Algebra 1

Vid Drobnič

Kazalo

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)

$$f : \mathcal{P} \to V$$
$$f(T) = \vec{OT}$$

f je bijekcija (vsaki točki priredi natanko en vektor).
$\vec{a} = \vec{OT}$

1.1 Operacije z vektorji

Seštevanje:

$$\vec{a}, \vec{b} \in V$$
$$\vec{a} = \vec{AB}, \vec{b} = \vec{BC}$$
$$\vec{a} + \vec{b} = \vec{AC}$$
$$\vec{AB} + \vec{BC} = \vec{AC}$$

LASTNOSTI:[1]

(1) $(\vec{a} + \vec{b}) + \vec{c} = \vec{a} + (\vec{b} + \vec{c})$ asociativnost

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

(3) $\vec{a} + \vec{0} = \vec{a}$

(4) $\vec{a} + (-\vec{a}) = \vec{0}$

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

Razliko dveh vektorjev definiramo tako:

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

Množenje s skalarjem

Skalar je realno število.

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

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

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

[1] 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) $\alpha(\beta\vec{a}) = (\alpha\beta)\vec{a}$

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

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

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

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

1.2 Linearna neodvisnost

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

$\vec{a}, \vec{b}$ sta linearno odvisna kadar je:
bodisi $\vec{b} = \alpha\vec{a}$ za ustrezen $\alpha \in \mathbb{R}$,
bodisi $\vec{a} = \beta\vec{b}$ za ustrezen $\beta \in \mathbb{R}$.

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

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

1. $\vec{OA}$ in $\vec{OB}$ sta linearno odvisna $\Leftrightarrow$ O, A, B kolinearne (ležijo na isti premici).
2. $\vec{a}, \vec{b}$ sta linearno neodvisna $\Leftrightarrow$ $(\alpha\vec{a} + \beta\vec{b} = \vec{0} \Rightarrow \alpha = \beta = 0)$

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

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

$\alpha\vec{a} + \beta\vec{b}$ - linearna kombinacija
$\mathcal{R}$ - ravnina določena z O, A, B (z vektorji $\vec{a}, \vec{b}$) in točko O.

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

Pri tem sta α in β enolično določena skalarja.

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

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

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

1. $\vec{a} = \vec{OA}, \vec{b} = \vec{OB}, \vec{c} = \vec{OC}$ so linearno odvisni $\Leftrightarrow O, A, B, C$ koplanarne (ležijo na isti ravnini)
2. $\vec{a}, \vec{b}, \vec{c}$ so linearno neodvisni $\Leftrightarrow (\alpha\vec{a} + \beta\vec{b} + \gamma\vec{c} = \vec{0} \Rightarrow \alpha = \beta = \gamma = 0)$

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

$\vec{a} = \vec{OA}$
$\vec{b} = \vec{OB}$
$\vec{c} = \vec{OC}$

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

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

V - množica vseh vektorjev prostora $\mathcal{P}$

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

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

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

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

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

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

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

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

Imena koordinat: abscisa, ordinata, aplikata

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

φ je bijekcija.

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

$$
\begin{aligned}
&\vec{r_1}, \vec{r_2} \in V \\
&\quad \vec{r_1} = \alpha_1\vec{a} + \beta_1\vec{b} + \gamma_1\vec{c} \\
&\quad \vec{r_2} = \alpha_2\vec{a} + \beta_2\vec{b} + \gamma_2\vec{c} \\
&\varphi(\vec{r_1}) = (\alpha_1, \beta_1, \gamma_1) \\
&\varphi(\vec{r_2}) = (\alpha_2, \beta_2, \gamma_2)
\end{aligned}
$$

$$
\begin{gathered}
\vec{r_1} + \vec{r_2} = (\alpha_1 + \alpha_2)\vec{a} + (\beta_1 + \beta_2)\vec{b} + (\gamma_1 + \gamma_2)\vec{c} \\
\varphi(\vec{r_1} + \vec{r_2}) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2, \gamma_1 + \gamma_2)
\end{gathered}
$$

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).

$$\begin{aligned} \varphi(\vec{a}) &= (1, 0, 0) \\ \varphi(\vec{b}) &= (0, 1, 0) \\ \varphi(\vec{c}) &= (0, 0, 1) \end{aligned}$$

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

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

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

OZNAKE:

$$\begin{aligned} \vec{i} &= (1, 0, 0) \\ \vec{j} &= (0, 1, 0) \\ \vec{k} &= (0, 0, 1) \end{aligned}$$

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 $\varphi, 0 \leq \varphi \leq \pi$

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

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

$$\begin{aligned} O &= (0,0,0) \\ \vec{i} &= (1,0,0) \\ \vec{j} &= (0,1,0) \\ \vec{k} &= (0,0,1) \end{aligned}$$

$$\begin{aligned} \vec{a} &= (a_1, a_2, a_3) \in \mathbb{R}^3 \\ \vec{b} &= (b_1, b_2, b_3) \in \mathbb{R}^3 \end{aligned}$$

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

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

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

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

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

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

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

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

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

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

Primer:

$$\mathbb{R}^3 \equiv \mathbb{R}^2 \times \{0\}$$
$$\vec{a} = (a_1, a_2, 0)$$
$$\vec{a} \text{ v } \mathbb{R}^2 : \vec{a} = (a_1, a_2)$$
$$\vec{a}\vec{b} = a_1b_1 + a_2b_2$$

p - ploščina paralelograma
p si želimo izraziti z a_1, a_2, b_1, b_2

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

$$\vec{a'}\perp\vec{a}$$
$$|\vec{a'}| = |\vec{a}|$$

$\vec{a}, \vec{a'}$ pozitivno orientirana
$\vec{a'} = (-a_2, a_1)$
$\psi = \frac{\pi}{2} - \varphi$ ali $\varphi - \frac{\pi}{2}$ če je orienacija $(\vec{a}, \vec{b})$ pozitivna.

$$|\vec{a}||\vec{b}| \sin\varphi = |\vec{a}||\vec{b}| \cos\theta = \vec{a'}\vec{b} = (-a2, a_1) \cdot (b_1, b_2) = a_1b_2 - a_2b_1$$

$p = a_1b_2 - a_2b_1$, če je orientacija $\vec{a}, \vec{b}$ pozitivna, če pa je negativna velja: $p = -(a_1b_2 - a_2b_1)$

1.4 Vektorski produkt

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

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

(1) $\vec{a} \times \vec{b}$ je pravokoten na $\vec{a}$ in $\vec{b}$.

(2) $|\vec{a} \times \vec{b}|$ je enaka ploščini paralelograma, ki ga določata $\vec{a}$ in $\vec{b}$. ($= 0$, kadar sta $\vec{a}$ in $\vec{b}$ linearno odvisna)

(3) Urejena trojica $(\vec{a}, \vec{b}, \vec{a} \times \vec{b})$ je pozitivno orientirana.

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

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

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

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

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

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

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

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

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

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

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

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

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

determinanta (reda 2)

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

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

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

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

Lastnosti:

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

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

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

Poseben primer:

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

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

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

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

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

1.5 Mešani produkt

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

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

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

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

$$(\vec{a}\times\vec{b})\vec{c} = (\vec{b}\times\vec{c})\vec{a} = \vec{a}(\vec{b}\times\vec{c})$$
$$(\vec{a}\times\vec{b})\vec{c} = \vec{a}(\vec{b}\times\vec{c}) = [\vec{a},\vec{b},\vec{c}]$$

$$\begin{aligned}
\vec{a} &= (a_1, a_2, a_3) \\
\vec{b} &= (b_1, b_2, b_3) \\
\vec{c} &= (c_1, c_2, c_3)
\end{aligned}$$

$$[\vec{a},\vec{b},\vec{c}] = \vec{a}(\vec{b}\times\vec{c}) = a_1e_1 + a_2e_2 + a_3e_3 =$$
$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} \equiv a_1\begin{vmatrix} b_2 & b_3 \\ c_2 & c_3 \end{vmatrix} - a_2\begin{vmatrix} b_1 & b_3 \\ c_1 & c_3 \end{vmatrix} + a_3\begin{vmatrix} b_1 & b_2 \\ c_1 & c_2 \end{vmatrix}$$

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

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 geomterija v $\mathbb{R}^3$

2.1 Premica

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

$\vec{r_0} = \vec{OR_0} = (x_0, y_0, z_0)$
$R \in p$
$\vec{r} = \vec{OR} = (x, y, z)$

Koorinatizirali smo premico.

$$\vec{R_0R} = \vec{r} - \vec{r_0}$$

$$\vec{r} = \vec{r_0} + \lambda\vec{e}, \lambda \in \mathbb{R}$$

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

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

$$\begin{aligned} x &= x_0 + \lambda a \\ y &= y_0 + \lambda b \\ z &= z_0 + \lambda c \end{aligned}$$

(Parametrična) enačba premice.

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

enačba premice (brez parametra)

$a = 0$?

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

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

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

To je kadar: $\vec{R_0 R} \times \vec{e} = \vec{0} \Leftrightarrow (\vec{r} - \vec{r_0}) \times \vec{e} = \vec{e} \times (\vec{r} - \vec{r_0}) = \vec{0}$
(vektorska enačba premice)

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

$$\Delta = |\vec{r_1} - \vec{r_0}| \sin\varphi$$

To enačbo lahko preoblikujemo da dobimo:

$$\Delta = \frac{|\vec{e} \times (\vec{r_1} - \vec{r_0})|}{|\vec{e}|}$$

To je posebej ugodno, kadar $|\vec{e}| = 1$, saj iz tega sledi $\Delta = |\vec{e} \times (\vec{r_1} - \vec{r_0})|$.

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

2.2 Ravnina

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

Da določimo kdaj točka leži na ravnini zapišemo:

$$R \in \Sigma \Leftrightarrow \vec{r} - \vec{r_0} \perp \vec{n} \Leftrightarrow \vec{n} \cdot (\vec{r} - \vec{r_0}) = 0$$

To pomeni da nam ravnino Σ določa enačba:

$$\vec{n} \cdot (\vec{r} - \vec{r_0}) = 0$$

Če zapišemo vektorje $\vec{r_0}, \vec{r}$ in $\vec{n}$ kot:

$$\begin{aligned} \vec{r_0} &= (x_0, y_0, z_0) \\ \vec{r} &= (x, y, z) \\ \vec{n} &= (a, b, c) \end{aligned}$$

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 en"acbo ravnine, dobimo da lahko ravnino Σ zapišemo kot:

$$((\vec{r_1} - \vec{r_0}) \times (\vec{r_2} - \vec{r_0})) \cdot (\vec{r} - \vec{r_0}) = 0$$

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

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

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

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

$$\Delta = \pm|\vec{r_1} - \vec{r_0}| \cos\varphi \tag{1}$$

To enačbo lahko s pomočjo enačbe ravnine preoblikujemo v:

$$\Delta = \frac{|\vec{n} \cdot (\vec{r_1} - \vec{r_0})|}{|\vec{n}|}$$

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

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

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

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

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

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:

- $\vec{e_1} \times \vec{e_2} \neq \vec{0}(p_1 \nparallel p_2)$
- $p_1 \cap p_2 = \varnothing$ (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 $S_1S_2 \perp p_1, p_2$. To pomeni:

$$\vec{S_1S_2} \perp \vec{e_1}, \vec{e_2}$$
$$\vec{S_1S_2} = \lambda\vec{e_1} \times \vec{e_2}, \lambda \in \mathbb{R}$$

Tu je spet v veliko pomoč skica. Ideja je, da z vzporednim premikom premaknemo vektor $\vec{e_2}$ v izhodišče vektorja $\vec{e_1}$. S tem lahko naredimo ravnino Σ_1, ki jo tvorita ta dva vektorja. Nato naredimo ravnino Σ_2 na podoben način – z vzporednim premikom premaknemo vektor $\vec{e_1}$ v izhošče vektorja $\vec{e_2}$. Velja $\Sigma_1 \parallel \Sigma_2$. Ker sta si ravnini vzporedni lahko premico p_1 z vzporednim premikom premaknemo iz Σ_1 v Σ_2 in dobimo premico p_1^*, ki se seka s premico p_2 v točko S_2. Podobno lahko premaknemo premico p_2 v ranino Σ_1 in dobimo točko S_1 kjer se sekata p_1 in p_2^*. Opazimo, da je daljica S_1S_2 pravokotna na premici p_1 in p_2 in je tudi najkrajša razdalja med tema premicama. To pomeni, da je dolžina daljice S_1S_2 razdalja med premicama p_1 in p_2.

