ALGEBRA 1 - ZAPISKI

Gal Anton Gorše

1 Vektorji v prostoru

Uporabljali bomo oznake $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in R\}$ in $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) : x, y, z \in \mathbb{R}\}$. Vsaki točki $T(x, y, z)$ lahko priredimo usmerjeno daljico, ki se začne v O in konča v tej točki. Tej daljici pravimo krajevni vektor točke T in jo označimo z $\vec{r} = (x, y, z)$ ali

$$\vec{r} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$

Množico $\mathbb{R}^3$ si sedaj lahko predstavljamo kot

$$\mathbb{R}^3 = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} : x, y, z \in \mathbb{R} \right\}.$$

1.1 Zveza z običajnimi vektorji

Enako usmerjene daljice lahko med seboj identificiramo. Vektor, ki poteka od točke $A(x_1, y_1, z_1)$ do točke $B(x_2, y_2, z_2)$, je

$$\overrightarrow{AB} = \begin{bmatrix} x_2 - x_1 \\ y_2 - y_1 \\ z_2 - z_1 \end{bmatrix}$$

Definicija 1.1. Osnovne operacije z vektorji v $\mathbb{R}^3$ definiramo naslednje:

- Seštevanje vektorjev $a = (x_1, y_1, z_1)$ in $b = (x_2, y_2, z_2)$: $\vec{a} + \vec{b} = (x_1 + x_2, y_1 + y_2, z_1 + z_2)$
- Množenje vektorja $a = (x_1, y_1, z_1)$ s skalarjem $\lambda \in \mathbb{R}$ definiramo kot: $\lambda\vec{a} = (\lambda x_1, \lambda y_1, \lambda z_1)$
- Ničelni vektor je $\vec{0} = (0, 0, 0)$
- Nasprotni vektor vektorja $a = (x_1, y_2, z_1)$ je $-\vec{a} = (-x_1, -y_1, -z_1)$

Trditev 1.1. *Naj bodo $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$ in $\alpha, \beta \in \mathbb{R}$. Potem velja:*

1. $\vec{a} + \vec{b} = \vec{b} + \vec{a}$ – *komutativnost*
2. $(\vec{a} + \vec{b}) + \vec{c} = \vec{a} + (\vec{b} + \vec{c})$ – *asociativnost*
3. $\vec{a} + \vec{0} = \vec{0} + \vec{a} = \vec{a}$ – *nevtralni element za seštevanje*
4. $\vec{a} + (-\vec{a}) = (-\vec{a}) + \vec{a} = \vec{0}$
5. $\alpha(\vec{a} + \vec{b}) = \alpha\vec{a} + \alpha\vec{b}$
6. $(\alpha + \beta)\vec{a} = \alpha\vec{a} + \beta\vec{a}$
7. $\alpha(\beta\vec{a}) = (\alpha\beta)\vec{a}$
8. $1 \cdot \vec{a} = \vec{a}$

Dokaz. Dokažimo 7. točko. Ostali dokazi sledijo podobno iz definicij.

$$\alpha(\beta\vec{a}) = \alpha \begin{bmatrix} \beta x_1 \\ \beta y_1 \\ \beta z_1 \end{bmatrix} = \begin{bmatrix} \alpha\beta x_1 \\ \alpha\beta y_1 \\ \alpha\beta z_1 \end{bmatrix} = (\alpha\beta) \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} = (\alpha\beta)\vec{a} \qquad \square$$

Definicija 1.2. Naj bodo $\overrightarrow{a_1}, \overrightarrow{a_2}, \dots \overrightarrow{a_n} \in \mathbb{R}$ in $\alpha_1, \alpha_2, \dots \alpha_n \in \mathbb{R}$

- Linearna kombinacija vektorjev $\overrightarrow{a_1}, \overrightarrow{a_2}, \dots \overrightarrow{a_n}$ je vektor oblike

$$\alpha_1\overrightarrow{a_1} + \alpha_2\overrightarrow{a_2} + \dots + \alpha_n\overrightarrow{a_n}.$$

- Vektorji $\overrightarrow{a_1}, \overrightarrow{a_2}, \dots \overrightarrow{a_n}$ v $\mathbb{R}^3$ so linearno neodvisni, če velja

$$\alpha_1\overrightarrow{a_1} + \alpha_2\overrightarrow{a_2} + \dots + \alpha_n\overrightarrow{a_n} = 0 \implies \alpha_1 = \alpha_2 = \dots = \alpha_n = 0.$$

Kaj pomeni, da so $\overrightarrow{a_1}, \overrightarrow{a_2}, \dots \overrightarrow{a_n}$ linearno odvisni? To pomeni, da obstajajo $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{R}$, da velja:

$$\alpha_1\overrightarrow{a_1} + \dots + \alpha_n\overrightarrow{a_n} = \vec{0}$$

in vsaj eden izmed $\alpha_1, \alpha_2, \dots, \alpha_n$ ni enak 0. Brez škode za splošnost predpostavimo $\alpha_1 \neq 0$. Potem se da $\overrightarrow{a_1}$ zapisati kot linearna kombinacija vektorjev $\overrightarrow{v_2}, \dots, \overrightarrow{v_n}$:

$$\overrightarrow{a_1} = -\frac{\alpha_2}{\alpha_1}\overrightarrow{a_2} - \dots - \frac{\alpha_n}{\alpha_1}\overrightarrow{a_n}.$$

Vprašanje: Največ koliko linearno neodvisnih vektorjev si lahko izberermo v $\mathbb{R}^3$? Ali se da preostale vektorje izraziti s pomočjo teh?

Izberimo $\vec{a} \neq \vec{0}$. Vektorji, ki so linearno odvisni od $\vec{a}$, so oblike $\alpha\vec{a},\ \alpha \in \mathbb{R}$. Izberemo $\vec{b}$, ki ni vzporeden $\vec{a}$. Vektorja $\vec{a}$ in $\vec{b}$ sta torej linearno neodvisna. Ponovimo korak: vektorji, ki so linearno odvisni od $\vec{a}$ in $\vec{b}$, so oblike $\alpha\vec{a} + \beta\vec{b},\ \alpha, \beta \in \mathbb{R}$. Sedaj lahko izberemo še $\vec{c}$, ki ne leži v ravnini, ki jo določata $\vec{a}$ in $\vec{b}$. Vidimo, da v $\mathbb{R}^3$ lahko izberemo največ tri linearno neodvisne vektorje. Ostali vektorji so linearne kombinacije teh treh: vsak vektor $\vec{x} \in \mathbb{R}^3$ lahko zapišemo kot $\vec{x} = \alpha\vec{a} + \beta\vec{b} + \gamma\vec{c}$.

Definicija 1.3. Naj bosta $\vec{a} = (a_1, a_2, a_3)$ in $\vec{b} = (b_1, b_2, b_3)$ vektorja v $\mathbb{R}^3$. Skalarni produkt vektorjev $\vec{a}$ in $\vec{b}$ je definiran kot $\vec{a} \cdot \vec{b} = a_1 \cdot b_1 + a_2 \cdot b_2 + a_3 \cdot b_3$.

Skalarni produkt vektorja s samim sabo je enak dolžini tega vektorja: $\vec{a} \cdot \vec{a} = a_1^2 + a_2^2 + a_3^2 = |\vec{a}|^2$.

Trditev 1.2. *Naj bodo $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$ in $\alpha \in \mathbb{R}$. Potem veljajo:*

1. $\vec{a} \cdot \vec{a} \geq 0$
2. $\vec{a} \cdot \vec{a} = 0$, *natanko tedaj, ko je* $\vec{a} = \vec{0}$
3. $\vec{a} \cdot \vec{b} = \vec{b} \cdot \vec{a}$
4. $(\vec{a} + \vec{b}) \cdot \vec{c} = \vec{a} \cdot \vec{c} + \vec{b} \cdot \vec{c}$
5. $(\alpha\vec{a}) \cdot \vec{b} = \alpha(\vec{a} \cdot \vec{b})$

Dokaz. Naj bodo $a = (a_1, a_2, a_3)$, $b = (b_1, b_2, b_3)$ in $c = (c_1, c_2, c_3)$.

