n \underbrace{\mathcal{A}v_n}_0 &= 0 \quad (*) \\ \alpha_1 u_1 + \dots + \alpha_r u_r = 0 &\Rightarrow \alpha_1 = \dots = \alpha_r = 0 \end{aligned}$$

Če to vstavimo v (\*) dobimo:

$$\alpha_{r+1} v_{r+1} + \dots + \alpha_n v_n = 0 \Rightarrow \alpha_{r+1} = \dots = \alpha_n = 0$$

Torej so  $v_1, \dots, v_n$  res linearno neodvisni.

□

POSLEDICA: Vsaka matrika je ekvivalentna matriki oblike  $A_0$ .

DOKAZ:  $A$  razumemo kot prelikavo. Matrika, ki pripada  $A$  glede na bazi  $\{P^{(1)}, \dots, P^{(n)}\}$  in  $\{Q^{(1)}, \dots, Q^{(m)}\}$ , naj bo  $A_0$ . Ker je  $A_0 = Q^{-1}AP$ , sta matriki  $A$  in  $A_0$  ekvivalentni.

**Opomba:**

$$\begin{aligned} A_0 &= Q^{-1}AP \iff AP = QA_0 \\ AP &= [Q^{(1)}, \dots, Q^{(r)}, 0, \dots, 0] \\ [AP^{(1)}, \dots, AP^{(r)}, \dots, AP^{(n)}] &= [Q^{(1)}, \dots, Q^{(r)}, 0, \dots, 0] \\ \iff AP^{(j)} &= Q^{(j)} \text{ za } j = 1, \dots, r \\ AP^{(j)} &= 0 \text{ za } j = r+1, \dots, n \end{aligned}$$

TRDITEV: Matriki  $A, B \in \mathcal{O}^{m \times n}$  sta ekvivalentni natanko takrat, kadar velja

$$\operatorname{rang} A = \operatorname{rang} B$$

DOKAZ:

( $\Rightarrow$ ) Naj bosta  $A, B$  ekvivalentni. Vemo, da velja

$$B = Q^{-1}AP$$

kjer sta  $P$  in  $Q$  obrnljivi matriki. Torej  $B$  pripada preslikavi  $A : \mathcal{O}^n \rightarrow \mathcal{O}^m$  glede na bazi  $\{P^{(1)}, \dots, P^{(n)}\}$  in  $\{Q^{(1)}, \dots, Q^{(m)}\}$ . Po neki trditvi velja  $\text{rang } B = \text{rang } A$ .

( $\Leftarrow$ ) Naj velja  $\text{rang } A = \text{rang } B = r$ . Vemo, da je  $A$  ekvivalentna  $A_0$ . Prav tako je  $B$  ekvivalentna  $B_0$ . Ker  $A, B \in \mathcal{O}^{m \times n}$  imata isti rang, zato je  $A_0 = B_0$ . Torej velja  $A \sim A_0 = B_0 \sim B$ . Iz tranzitivnosti sledi  $A \sim B$ .

□

#### 4.8.11 Podobnost matrik

Naj bo  $\mathcal{A} \in \mathcal{L}(V)$ ,  $\dim V = n$ . In naj bosta  $\mathcal{V}, \mathcal{V}'$  urejeni bazi  $V$ , ter  $P$  prehodna matrika. Matrika  $A \in \mathcal{O}^{n \times n}$  naj pripada preslikavi  $\mathcal{A}$  glede na bazo  $\mathcal{V}$ , matrika  $A' \in \mathcal{O}^{n \times n}$  pa naj pripada preslikavi  $\mathcal{A}$  glede na bazo  $\mathcal{V}'$ . Vemo, da je zveza med  $A'$  in  $A$

$$A' = P^{-1}AP$$

DEFINICIJA: Matrika  $B \in \mathcal{O}^{n \times n}$  je *podobna* matriki  $A \in \mathcal{O}^{n \times n}$ , kadar obstaja taka obrnljiva matrika  $P \in \mathcal{O}^{n \times n}$ , da velja

$$B = P^{-1}AP$$

Označimo z  $B \stackrel{p}{\sim} A$ .

Relacija podobnosti je ekvivalenčna relacija

- refleksivnost:  $A \stackrel{p}{\sim} A$ , za  $P$  vzamemo  $I$ .
- simetričnost  $B = P^{-1}AP \Rightarrow A = PBP^{-1} = (P^{-1})^{-1}BP^{-1}$
- tranzitivnost:  $B \stackrel{p}{\sim} A, B \stackrel{p}{\sim} C \Rightarrow A = P^{-1}BP, B = Q^{-1}CQ \Rightarrow A = P^{-1}Q^{-1}CQP = (QP)^{-1}C(QP) \Rightarrow A \stackrel{p}{\sim} C$

Vse matrike, ki pripadajo danemu endomorfizmu so med seboj podobne.