Z nadaljnim premislekom in zelo natančno narisano skico opazimo, da vektorji $\vec{e_1}, \vec{e_2}$ in $\vec{r_1} - \vec{r_2}$ tvorijo paralelepiped, katerega višina je enaka daljici S_1S_2. To pomeni, da lahko uporabimo naše znanje o mešanem produktu in naredimo naslednje:

$$V = |[\vec{r_1} - \vec{r_2}, \vec{e_1}, \vec{e_2}]$$
$$V = |\vec{e_1} \times \vec{e_2}| \cdot \Delta$$

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 $f : A \to B$ 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 $f : A \to B$ je množica $\{f(x) : x \in A\} \subseteq B$.

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

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

$f : A \to B$ 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:

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

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

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

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

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

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

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

za vsak $x \in A$.

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

$$\begin{gathered} id_A : A \to A \\ \forall x \in A : id_A(x) = x \end{gathered}$$

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

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

Graf preslikave $f : A \to B$ 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 *binarjna 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) $A = \{p : p$ - premica v prostoru$\}$

R relacija vzporednosti

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

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

$$x, y \in A \qquad (x \subseteq A, y \subseteq A)$$
$$xRy \equiv x \subseteq y$$

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 ekvivalnečnega 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:

$$\begin{gathered}[a] \subseteq [b] \\ [b] \subseteq [a]\end{gathered}$$

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 $[a] \cap [b] \neq \varnothing$:

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

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

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

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

Primera:

(1) $A = \{\overrightarrow{MN} : M, N -$ 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.

$$\left[\overrightarrow{MN}\right] = \left\{\overrightarrow{XY} : \overrightarrow{XY} \sim \overrightarrow{MN}\right\} = M\vec{N}$$

(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

$M \neq \varnothing$

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

$a \circ b$ 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) $A \neq \varnothing$

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

$\circ$ 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 relacaijo $\sim$, kadar velja sklep:

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

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

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

$\sim$ iz primera (2)

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

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

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

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

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

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

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

3.3 Grupe

Definicije:

- $(M, \circ)$ grupoid

  $e \in M$ je *enota* ali *nevtralni 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

  $$\Rightarrow e_1 = e_2$$

  $\square$

- 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.

  $$a \circ b_1 = b_1 \circ a = e$$
  $$a \circ b_2 = b_2 \circ a = e$$

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

  $\square$

  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) $\forall a, b, c \in G : (ab)c = a(bc)$
  (2) $\exists e \in G \forall a \in G : ae = ea = a$
  (3) $\forall a \in G \exists b \in G : ab = ba = e$
- $(M, \circ)$ 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) $A \neq \varnothing, M = F(A) = \{f : A \to A\}$
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:

$$A = \{1, 2, \ldots, n\}$$
$$S(A) \equiv S_n$$

S_n je *simetrična grupa*.

$$\pi \in S_n$$
$$\pi : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

Če preslikamo vse elemente s preslikavo π dobimo:

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

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

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

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

$$\pi(k) = i_k$$

S tem lahk permutacijo π zapišemo kot:

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

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

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

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

kjer $\rho, \sigma \in S_3$

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

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:

$$ab = ac \Rightarrow b = c$$
$$ab = ca \not\Rightarrow b = c$$
$$b \neq c \Rightarrow ab \neq ac$$

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 prejšen 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 nahajat 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:

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

Za negativne cele eksponente velja podobno:

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

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

$$a^0 \equiv e$$

Sedaj lagko 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:

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

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

Definicija transpozicije:

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

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

τ je *transpozicija.*

Vsaka permutacija je kompozitum samih transpozicij.

Primer:

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

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

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

Startegija 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

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

$$1 \leq j < k \leq n$$

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

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

Primer:

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

Inverzije v π so:

$$(1,3),(1,5)$$
$$(2,3),(2,5)$$
$$(4,5)$$

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

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:

π je soda $\iff s(\pi) = 1$
π 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) $\tau = (i_k, i_{k+1})$

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

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

τ dosežemo s produktom transpozicij podobni tisti v primeru (1). To pomeni, da najprej element i_k premikamo v desno proti i_{k+p}, vsakič za eno mesto, nato pa še element i_{k+p} premikamo nazaj na prvotno mesto elementa i_k. Če znamo vsaj malo algoritmov, se lahko spomnimo na bubble sort. Za ostale, ki ne znajo algoritmov pa obstaja skica, ki se žal ponovno nahaja samo v zvezku in domišliji bralca.

Torej potrebujemo p transpozicij, da premakno element i_k na mesto elementa i_{k+p}. V tem trenutnku, 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 premutacije zamenja, zato velja:

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

saj je $2p - 1$ liho število. □

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

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

kjer so τ_i transpozicije.

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

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

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

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

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

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

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

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

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

kjer τ_i transpozicija in k je sodo.

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

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

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

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

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

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

Definirajmo podgrupo:

Naj bo $(G, \cdot)$ grupa in $H \subseteq G, H \neq \varnothing$. 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.

$$a \in H \overset{(2)}{\Rightarrow} a^{-1} \in H$$
$$a, a^{-1} \in H \overset{(1)}{\Rightarrow} e = aa^{-1} \in H$$

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 $m_1 < m_2$.

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

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

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

in veja:

$$a^{k+1} = a^k a = a$$
$$a^{k+2} = a^k a^2 = a^2$$

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

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

3.4 Abelove 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:

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

Oznake v abelovi grupi:

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

  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 $H\subseteq G, H\neq\varnothing$, 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.

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

$\sim$ 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* $a \sim b \wedge b \sim c \Rightarrow a \sim c$

$$\begin{gathered} a - b \in H \\ b - c \in H \end{gathered}$$

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

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

$\square$

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

$$\begin{gathered} x - a \in H \\ y - b \in H \end{gathered}$$

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

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

$\square$

Zato lahko operacijo + prenesemo na kvocientno množico:

$$G/_\sim = \{[a] : a \in G\}$$
$$\forall a, b \in G : [a] + [b] = [a + b]$$

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

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

Oznaka: $G/_H$ (namesto $G/_\sim$, ker $\sim$ definiramo s pomočjo H)

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

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

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

Uvedemo novi oznaki:

$$[q] \equiv q + H$$
$$[0] = H$$

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

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

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

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

V splošnem zapišemo:

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

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

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

Običajno skrajšamo zapis in pišemo:

$$[j] \equiv j$$
$$\mathbb{Z}/_{n\mathbb{Z}} \equiv \mathbb{Z}_n$$

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

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

Tabela 1: Tabela za $\mathbb{Z}_4$

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

3.5 Homomorfizmi

Definicija: Naj bosta $(G_1, \circ), (G_2, \circ)$ grupoida. Preslikava $f : G_1 \to G_2$ 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 $f : G_1 \to G_2$ homomorfizem, potem je f *endomorfizem*.

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

Trditev: Bijektven homomorfizem je izomorfizem.

Dokaz: Naj bo $f : G_1 \to G_2$ bijektiven homomorfizem, kjer sta G_1 in G_2 grupoida. Trdimo, da je $f^{-1} : G_2 \to G_1$ 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. $\square$

Primeri:

(1) $f : \mathbb{Z} \to G$, $(G, \circ)$ 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:

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

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) $f:\mathbb{Z}_n\to C_n$ 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

$$f(j+k)=z_0^{j+k}=z_0^jz_0^k=f(j)f(k)$$

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

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

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

$$\begin{aligned} f:(\mathbb{R},+)&\to(\mathbb{R}^+,\circ)\\ \mathbb{R}&\to\mathbb{R}^+\end{aligned}$$

Predpis definiramo kot:

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

f je homomorfizem

$$f(x+y)=2^{x+y}=2^x2^y=f(x)f(y)$$

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 $f : G_1 \to G_2$ homomorfizem. Potem velja:

(1) f enoto grupe G_1 preslika v enoto grupe G_2

(2) $\mathrm{im} f = \{f(x) : x \in G_1\}$ (zaloga vrednosti) je podgrupa v G_2[3]

(3) $\ker f = \{x \in G_1 : f(x) = e_2\}$ (e_2 je enota grupe G_2) je podgrupa v G_1[4]

DOKAZ: e_1 enota G_1, e_2 enota G_2

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

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

Označimo

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

Dobili smo:

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

Torej:

$$e_2 = x$$

Sklep: $f(e_1) = e_2$ □

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

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

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

[3] $\mathrm{im} f$ je slika (image) of f

[4] $\ker f$ je jedro (kernel) od f

Velja:

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

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

Podgrupa potrebuje tudi zaprtost za invertiranje:

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

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

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

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

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

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

Množenje definiramo podobno kot seštevanje:

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

Primer množenja v $\mathbb{Z}_6$:

$$3 \cdot 5 = 3$$
$$3 \cdot 4 = 0$$

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

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

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

$(\mathbb{R}^2, +, \cdot)$ 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) $M \neq \varnothing, K = \{f : M \to R\} = \mathbb{R}^M$

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

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

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 niča*. Pravimo, da je a *levi* delitelj niča in b *desni delitelj* niča.

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

4 Vektorski prostori

Definicija: *Vektorski prostor* na obsegom $\mathcal{O}$je Abelova grupa $(V, +)$ skupaj z *zunanjo operacijo*

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

ki ustreza naslednjim pogojem:

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

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 operacijie 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) $M \neq \varnothing \qquad \mathcal{F}(M, \mathbb{R}) \equiv \mathbb{R}^M = \{f : M \to \mathbb{R}\}$

Operaciji definiramo po točkah:

$$(\alpha f)(t) = \alpha f(t) \qquad \forall t \in M (\alpha \in \mathbb{R})$$
$$(f + g)(t) = f(t) + g(t) \qquad \forall t \in M$$

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

V je vekotrski prostor nad $\mathbb{R}$.

4.1 Nekaj osnovnih lastnosti vektorskih prostorov

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

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

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

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

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

Dokaz:

(1)

$$0v = x \in V \Rightarrow$$
$$x + x = 0v + 0v = (0+0)v = 0v = x$$
$$\Rightarrow x + x = x \Rightarrow x = 0$$
$$\Rightarrow 0v = 0$$

(2) Podoben dokaz kot za (1).