1. $\vec{a} \cdot \vec{a} = a_1^2 + a_2^2 + a_3^2 \geq 0$
2. $\vec{a} \cdot \vec{a} = 0 \iff a_1^2 + a_2^2 + a_3^2 = 0 \iff a_1 = a_2 = a_3 = 0$
3. $\vec{a} \cdot \vec{b} = a_1b_1 + a_2b_2 + a_3b_3 = b_1a_1 + b_2a_2 + b_3a_3 = \vec{b} \cdot \vec{a}$

4. $(\vec{a}+\vec{b})\vec{c} = \begin{bmatrix} a_1+b_1 \\ a_2+b_2 \\ a_3+b_3 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = (a_1+b_1)c_1 + (a_2+b_2)c_2 + (a_3+b_3)c_3 = (a_1c_1 + a_2c_2 + a_3c_3) + (b_1c_1 + b_2c_2 + b_3c_3) = \vec{a}\cdot\vec{c} + \vec{b}\cdot\vec{c}$

5. $(\alpha\vec{a})\cdot\vec{b} = \begin{bmatrix} \alpha a_1 \\ \alpha a_2 \\ \alpha a_3 \end{bmatrix} \cdot \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \alpha a_1 b_1 + \alpha a_2 b_2 + \alpha a_3 b_3 = \alpha(a_1b_1 + a_2b_2 + a_3b_3) = \alpha(\vec{a}\cdot\vec{b})$ □

Naj bosta $\vec{a}, \vec{b} \in \mathbb{R}^3$ in $0 \leq \alpha \leq \pi$ kot med njima. Po kosinusnem izreku (ki ima več geometrijskih dokazov) velja $|\vec{a}-\vec{b}|^2 = |\vec{a}|^2 + |\vec{b}|^2 - 2|\vec{a}||\vec{b}|\cos\alpha$. Od tod pa sledi $\vec{a}\cdot\vec{b} = |\vec{a}||\vec{b}|\cos\alpha$. Naj bosta $\vec{a}, \vec{b}$ neničelna vektorja. Kaj pomeni $\vec{a}\cdot\vec{b} = 0$? Po formuli za skalarni produkt, ki smo jo izpeljali, velja $|\vec{a}||\vec{b}|\cos\alpha = 0$. Ker sta vektorja $\vec{a}, \vec{b}$ neničelna, mora veljati $\cos\alpha = 0$, od tod pa sledi $\alpha = \frac{\pi}{2}$. Torej sta vektorja $\vec{a}, \vec{b}$ pravokotna.

Definicija 1.4. Naj bosta $\vec{a} = (a_1, a_2, a_3)$ in $\vec{b} = (b_1, b_2, b_3)$ vektorja v $\mathbb{R}^3$. Vektorski produkt vektorjev $\vec{a}$ in $\vec{b}$ je vektor

$$\vec{a}\times\vec{b} = \begin{bmatrix} a_2b_3 - a_3b_2 \\ a_3b_1 - a_1b_3 \\ a_1b_2 - a_2b_1 \end{bmatrix}$$

Trditev 1.3. *Naj bodo $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$ in $\alpha \in \mathbb{R}$. Potem velja:*

1. $\vec{a}\times\vec{a} = 0$
2. $\vec{a}\times\vec{b} = -(\vec{b}\times\vec{a})$ – *antikomutativnost*
3. $\vec{a}\times(\vec{b}+\vec{c}) = (\vec{a}\times\vec{b}) + (\vec{a}\times\vec{c})$
4. $(\alpha\vec{a})\times\vec{b} = \alpha(\vec{a}\times\vec{b})$
5. $(\vec{a}\times\vec{b})\times\vec{c} = (\vec{a}\cdot\vec{c})\cdot\vec{b} - (\vec{b}\cdot\vec{c})\cdot\vec{a}$ – *formula za dvojni vektorski produkt*

Dokaz. Vse točke te trditve lahko dokažemo z izračunom komponent. □

Definicija 1.5. Naj bodo $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$. Mešani produkt vektorjev $\vec{a}, \vec{b}, \vec{c}$ je $\left[\vec{a}, \vec{b}, \vec{c}\right] = (\vec{a}\times\vec{b})\cdot\vec{c}$.

Trditev 1.4. *Zamenjava dveh sosednjih členov v mešanem produktu: za poljubne $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$ velja $[\vec{a}, \vec{b}, \vec{c}] = -[\vec{a}, \vec{c}, \vec{b}]$ in $[\vec{a}, \vec{b}, \vec{c}] = -[\vec{b}, \vec{a}, \vec{c}]$.*

Dokaz. Ponovno to sledi iz računa s komponentami. □

Opomba. Naj bosta $\vec{a}, \vec{b} \in \mathbb{R}^3$. Potem velja $[\vec{c}, \vec{b}, \vec{a}] = -[\vec{b}, \vec{c}, \vec{a}] = [\vec{b}, \vec{a}, \vec{c}] = -[\vec{a}, \vec{b}, \vec{c}]$

Trditev 1.5 (Langrangeva identiteta)**.** *Naj bosta $\vec{a}, \vec{b} \in \mathbb{R}^3$. Potem velja*

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

Dokaz.

$$\begin{aligned}
|\vec{a}\times\vec{b}|^2+(\vec{a}\cdot\vec{b})^2 &= (\vec{a}\times\vec{b})\cdot(\vec{a}\times\vec{b})+(\vec{a}\cdot\vec{b})^2\\
&= [\vec{a},\vec{b},\vec{a}\times\vec{b}]+(\vec{a}\cdot\vec{b})^2\\
&= -[\vec{a}\times\vec{b},\vec{b},\vec{a}]+(\vec{a}\cdot\vec{b})^2\\
&= -((\vec{a}\times\vec{b})\times\vec{b})\cdot\vec{a}+(\vec{a}\cdot\vec{b})^2\\
&= -((\vec{a}\cdot\vec{b})\cdot\vec{b}-(\vec{b}\cdot\vec{b})\cdot\vec{a})\cdot\vec{a}+(\vec{a}\cdot\vec{b})^2\\
&= -(\vec{a}\cdot\vec{b})\cdot(\vec{b}\cdot\vec{a})+(\vec{b}\cdot\vec{b})\cdot(\vec{a}\cdot\vec{a})+(\vec{a}\cdot\vec{b})\cdot(\vec{a}\cdot\vec{b})\\
&= (\vec{b}\cdot\vec{b})\cdot(\vec{a}\cdot\vec{a}) = |\vec{a}|^2|\vec{b}|^2
\end{aligned}$$

□

Trditev 1.6 (Geometrijska interpretacija vektorskega produkta)**.** *Naj bosta* $\vec{a},\vec{b}\in\mathbb{R}^3$.

1. $\vec{a}\times\vec{b}$ *je pravokoten na* $\vec{a}$ *in* $\vec{b}$.
2. $|\vec{a}\times\vec{b}|$ *je ploščina paralelograma med* $\vec{a}$ *in* $\vec{b}$.

Dokaz. Dokažimo zgornjo trditev:

1. Trditev sledi direktno iz lastnosti skalarnega produkta.

   $$(\vec{a}\times\vec{b})\cdot a = [\vec{a},\vec{b},\vec{a}] = -[\vec{a},\vec{a},\vec{b}] = -(\vec{a}\times\vec{a})\cdot\vec{b} = 0$$

   Podobno sledi tudi za $(\vec{a}\times\vec{b})\cdot\vec{b}$. Torej je vektor $\vec{a}\times\vec{b}$ pravokoten na vektorja $\vec{a}$ in $\vec{b}$.

2. Iz Lagrangeve identitete sledi:

   $$\begin{aligned}
   |\vec{a}\times\vec{b}|^2 &= |\vec{a}|^2|\vec{b}|^2-(\vec{a}\cdot\vec{b})^2\\
   &= |\vec{a}|^2|\vec{b}|^2-|\vec{a}|^2|\vec{b}|^2\cos^2\alpha\\
   &= |\vec{a}|^2|\vec{b}|^2(1-\cos^2\alpha)\\
   &= |\vec{a}|^2|\vec{b}|^2(\sin^2\alpha)
   \end{aligned}$$

   Ker je $\alpha\in[0,\pi]$, velja $|\vec{a}\times\vec{b}| = |\vec{a}||\vec{b}|\sin\alpha$. □

Smer $\vec{a}\times\vec{b}$ določimo po pravilu desne roke; desno roko postavimo na $\vec{a}$ in v najkrajšem loku zavrtimo do $\vec{b}$. Palec kaže v smeri $\vec{a}\times\vec{b}$.

Trditev 1.7 (Geometrijska interpretacija mešanega produkta)**.** *Naj bodo* $\vec{a},\vec{b},\vec{c}\in\mathbb{R}^3$*. Potem je* $|[\vec{a},\vec{b},\vec{c}]|$ *volumen paralepipeda, ki ga oklepajo vektorji* $\vec{a},\vec{b},\vec{c}$.