#### 4.8.12 Diagonalne matrike in diagonalizacija

Naj bo  $A \in \mathcal{O}^{n \times n}$ ,  $A = [a_{ij}]$   $i, j = 1, \dots, n$ . Pravimo, da je  $A$  *diagonalna*, kadar je  $a_{ij} = 0$  za vsak  $i \neq j$ . Oblika  $A$ :

$$A = \begin{bmatrix} a_{11} & & & & \\ & a_{22} & & & \\ & & a_{33} & & \\ & & & a_{44} & \\ & & & & \ddots \\ & & & & & a_{nn} \end{bmatrix}$$

**Zapis:**  $A = \text{diag}(a_{11}, a_{22}, \dots, a_{nn}) = \text{diag}(b_1, b_2, \dots, b_n)$ .

Velja:

$$\begin{aligned} \text{diag}(a_1, \dots, a_n) + \text{diag}(b_1, \dots, b_n) &= \text{diag}(a_1 + b_1, \dots, a_n + b_n) \\ \text{diag}(a_1, \dots, a_n) \text{diag}(b_1, \dots, b_n) &= \text{diag}(a_1 b_1, \dots, a_n b_n) \end{aligned}$$

DEFINICIJA: Endomorfizem  $\mathcal{A} \in \mathcal{L}(V)$  se da *diagonalizirati*, kadar obstaja taka baza  $\mathcal{V} \in V$ , da je matrika  $A$ , ki pripada  $\mathcal{A}$  v tej bazi, diagonalna.

Naj preslikavi  $\mathcal{A}$  v bazi  $\mathcal{V}$  pripada matrika  $A = \text{diag}(a_1, \dots, a_n)$  in naj bo  $\mathcal{V} = \{v_1, \dots, v_n\}$ . Takrat velja:

$$\mathcal{A}v_j = 0v_1 + 0v_2 + \dots + a_j v_j + \dots + 0v_n = a_j v_j \quad j = 1, \dots, n$$

Torej velja:

$$\mathcal{A}v_j = a_j v_j \quad \forall j$$

DEFINICIJA: Vektor  $x \in V \setminus \{0\}$  imenujemo *lastni vektor* endomorfizma  $\mathcal{A} \in \mathcal{L}(V)$ , kadar velja

$$\mathcal{A}x = \lambda x$$

za kakšen  $\lambda \in \mathcal{O}$ . Velja, da je  $\lambda$  enolično določen z  $\mathcal{A}$  in lastnim vektorjem  $x$ .  $\lambda$  imenujemo *lastna vrednost* endomorfizma  $\mathcal{A}$ , ki pripada danemu vektorju  $x$ .

DOKAZ enoličnosti  $\lambda$ :

Naj velja  $\mathcal{A}x = \lambda x$  in  $\mathcal{A}x = \mu x$ . Potem velja

$$\lambda x = \mu x \Rightarrow (\lambda - \mu) \underbrace{x}_{\neq 0} = 0 \Rightarrow \lambda - \mu = 0 \Rightarrow \lambda = \mu$$

Naj bo  $\mathcal{A} \in \mathcal{L}(V)$ ,  $\lambda \in \mathcal{O}$ .  $\lambda$  je lastna vrednost end.  $\mathcal{A}$ , kadar obstaja kakšen lasten vektor  $x$ , da je

$$\mathcal{A}x = \lambda x$$

Poglejmo si množico  $\{x \in V : \mathcal{A}x = \lambda x\}$  za fiksiran  $\lambda \in \mathcal{O}$ .

$$\{x \in V : \mathcal{A}x = \lambda x\} = \{x \in V : (\mathcal{A} - \lambda \mathcal{I})x = 0\} = \ker(\mathcal{A} - \lambda \mathcal{I})$$

kjer je  $\mathcal{I} = id_V$ .

$\ker(\mathcal{A} - \lambda \mathcal{I})$  se imenuje *lastni podprostor* end.  $\mathcal{A}$ , ki pripada l. vrednosti  $\lambda$ .

Če je  $x$  lastni vektor (za  $\mathcal{A}$  in  $\lambda$ ), potem je  $\alpha x$  lastni vektor, če je  $\alpha \neq 0$ .

V  $\ker(\mathcal{A} - \lambda \mathcal{I})$  so vsi lastni vektorji end.  $\mathcal{A}$ , ki pripadajo l. vrednosti  $\lambda$ , poleg njih pa še vektor 0.

**TRDITEV:** Endomorfizem  $\mathcal{A}$  se da diagonalizirati natanko takrat, kadar obstaja baza v. p.  $V$ , sestavljena iz lastnih vektorjev end.  $\mathcal{A}$ . Pripadajoča diagonalna matrika ima na diagonalni lastne vrednosti  $\mathcal{A}$ .

**DOKAZ:** Naj se da  $\mathcal{A}$  diagonalizirati v  $\{v_1, \dots, v_n\} \Rightarrow \mathcal{A}v_j = a_j v_j \quad \forall j$ .

$$A = \text{diag}(a_1, \dots, a_n)$$

$v_j$  je l. vektor  $\forall j (v_j \neq 0)$ .  $a_j$  je lastna vrednost za  $\mathcal{A}$  in  $v_j$ .