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

$$\alpha \neq 0 \Rightarrow \exists \alpha^{-1} \in \mathcal{O} \Rightarrow$$
$$\Rightarrow \alpha^{-1}(\alpha v) = \alpha^{-1} 0 = 0$$
$$\underbrace{(\alpha^{-1}\alpha)}_{1} v = 1v = v$$
$$\Rightarrow v = 0$$

(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 $U \subseteq V, U \neq \varnothing$. 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 je ravnina skozi 0 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:

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

4.3 Linearna ogrinjača

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

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

Velja:

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

Lin$M$ je vektorski podprostor vektorskega prostora V (Lin$M \leq V$)

- Zaprtost za seštevanje:

$$\alpha_1 x_1 + \ldots + \alpha_k x_k \in \text{Lin}M$$
$$\beta_1 x_1 + \ldots + \beta_n y_n \in \text{Lin}M$$

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

- Zaprtost za množenje s skalarjem:

$$\beta(\alpha_1 x_1 + \ldots + \alpha_k x_k) = (\beta\alpha_1)x_1 + \ldots + (\beta\alpha_k)x_k \in \text{Lin}M$$
$$x_1, \ldots, x_k \in M$$

□

Iz tega sledi, da je 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:

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

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 podrpostor, zato okoli naredimo linearno ogrinjačo. Poglejmo si eno zanimivost:

$$x \in \text{Lin}(V_1 \cup V_2)$$
$$x = \underbrace{\alpha_1 x_1 + \ldots \alpha_k x_k}_{\in V_1} + \underbrace{\beta_1 y_1 + \ldots + \beta_n y_n}_{\in V_2} = u + v$$

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:

$$\text{Lin}(V_1 \cup V_2 \cup \ldots \cup V_k) = V_1 + V_2 + \ldots + V_k$$
$$V_i \leq V \forall i$$
$$V_1 + \ldots + V_k = \{x_1 + \ldots + x_k : x_i \in V_i \forall i\}$$

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

$$V_1 \oplus \ldots \oplus V_k$$

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

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

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

$$\begin{aligned}
&\Rightarrow z \in V_1 \cap V_2 = \{0\}\\
&\Rightarrow x = 0 \Rightarrow\\
&\Rightarrow x_1' = x_1 \wedge x_2' = x_2
\end{aligned}$$

$$V_1 \oplus V_2$$

$\square$

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:

$$[x] + [y] = [x + y] \forall x, y \in V$$
$$[z] = z + U \forall z \in V$$

V $V/_U$ uvedemo množenje s skalarji:

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

Definicija je dobra če velja:

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

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

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

$\square$

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 $\mathcal{A} : V \to U$ je *linearna* (= homomorfizem vektorskih prostorov), kadar velja:

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

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

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) $\qquad \forall x \in V$
- $\mathcal{A}(x - y) = \mathcal{A}x - \mathcal{A}y \qquad \forall x, y \in V$

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

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

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: $\mathcal{A}V \to U$ 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 $\mathcal{A} : V \to U$ linearna bijekcija. $\underline{\mathcal{A}^{-1} : U \to V \text{ je linearna}}$

Aditivnost sledi iz dejstva, da je 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 $\square$

PRIMERI:

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

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

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

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

4.5.1 Slika in jedro linearnih preslikav

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

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

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

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

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

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

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

(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 $x = 0 \Rightarrow \ker A = \{0\}$.

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

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

$\square$

Izrek: Naj bo $\mathcal{A} : V \to U$ linearna preslikava. Potem obstaja izomorfizem med vektorskima prostoroma $V/_{\ker\mathcal{A}}$ in $\mathrm{im}\mathcal{A}$. 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

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

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

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

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

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

POSLEDICI: Naj bo $\mathcal{A} : V \to U$ 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 $\mathrm{im}\mathcal{A}$

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

4.6 Vektorski prostor linearnih preslikav

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

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

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

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

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

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
- $\mathcal{A} \in \mathcal{L}(V,U); -\mathcal{A} = -\mathcal{A}x \forall x \in V$

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

Množenje s skalarji definiramo po točkah:

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

$\mathcal{L}(V,U)$ 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).

$$\mathcal{A}, \mathcal{B} \in \mathcal{L}(V)$$
$$(\mathcal{A}\mathcal{B})x = A(Bx), \forall x \in V$$

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

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

- $\mathcal{A}(\mathcal{B} + \mathcal{C}) = \mathcal{A}\mathcal{B} + \mathcal{A}\mathcal{C}$
- $(\mathcal{B} + \mathcal{C})\mathcal{A} = \mathcal{B}\mathcal{A} + \mathcal{C}\mathcal{A}$

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

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

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

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

ki ustreza pogojem:

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

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 $\mathcal{L}(V)$

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

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 $\text{Lin}M = V$

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

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

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

$$M = \{v_1, \dots v_m\} \text{ ogrodje v.p. } V$$
$$x \in V \Rightarrow x = \alpha_1 v_1 + \cdots + \alpha_m v_m, \quad \alpha_1, \dots \alpha_m \in \mathcal{O}$$

Poglejmo si kako je z enolišnostjo zapisa. Naj bo

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

Če je zapis enoličen, velja sklep

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

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

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

Torej velja enoličnost zapisa.

Definicija: Vektorji $v_1, \ldots v_m$ 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 $M = \{v_1, \ldots, v_m\}$ 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 $\alpha_1, \ldots, \alpha_m$ enolično določeni z x natanko takrat, kadar so $v_1, \ldots v_m$ linearno neodvisni.

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

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

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

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

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

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

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

$$p(x) \in \mathbb{R}[x]$$
$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$

Baza tega prostora je

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

Definicija: Vektorji $v_1, \ldots v_m$ so *linearno odvisni*, kadar niso linearno neodvisni.

Naj bodo $v_1, \ldots v_m$ linearno odvisni ($m > 1$). Potem obstajajo tudi skalarji $\alpha_1, \ldots \alpha_m \in \mathcal{O}$, 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 elemetnov $v_2, \ldots v_m$.

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

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

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

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

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

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

$$\exists \alpha_j \neq 0 : j > 1$$
$$k = \max\{j : \alpha_j \neq 0\} \quad (k > 1)$$
$$\Rightarrow v_k = \beta_1 v_1 + \cdots + \beta_1 k - 1 v_{k-1}$$

$\square$

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 $x_i, i \in \{1, \dots, m\} \backslash \{j\}$, potem vektorji $\{x_i : i \in \{1, \dots, m\} \backslash \{j\}\}$ 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 ogorodje, 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 ogrodji in so linearno odvisni. Odstranimo vektor, ki je linearna kombinacija predhotnih. 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: $m \geq n$ $\square$

Posledica: Vse baze netrivialnega končno razsežnege vektorksega 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

$$X = \{x_1, \dots, x_m\}$$
$$Y = \{y_1, \dots, y_n\}$$

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).

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

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

$$\Phi_v : V \to \mathcal{O}^n$$
$$\Phi_v(x) = (\alpha_1, \dots, \alpha_n)$$

Φ_v je odvisen od vrstenga reda baze in je izomorfen . Zapišemo lahko tudi preslikavo

$$\Psi_v : \mathcal{O}^n \to V$$
$$\Psi_v(\alpha_1, \dots, \alpha_n) = \alpha_1 v_1 + \dots + \alpha_n v_n$$

Ψ_v je inverz preslikave $\Phi_v \Rightarrow \Psi_v, \Phi_v$ sta bijekciji. Zadoš'ca dokazati, da je Ψ 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 Φ, Ψ:

$$\Phi : V \to \mathcal{O}^n$$
$$\Psi : \mathcal{O}^n \to U$$

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

($\Rightarrow$) Naj bo $F : V \to U$ 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

$$\alpha_1 F(v_1) + \dots + \alpha_n F(v_n) = 0$$
$$F(\alpha_1 v_1 + \dots + \alpha_n v_n) = F(0)$$
$$\Rightarrow \alpha_1 v_1 + \dots + \alpha_n v_n = 0 \Rightarrow$$
$$\Rightarrow \alpha_1 = \dots = \alpha_n = 0$$

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

$$u \in U \Rightarrow \exists v \in V : F(v) = u$$
$$v = \beta_1 v_1 + \dots + \beta_n v_n \Rightarrow$$
$$\Rightarrow u = f(v) = F(\beta_1 v_1 + \dots + \beta_n v_n) =$$
$$= \beta_1 F(v_1) + \dots + \beta_n F(v_n)$$

$\square$

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

Dokaz: $u_1, \ldots, u_n$ naj tvorijo ogrodje V.

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

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

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

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

Če $\mathcal{U}$ ni ogrodje vektorskega prostora U, obstaja tak $u \in U$ da u ni linearna kombinacija vektorjev $u_1, \ldots, u_m$ ($u \notin \text{Lin}\mathcal{U}$). Potem so vektorji $u_1, \ldots, u_m, u$ 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 $U = V$.

$\square$

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 $U \neq \{0\}, \{u_1, \ldots, u_m\}$ baza U. Dopolnimo jo do baze V

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

Postavimo $W = \text{Lin}\{u_{m+1}, \ldots, u_{m+k}\}$. Če dopolnimo tako, da nič ne dopolnimo potem:

$$W = \mathrm{Lin}\{\} = \{0\}$$
$$U = V$$

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

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

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

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

$\Rightarrow V = U \oplus W$

$\square$

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

$$\{u_1, \ldots, u_m\} \text{ baza } U, \dim U = m$$
$$\{w_1, \ldots, w_n\} \text{ baza } W, \dim W = n$$

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

1. linearna neodvisnost

$$\alpha_1 u_1 + \cdots + \alpha m u_m + \beta_1 w_1 + \cdots + \beta_n w_n = 0$$
$$z = \underbrace{\alpha_1 u_1 + \cdots + \alpha_m u_m}_{\in U} = \underbrace{(-\beta_1) w_1 + \cdots + (-\beta_n) w_n}_{\in W}$$
$$z \in U \cap W = \{0\} \Rightarrow z = 0$$
$$\Rightarrow \alpha_1 = \cdots = \alpha_m = 0,$$
$$\beta_1 = \cdots = \beta_n = 0$$

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

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

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

$$
\begin{gathered}
x \in U \oplus W \Rightarrow \\
\Rightarrow x = u + 2, u \in U, w \in W \\
u = \alpha_1 u_1 + \cdots + \alpha_m u_m \\
w = \beta_1 w_1 + \cdots + \beta_n w_n \\
\Rightarrow x = \alpha_1 u_1 + \cdots + \alpha_m u_m + \beta_1 w_1 + \cdots + \beta_n w_n
\end{gathered}
$$

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

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 $U + W = U \oplus Z$.

$\Rightarrow \dim(U + W) = \dim U + \dim Z$ in
$W = (U \cap W) \oplus \Rightarrow \dim W = \dim(U \cap W) + \dim Z$

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:

$$
\begin{gathered}
f : W \to V/_U \\
f(w) = [w] = w + U
\end{gathered}
$$

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 injektvina

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

f je surjektivna:

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

$f(w) = [v]$

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

$\square$

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 $\mathcal{A}$:

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

4.8.1 Poseben primer

$$V = \mathcal{O}^n, \quad U = \mathcal{O}^m$$
$$A = \mathcal{L}(\mathcal{O}^n, \mathcal{O}^m)$$
$$\{e_1, \dots, e_n\} \text{ standardna baza } \mathcal{O}^n$$
$$e_j = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \end{bmatrix}$$
$$x \in \mathcal{O}^n, \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

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

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

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

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

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

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

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

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

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

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

$$Ax = y$$

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

y izračunamo kot:

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

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

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

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

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

$$A^{(3)} = A\vec{k} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

$$A^{(1)} = A\vec{i} = \begin{bmatrix} \cos\varphi'' \sin\varphi \\ 0 \end{bmatrix}$$

$$A^{(2)} = A\vec{j} = \begin{bmatrix} -\sin\varphi \\ \cos\varphi \\ 0 \end{bmatrix}$$

$$A = \begin{bmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

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

$$(A + B)x = Ax + Bx \quad \forall x \in \mathcal{O}^n$$

$$(\underbrace{A + B}_{C\in\mathcal{O}^{m\times n}})e_j = Ae_j + Be_j = A^{(j)} + B^{(j)}$$

$$\Rightarrow C^{(j)} = Ce_j = A^{(j)} + B^{(j)}$$

$$\Rightarrow c_{ij} = a_{ij} + b_{ij} \quad \forall i, j$$

$\Rightarrow$ 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 $\mathcal{O}$.