Dokaz.

$$V = S\cdot v = |\vec{a}\times\vec{b}||\vec{c}|\cos\phi = \left|(\vec{a}\times\vec{b})\cdot\vec{c}\right| = \left|[\vec{a},\vec{b},\vec{c}]\right|$$

□

Zgled 1.1. *Izračunajmo volumen tristrane piramide, ki jo oklepajo vektorji* $\vec{a},\vec{b},\vec{c}\in\mathbb{R}^3$*:*

$$V = \frac{S\cdot v}{3} = \frac{\frac{S_{par}}{2}\cdot v}{3} = \frac{[\vec{a},\vec{b},\vec{c}]}{6}$$

1.2 Enačba premice v prostoru

Dve različni točki v prostoru določata natanko eno premico. Lahko pa premico opišemo tudi z eno točko, ki leži na njej (na primer T_1), in neničelnim vektorjem $\vec{s}$, ki leži na njej (smerni vektor). Tako

iz $\vec{r} = \overrightarrow{r_1} + \overrightarrow{T_1T}$ dobimo vektorsko enačbo premice: $\vec{r} = \overrightarrow{r_1} + t\vec{s},\ t \in \mathbb{R}$. To enačbo lahko prepišemo v koordinatah: $T_1(x_1, y_1, z_1)$, $\vec{s} = (s_1, s_2, s_3)$ in $T(x, y, z)$. Sedaj velja enakost $(x, y, z) = (x_1, y_1, z_1) + t(s_1, s_2, s_3)$ in od tod sledi parametrična enačba premice:

$$x = x_1 + ts_1,\ y = y_1 + ts_2,\ z = z_1 + ts_3.$$

Iz teh enačb pa lahko tudi izrazimo t in dobimo kanonično enačbo premice:

$$\frac{x - x_1}{s_1} = \frac{y - y_1}{s_2} = \frac{z - z_1}{s_3}.$$

Zgled 1.2. *Premico, ki ima kanonično obliko*

$$\frac{x - 1}{2} = \frac{y + 2}{0} = \frac{z - 3}{-1},$$

lahko zapišemo v parametrični obliki $x = 1 + 2t,\ y = -2,\ z = 3 - t$.

Ko računamo razdaljo med točko in premico, računamo najmanjšo možno razdaljo med točko T s krajevnim vektorjem $\vec{t}$ in točkami na premici p s smernim vektorjem $\vec{s}$. Označimo to razdaljo z d. Naj bo T_1 poljubna točka na p s krajevnim vektorjem $\overrightarrow{r_1}$. Vektorja $\vec{r} - \overrightarrow{r_1}$ in $\vec{s}$ sta stranici paralelograma z višino d na stranico $\vec{s}$. Sedaj lahko na dva načina izračunamo ploščino tega paralelograma:

$$|(\vec{r} - \overrightarrow{r_1}) \times \vec{s}| = |\vec{s}|d \iff d = \frac{|(\vec{r} - \overrightarrow{r_1}) \times \vec{s}|}{|\vec{s}|}$$

1.3 Enačba ravnine

1. Položaj ravnine je natanko določen s tremi točkami na ravnini, ki ne ležijo na isti premici.
2. Položaj ravnine je natanko določen s točko na ravnini in vektorjem, ki je pravokoten na to ravnino (normala).

Naj bo T_1 poljubna točka na ravnini in $\vec{n}$ normala na ravnino. Potem za vsako točko T na ravnini velja vektorska enačba ravnine oziroma $(\vec{r} - \overrightarrow{r_1}) \cdot \vec{n} = 0$. V koordinatah to zapišemo: $T(x, y, z)$, $T_1(x_1, y_1, z_1)$ in $\vec{n} = (a, b, c)$. Od tod pa sledi

$$\left(\begin{bmatrix} x \\ y \\ z \end{bmatrix} - \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} \right) \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix} = 0$$

in iz $(x - x_1)a + (y - y_1)b + (z - z_1)c = 0$ dobimo enačbo za ravnino: $ax + by + cz = d$. Ravnine skozi tri nekolinearne točke torej poiščemo tako, da vzamemo T_1 za prvo točko, za normalo pa vzamemo vektor $\vec{n} = \overrightarrow{T_1T_2} \times \overrightarrow{T_1T_3}$.

Ponovno naj bo T_1 poljubna točka na ravnini s krajevnim vektorjem $\overrightarrow{r_1}$. Dolžina d točke T s krajevnim vektorjem $\vec{r}$ do ravnine je enaki dolžini pravokotne projekcije vektorja $\overrightarrow{T_1T}$ na $\vec{n}$. Tako dobimo formulo za razdaljo točke do ravnine.

$$d = \frac{|\vec{n} \cdot \overrightarrow{T_1T}|}{|\vec{n}|}$$

Pri razdalji med dvema premicama v prostoru moramo obravnavati tri primere: izbrani premici se ali sekata ($d = 0$), ali sta vzporedni ali pa mimobežni. Naj bosta dani premici mimobežni. Naj bosta T_1, T_2 zaporedoma točki na prvi in drugi premici s krajevnima vektorjema $\overrightarrow{r_1}, \overrightarrow{r_2}$. Naj bo $\overrightarrow{s_1}$ smerni vektor prve in $\overrightarrow{s_2}$ smerni vektor druge premice. Potem je dolžina med premicama d enaka dolžini projekcije $\overrightarrow{T_1T_2}$ na $\overrightarrow{s_1} \times \overrightarrow{s_2}$:

$$d = \frac{\left|(\overrightarrow{s_1} \times \overrightarrow{s_2}) \cdot \overrightarrow{T_1T_2}\right|}{|\overrightarrow{s_1} \times \overrightarrow{s_2}|}$$

Tudi pri razdalji med premico in ravnino ali dvema ravninama moramo obravnavati več primerov. Premica in ravnina sta bodisi vzporedni ($\vec{s} \cdot \vec{n} = 0$) bodisi premica seka ravnino. Podobno pa sta tudi dve poljubni ravnini bodisi vzporedni ali pa se sekata.

Zgled 1.3. *Izračunajmo razdaljo med premicama* $p_1 : \frac{x-1}{3} = \frac{y}{2} = \frac{z-3}{0}$ *in* $p_2 : \frac{x+1}{2} = \frac{y-1}{3} = \frac{z}{1}$. *Izračunati moramo smerna vektorja premic in točki* T_1, T_2. *Tako dobimo vektorja* $\overrightarrow{s_1} = (3, 2, 0)$ *in* $\overrightarrow{s_2} = (2, 2, 1)$ *ter točki* $T(1, 0, 3)$ *in* $T_2(-1, 1, 0)$. *Sedaj pa lahko izračunamo preostalo:*

- $\overrightarrow{T_1T_2} = (-2, 1, -3)$
- $s_1 \times s_2 = (3, 2, 0) \times (2, 3, 1) = (2, -3, 5)$
- $d = \frac{\left|(\overrightarrow{s_1} \times \overrightarrow{s_2}) \cdot \overrightarrow{T_1T_2}\right|}{|\overrightarrow{s_1} \times \overrightarrow{s_2}|} = \frac{|(2,-3,5)\cdot(-2,1,-3)|}{\sqrt{2^2+(-3)^2+5^2}} = \frac{22}{\sqrt{38}}$

Zgled 1.4. *Izračunajmo razdaljo med ravnino* $x + 2y + 3z = 7$ *in točko* $T(2, 3, 5)$. *Izberemo točko na ravnini* $T_1(7, 0, 0)$ *in izberemo normalo na to ravnino* $\vec{n} = (1, 2, 3)$. *Sedaj lahko izračunamo vektor* $\overrightarrow{T_1T} = (-5, 3, 5)$ *in naposled še razdaljo*

$$d = \frac{|\vec{n} \cdot \overrightarrow{T_1T_2}|}{|\vec{n}|} = \frac{|(1, 2, 3) \times (-5, 3, 5)|}{\sqrt{1^2 + 2^2 + 3^2}} = \frac{16}{\sqrt{14}}$$

2 Relacije, operacije in algebraične strukture

Definicija 2.1. Naj bo X neprazna množica. Relacija na X je neka podmnožica v $X \times X$. Pri tem $(x, y) \in R$ zapišemo tudi kot xRy in pravimo, da je x v relaciji R z y-om.