Obratno:  $\{v_1, \dots, v_n\}$  je baza iz l. vektorjev  $\mathcal{A}v_j = \lambda_j v_j$ .  $A = \text{diag}(\lambda_1, \dots, \lambda_n)$

**TRDITEV:** Naj bodo  $\lambda_1, \dots, \lambda_h$  različne lastne vrednosti endomorfizma  $\mathcal{A} \in \mathcal{L}(V)$  in  $x_1, \dots, x_h$  pripadajoči vektorji. Potem so  $x_1, \dots, x_h$  linearno neodvisni.

**DOKAZ:** Recimo, da so  $x_1, \dots, x_h$  linearno odvisni. Izberemo najmanjši  $j > 1$ , tako da je  $x_j = \alpha_1 x_1 + \dots + \alpha_{j-1} x_{j-1}$ . Preslikamo z  $\mathcal{A}$ :

$$\begin{aligned} \mathcal{A}x_j &= \alpha_1 \mathcal{A}x_1 + \dots + \alpha_{j-1} \mathcal{A}x_{j-1} \\ \Rightarrow \lambda_j x_j &= \alpha_1 \lambda_1 x_1 + \dots + \alpha_{j-1} \lambda_{j-1} x_{j-1} \end{aligned}$$

Velja tudi:

$$\lambda_j x_j = \lambda_j \alpha_1 x_1 + \dots + \lambda_j \alpha_{j-1} x_{j-1}$$

Če te enačbi odštejemo dobimo:

$$\begin{aligned} (\alpha_1 \lambda_1 - \lambda_j \alpha_1) x_1 + \dots + (\alpha_{j-1} \lambda_{j-1} - \lambda_j \alpha_{j-1}) x_{j-1} &= 0 \\ \alpha_1 (\lambda_1 - \lambda_j) x_1 + \alpha_2 (\lambda_2 - \lambda_j) x_2 + \dots + \alpha_{j-1} (\lambda_{j-1} - \lambda_j) x_{j-1} &= 0 \end{aligned}$$

Zaradi izbire  $j$  (minimalnost) so  $x_1, \dots, x_{j-1}$  linearno neodvisni.

$$\begin{aligned} \Rightarrow \alpha_1 \underbrace{(\lambda_1 - \lambda_j)}_{\neq 0} &= \dots = \alpha_{j-1} \underbrace{(\lambda_{j-1} - \lambda_j)}_{\neq 0} = 0 \\ \Rightarrow \alpha_1 &= \dots = \alpha_{j-1} = 0 \end{aligned}$$

Torej je  $x_j = 0 \rightarrow \leftarrow$ .

Zato so  $x_1, \dots, x_h$  linearno neodvisni.

POSLEDICA: Če ima endomorfizem  $\mathcal{A} \in \mathcal{L}(V)$   $n$  različnih lastnih vrednosti, kjer je  $n = \dim(V)$ , potem se da  $\mathcal{A}$  diagonalizirati.

DOKAZ:  $\lambda_1, \dots, \lambda_n$  različne lastne vrednosti.

$$\begin{aligned} \mathcal{A}x_j &= \lambda_j x_j, & j &= 1, \dots, n \\ x_j &\neq 0 & \forall j \end{aligned}$$

$\Rightarrow \{x_1, \dots, x_n\}$  je baza  $V$  sestavljena iz lastnih vektorjev. Zato se da  $\mathcal{A}$  diagonalizirati.

Naj bo  $A \in \mathcal{O}^{n \times n} = \mathcal{L}(\mathcal{O}^n)$ .  $A$  se da diagonalizirati, kadar je  $A$  podobna diagonalni matriki:

$$\exists P \in \mathcal{O}^{n \times n} \text{ obrnljiva} : P^{-1}AP = D = \text{diag}(d_1, \dots, d_n)$$

Velja:

$$\begin{aligned} AP &= PD \\ \Rightarrow AP^{(j)} &= PD^{(j)} & j &= 1, \dots, n \\ PD^{(j)} &= P(d_j e_j) = d_j P e_j \\ \Rightarrow AP^{(j)} &= d_j P^{(j)} & \forall j \end{aligned}$$

$\Rightarrow P^{(1)}, \dots, P^{(n)}$  so lastni vektorji matrike  $A$ .  $d_1, \dots, d_n$  so pripadajoče lastne vrednosti.

#### 4.8.13 Iskanje lastnih vrednosti in lastnih vektorjev

Naj bo  $\mathcal{A} \in \mathcal{L}(V)$ ,  $\dim V = n$

$$Ax = \lambda x \iff x \in \ker(\mathcal{A} - \lambda \mathcal{I})$$

$\lambda$  je lastna vrednost endomorfizma  $\mathcal{A} \iff \ker(\mathcal{A} - \lambda \mathcal{I}) \neq \{0\} \iff \mathcal{A} - \lambda \mathcal{I}$  ni bijekcija (nima inverza)  $\iff \text{rang}(\mathcal{A} - \lambda \mathcal{I}) < n$ .