$$
\begin{aligned}
\dim V &= n \\
\dim U &= m \\
\mathcal{V} &= \{v_1, \dots, v_n\} \text{ urejena baza } V \\
\mathcal{U} &= \{u_1, \dots, u_n\} \text{ urejena baza } U
\end{aligned}
$$

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

$$
\begin{aligned}
&\Phi_{\mathcal{V}} : V \to \mathcal{O}^n \text{ izomorfizem} \\
&v \in V \\
&v = \alpha_1 v_1 + \cdots + \alpha_n v_n \\
&v \to (\alpha_1, \dots, \alpha_n) = \Phi_{\mathcal{V}}(v) = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}
\end{aligned}
$$

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

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

$$
\begin{tikzcd}
\mathrm{V} \arrow[r, "\mathcal{A}"] \arrow[d, "\Phi_{\mathcal{V}}"'] & \mathrm{U} \arrow[d, "\Phi_{\mathcal{U}}"] \\
\mathcal{O}^n \arrow[r, "A"'] & \mathcal{O}^m
\end{tikzcd}
$$

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 $A \in \mathcal{O}^{m\times n}$.

$$F : \mathcal{L}(V, U) \to \mathcal{O}^{m\times n}$$
$$\mathcal{A} \mapsto A = F(\mathcal{A})$$
$$F(\mathcal{A}) = \Phi_{\mathcal{U}}\mathcal{A}\,(\Phi_{\mathcal{V}})^{-1}$$

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

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

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

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

$$E_{pq} = [e_{ij}] \quad i = 1, \ldots, m \quad j = 1, \ldots, n$$
$$e_{ij} = \begin{cases} 1 & i = p \wedge j = q \\ 0 & \text{sicer} \end{cases}$$

4.8.3 Množenje matrik

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

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

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

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

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

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 $\mathcal{U} = \mathcal{V} = \mathbb{V}$. Skonstruiramo preslikavo

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

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 $\underline{F(\mathcal{A}\mathcal{B}) = F(\mathcal{A})F(\mathcal{B})}$

$$F(\mathcal{AB}) = \Phi_\mathcal{V}(\mathcal{AB})\Phi_\mathcal{V}^{-1}$$
$$F(\mathcal{A})F(\mathbb{B}) = \Phi_\mathcal{V}\mathcal{A}\Phi_\mathcal{V}^{-1}\Phi_\mathcal{V}\mathcal{B}\Phi_\mathcal{V}^{-1} = \Phi_\mathcal{V}\mathcal{AB}\Phi_\mathcal{V}^{-}1$$

□

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 δ_{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 ($\exists \mathcal{B} \in \mathcal{L}(V) : \mathcal{A}\mathbb{B} = \mathcal{BA} = id_V$). 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 vektorksa prostora nad $\mathcal{O}$ in $\mathcal{A} \in \mathcal{L}(V, U)$.

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

$$\dim(\mathrm{im}\mathcal{A}) + \dim(\ker\mathcal{A}) = \dim V \tag{2}$$

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

$\square$

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

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

1. $\mathcal{A}$ je injektivna $\iff$ $\operatorname{rang} \mathcal{A} = \dim V$
2. $\mathcal{A}$ je surjektivna $\iff$ $\operatorname{rang} A = \dim U$
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 $\iff$ $\mathrm{im}\mathcal{A} = U$
$$\mathrm{im}\mathcal{A} = U \iff \underbrace{\dim(\mathrm{im}\mathcal{A})}_{\operatorname{rang} \mathcal{A}} = \dim U$$
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 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 $\mathcal{A}$ gelde na dai baz $\mathcal{V} \in V, \mathcal{U} \in U$. Potem velja:

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

DOKAZ: Narišemo si diagram in opazimo, da komutira.

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

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

$$\begin{gathered} \dim(\text{im}\mathcal{A}) = \dim(\text{im}A) \\ \operatorname{rang} \mathcal{A} = \operatorname{rang} A \end{gathered}$$

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

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

TRDITEV: Stolpci matrike A tvorijo ogrodje vektorskega prostora 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

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

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

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

Velja podoben razmislek kot pri S2, zato zadošča

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

V1, V2, V3 ohranjajo $\ker A$

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

V1) očitno iz zgornje enakosti

V2)

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

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)

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

Pokazati moramo

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

($\Leftarrow$) očitno

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

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

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 $\operatorname{rang} A$ 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 $\operatorname{rang} A = \operatorname{rang} A_0 = 2$.

POSLEDICA Rang matrike je enak rangu njene *transponiranke*.

$$\operatorname{rang} A = \operatorname{rang} A^{\mathsf{T}}$$

Če je $A = [a_{ij}] \in \mathcal{O}^{m\times n}$, transponiranko $B = A^\intercal$, 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 $A^\intercal$. 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 $A \in \mathcal{O}^{m\times n}, \quad A = [a_{ij}]$. 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 $\mathcal{R} = \varnothing$, 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

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

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): $\mathcal{R} \neq \varnothing$ natanko takrat, kadar je

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

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

$$\begin{gathered} \operatorname{im}[A|b] = \operatorname{Lin}\{A^{(1)}, \ldots, A^{(n)}, b\} \\ \operatorname{im} A = = \operatorname{Lin}\{A^{(1)}, \ldots, A^{(n)}\} \\ \dim(\operatorname{im}[A|b]) = \dim(\operatorname{im} A) \iff \operatorname{im} A = \operatorname{im}[A|b] \iff b \in \operatorname{im} A \end{gathered}$$

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

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

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

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

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

rešitve enačbe pa so

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

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.

$$\begin{bmatrix}1&2&3&4&|&1\\5&4&3&2&|&-1\\3&4&5&6&|&p\end{bmatrix}\to\begin{bmatrix}1&2&3&4&|&1\\0&-6&-12&-18&|&-6\\0&-2&-4&-6&|&p-3\end{bmatrix}\to\begin{bmatrix}1&2&3&4&|&1\\0&1&2&3&|&1\\0&-2&-4&-6&|&p-3\end{bmatrix}\to$$
$$\begin{bmatrix}1&2&3&4&|&1\\0&1&2&3&|&1\\0&0&0&0&|&p-1\end{bmatrix}\to\begin{bmatrix}1&0&-1&-2&|&-1\\0&1&2&3&|&1\\0&0&0&0&|&p-1\end{bmatrix}$$

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 α_1 in α_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

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

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

4.8.8 Simultano reševanje sistemov z isto matriko koeficienotv

$$\begin{aligned} AX^{(1)} &= B^{(1)} \\ AX^{(2)} &= B^{(2)} \\ &\dots \\ AX^{(p)} &= B^{(p)} \end{aligned}$$

Zapišemo lahko

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

Torej rešujemo sistem $AX = B$.

Z Gaussom dobimo $\begin{bmatrix} A & \mid & B \end{bmatrix} \to \begin{bmatrix} A' & \mid & B' \end{bmatrix}$.

Poseben primer:

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

$A' = I$.

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

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

$$\begin{bmatrix} A & \mid & I \end{bmatrix} \to \begin{bmatrix} I & \mid & A^{-1} \end{bmatrix}$$

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

$$v_j' = p_{1j}v_1 + p_{2j}v_2 + \dots + p_{nj}v_n$$
$$P = \left[p_{ij}\right] i,j = 1,\dots,n \quad \in \mathcal{O}^{n\times n}$$

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

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

$$P = \Phi_{\mathcal{V}}(\Phi_V')^{-1}$$
$$id_V v_j' = v_j' = p_{1j}v_1 + \dots + p_{nj}v_n$$

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 $A' \in \mathcal{O}^{m\times n}$ 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 Ekvivalentnost 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 $r = \operatorname{rang} \mathcal{A}$.

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

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

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

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

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

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

Trdimo, da je $\{v1, \ldots, v_n\}$ baza V. Zadošča ugotoviti, da so ti vektorji linearno neodvisni (ker je $\dim V = n$).

$$\begin{gathered}
\alpha_1 v_1 + \cdots + \alpha_r v_r + \alpha_{r+1} v_{r+1} + \cdots + \alpha_n v_n = 0 \\
\alpha_1 \underbrace{\mathcal{A}v_1}_{u_1} + \cdots + \alpha_r \underbrace{\mathcal{A}v_r}_{u_r} + \alpha_{r+1} \underbrace{\mathcal{A}v_{r+1}}_{0} + \cdots + \alpha_n \underbrace{\mathcal{A}v_n}_{0} = 0 \qquad (*) \\
\alpha_1 u_1 + \cdots + \alpha_r u_r = 0 \Rightarrow \alpha_1 = \cdots = \alpha_r = 0
\end{gathered}$$

Če to vstavimo v (*) dobimo:

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

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

$\square$

Posledica: Vsaka matrika je ekvivalentna matriki oblike A_0.

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

Opomba:

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

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

$$\mathrm{rang}\, A = \mathrm{rang}\, B$$

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 $A : \mathcal{O}^n \to \mathcal{O}^m$ glede na bazi $\{P^{(1)}, \ldots, P^{(n)}\}$ in $\{Q^{(1)}, \ldots, Q^{(m)}\}$. Po neki trditvi velja $\operatorname{rang} B = \operatorname{rang} A$.

($\Leftarrow$) Naj velja $\operatorname{rang} A = \operatorname{rang} B = r$. 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 $A \sim B$.

$\square$

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 $A' \in \mathcal{O}^{m\times n}$ 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 $B \overset{p}{\sim} A$.

Relacija podobnosti je ekvivalenčna relacija

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

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

4.8.12 Diagonalne matrike in diagonalizacija

Naj bo $A \in \mathcal{O}^{n\times n}, A = [a_{ij}] \quad i,j = 1,\ldots,n$. 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: $A = \operatorname{diag}(a_{11}, a_{22}, \ldots, a_{nn}) = \operatorname{diag}(b_1, b_2, \ldots, b_n)$.

Velja:

$$\begin{aligned} \operatorname{diag}(a_1,\ldots,a_n) + \operatorname{diag}(b_1,\ldots,b_n) &= \operatorname{diag}(a_1+b_1,\ldots,a_n+b_n) \\ \operatorname{diag}(a_1,\ldots,a_n)\operatorname{diag}(b_1,\ldots,b_n) &= \operatorname{diag}(a_1b_1,\ldots,a_nb_n) \end{aligned}$$

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 $A = \operatorname{diag}(a_1,\ldots,a_n)$ in naj bo $\mathcal{V} = \{v_1,\ldots,v_n\}$. Takrat velja:

$$\mathcal{A}v_j = 0v_1 + 0v_2 + \cdots + a_jv_j + \cdots + 0v_n = a_jv_j \qquad j = 1,\ldots,n$$

Torej velja:

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

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 λ enolično določen z $\mathcal{A}$ in lastnim vektorjem x. λ imenujemo *lastna vrednost* endomorfizma $\mathcal{A}$, ki pripada danemu vektorju x.

Dokaz enoličnosti λ:

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 $\mathcal{A} \in \mathcal{L}(V), \lambda \in \mathcal{O}$. λ 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 λ.

Če je x lastni vektor (za $\mathcal{A}$ in λ), potem je αx 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 λ, 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 diagonali lastne vrednosti $\mathcal{A}$.