Zgled 2.1. *$R \subseteq \mathbb{R} \times \mathbb{R}$ je relacija na $\mathbb{R}$, definirana kot $(x, y) \in R \iff x < y$ oziroma $xRy \iff x < y$. To relacijo poznamo kot 'je manjše' in jo zapišemo s simbolom $<$.*

Definicija 2.2. Naj bo R relacija na X. Pravimo, da je R:

- refleksivna, če: $xRx \quad \forall x \in X$
- simetrična, če: $xRy \implies yRx \quad \forall x, y \in X$
- antisimetrična, če: $xRy \wedge yRx \implies x = y \quad \forall x, y \in X$
- tranzitivna, če: $xRy \wedge yRz \implies xRz \quad \forall x, y, z \in X$

Definicija 2.3. Relacija je

- ekvivalenčna, če je refleksivna, simetrična in tranzitivna
- delna urejenost, če je refleksivna, antisimetrična in tranzitivna

2.1 Ekvivalenčne relacije

Definicija 2.4. Naj bo $\sim$ ekvivalenčna relacija na X. Ekvivalenčni razred elementa $x \in X$ je $[x] = \{a \in X : x \sim a\}$, kvocientna množice X glede na $\sim$ je $X/_\sim = \{[x] : x \in X\}$

Trditev 2.1. *Naj bo $\sim$ ekvivalenčna relacija na X, $a, b \in X$. Potem velja ali $[a] \cap [b] = \emptyset$ ali $[a] = [b]$.*

Dokaz. Denimo, da velja $[a] \cap [b] \neq \emptyset$. Potem obstaja $x \in [a] \cap [b]$, za katerega po definiciji velja $x \in [a] : x \sim a$ in $x \in [b] : x \sim b$. Zaradi simetričnosti $\sim$ velja $a \sim x$ in $x \sim b$, iz tega pa iz tranzitivnosti velja $a \sim b \implies a \in [b]$. Prav tako pa velja $b \sim a \implies b \in [a]$. Sedaj moramo dokazati $[a] = [b]$.

$$y \in [a] : y \sim a \text{ in } a \sim b \overset{\text{TRANZ.}}{\implies} y \sim b \implies y \in [b]$$
$$y \in [b] : y \sim b \text{ in } b \sim a \overset{\text{TRANZ.}}{\implies} y \sim a \implies y \in [a]$$

Torej je vsak element $[a]$ tudi element $[b]$ in obratno, kar pa smo želeli dokazati. □

Množica X je torej disjunktna unija vseh ekvivalenčnih razredov.

Zgled 2.2. *Na množici $\mathbb{Z}$ definiramo relacijo: $x \sim y \overset{DEF}{\iff} n \big| (x - y)$, kjer je $n \in N$ fiksiran. Dokazali bomo, da je $\sim$ ekvivalenčna relacija. Dokažimo le tranzitivnost. Tranzitivnost: iz $n \big| (x - y)$ in $n \big| (y - z)$ sledi $n \big| (x - y) + (y - z) \implies n \big| (x - z)$. Analogno iz $x \sim y$ in $y \sim z$ sledi $x \sim z$, kar smo želeli pokazati. Ta relacija razdeli množico $\mathbb{Z}$ na ekvivalenčne razrede: $[0] = \{kn : k \in \mathbb{Z}\}$, $[1] = \{kn + 1 : k \in \mathbb{Z}\}$, $\ldots$, $[n-1] = \{kn + (n-1) : k \in \mathbb{Z}\}$. Kvocientna množica te relacije je*

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

Zgled 2.3. *Na množici* $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ *definiramo relacijo:* $(m,n) \sim (p,r) \overset{DEF}{\iff} mr = pn$. *Dokažimo, da je* $\sim$ *ekvivalenčna relacija (DN). Dokaza za refleksivnost in simetričnost sta trivialna. Tranzitivnost velja, ker iz* $mr = pn$ *in* $pt = sr$ *sledi* $mt = sn$ *(če* $n, r, t \neq 0$*). To pomeni, da iz* $(m,n) \sim (p,r)$ *in* $(p,r) \sim (s,t)$ *sledi* $(m,n) \sim (s,t)$*, kar smo želeli dokazati. Ekvivalenčni razredi te relacije so:* $[(m,n)] = \frac{m}{n}$*, njena kvocientna množica pa je*

$$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \,/_{\sim} = \mathbb{Q}.$$

Zgled 2.4. *DN: Na* $\mathbb{R}$ *definiramo relacijo* $x \sim y \overset{DEF}{\iff} x - y \in \mathbb{Z}$. *Dokažimo, da je to ekvivalenčna relacija. Kako si lahko geometrijsko predstavljamo* $\mathbb{R}/\sim$*? Ponovno sta dokaza refleksivnosti in simetričnosti trivialna. Za dokaz tranzitivnosti je dovolj, da vidimo, da iz iz* $x - y \in \mathbb{Z}$ *in* $y - z \in \mathbb{Z}$ *sledi* $(x-y) + (y-z) = x - z \in \mathbb{Z}$ *oziroma* $x \sim z$*. Ena izmed geometrijskih interpretacij* $\mathbb{R}/\sim$ *je kar interval* $[0, 1)$.

2.2 Operacije

Definicija 2.5. Naj bo X neprazna množica. Operacija na množici X je preslikava $X \times X \to X$.

Zgled 2.5. *Vzemimo množico* $\mathbb{N}$. *Seštevanje je preslikava* $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(x,y) \mapsto x + y$ *in je zato operacija na množici* $\mathbb{N}$. *Odštevanje pa je operacija na množici* $\mathbb{Z}$*, a ne na* $\mathbb{N}$.

Zgled 2.6. *Vzemimo vektorski prostor* $\mathbb{R}^3$.

1. *Seštevanje je preslikava* $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$, $(\vec{x}, \vec{y}) \mapsto \vec{x} + \vec{y}$ *in je operacija.*
2. *Množenje s skalarjem je preslikava* $\mathbb{R} \times \mathbb{R}^3 \to \mathbb{R}^3$, $(\lambda, \vec{x}) \mapsto \lambda\vec{x}$ *in ni operacija.*
3. *Skalarni produkt je preslikava* $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$, $(\vec{x}, \vec{y}) \mapsto \vec{x} \cdot \vec{y}$ *in ni operacija.*
4. *Vektorski produkt je preslikava* $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$, $(\vec{x}, \vec{y}) \mapsto \vec{x} \times \vec{y}$ *in je operacija.*

V splošnem uporabljemo oznako $(X, \circ)$, kjer je $\circ$ neka operacija na neprazni množici X.

Definicija 2.6. Naj bo $\circ$ operacija na X. Za to operacijo pravimo, da je:

- komutativna, če $a \circ b = b \circ a, \ \forall a, b \in X$
- asociativna, če $(a \circ b) \circ c = a \circ (b \circ c), \ \forall a, b, c \in X$

Definicija 2.7. Naj bo $\circ$ operacija na X. Za element $e \in X$, pravimo, da je enota (nevtralni element) za $\circ$, če velja $e \circ x = x \circ e = x, \ \forall x \in X$.

Zgled 2.7. *Vzemimo množico* $(\mathbb{N}, +)$*: operacija seštevanja je komutativna in asociativna, nima pa enote, saj* $0 \notin \mathbb{N}$ *(dogovor pri algebri).*

Trditev 2.2. *Naj bo* $\circ$ *operacija za množico* X. *Če obstaj enota za to operacijo, je enolično določena.*

Dokaz. Recimo, da sta e in f enoti. Potem velja: $e \circ f = f \circ e = f$ in $e \circ f = f \circ e = e$ ter posledično $e = f$. □

Definicija 2.8. Naj bo $(X, \circ)$ množica z operacijo:

1. $(X, \circ)$ je polgrupa, če je $\circ$ asociativna
2. $(X, \circ)$ je monoid, če je polgrupa in imamo enoto za $\circ$.
3. $(X, \circ)$ je grupa, če je monoid in ima vsak element množice X inverz glede na $\circ$:

$$\forall a \in X : \exists b \in X : a \circ b = b \circ a = e$$

Kadar je operacija $\circ$ komutativna, govorimo o komutativni polgrupi, komutativnem monoidu ali komutativni grupi (oz. Abelovi grupi).

Zgled 2.8. *Oglejmo si nekaj primerov grup, ki so nam že znane.*

- $(\mathbb{N}, +)$ *je komutativna polgrupa,* $(\mathbb{N}, \cdot)$ *pa komutativni monoid.*
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^3, +)$ *so Abelove grupe.*
- $(\mathbb{Q} \setminus \{0\})$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ *so prav tako Abelove grupe.*

Definicija 2.9. Naj bo $(X, \circ)$ naj bo množica z operacijo $\circ$. Naj bo $Y \subseteq X$ neprazna podmnožica. Pravimo, da je podmnožica Y zaprta za operacijo $\circ$, če velja: $\forall a, b \in Y : a \circ b \in Y$.

Opomba. Če je Y zaprta za operacijo $\circ$, potem je tudi Y opremljena s to operacijo.

Zgled 2.9. *Oglejmo si nekaj primerov podmnožic z operacijo.*

- $(\mathbb{Z}, -)$*: podmnožica* $\mathbb{N}$ *ni zaprta za operacijo odštevanja, zato ni podgrupa za to operacijo.*
- $(\mathbb{R}, \cdot)$*: podmnožica* $\mathbb{R} \setminus \{0\}$ *je zaprta za operacijo množenja, saj za* $a, b \in \mathbb{R} \setminus \{0\}$ *velja* $a \cdot b \notin \mathbb{R} \setminus \{0\}$*. Kot smo že omenili v enem od prejšnjih zgledov, je* $(\mathbb{R} \setminus \{0\}, \cdot)$ *grupa,* $(\mathbb{R}, \cdot)$ *pa le monoid.*

2.3 Grupe

Trditev 2.3. *V grupi je inverz elementa enolično določen.*

Dokaz. Naj bo $(G, \circ)$ grupa in $a \in G$. Naj bosta b in c inverza od a. Od tod sledi $a \circ b = b \circ a = e$ in $a \circ c = c \circ a = e$. Potem pa velja:

$$b = b \circ e = b \circ (a \circ c) \overset{\text{ASOC}}{=} (b \circ a) \circ c = e \circ c = c \qquad \square$$

Oznaka: Če je G grupa in $a \in G$, je inverz od a a^{-1}.

Trditev 2.4. *DN: V grupi veljajo naslednje trditve:*

1. $e^{-1} = e$
2. $(a^{-1})^{-1} = a$
3. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Dokaz. Ker vemo, da je inverz elementa grupe enolično določen, je dovolj preveriti, da je produkt enak enoti.

1. Če je e enota za $\circ$, potem za vsak $a \in G$ velja $a \circ e = e \circ a = a$. Iz tega sledi, da velja $e \circ e = e$ in smo dokazali.
2. Dovolj je pokazati $a^{-1} \circ a = a \circ a^{-1} = e$, kar je očitno. Iz tega sledi, da je inverz od a^{-1} kar a oziroma: $(a^{-1})^{-1} = a$.

3. Dovolj je pokazati, da je produkt enak e.

$$\begin{aligned}(a \circ b) \circ (b^{-1} \circ a^{-1}) &\overset{\text{ASOC}}{=} ((a \circ b) \circ b^{-1}) \circ a^{-1} \\ &\overset{\text{ASOC}}{=} (a \circ (b \circ b^{-1})) \circ a^{-1} \\ &= (a \circ e) \circ a^{-1} \\ &= a \circ a^{-1} = e\end{aligned}$$

Z enakim argumentom pokažemo, da je $(b^{-1} \circ a^{-1}) \circ (a \circ b) = e$. □

Definicija 2.10. Naj bo $(G, \circ)$ grupa in $H \subseteq G$ neprazna podmnožica. Pravimo, da je H podgrupa v grupi G, če je H za isto operacijo tudi grupa.

Trditev 2.5. *H je podgrupa v $G \iff$ H zaprta za $\circ$ in za inverze.*

Dokaz. Implikacija v desno je očitna. Dokažimo implikacijo v levo. Naj bo $(G, \circ)$ grupa in naj bo $H \subseteq G$, tako da je H zaprta za operacijo $\circ$ in za inverze (tj. $\forall a \in H : a^{-1} \in H$). Iz teh dveh predpostavk sledi

$$a \in H \implies a^{-1} \in H \implies a \circ a^{-1} \in H \implies e \in H,$$

torej ima podgrupa H tudi enoto. Ker se asociativnost podeduje na H, ima $(H, \circ)$ vse lastnosti podgrupe v G. □

Zgled 2.10. *Množica $(\mathbb{R}, +)$ je Abelova grupa. Množica $\mathbb{Z} \subseteq \mathbb{R}$ je zaprta za operacijo seštevanja in inverze (inverz od a je $-a$), zato je $(\mathbb{Z}, +)$ podgrupa $(\mathbb{R}, +)$.*

2.4 Preslikave med grupami

Definicija 2.11. Naj bosta $(G, \circ)$ in $(H, *)$ grupi. Preslikava $f : (G, \circ) \to (H, *)$ je homomorfizem grup, če velja

$$\forall a, b \in G : f(a \circ b) = f(a) * f(b).$$

Bijektivnim homomorfizmom pravimo izomorfizmi. Grupi $(G, \circ)$ in $(H, *)$ sta izomorfni, če obstaja izomorfizem $G \to H$.

Zgled 2.11. *$(\mathbb{R}, +)$ in $(\mathbb{R} \setminus \{0\}, \cdot)$ sta grupi, $((0, \infty), \cdot)$ pa je podgrupa v grupi $(\mathbb{R} \setminus \{0\}, \cdot)$. Iščemo tako bijektivno preslikavo $f : (\mathbb{R}, +) \to ((0, \infty), \cdot)$, da bo veljalo $f(a + b) = f(a) \cdot f(b)$. Taka f je na primer $f(x) = e^x$. Torej je $(\mathbb{R}, +)$ izomorfna $((0, \infty), \cdot)$.*

Trditev 2.6. *Naj bo $f : (G, \circ) \to (H, *)$ homomorfizem grup, e_G enota v G in e_H enota v H. Potem velja $f(e_G) = e_H$ in $f(a^{-1}) = f(a)^{-1}$, $\forall a \in G$.*

Dokaz. Dokažimo oba dela trditve.

- Označimo $x := f(e_G)$; sedaj velja

$$\begin{aligned}x * x = f(e_G) * f(e_G) = f(e_G \circ e_G) = f(e_G) = x \\ e_H = x * x^{-1} = (x * x) * x^{-1} = x * (x * x^{-1}) = x * e_H = x\end{aligned}$$

- Izberimo poljuben $a \in G$:

$$f(a^{-1}) * f(a) = f(a^{-1} \circ a) = f(e_G) = e_H$$
$$f(a) * f(a^{-1}) = f(a \circ a^{-1}) = f(e_G) = e_H$$

  Sledi: $f(a^{-1})$ je inverz od $f(a)$. □

Definicija 2.12. Naj bo $f : (G, \circ) \to (H, *)$ homomorfizem grup, e_G enota v G in e_H enota v H. Postem sta jedro in slika homomorfizma f definirana kot

$$\ker f = \{g \in G : f(g) = e_H\}, \quad \operatorname{im} f = \{f(g) : g \in G\}.$$

Trditev 2.7. *Naj bo $f : G \to H$ homomorfizem grup. Potem je jedro* $\ker f$ *podgrupa v G in slika* $\operatorname{im} f$ *podgrupa v H.*

Dokaz. Dokažimo izrek posebej za $\ker f$ in $\operatorname{im} f$.

1. Velja $e_G \in \ker f$, zato je $\ker f \neq \emptyset$. Naj bosta $a, b \in \ker f$; sledi

$$f(a \circ b) = f(a) * f(b) = e_H * e_H = e_H \implies a \circ b \in \ker f$$
$$f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H \implies a^{-1} \in \ker f$$

2. Očitno velja $\operatorname{im} f \neq \emptyset$. Naj bosta $x, y \in \operatorname{im} f$; potem obstajata $a, b \in G$, da je $f(a) = x$ in $f(b) = y$. Od tod sledi

$$x * y = f(a) * f(b) = f(a \circ b) \implies x * y \in \operatorname{im} f$$
$$x^{-1} = f(a)^{-1} = f(a^{-1}) \implies x^{-1} \in \operatorname{im} f$$ □

Trditev 2.8. *Naj bo $f : G \to H$ homomorfizem grup. Velja:*

- *f je surjektivna* $\iff \operatorname{im} f = H$
- *f je injektivna* $\iff \ker f = \{e_G\}$

Dokaz. Prva točka dokaza je očitna. Dokazali bomo le drugo točko. Dokažimo najprej implikacijo v desno ($\Rightarrow$). Vzemimo $x \in \ker f$. Potem velja

$$f(x) = e_H = f(e_G) \overset{\text{f inj.}}{\implies} x = e_G.$$

Dokažimo še implikacijo v levo ($\Leftarrow$). Recimo, da za $x, y \in G$ velja $f(x) = f(y)$; potem velja

$$f(x) * f(y)^{-1} = e_H \iff f(x) * f(y^{-1}) = e_H$$
$$\iff f(x \circ y^{-1}) = e_H,$$

od tod pa sledi $x \circ y^{-1} = e_G$ in posledično $x = y$. □

2.5 Simetrijska grupa in permutacije

Naj bo X neprazna množica. Potem lahko definiramo simetrijsko množico kot

$$Sym\ X = \{\text{vse bijektivne preslikave } X \to X\}.$$

Na tej množici imamo operacijo kompozitum, za katero je $(Sym\ X, \circ)$ simetrijska grupa.