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

$A = \mathrm{diag}(a_1, \ldots, a_n)$

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

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

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

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

$$\mathcal{A}x_j = \alpha_1\mathcal{A}x_1 + \cdots + \alpha_{j-1}\mathcal{A}x_{j-1}$$
$$\Rightarrow \lambda_j x_j = \alpha_1\lambda_1 x_1 + \cdots + a_{j-1}\lambda_{j-1}x_{j-1}$$

Velja tudi:

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

Če te enačbi odštejemo dobimo:

$$(\alpha_1\lambda_1 - \lambda_j\alpha_1)x_1 + \cdots + (\alpha_{j-1}\lambda_{j-1} - \lambda_j\alpha_{j-1})x_{j-1} = 0$$
$$\alpha_1(\lambda_1 - \lambda_j)x_1 + \alpha_2(\lambda_2 - \lambda_j)x_2 + \cdots + \alpha_{j-1}(\lambda_{j-1} - \lambda_j)x_{j-1} = 0$$

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

$$\Rightarrow \alpha_1 \underbrace{(\lambda_1 - \lambda_j)}_{\neq 0} = \cdots = \alpha_{j-1} \underbrace{(\lambda_{j-1} - \lambda_j)}_{\neq 0} = 0$$
$$\Rightarrow \alpha_1 = \cdots = \alpha_{j-1} = 0$$

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

Zato so $x_1, \ldots, x_h$ 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: $\lambda_1, \ldots, \lambda_n$ različne lastne vrednosti.

$$\mathcal{A}x_j = \lambda_j x_j, \qquad j = 1, \ldots, n$$
$$x_j \neq 0 \quad \forall j$$

$\Rightarrow$ $\{x_1, \ldots, x_n\}$ 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:

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

Velja:

$$AP = PD$$
$$\Rightarrow AP^{(j)} = PD^{(j)} \quad j = 1, \ldots, n$$
$$PD^{(j)} = P(d_j e_j) = d_j P e_j$$
$$\Rightarrow AP^{(j)} = d_j P^{(j)} \quad \forall j$$

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

4.8.13 Iskanje lastnih vrednosti in lastnih vektorjev

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

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

λ 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) $\iff \operatorname{rang}(\mathcal{A}-\lambda\mathcal{I}) < n$.

Primer: $n = 3$, $\quad \mathcal{O} = \mathbb{R}$. Kdaj je $\operatorname{rang}(A - \lambda I) < 3$?

$\iff$ stolpci oziroma vrstice matrike $A - \lambda I$ so linearno odvisni
$\iff$ mešani produkt vseh vrstic matrike $A - \lambda I$ je enak 0
$\iff$ $\det(A - \lambda I) = 0$

$$\det(A-\lambda I) = \begin{vmatrix} a_{11}-\lambda & a_{12} & a_{13} \\ a_{21} & a_{22}-\lambda & a_{23} \\ a_{31} & a_{32} & a_{33}-\lambda \end{vmatrix} = a_0 + a_1\lambda + a_2\lambda^2 + a_3\lambda^3$$

Hitro lahko razberemo, da je $a_3 = -1$. Torej je λ lastna vrednost $A \iff \Delta_A(\lambda) = 0$, kjer je

$$\Delta_A(\lambda) = a_0 + a_1\lambda + a_2\lambda^2 - \lambda^3$$

Ničle polinoma $\Delta_A(\lambda)$, $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$, so lastne vrednosti matrike A. Pravimo, da je $\Delta_A(\lambda)$ *karakteristični polinom* matrike A.

4.8.14 Determinante

Naj bosta V in U vektorska porstora nad $\mathcal{O}$. Definiramo

$$V^n = \underbrace{V \times V \times \cdots \times V}_{n}$$

Velja

$$(v_1, v_2, \ldots, v_n) \in V^n$$
$$\forall j \quad v_j \in V$$

Definicija: $F : V^n \to U$ je n-*linearna*, kadar so za vsak $(v_1, \ldots, v_n) \in V^n$ preslikave $F_j : V \to U \quad (j = 1, \ldots n)$, definirane s predpisom

$$F_j(x) = F(v_1, \ldots, v_{j-1}, x, v_{j+1}, \ldots, v_n)$$

linearne.

Če je $n = 2$ pravimo da je preslikava *bilinearna*, če je $n = 3$ pa pravimo, da je preslikava *trilinearna*.

Primeri:

(1) Skalarni produkt na $\mathbb{R}^3$

$$F : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$$
$$V = \mathbb{R}^3, \quad U = \mathbb{R}$$
$$F(\vec{a}, \vec{b}) = \vec{a} \cdot \vec{b}$$

F je bilinearna preslikava

$F_1(\vec{x}) = F(\vec{x}, \vec{b}) = \vec{x} \cdot \vec{b} F_1(\vec{x} + \vec{y}) = (\vec{x} + \vec{y}) \cdot \vec{b} = \vec{x}\vec{b} + \vec{y}\vec{b} = F_1(\vec{x}) + F_1(\vec{y})$

Torej je F_1 aditivna. Podobno hitro se preveri, da je tudi homogena. Zato je F_1 linearna. Podobno velja tudi za F_2, zato je F bilinearna.

(2) Vektroski produkt v $\mathbb{R}^3$

$$F : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$$
$$V = \mathbb{R}^3, \quad U = \mathbb{R}^3$$
$$F(\vec{a}, \vec{b}) = \vec{a} \times \vec{b}$$

Podbno kot v prvem primeru preverimo linearnost preslikav F_1 in F_2 in opazimo, da je tudi v tem primeru F bilinearna.

(3) Mešani produkt v $\mathbb{R}^3$

$$F : \mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$$
$$V = \mathbb{R}^3, \quad U = \mathbb{R}$$
$$F(\vec{a}, \vec{b}, \vec{c}) = (\vec{a} \times \vec{b}) \cdot \vec{c}$$

Podobno kot v prvih dveh primerih preverimo linearnost preslikav F_1, F_2 in F_3 in opazimo, da je F trilinearna preslikava.

Primer računanja: Naj bo $F : V^2 \to U$ bilinearna

$$\begin{aligned} F(u, w) &= F(\alpha_1 v_1 + \cdots + \alpha_n v_n, \beta_1 w_1 + \cdots + \beta_n w_n) = \\ &= \alpha_1 F(v_1, w) + \alpha_2 F(v_2, w) + \cdots + \alpha_n F(v_n, w) = \\ &= \alpha_1 F(v_1, \beta_1 w_1 + \cdots + \beta_n w_n) + \cdots = \\ &= \alpha_1(\beta_1 F(v_1, w_1) + \beta_2 F(v_1, w_2) + \cdots + \beta_n(v_1, w_n)) = \\ &= \sum_{1 \le i,j \le n} \alpha_i \beta_j F(v_1, w_j) \end{aligned}$$

Definicija: $F : V^n \to U$ je *antisimetrična*, kadar velja za vsak $(v_1, \ldots, v_n) \in V^n$ enakost

$$F(v_1, \ldots, v_j, \ldots, v_k, \ldots, v_n) = -F(v_1, \ldots, v_k, \ldots, v_j, \ldots, v_n)$$

Primera: Vektorski in mešani produkt.

Naj bo $\mathcal{O}$ obseg, kjer $1 + 1 \neq 0$. Potem je $F(v_1, \ldots, v_n) = 0$, če je $v_j = v_k$ za kakšen $j \neq k$.

$$\begin{gathered} F(v_1, \ldots, v_n) = -F(v_1, \ldots, v_n) \Rightarrow \\ 2F(v_1, \ldots, v_n) = 0 \Rightarrow F(v_1, \ldots, v_n) = 0 \end{gathered}$$

Naj bo $\pi \in S_n, \pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$ Potem velja:

$$F(v_{i_1}, v_{i_2}, \ldots, v_{i_n}) = s(\pi) F(v_1, \ldots, v_n)$$

Kjer je

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

Determinanta reda 3 je trilinearna in antisimetrična. Če želimo to posplošiti, iščemo n-linearen antisimetričen funkcional.

Naj bo $V = \mathcal{O}^n, U = \mathcal{O}$ in naj bo $F : V^n \to U$, to je $F : (\mathcal{O}^n)^n \to \mathcal{O}$. Poglejmo si $(\mathcal{O}^n)^n$.

$$(\mathcal{O}^n)^n = \underbrace{\mathcal{O}^n \times \mathcal{O}^n \times \cdots \times \mathcal{O}^n}_{n}$$

Torej lahko matriko $\mathcal{O}^{n \times n}$ identificiramo z $(\mathcal{O}^n)^n$, to je $(A^{(1)}, \ldots, A^{(n)}) \equiv A$.

Torej iščemo n-linearen antisimetričen funkcional $F : \mathcal{O}^{n \times n} \equiv (\mathcal{O}^n)^n \to \mathcal{O}$. Recimo, da je F tak funkcional.

$$\begin{aligned} F(A) &= F(A^{(1)}, A^{(2)}, \ldots, A^{(n)}) = \\ &= F(\underbrace{a_{11}e_1 + a_{21}e_2 + \cdots + a_{n1}e_n}_{A^{(1)}}, \underbrace{a_{12}e_1 + \cdots + a_{n2}e_n}_{A^{(2)}}, \ldots, \underbrace{a_{1n}e_1 + \cdots + a_{nn}e_n}_{A^{(n)}}) = \\ &= \sum_{1 \leq i_1, i_2, \ldots, i_n \leq n} F(a_{i_1 1} e_{i_1}, a_{i_2 2} e_2, \ldots, a_{i_n n} e_n) = \\ &= \sum_{1 \leq i_1, i_2, \ldots, i_n \leq n} a_{i_1 1} a_{i_2 2} \cdots a_{i_n n} F(e_{i_1}, e_{i_2}, \ldots, e_{i_n}) = \\ &= \sum_{\pi \in S_n} s(\pi) a_{i_1 1} a_{i_2 2} \cdots a_{i_n n} F(e_1, \ldots, e_n) \end{aligned}$$

kjer je $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$. $i_1, i_2, \dots, i_n$ so različni. Ostali sumandi so $s_0 = 0$ zaradi antisimetričnosti.

Determinatno definiramo kot

$$\det A = \sum_{\pi \in S_n} s(\pi) a_{i_1 1} a_{i_2 2} \cdots a_{i_n n}$$

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

$$\begin{aligned} \det : \mathcal{O}^{n \times n} &\to \mathcal{O} \\ A &\mapsto \det A \end{aligned}$$

Ugotovili smo, da če je $F : \mathcal{O}^{n \times n} \to \mathcal{O}$ n-linearen antisimetričen funkcional, potem velja

$$F(A) = F(I) \cdot \det A$$

Trditev: $\det : \mathcal{O}^{n \times n} \to \mathcal{O}$ je n-linearen antisimetričen funkcional.

Dokaz:

- n-linearnost (na prvem faktorju, ker zaradi antisimetričnosti velja na ostalih)

  Homogenost:

$$\begin{aligned} &\det(\alpha A^{(1)}, A^{(2)}, \dots, A^{(n)}) = \\ &\qquad = \sum_{\pi \in S_n} s(\pi)(\alpha a_{i_1 1}) a_{i_2 2} \cdots a_{i_n n} = \\ &\qquad\qquad = \alpha \det A \end{aligned}$$

  Aditivnost:

$$\begin{aligned} &\det(B^{(1)} + C^{(1)}, A^{(2)}, \dots, A^{(n)}) = \\ &\qquad = \sum_{\pi \in S_n} s(\pi)(b_{i_1 1} + c_{i_1 1}) a_{i_2 2} \cdots a_{i_n n} = \\ &\qquad = \sum_{\pi \in S_n} s(\pi) b_{i_1 1} a_{i_2 2} \cdots a_{i_n n} + \sum_{\pi \in S_n} c_{i_1 1} a_{i_2 2} \cdots a_{i_n n} = \\ &\qquad = \det(B^{(1)}, A^{(2)}, \dots, A^{(n)}) + \det(C^{(1)}, A^{(2)}, \dots, A^{(n)}) \end{aligned}$$

- antisimetričnost:

$$\begin{aligned}
&\det(A^{(2)}, A^{(1)}, A^{(3)}, \ldots, A^{(n)}) = \\
&\qquad = \sum_{\pi \in S_n} a_{i_1 2} a_{i_2 1} a_{i_3 3} \cdots a_{i_n n} = \\
&\qquad = \sum_{\pi \in S_n} a_{i_2 1} a_{i_1 2} a_{i_3 3} \cdots a_{i_n n} = \\
&\qquad = \sum_{\rho \in S_n} s(\rho) a_{i_2 1} a_{i_1 2} a_{i_3 3} \cdots a_{i_n n} = -\det A
\end{aligned}$$

kjer je $\rho = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_2 & i_1 & i_3 & \ldots & i_n \end{pmatrix}$, torej je $s(\rho) = -s(\pi)$.

Torej so n-linearni antisimetrični funkcionali $F : \mathcal{O}^{n \times n} \to \mathcal{O}$ točno vsi funkcionali oblike $F(A) = \alpha \det(A)$, kjer je $\alpha \in \mathcal{O}$. Pri tem je $\alpha = F(I)$.

4.8.15 Lastnosti determinante

1. Velja $\det(A^\intercal) = \det A$.

   Dokaz: Naj bo $B = A^\intercal, B = [b_{ij}]$ kjer je $b_{ij} = a_{ji}, \quad \forall i, j$.

   $$\det B = \sum_{\pi \in S_n} s(\pi) b_{i_1 1} b_{i_2 2} \cdots b_{i_n n} =$$

   $$= \sum_{\pi \in S_n} s(\pi) a_{1 i_1} a_{2 i_2} \cdots a_{n i_n} = \sum_{\rho \in S_n} s(\rho) a_{j_1 1} a_{j_2 2} \cdots a_{j_n n}$$

   Ustrezna permutacija $\rho = \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}$ je enaka $\rho = \begin{pmatrix} i_1 & i_2 & \ldots & i_n & \\ 1 & 2 & 2 & \ldots & n \end{pmatrix} = \pi^{-1}$. Ker velja $s(\rho) = s(\pi)$, dobimo

   $$\det B = \det A$$

   Torej je
   $$\det A^\intercal = \det A$$

2. **Determinanta in operacije za računanje ranga**

   - Pri medsebojni zamenjavi dveh stolpcev (vrstic), se determinanta pomnoži z -1 zaradi antisimetričnosti. Za vrstice velja $\det A^\intercal = \det A$.

- Pri množenju stolpca (vrstice) z α, se determinanta pomnoži z α, ker je n-linearen funkcional.
- Če stolpcu prištejemo večkratnik kakega drugega stolpca (analogno za vrstice), se determinanta ohrani.

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

Iz definicije determinante sledi, da če ima A kak stolpec (ali vrstico) enak 0, je $\det A = 0$.

Če stolpcu prištejemo linearno kombinacijo drugih stolpcev, se determinanta ohrani.

Recimo, da so stolpci matrike A linearno odvisni. Npr $A^{(1)} = \alpha_2 A^{(2)} + \cdots + \alpha_n A^{(n)}$. $A^{(1)}$ prištejemo $(-\alpha_2)A^{(2)} + \cdots + (-\alpha_n)A^{(n)}$ in dobimo stolpec 0. Ker se determinanta ohrani, je $\det A = 0$.

Trditev: Če matrika ni obrnljiva je $\det A = 0$ ($\det A \neq 0 \Rightarrow \exists A^{-1}$).

Dokaz: A ni obrnljiva $\Rightarrow$ rang $A < n \Rightarrow$ stolpci matrike A so linearno odvisni $\Rightarrow \det A = 0$.

Naj bo A zgornje ali spdnje trikotna matrika. Potem velja

$$\det A = \prod_{i=1}^{n} a_{ii}$$

To hitro vidimo, če si narišemo shemo matrike, kar je v zvezku.

Če je v zgornje trikotni matriki $a_{ii} \neq 0$ za $i = 1, \dots n$, je ta matrika obrnljiva.

3. **Multiplikativnost** Za $A, B \in \mathcal{O}^{n\times n}$ velja

$$\det(AB) = \det A \cdot \det B$$

Dokaz: Naj bo $F : \mathcal{O}^{n\times n} \to \mathcal{O}$ in $A \in \mathcal{O}^{n\times n}$. F definiramo kot

$$F(X) = \det(AX)$$

F je n-linearna antisimetrična preslikava. Velja

$$F(X) = F(X^{(1)}, \dots, X^{(n)}) = \det(AX^{(1)}, \dots, AX^{(n)})$$

Vemo, da velja

$$F(X) = F(I) \det X$$
$$F(I) = \det(AI) = \det A$$

Od tod sledi

$$\det(AX) = (\det A)(\det X)$$

$\square$

Recimo, da je A obrnljiva. Potem velja

$$AA^{-1} = I \Rightarrow \underbrace{\det(AA^{-1})}_{(\det A)(\det A^{-1})} = \det I = 1 \Rightarrow \det(A^{-1}) = (\det A)^{-1}$$

Torej velja, da če je A obrnljiva, je $\det A \neq 0$. Vemo že, da velja obratno, torej velja

$$\exists A^{-1} \iff \det A \neq 0$$

4. **Razvoj determinante**

Definicija: Naj bo $A \in \mathcal{O}^{n\times n}$ in $n > 0$.. $A_{ij} \in \mathcal{O}^{(n-1)\times(n-1)}$ dobimo tako, da iz A odstranimo i-to vrstico in j-ti stolpec. Pravimo, da je A_{ij} *podmatrika.*

Poddeterminanto matrike A definiramo kot

$$(-1)^{i+j} \det A_{ij} \equiv \widetilde{a_{ij}}$$

Matrika $\widetilde{A} = [\widetilde{a_{ij}}]$ $i, j = 1, \ldots, n \in \mathcal{O}^{n\times n}$ je *prirejenka* matrike A.

Poglejmo si naslednjo determinanto

$$\det \begin{bmatrix} A^{(1)} & \ldots & A^{(n-1)} & e_n \end{bmatrix} =$$
$$\sum_{\pi\in S_n} s(\pi) a_{i_1 1} a_{i_2 2} \cdots a_{i_{n-1} n-1} = \sum_{\rho \in S_{n-1}} s(\rho) a_{i_1 1} \cdots a_{i_{n-1} n-1} = \det A_{nn}$$

Kjer je $\pi = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & n \end{pmatrix}$, ker je drugače $a_{i_n n} = 0$. ρ definiramo kot $\rho = \begin{pmatrix} 1 & \cdots & n-1 \\ i_1 & \cdots & i_{n-1} \end{pmatrix} \in S_{n-1}$. Velja $s(\pi) = s(\rho)$.

Poglejmo si še

$$\det \begin{bmatrix} A^{(1)} & \ldots & e_i & \ldots & A^{(n)} \end{bmatrix}$$

Kjer je e_i na j-tem mestu. Želeli bi si matriko preoblikovati v takšno obliko, kot smo jo obravnavali v prejšnjem primeru. Žal ne moremo kar zamenjati i-te in n-te vrstice, ter j-tega in n-tega stolpca, ker bi s tem spremenili vsrtni red stolpcev in vrstic v matriki. Lahko pa postopoma premikamo stolpec/vrstico, tako da delamo neke vrste transpozicije (skica v zvezku). S tem pridelamo podmatriko A_{ij}, ki ima v zadnjem stolpcu enotski vektor e_n. Zaradi antisimteričnosti se nam spremeni predznak determinante. Torej dobimo

$$\det \begin{bmatrix} A^{(1)} & \dots & e_i & \dots & A^{(n)} \end{bmatrix} = \\ = (-1)^{(n-i)+(n-j)} \det A_{ij} = (-1)^{i+j} \det A_{ij} = \widetilde{a_{ij}}$$

Poglejmo si, *razvoj* determinante po j-tem stolpcu.

$$\det A = \det \begin{bmatrix} A^{(1)} & \cdots & \underbrace{a_{1j}e_1 + a_{2j}e_2 + \cdots + a^{nj}e_n}_{A^{(j)}} & \cdots & A^{(n)} \end{bmatrix} = \\ = \sum_{i=1}^{n} a_{ij} \det \begin{bmatrix} A^{(1)} & \cdots & e_i & \cdots & A^{(n)} \end{bmatrix} = \sum_{i=1}^{n} a_{ij}\widetilde{a_{ij}}$$

Torej velja

$$\sum_{i=1}^{n} a_{ij}\widetilde{a_{ij}} = \det A \quad \forall j$$

Če zamenjamo A z $A^\intercal$, dobimo podobno formulo za razvoj determinante po i-it vrstici

$$\sum_{j=1}^{n} a_{ij}\widetilde{a_{ij}} = \det A \quad \forall i$$

Za $j \neq k$ velja

$$\sum_{i=1}^{n} a_{ij}\widetilde{a_{ik}} = \det \begin{bmatrix} A^{(1)} & \cdots & \underbrace{A^{(j)}}_{j\text{-to mesto}} & \cdots & \underbrace{A^{(j)}}_{k\text{-to mesto}} & \cdots & A^{(n)} \end{bmatrix} = 0$$

Torej velja

$$\sum_{i=1}^{n} a_{ij}\widetilde{a_{ik}} = 0 \quad \forall j,k : j \neq k$$

Če A zamenjamo z $A^\intercal$ dobimo podobno za vrstice

$$\sum_{j=1}^{n} a_{ij}\widetilde{a_{kj}} = 0 \quad \forall i,k : i \neq k$$

Te formule lahko združimo v naslednje

$$A\widetilde{A}^\intercal = \begin{bmatrix} \det A & 0 & \cdots & 0 \\ 0 & \det A & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \det A \end{bmatrix} = (\det A)I$$

Podobno lahko zapišemo

$$\widetilde{A}^{\mathsf{T}} A = (\det A) I$$

To dvoje lahko združimo v

$$\widetilde{A}^{\mathsf{T}} A = A \widetilde{A}^{\mathsf{T}} = (\det A) I$$

Posledica: Če je $\det A \neq 0$ velja

$$A^{-1} = (\det A)^{-1} \widetilde{A}^{\mathsf{T}}$$

Determinante nekatirh matrik posebne oblike:

$$\det \begin{bmatrix} A & * \\ 0 & B \end{bmatrix} = (\det A)(\det B)$$

kjer sta A in B kvadratni matriki.

Osnovna ideja dokaza:

Delamo indukcijo glede na velikost matirke A in razvoj determinante po prvem stolpcu.

Za $k = 1$ velja:

$$\det \begin{bmatrix} a_{11} & * \\ 0 & B \end{bmatrix} = a_{11} \det B$$

Za $k = 2$ veja:

$$\det \begin{bmatrix} a_{11} & a_{12} & \\ a_{21} & a_{22} & \\ & & B \end{bmatrix} = a_{11}(a_{22} \det B) - a_{21}(a_{12} \det B) =$$

$$= \det B(a_{11}a_{22} - a_{12}a_{21}) = (\det A)(\det B)$$

Sorodno naredimo za $k \rightsquigarrow k + 1$.

Če imamo bločno zgornje trikotno matriko velja

$$\det \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix} = (\det A_1)(\det A_2) \cdots (\det A_k)$$

Podobno velja tudi za bločno spodnje trikotne.