Dokaz. DN: Dokažimo zaprtost za operacijo: naj bosta $f : X \to X$ in $g : X \to X$ bijekciji. Očitno je, da bo tudi funkcija $g \circ f : X \to X$ slikala iz množice X nazaj v X. Dokažimo, da je $g \circ f$ tudi bijekcija. Ker sta f in g injektivni, za poljubna $x_1, x_2 \in X$ velja:

$$\begin{aligned}(g \circ f)(x_1) = (g \circ f)(x_2) &\iff g(f(x_1)) = g(f(x_2)) \\ &\overset{\text{g inj.}}{\implies} f(x_1) = f(x_2) \\ &\overset{\text{f inj.}}{\implies} x_1 = x_2\end{aligned}$$

in je funkcija $g \circ f$ tudi injektivna. Podobno sledi surjekcija: ker sta f in g surjektivni, za poljuben $y \in X$ obstaja $z \in X$, da je $y = g(z)$, in za poljuben $z \in X$ obstaja tak $x \in X$, da je $z = f(x)$. Od tod pa hitro sledi, da za poljuben $y \in X$ obstaja tak $x \in X$, da je $y = g(f(x))$, kar pa smo želeli dokazati. Sedaj pa dokažimo še asociativnost: naj bodo $f, g, h \in Sym\ X$. Upoštevamo dejstvo $(g \circ f)(x) = g(f(x))$ in dobimo

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))).$$

Po drugi strani pa:

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$$

in velja $((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x)$, torej smo dokazali asociativnost $\circ$. Enota za operacijo $\circ$ v tej grupi $e : X \to X$ je identična funkcija $e(x) = x$, inverz poljubne funkcije f pa je inverzna funkcija f^{-1} (obstaja zaradi bijektivnosti f). □

$Sym\ X$ je grupa simetrij množice X. V splošnem je to nekomutativna grupa. Obravnavali bomo poseben primer te grupe, kjer je X končna množica $X = \{1, 2, \ldots, n\}$. To grupo označimo s S_n in ji pravimo „simetrična grupa na n elementih“. Elementom grupe S_n pravimo permutacije in jih zapišemo kot

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

Množica S_n ima $n!$ elementov oz. $|S_n| = n!$. Permutacije običajno označujemo z malimi grškimi črkami. Poseben tip permutacij so cikli. V splošnem so to permutacije $\sigma = \begin{pmatrix} j_1 & j_2 & \ldots & j_k \end{pmatrix}$, ki slikajo po pravilu $j_1 \mapsto j_2,\ j_2 \mapsto j_3, \ldots,\ j_k \mapsto j_1$. Temu pravimo cikel dolžine k. Ciklom dolžine 2 rečemo tudi transpozicije. Primer cikla je na primer

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

Zgled 2.12. *Vzemimo poljubno permutacijo σ.*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 5 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 4 & 5 \end{pmatrix}$$

Permutacijo σ lahko zapišemo kot kompozitum (produkt) disjunktnih ciklov. Izkaže se, da to lahko naredimo za vsako permutacijo.

Trditev 2.9. *DN: Vsaka permutacija se da zapisati kot produkt disjunktnih ciklov.*

Dokaz. Naj bo $\sigma \in S_n$ permutacija. Vzemimo poljuben element $x \in \{1, 2, \ldots, n\}$ in ga permutiramo, dokler ne dobimo nazaj x. Tako dobimo cikel

$$C_x = \begin{pmatrix} x & \sigma(x) & \sigma^2(x) & \ldots & \sigma^k(x) \end{pmatrix},$$

kjer je $k+1 \in \mathbb{N}$ najmanjše naravno število, za katerega velja $\sigma^{k+1}(x) = x$ (tak $k+1$ obstaja, ker je $\{1, 2, \ldots, n\}$ končna množica). Sedaj lahko dokažemo, da so vsi elementi cikla C_x paroma različni:

naj velja $\sigma^i(x) = \sigma^j(x)$ za neka $0 \leq i < j \leq k$. Potem sledi: $\sigma^{j-i} = x$, kar pa je nemogoče, ker je $j - i < k + 1$. Konstruiramo lahko množico vseh elementov C_x

$$E_x = \{x, \sigma(x), \ldots, \sigma^k(x)\}.$$

Sedaj imamo algoritem, kako σ izraziti kot produkt disjunktnih ciklov: izberemo $x_1 = 1$ in dobimo cikel C_{x_1} in množico E_{x_1}. Nato izberemo $x_2 \in \{1, 2, \ldots, n\} \setminus E_{x_1}$ in ponovno dobimo C_{x_2} in E_{x_2}. Proces ponavljamo, dokler nismo uporabili vseh elementov množice $\{1, 2, \ldots, n\}$, kar seveda dosežemo v končnem številu korakov. Tedaj lahko začetno permutacijo σ zapišemo kot produkt disjunktnih ciklov:

$$\sigma = C_{x_1} \circ C_{x_2} \circ \cdots \circ C_{x_l}$$ □

Trditev 2.10. *DN: Vsaka permutacija se da zapisati kot produkt (ne nujno disjunktnih) transpozicij.*

Dokaz. V prejšnji trditvi smo že pokazali, da se vsaka permutacija da zapisati kot produkt disjunktnih ciklov. Dovolj je, da pokažemo, da se poljuben cikel da zapisati kot produkt transpozicij:

$$(j_1 \quad j_2 \quad j_3 \quad \ldots \quad j_k) = (j_2 \quad j_3) \cdots (j_{k-1} \quad j_k)\,(j_1 \quad j_k)$$

in smo končali. □

Definicija 2.13. Naj bo σ permutacija množice $\{1, 2, \ldots, n\}$, i in j naj bosta iz $\{1, 2, \ldots, n\}$, $i < j$. Pravimo, da je par (i, j) inverzija za σ, če velja $\sigma(i) > \sigma(j)$. Številu vseh parov (i, j), ki so inverzije, pravimo indeks permutacije σ; *ind* σ, številu $(-1)^{ind\ \sigma}$ pa signatura (znak) permutacije σ; *sgn* σ.

Zgled 2.13. *Vzemimo permutacijo*

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

Inverzije te permutacije so: $\{(1,2), (1,4), (1,5), (2,4), (2,5), (3,4), (3,5)\}$*, torej za to permutacijo velja* $ind\ \sigma = 7$ *in* $sgn\ \sigma = (-1)^7 = -1$.

Definicija 2.14. Permutacijam $\sigma \in S_n$, za katere velja $sgn\ \sigma = 1$, pravimo sode permutacije, permutacijam s $sgn\ \sigma = -1$ pa lihe permutacije.

Trditev 2.11. *Naj bosta*

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & i & i+1 & \ldots & n \\ j_1 & j_2 & \ldots & j_i & j_{i+1} & \ldots & j_n \end{pmatrix}, \quad \widetilde{\sigma} = \begin{pmatrix} 1 & 2 & \ldots & i & i+1 & \ldots & n \\ j_1 & j_2 & \ldots & j_{i+1} & j_i & \ldots & j_n \end{pmatrix}.$$

Potem je $sgn\ \sigma = -sgn\ \widetilde{\sigma}$.

Dokaz. Oglejmo si vse možne pare (k, l): Pari (k, l), $k, l \notin \{i, i+1\}$:

$$(k,l) \text{ inverzija za } \sigma \iff (k,l) \text{ inverzija za } \widetilde{\sigma}$$

Par $(i, i+1)$:

$$(i, i+1) \text{ inverzija za } \sigma \iff (i, i+1) \text{ ni inverzija za } \widetilde{\sigma}$$

Pari (k, i), $k < i$:

$$(k,i) \text{ inverzija za } \sigma \implies (k, i+1) \text{ inverzija za } \widetilde{\sigma}$$
$$(k,i) \text{ ni inverzija za } \sigma \implies (k, i+1) \text{ ni inverzija za } \widetilde{\sigma}$$

Pari $(k, i+1)$, $k < i$:

$$(k, i+1) \text{ inverzija za } \sigma \implies (k, i) \text{ inverzija za } \widetilde{\sigma}$$
$$(k, i+1) \text{ ni inverzija za } \sigma \implies (k, i) \text{ ni inverzija za } \widetilde{\sigma}$$

Pari $(i+1, l)$, $l > i+1$:

$$(i+1, l) \text{ inverzija za } \sigma \implies (i, l) \text{ inverzija za } \widetilde{\sigma}$$
$$(i+1, l) \text{ ni inverzija za } \sigma \implies (i+1, l) \text{ ni inverzija za } \widetilde{\sigma}$$

Pari (i, l), $l > i+1$:

$$(i, l) \text{ inverzija za } \sigma \implies (i+1, l) \text{ inverzija za } \widetilde{\sigma}$$
$$(i, l) \text{ ni inverzija za } \sigma \implies (i+1, l) \text{ ni inverzija za } \widetilde{\sigma}$$ □

Posledica 2.12. *Če sta*

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & i & \dots & k & \dots & n \\ j_1 & j_2 & \dots & j_i & \dots & j_k & \dots & j_n \end{pmatrix}, \quad \widetilde{\sigma} = \begin{pmatrix} 1 & 2 & \dots & i & \dots & k & \dots & n \\ j_1 & j_2 & \dots & j_k & \dots & j_i & \dots & j_n \end{pmatrix},$$

potem je $sgn\ \sigma = -sgn\ \widetilde{\sigma}$.