Bločno diagonalno matriko lahko zapišemo kot

$$\begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix} = \operatorname{diag}(A_1, A_2, \ldots, A_k)$$

in velja

$$\det(\operatorname{diag}(A_1, \ldots, A_k)) = (\det A_1) \cdots (\det A_k)$$

4.8.16 Determinanta endomorfizma

Naj bo preslikava $\mathcal{A} \in \mathcal{L}(V)$ in naj bosta A, A' matriki, ki pripada preslikavi $\mathcal{A}$. Ker sta si A in A' podobni, velja

$$\begin{aligned} A' &= P^{-1}AP \\ PA' &= AP \end{aligned}$$

Od tod sledi

$$\begin{aligned} \det(PA') &= \det(AP) \\ (\det P)(\det A') &= (\det A)(\det P) \\ \exists P^{-1} &\Rightarrow \det P \neq 0 \\ &\Rightarrow \det A' = \det A \end{aligned}$$

Podobni matriki imata enako determinanto. Zato je smiselno definirati

$$\det \mathcal{A} = \det A$$

(neodvisno od izbire baze v V)

CRAMERJEVA FORMULA:

Naj bo $Ax = b, A \in \mathcal{O}^{n \times n}$ sistem enačb innaj bo $\det A \neq 0$. Vemo, da je $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$. Definiramo

$$A_j = \left[A^{(1)}, \ldots, A^{(j-1)}, b, A^{(j+1)}, \ldots, A^{(n)}\right]$$

Cramerjeva formula pravi, da velja

$$x_j = \frac{\det A_j}{\det A}, \quad j = 1, \ldots, n$$

Dokaz:

Ker $\det A \neq 0$, obstja A^{-1}. Vemo, da velja

$$A^{-1} = \frac{1}{\det A}\widetilde{A}^{\intercal}$$

Zato velja

$$Ax = b \Rightarrow x = A^{-1}b = \frac{1}{\det A}\widetilde{A}^{\intercal}b \Rightarrow$$

$$\Rightarrow x_j = \frac{1}{\det A}\left(\widetilde{A}^{\intercal}b\right)_j = \frac{1}{\det A}\underbrace{\left(\widetilde{a_{1j}}b_1 + \widetilde{a_{2j}}b_2 + \cdots + \widetilde{a_{nj}}b_n\right)}_{\text{razvoj determinante po } j\text{-tem stolpcu}} =$$

$$\frac{1}{\det A}\det\left[A^{(1)}, \ldots, b, \ldots, A^{(n)}\right]$$

4.8.17 Karakteristični polinom in minimalni polinom

Naj bo $A \in \mathcal{O}^{n\times n}$. Potem je

$$\Delta_A(\delta) = \det(A - \lambda I)$$

karakteristični polinom matrike A (glej $A \in \mathbb{R}^3$). $\Delta_A(\delta)$ je polinom n-te stopnje s koeficienti v $\mathcal{O}$.

$$\Delta_A(\delta) = \det\begin{bmatrix} a_{11}-\lambda & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-\lambda & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-\lambda \end{bmatrix} =$$

$$= (a_{11}-\lambda)(a_{22}-\lambda)\cdots(a_{nn}-\lambda) + \underbrace{p(\lambda)}_{\text{st} \leq n-2} = a_0 + a_1\lambda + \cdots + a_{n-1}\lambda^{n-1} + a_n\lambda^n$$

Iz tega zapisa lahko hitro razberemo, da veljajo naslednje enačbe

$$a_n = (-1)^n$$

$$a_{n-1} = (-1)^{n-1}\overbrace{(a_{nn} + a_{22} + \cdots + a_{nn})}^{slA}$$

$$a_0 = \det A$$

Izrek: Naj bo $A \in \mathcal{O}^{n\times n}$ in $\Delta_A(\delta)$ njen karakteristični polinom. Potem je $\alpha \in \mathcal{O}$ lastna vrednost matrike A natanko takrat, kadar je

$$\Delta_A(\alpha) = 0$$

DOKAZ: $\alpha \in \mathcal{O}$:

α je lastna vrednost $A \iff A-\alpha I$ ni obrnljiva $\iff \det(A-\alpha I)=0 \iff \Delta_A(\alpha)=0$

$\square$

Za lastne vektorje rešujemo homogen sistem $(A-\alpha I)x=0$.

Naj bo preslikava $\mathcal{A} \in \mathcal{L}(V)$ in naj ji pripadata matriki A, A'. Vemo $A' = P^{-1}AP$. Velja

$$\begin{aligned}\Delta_{A'} = \det(A' - \lambda I) = &\\ &= \det(P^{-1}AP - \lambda I) = \det(P^{-1}(A-\lambda I)P) = \\ &= \underbrace{(\det(P^{-1}))}_{(\det P)^{-1}} \det(A-\lambda I)(\det P) = \\ &\qquad = \det(A-\lambda I) = \Delta_A\end{aligned}$$

Torej velja

$$\Delta_{A'}(\lambda) = \Delta_A(\lambda)$$

Zato je smiselno definirati

$$\Delta_{\mathcal{A}}(\lambda) = \Delta_A(\lambda)$$

Torej je α lastna vrednost endomorfizma $\mathcal{A}$ natanko takrat, ko je $\Delta_{\mathcal{A}}(\alpha)=0$.

POLINOM Z MATRIČNIMI KOEFICIENTI

Naj bo

$$p(\lambda) = A_0 + A_1\lambda + \cdots + A_k\lambda^k, \quad A_j \in \mathcal{O}^{n\times n}$$

To lahko zapišemo v matriko kot

$$p(\lambda) = \begin{bmatrix} p_{11}(\lambda) & \cdots & \cdots \\ \vdots & & \vdots \\ \cdots & \cdots & p_{nn}(\lambda) \end{bmatrix} = [p_{ij}(\lambda)], \quad i,j = 1,\dots,n$$

kjer je $p_{ij}(\lambda)$ polinom s koeficienti v $\mathcal{O}$ in stopnja $p_{ij}(\lambda) \leq k$.

Naj bo $B \in \mathcal{O}^{n\times n}$. Potem je

$$p(B) = A_0 + A_1B + A_2B^2 + \cdots + A_kB^k$$

in B je ničla polinoma $p(\lambda)$, če je $p(B)=0$.

Naj bo
$$q(\lambda) = a_0 + a_1\lambda + \cdots + a_k\lambda^k$$
in $a_i \in \mathcal{O}, \quad i = 0, 1, \ldots, k$. Naj bo $B \in \mathcal{O}^{n\times n}$. Potem je
$$q(B) = a_0 I + a_1 B + a_2 B^2 + \cdots + a_k B^k$$
B je ničla polinoma $q(\lambda)$, če je $q(B) = 0$.

Izrek (Cayley, Hamilton): Kvadratna matrika je ničla svojega karakterističnega polinoma.

Dokaz:
$$(A - \lambda I)\widetilde{(A - \lambda I)}^{\mathsf{T}} = (\det(A - \lambda I))I$$
$$\begin{aligned}\widetilde{(A - \lambda I)}^{\mathsf{T}} &= [p_{ij}(\lambda)] \quad i, j = 1, \ldots, n \\ &= B_0 + B_1\lambda + \cdots + B_{n-1}\lambda^{n-1} \\ \Rightarrow (A - \lambda I)(B_0 + B_1\lambda + \cdots &+ B_{n-1}\lambda^{n-1}) = \\ = \Delta_A(\lambda)I &= (a_0 + a_1\lambda + \cdots + a_n\lambda^n)I\end{aligned}$$
Zmnožimo in uredimo po potencah λ, nato izenačimo keoficiente:
$$\begin{aligned} AB_0 &= a_0 I & & \\ AB_1 - B_0 &= a_1 I & &\cdot A \\ AB_2 - B_1 &= a_2 I & &\cdot A^2 \\ &\vdots & & \\ AB_{n-1} - B_{n-2} &= a_{n-1} I & &\cdot A^{n-1} \\ -B_{n-1} &= a_n I & &\cdot A^n \end{aligned}$$
Če te enačbe šeštejemo, dobimo
$$0 = \underbrace{a_0 I + a_1 A + a_2 A^2 + \cdots + a_n A^n}_{\Delta_A(A)}$$
$$\Rightarrow \Delta_A(A) = 0$$
Naj bo $A \in \mathcal{O}^{n\times n}$. Označimo
$$P = \{p(\lambda) : p(A) = 0\}$$
in velja $\Delta(\lambda) \in P$.

Definicija: *Minimalni polinom* matrike A:
$$m_A(\lambda) \in P$$
Vodilni koeficient $m_A(\lambda)$ je 1 in velja
$$\operatorname{st} m_A(\lambda) \leq \operatorname{st} p(\lambda), \quad p \in P \setminus \{0\}$$

Lastnosti:

(1) $m_A(\lambda) | \Delta_A(\lambda) \quad (\exists q(\lambda) : \Delta_A(\lambda) = q(\lambda) \cdot m_A(\lambda))$

Dokaz:

$$\Delta_A(\lambda) = q(\lambda) m_A(\lambda) + o(\lambda)$$
$$\operatorname{st} o(\lambda) < \operatorname{st} m_A(\lambda)$$

λ zamenjamo z A in dobimo

$$\underbrace{\Delta_A(A)}_{0} = q(A) \underbrace{m_A(A)}_{0} + o(A)$$

Od tod sledi

$$\begin{aligned} &\Rightarrow o(A) = 0 \\ &\Rightarrow o(\lambda) = 0 \quad \text{drugače protislovje z def.}\, m_A(\lambda) \\ &\Rightarrow \Delta_A(\lambda) = q(\lambda) m_A(\lambda) \end{aligned}$$

(2) $\alpha \in \mathcal{O} : m_A(\alpha) = 0 \iff \Delta_A(\alpha) = 0$

Dokaz:

($\Rightarrow$) Uporabimo (1).

($\Leftarrow$) $\Delta_A(\alpha) = 0 \Rightarrow \alpha$ je lastna vrednost A, zato obstaja $x \in \mathcal{O}^n, x \neq 0$, ki je lasten vektor matrike A, to je, $Ax = \alpha x$. Torej velja

$$\begin{gathered} m_A(\lambda) = q(\lambda)(\lambda - \alpha) + m_A(\alpha) \\ \lambda \leftrightarrow A \\ \underbrace{m_A(A)}_{0} = q(A)(A - \alpha I) + m_A(\alpha) I \qquad | \cdot x \\ \Rightarrow 0 = q(A) \underbrace{(A - \alpha I)x}_{Ax - \alpha x = 0} + m_A(\alpha) x \\ \Rightarrow m_A(\alpha) x = 0 \Rightarrow m_A(\alpha) = 0 \end{gathered}$$

$\square$

Poglejmo si obseg kompleksni števil $\mathcal{O} = \mathbb{C}$.

$$\Delta_A(\lambda) = (-1)^n (\lambda - \lambda_i)^{n_1} \cdots (\lambda - \lambda_k)^{n_k}$$

$\lambda_1, \dots, \lambda_k$ so različne ničle $\Delta_A(\lambda)$ in so edine lastne vrednosti matrike A. n_j je *algebrajska kratnost* lastne vrednost λ_j. Zapišemo lahko

$$m_A(\lambda) = (\lambda - \lambda_1)^{m_1} \cdots (\lambda - \lambda_k)^{m_k}$$

in velja $1 \leq m_j \leq n_j \quad \forall j$.

PRIMER:

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$
$$\Delta_A(\lambda) = \det(A - \lambda I) = \det \begin{bmatrix} -\lambda & -1 \\ -1 & -\lambda \end{bmatrix} = \lambda^2 + 1 = (\lambda - i)(\lambda + i)$$

Torej sta i in $-i$ kompleksni lastni vrednosti matrike A.

TRDITEV: Podobni matriki imata isti minimalni polinom.