Dokaz. Pri vsaki zaporedni menjavi j_i z j_{i+1} se predznak signature spremeni. Da zamenjamo j_i z j_k pa potrebujemo $2(j-k)-1$ takšnih menjav. Torej zaradi lihega števila zaporednih menjav velja $sgn\ \sigma = -sgn\ \widetilde{\sigma}$. □

Posledica 2.13. *Permutacija je soda natanko tedaj, ko jo lahko zapišemo kot produkt sodega števila transpozicij, in liha natanko tedaj, ko jo lahko zapišemo kot produkt lihega števila transpozicij.*

Dokaz. Dokažimo najprej v levo smer ($\Leftarrow$). Naj bo

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & i & \dots & k & \dots & n \\ j_1 & j_2 & \dots & j_i & \dots & j_k & \dots & j_n \end{pmatrix}$$

poljubna permutacija in $\tau = \begin{pmatrix} j_i & j_k \end{pmatrix}$ poljubna transpozicija. Potem velja

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & \dots & i & \dots & k & \dots & n \\ j_1 & j_2 & \dots & j_k & \dots & j_i & \dots & j_n \end{pmatrix}$$

in po prejšnji posledici $sgn\ (\tau \circ \sigma) = -sgn\ \sigma$. Sedaj predpostavimo, da σ lahko zapišemo kot produkt l permutacij:

$$\sigma = \tau_l \circ \tau_{l-1} \circ \dots \circ \tau_1 = \tau_l \circ \tau_{l-1} \circ \dots \circ \tau_1 \circ id.$$

Izračunamo $sgn\ \sigma$ in po indukciji je očitno, da je za sodi l $sgn\ \sigma = 1$ in za lihi l $sgn\ \sigma = -1$:

$$\begin{aligned} sgn\ \sigma &= sgn\ (\tau_l \circ \tau_{l-1} \circ \dots \circ \tau_1 \circ id) \\ &= -sgn\ (\tau_{l-1} \circ \dots \circ \tau_1 \circ id) \\ &= sgn\ (\tau_{l-2} \circ \dots \circ \tau_1 \circ id) \\ &\dots \\ &= \pm sgn\ id = \pm 1. \end{aligned}$$

Dokažimo še v desno smer($\Rightarrow$). Vsaka permutacija σ se da zapisati kot produkt transpozicij, kot smo že dokazali. Sedaj uporabimo sklpe iz prejšnje točke: če je σ soda, potem mora biti produkt sodega števila transpozicij (sicer bi bila liha). Podobno sledi, da mora biti liha permutacija σ produkt lihega števila permutacij, sicer bi bila soda. □

Posledica 2.14. *Za poljubni permutaciji $\tau, \sigma \in S_n$ velja $sgn\ \sigma^{-1} = sgn\ \sigma$ in $sgn\ (\sigma \circ \tau) = sgn\ \sigma \cdot sgn\ \tau$.*

Dokaz. Permutacijo σ lahko zapišemo kot produkt transpozicij $\sigma = \begin{pmatrix} i_1 & j_1 \end{pmatrix} \begin{pmatrix} i_2 & j_2 \end{pmatrix} \dots \begin{pmatrix} i_k & j_k \end{pmatrix}$. Potem po pravilu za grupo $(G, \circ)$, $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ velja

$$\begin{aligned} \sigma^{-1} &= \begin{pmatrix} i_k & j_k \end{pmatrix}^{-1} \dots \begin{pmatrix} i_2 & j_2 \end{pmatrix}^{-1} \begin{pmatrix} i_1 & j_1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} i_k & j_k \end{pmatrix} \dots \begin{pmatrix} i_2 & j_2 \end{pmatrix} \begin{pmatrix} i_1 & j_1 \end{pmatrix} \end{aligned}$$

Po prejšnji posledici sledi $sgn\ \sigma = sgn\ \sigma^{-1}$. Sedaj lahko zapišemo še τ kot produkt transpozicij $\tau = \begin{pmatrix} a_1 & b_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \end{pmatrix} \dots \begin{pmatrix} a_l & b_l \end{pmatrix}$. Zapišemo produkt permutacij $\sigma \circ \tau$ in dobimo $sgn\ (\sigma \circ \tau)$:

$$\sigma \circ \tau = \begin{pmatrix} i_1 & j_1 \end{pmatrix} \begin{pmatrix} i_2 & j_2 \end{pmatrix} \dots \begin{pmatrix} i_k & j_k \end{pmatrix} \begin{pmatrix} a_1 & b_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \end{pmatrix} \dots \begin{pmatrix} a_l & b_l \end{pmatrix}.$$

Iz tega je razvidno:

$$sgn\ (\sigma \circ \tau) = (-1)^{k+l} = (-1)^k \cdot (-1)^l = sgn\ \sigma \cdot sgn\ \tau$$ □

2.6 Kolobarji, obsegi in polja

Definicija 2.15. Naj bo K neprazna množica z operacijama $+$ in $\cdot$. Pravimo, da je $(K, +, \cdot)$ kolobar, če velja

1. $(K, +)$ je Abelova grupa:
   - enoto označimo z 0: $a + 0 = 0 + a = a,\ \forall a \in K$
   - inverz a označimo z $-a$: $a + (-a) = (-a) + a = 0,\ \forall a \in K$
2. $(K, \cdot)$ je polgrupa: $\forall a, b, c \in K : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. Leva in desna distributivnost: $\forall a, b, c \in K$ velja $a \cdot (b + c) = ab + ac$ in $(b + c) \cdot a = ba + bc$.

Definicija 2.16. Naj bo $(K, +, \cdot)$ kolobar.

- Če ima K nevtralen element za množenje, pravimo, da je K kolobar z enico; nevtralni element za množenje označimo z 1.
- Če je množenje v K komutativno, pravimo, da je K komutativen kolobar.
- Če je K kolobar z enico, za katerega velja, da je $(K \setminus \{0\}, \cdot)$ grupa, pravimo, da je K obseg.
- Komutativnim obsegom pravimo polja.

Zgled 2.14. *Oglejmo si nekaj osnovnih zgledov kolobarjev.*

1. *$(\mathbb{Z}, +, \cdot)$ je komutativen kolobar z enico.*
2. *Naj bo $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$. Očitno je, da sta $+$ in $\cdot$ operaciji na $2\mathbb{Z}$ (oz. $2\mathbb{Z}$ je zaprta za $+$ in $\cdot$). $(2\mathbb{Z}, +)$ je Abelova grupa, $(2\mathbb{Z}, \cdot)$ pa je komutativna polgrupa. Distributivnost velja, vendar pa ni enote za $\cdot$. Torej je $(2\mathbb{Z}, +, \cdot)$ komutativen kolobar brez enice.*
3. *$(\mathbb{Q}, +, \cdot)$ je komutativen kolobar z enico. Ker ima vsak $a \in \mathbb{Q} \setminus \{0\}$ inverz $\frac{1}{a}$, je $(\mathbb{Q} \setminus \{0\}, \cdot)$ grupa. Torej je $(\mathbb{Q}, +, \cdot)$ polje. Enako velja za $(\mathbb{R}, +, \cdot)$ in $(\mathbb{C}, +, \cdot)$.*

Definicija 2.17. Naj bo $(K, +, \cdot)$ kolobar in $L \subseteq K$ neprazna podmnožica. Pravimo, da je L podkolobar v K, če je $(L, +, \cdot)$ tudi kolobar.

To pomeni, da je L podkolobar K natanko tedaj, ko veljajo naslednje tri točke:

1. $(L,+)$ je podgrupa v $(K,+)$: $\forall a,b \in L : a+b \in L,\ -a \in L$,
2. L je zaprta za operacijo $\cdot$: $\forall a,b \in L : a \cdot b \in L$ in
3. distributivnost se avtomatično podeduje

Definicija 2.18. Naj bosta $(K,+_1,\cdot_1)$ in $(L,+_2,\cdot_2)$ kolobarja. Homomorfizem kolobarjev je preslikava $f : K \to L$, za katero velja

$$f(a +_1 b) = f(a) +_2 f(b)$$
$$f(a \cdot_1 b) = f(a) \cdot_2 f(b)$$

Če je f bijektiven homomorfizem kolobarjev, mu pravimo izomorfizem. Kolobarja K in L sta izomorfna, če obstaja izomorfizem kolobarjev $K \to L$.

Definicija 2.19. Naj bo $f : K \to L$ homomorfizem kolobarjev . Kot prej definiramo jedro in sliko f kot

$$\ker f = \{k \in K : f(k) = 0_L\}, \quad \operatorname{im} f = \{f(k) : k \in K\}$$

DN: Jedro $\ker f$ je podkolobar v K, slika $\operatorname{im} f$ pa je podkolobar v L.