DOKAZ:

$$B = P^{-1}AP$$
$$B^2 = (P^{-1}AP)(P^{-1}AP) = P^{-1}A^2P$$
$$B^j = \underbrace{(P^{-1}AP) \cdots (P^{-1}AP)}_{j} = P^{-1}A^jP$$
$$p(\lambda) = a_0 + a_1\lambda + \cdots + a_k\lambda^k$$
$$p(B) = a_0I + a_1B + \cdots + a_kB^k = P^{-1}(a_0I + a_1A + \cdots + a_kA^k)P = P^{-1}p(A)P$$
$$\Rightarrow p(B) = P^{-1}p(A)P$$
$$\Rightarrow p(B) = 0 \iff p(A) = 0$$
$$\Rightarrow m_B(\lambda) = m_A(\lambda)$$

Zato definiramo minimalni polinom endomirfizma $\mathcal{A}$ s predpisom

$$m_{\mathcal{A}}(\lambda) = m_A(\lambda)$$

kjer A pripada $\mathcal{A}$ v katerikoli bazi.

Velja

$$\begin{aligned} m_{\mathcal{A}}(\mathcal{A}) &= 0 \\ m_{\mathcal{A}}(\lambda) &= a_0 + a_1\lambda + \cdots + \lambda^k \\ m_{\mathcal{A}}(\mathcal{A}) &= a_0 id_V + a_1\mathcal{A} + \cdots + \mathcal{A}^k = 0 \end{aligned}$$

4.8.18 Invariantni podprostori

$\mathcal{A} \in \mathcal{L}(V)$, vektorski podprostor $U \subseteq V$ je *invarianten* za $\mathcal{A}$, kadar velja

$$x \in U \Rightarrow \mathcal{A}x \in U$$

λ - lastna vrednost $\mathcal{A}$
$\ker(\mathcal{A} - \lambda I)$ - lastni podprostor endomorfizma $\mathcal{A}$
$\ker(\mathcal{A} - \lambda I)$ je invarianten za $\mathcal{A}$

$$\begin{aligned} x \in \ker(\mathcal{A} - \lambda I) \Rightarrow (\mathcal{A} - \lambda I)(\mathcal{A}x) = \\ = (\mathcal{A}^2 - \lambda\mathcal{A})x = \mathcal{A}\underbrace{(\mathcal{A} - \lambda I)x}_{0} = 0 \\ \Rightarrow \mathcal{A}x \in \ker(\mathcal{A} - \lambda I) \end{aligned}$$

Naj bo U invarianten za $\mathcal{A}$. Potem lahko definiramo preslikavo

$$\begin{aligned} &\mathcal{A}_U : U \to U \\ &\mathcal{A}_U x = \mathcal{A}x \quad \forall x \in U \end{aligned}$$

$\mathcal{A}_U$ je zožitev $\mathcal{A}$ na U in $\mathcal{A}_U \in \mathcal{L}(U)$.

Naj bo $\mathcal{A} \in \mathcal{L}(V)$ Potem je

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$$

kjer je V_j invarianten za $\mathcal{A}$ za vse $j = 1, \ldots, k$. Označimo

$$\mathcal{A}_j := \mathcal{A}_{V_j} \in \mathcal{L}(V_j)$$

To zapišemo v obliki

$$\mathcal{A} = \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \cdots \oplus \mathcal{A}_k$$

Naj bodo $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_k$ urejene baze $V_1, V_2, \ldots, V_k$ in A_j matrika, ki pripada endomorfizmu $\mathcal{A}_j$ v bazi $\mathcal{B}_j$. Potem je

$$\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \cdots \cup \mathcal{B}_k$$

urejena baza prostora V, ker $\mathcal{B}_i \cap \mathcal{B}_j = \varnothing$ za vsak $i \neq j$.

Naj bo A matirka, ki pripada endomorfizmu $\mathcal{A}$ v bazi $\mathcal{B}$. Velja

$$A = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix} = \mathrm{diag}(A_1, A_2, \ldots, A_k)$$

Ker dokaz vsebuje veliko skica in je relativno očiten, obstaja samo v zvezku.

Naj bo V kompleksen končno razsežen vektorski prostor.

$$\mathcal{A} \in \mathcal{L}(V) \quad (\mathcal{O} \in \mathbb{C})$$
$$\Delta_{\mathcal{A}}(\lambda) = (-1)^n(\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_k)^{n_k}$$
$$m_{\mathcal{A}}(\lambda) = (\lambda - \lambda_1)^{m_1} \cdots (\lambda - \lambda_k)^{m_k}$$

$\lambda_1, \dots, \lambda_k$ so različne lastne vrednosti $\mathcal{A}$ in velja $1 \leq m_j \leq n_j$ za vsak j.

$$W_j = \ker(\mathcal{A} - \lambda_j I)^{m_j} \quad j = 1, \dots, k$$

W_j je *korenski podprostor* endomorfizma $\mathcal{A}$ (pripada lastni vrednost λ_j).

Izrek: Korenski podprostori $W_j, j = 1, \dots, k$ so invariantni za $\mathcal{A}$, poleg tega pa velja

$$V = W_1 \oplus \cdots \oplus W_k$$

Dokaz: invariantnost

$$x \in W_j \Rightarrow (\mathcal{A} - \lambda_j I)^{m_j} \mathcal{A}x = \mathcal{A}\underbrace{(\mathcal{A} - \lambda_j I)^{m_j}}_{0} x = 0$$
$$\Rightarrow \mathcal{A}x \in W_j$$

Naj bo

$$p_j(\lambda) = \prod_{\substack{i=1\\ i \neq j}}^{k} (\lambda - \lambda_i)^{m_i}$$

$p_1(\lambda), p_2(\lambda), \dots, p_k(\lambda)$ so tuji, ker nimajo nobene skupne ničle. Potem obstajajo taki polinomi $q_1(\lambda), q_2(\lambda), \dots, q_k(\lambda)$, da velja

$$p_1(\lambda)q_1(\lambda) + p_2(\lambda)q_2(\lambda) + \cdots + p_k(\lambda)q_k(\lambda) = 1$$

Torej velja

$$\sum_{i=1}^{k} p_i(\mathcal{A})q_i(\mathcal{A}) = \mathcal{I} \quad (\mathcal{I} = id_V)$$

$$x \in V \Rightarrow x = \mathcal{I}x = \sum_{i=1}^{k} \underbrace{p_i(\mathcal{A})q_i(\mathcal{A})x}_{x_i} = \sum_{i=1}^{k} x_i$$

Trdimo, da je $x_i \in W_i$ (od tod sledi $V = W_1 + \cdots + W_k$).

$$x_i \in \ker(\mathcal{A} - \lambda_i \mathcal{I})^{m_i} \quad ?$$
$$(\mathcal{A} - \lambda_i I)^{m_i} x_i = 0 \quad ?$$
$$m_{\mathcal{A}}(\lambda) = p_i(\lambda)(\lambda - \lambda_i)^{m_i}$$
$$\underbrace{(\mathcal{A} - \lambda_i \mathcal{I})^{m_i} p_i(\mathcal{A})}_{m_{\mathcal{A}}(\mathcal{A}) = 0} q_i(\mathcal{A})x = 0$$

$V = W_1 \oplus \cdots \oplus W_k$ „direktnost"

$$x \in V$$
$$x = x_1 + x_2 + \cdots + x_k, \quad x_i \in W_i \forall i \quad \text{(vemo)}$$
$$x = x_1' + x_2' + \cdots + x_k' \quad x_i \in W_i \forall i$$
$$\Rightarrow x_i = x_i' \forall i \quad ?$$
$$\underbrace{(x_1 - x_1')}_{\in W_1} + \cdots + (\underbrace{x_k - x_k'}_{})_{\in W_k} = 0$$
$$y_i = x_i - x_i' \in W_i \quad \forall i$$
$$y_1 + y_2 + \cdots + y_k = 0$$
$$\Rightarrow y_i = 0 \quad \forall i \quad ?$$
$$y_i \in W_i \Rightarrow (\mathcal{A} - \lambda_i I)^{m_i} y_i = 0$$
$$p_j(\lambda) = \prod_{\substack{i=1 \\ i \neq j}} (\lambda - \lambda_i)^{m_i}$$
$$j \neq i \Rightarrow p_j(\lambda) \text{ vsebuje faktor } (\lambda - \lambda_i)^{m_i}$$
$$\Rightarrow p_j(\mathcal{A}) y_i = 0 \quad \forall i \neq j$$
$$y_1 + y_2 + \cdots + y_k = 0$$
$$\Rightarrow p_j(\mathcal{A})(y_1 + y_2 + \cdots + y_k) = 0$$
$$\Rightarrow p_j(\mathcal{A}) y_j = 0$$
$$y_j = \mathcal{I} y_j = \left(\sum_{i=1}^{k} p_i(\mathcal{A}) q_i(\mathcal{A}) \right) y_j = \sum_{i=1}^{k} q_i(\mathcal{A}) p_i(\mathcal{A}) y_j = 0 \quad \forall j$$

□

Torej velja

$$\mathcal{A} \in \mathcal{L}(V) \Rightarrow \mathcal{A} = \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \cdots \oplus \mathcal{A}_k$$
$$\mathcal{A}_j := \mathcal{A}_{W_j}$$

Izrek: Za zožitve $\mathcal{A}_j \in \mathcal{L}(W_j), j = 1, \ldots, k$, veljajo še naslednje lastnosti:

(i) λ_j je edina lastna vrednost $\mathcal{A}_j$

(ii) $\Delta_{\mathcal{A}_j}(\lambda) = (-1)^{n_j} (\lambda - \lambda_j)^{n_j}$

(iii) $m_{\mathcal{A}_j}(\lambda) = (\lambda - \lambda_j)^{m_j}$

Posledica:

$$\dim W_j = n_j \quad \forall j$$

Dokaz:

$$(\mathcal{A}_j - \lambda_j \mathcal{I}_j)^{m_j} x = (\mathcal{A} - \lambda_j \mathcal{I})^{m_j} x = 0$$
$$\Rightarrow (A_j - \lambda_j \mathcal{I}_j)^{m_j} = 0 \Rightarrow \mathcal{A}_j \text{ je ničla polinoma } (\lambda - \lambda_j)^{m_j}$$

Zato je $m_{\mathcal{A}_j}(\lambda) = (\lambda - \lambda_j)^{t_j}, t_j \leq m_j \quad \forall j$.

$$\Delta_{\mathcal{A}_j}(\lambda) = (-1)^{s_j}(\lambda - \lambda_j)^{s_j}, s_j \geq t_j \quad \forall j$$
$$\Delta_{\mathcal{A}}(\lambda) = \Delta_A(\lambda) = \det(A - \lambda I) = \det(A_1 - \lambda I_1) \cdots \det(A_k - \lambda I_k) =$$
$$= \Delta_{\mathcal{A}_1}(\lambda) \cdots \Delta_{\mathcal{A}_k}(\lambda)$$
$$(-1)^n (\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_k)^{n_k} = (-1)^{s_1}(\lambda - \lambda_1)^{s_1} \cdots (-1)^{s_k}(\lambda - \lambda_k)^{s_k}$$
$$\Rightarrow s_i = n_i \quad \forall i$$
$$m_{\mathcal{A}_j}(\lambda) = (\lambda - \lambda_j)^{t_j} \quad t_j \leq m_j$$
$$r(\lambda) = (\lambda - \lambda_1)^{t_1} \cdots (\lambda - \lambda_k)^{t_k}$$
$$\mathrm{st}(r) = t_1 + t_2 + \cdots + t_k \leq m_1 + m_2 + \cdots + m_k = \mathrm{st}(m_{\mathcal{A}}(\lambda))$$

Ker je $(\mathcal{A}_j - \lambda \mathcal{I}_j)^{t_j} = 0$, velja

$$r(\mathcal{A}) = (\mathcal{A} - \lambda_1 \mathcal{I}_1)^{t_1} \cdots (\mathcal{A} - \lambda_k \mathcal{I}_k)^{t_k} = 0$$

Zato je $t_1 + \cdots + t_k = m_1 + \cdots + m_k$. Od tod dobimo $t_j = m_j \quad \forall j$.