Dokaz. Dokažimo, da je $\ker f$ podkolobar v K. V prejšnjem dokazu smo pokazali, da je $(\ker f,+)$ podgrupa v $(K,+)$. Preostane nam le še, da dokažemo, da je $\ker f$ zaprt za operacijo $\cdot$. Naj bosta $a,b \in \ker f$; sledi

$$f(a \cdot b) = f(a) \cdot f(b) = 0_L \cdot 0_L = 0_L \implies a \cdot b \in \ker f.$$

Dokažimo še, da je $\operatorname{im} f$ podkolobar v L. Tudi to, da je $(\operatorname{im} f,+)$ podgrupa v $(L,+)$, smo že dokazali. Kot v prejšnjem primeru nam preostane, da dokažemo, da je $\operatorname{im} f$ zaprt za operacijo $\cdot$. Naj bosta $x,y \in \operatorname{im} f$; potem velja $\exists a \in K : f(a) = x$ in $\exists b \in K : f(b) = y$. Od tod sledi

$$x \cdot y = f(a) \cdot f(b) = f(a \cdot b) \implies x \cdot y \in \operatorname{im} f$$ □

3 Vektorski prostori

Definicija 3.1. Naj bo $V \neq \emptyset$ z operacijo $V \times V \to V$, $(u, v) \mapsto u + v$. Naj bo $\mathbb{F}$ polje in recimo, da imamo preslikavo $\mathbb{F} \times V \to V$, $(\alpha, v) \mapsto \alpha v$. Pravimo, da je V vektorski prostor nad poljem $\mathbb{F}$, če veljajo naslednje trditve:

1. $(V, +)$ je Abelova grupa (enota za $+$: 0, inverz od v: $-v$)
2. $(\alpha + \beta)v = \alpha v + \beta v, \ \forall \alpha, \beta \in \mathbb{F}, \ \forall v \in V$
3. $\alpha(u + v) = \alpha u + \alpha v, \ \forall \alpha \in \mathbb{F}, \ \forall u, v \in V$
4. $\alpha(\beta v) = (\alpha\beta) \cdot v, \ \forall \alpha, \beta \in \mathbb{F}, \ \forall v \in V$
5. $1 \cdot v = v, \ \forall v \in V$

Elementom V pravimo vektorji, elementom $\mathbb{F}$ pa skalarji.

Zgled 3.1. *Oglejmo si nekaj primerov vektorskih prostorov.*

1. *Množica $\mathbb{R}^3$ z običajnim seštevanjem in množenjem s skalarjem je vektorski prostor nad $\mathbb{R}$.*
2. *Naj bo $\mathbb{F}$ poljubno polje. Na množici $\mathbb{F}^n = \underbrace{\mathbb{F} \times \mathbb{F} \times \cdots \times \mathbb{F}}_{n}$ z elementi $v = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, kjer so $\alpha_i \in \mathbb{F}$, vpeljemo seštevanje in množenje s skalarjem:*

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} + \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} \alpha_1 + \beta_1 \\ \alpha_2 + \beta_2 \\ \vdots \\ \alpha_n + \beta_n \end{bmatrix}, \qquad \alpha \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \alpha\alpha_1 \\ \alpha\alpha_2 \\ \vdots \\ \alpha\alpha_n \end{bmatrix}$$

Potem je $\mathbb{F}^n$ s takim seštevanjem in množenjem s skalarjem vektorski prostor nad $\mathbb{F}$.

Dokaz. Dokažimo le 1. aksiom, saj ostali sledijo iz računa s komponentami in tega, da je $\mathbb{F}$ polje.

1. Asociativnost: naj bodo $a = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $b = (\beta_1, \beta_2, \ldots, \beta_n)$ in $c = (\gamma_1, \gamma_2, \ldots, \gamma_n)$.

$$(a + b) + c = \begin{bmatrix} (\alpha_1 + \beta_1) + \gamma_1 \\ (\alpha_2 + \beta_2) + \gamma_2 \\ \vdots \\ (\alpha_n + \beta_n) + \gamma_n \end{bmatrix} \overset{\mathbb{F} \text{ polje}}{=} \begin{bmatrix} \alpha_1 + (\beta_1 + \gamma_1) \\ \alpha_2 + (\beta_2 + \gamma_2) \\ \vdots \\ \alpha_n + (\beta_n + \gamma_n) \end{bmatrix} = a + (b + c)$$

2. Komutativnost:

$$a + b = \begin{bmatrix} \alpha_1 + \beta_1 \\ \alpha_2 + \beta_2 \\ \vdots \\ \alpha_n + \beta_n \end{bmatrix} = \begin{bmatrix} \beta_1 + \alpha_1 \\ \beta_2 + \alpha_2 \\ \vdots \\ \beta_n + \alpha_n \end{bmatrix} = b + a$$

3. Enota in inverz za seštevanje v tem vektorskem prostoru sta

$$\vec{0} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad -a = \begin{bmatrix} -\alpha_1 \\ -\alpha_2 \\ \vdots \\ -\alpha_n \end{bmatrix}$$

□

Zgled 3.2. *Naj bo X neprazna množica in $\mathbb{F}$ poljubno polje in $\mathbb{F}^X = \{$vse funkcije $f : X \to \mathbb{F}\}$. Na množici $\mathbb{F}^X$ vpeljemo seštevanje in množenje s skalarjem iz $\mathbb{F}$. Seštevanje za $f, g \in \mathbb{F}^X$ definiramo kot $(f+g)(x) = f(x) + g(x)$, množenje s skalarjem za $\lambda \in \mathbb{F}$ pa kot $(\lambda f)(x) = \lambda \cdot f(x)$.*

Dokaz. Dokažimo, da je $\mathbb{F}^X$ vektorski prostor nad $\mathbb{F}$. Dokažimo le prvi aksiom, saj vsi ostali zgolj sledijo iz lastnosti polja $\mathbb{F}$.

- Asociativnost: naj bodo $f, g, h \in \mathbb{F}^X$; od tod za $\forall x \in X$ sledi

$$\begin{aligned}((f+g)+h)(x) &= (f+g)(x) + h(x)\\ &= (f(x)+g(x)) + h(x)\\ &= f(x) + (g(x)+h(x))\\ &= f(x) + (g+h)(x)\\ &= (f+(g+h))(x)\end{aligned}$$

- Komutativnost: naj bosta $f, g \in \mathbb{F}^X$; za $\forall x \in X$ sledi

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

- Enota za seštevanje: rabimo tako funkcijo $e : X \to \mathbb{F}$, da za $\forall f : X \to \mathbb{F}$ velja $f+e = e+f = f$. Temu ustreza ničelna funkcija $e : X \to \mathbb{F},\ e(x) = 0$ (0 v polju $\mathbb{F}$).
- Inverz za seštevanje: naj bo $f : X \to \mathbb{F}$. Potrebujemo funkcijo $-f : X \to \mathbb{F}$, da bo veljalo $f + (-f) = (-f) + f = e$. To pa je funkcija $(-f)(x) \overset{\text{DEF}}{=} -f(x)$. □

DN: Če je $|X| = n$, potem lahko identificiramo $\mathbb{F}^X$ z $\mathbb{F}^n$. Naj bo $X = \{x_1, x_2, \ldots, x_n\}$. Potem lahko vsakemu elementu $f : X \to \mathbb{F}$ iz $\mathbb{F}^X$ enolično priredimo element $(f(x_1), f(x_2), \ldots, f(x_n)) \in \mathbb{F}^n$ in obratno. Torej obstaja bijekcija med $\mathbb{F}^n$ in $\mathbb{F}^X$. Izkaže se, da je za tako definirane operacije na vektorskih prostorih taka bijekcija tudi homomorfizem. Torej obstaja izomorfizem med $\mathbb{F}^n$ in $\mathbb{F}^X$, oziroma $\mathbb{F}^n \cong \mathbb{F}^X$.

Trditev 3.1. *Naj bo V vektorski prostor nad $\mathbb{F}$.*

1. $0 \cdot v = 0,\ \forall v \in V$
2. $\alpha \cdot 0 = 0,\ \forall \alpha \in \mathbb{F}$
3. $(-1) \cdot v = -v,\ \forall v \in V$

Dokaz. Dokažimo trditev po točkah, pri čemer pri prvih dveh uporabimo dejstvo, da v polju $\mathbb{F}$ velja pravilo krajšanja ($u + u = u \implies u = 0$, podoben sklep smo uporabili pri 2.6).

1. $0 \cdot v = (0+0) \cdot v \overset{(2)}{=} 0 \cdot v + 0 \cdot v$
2. $\alpha \cdot 0 = \alpha(0+0) \overset{(3)}{=} \alpha \cdot 0 + \alpha \cdot 0$
3. $(-1)v + v \overset{(5)}{=} (-1)v + 1 \cdot v \overset{(2)}{=} ((-1)+1)v = 0 \cdot v \overset{(a)}{=} 0$ □

Definicija 3.2. Naj bo V vektorski prostor nad $\mathbb{F}$ in U neprazna podmnožica v V. Pravimo, da je U vektorski podprostor v V, če je U za dano seštevanje in množenje s skalarjem tudi vektorski prostor nad $\mathbb{F}$. To označimo $U \leq V$.

Opomba. To pomeni, da je $(U, +)$ je podgrupa v $(V, +)$ in U je zaprta za množenje s skalarjem v V:

- $\forall u_1, u_2 \in U$ velja $u_1 + u_2 \in U$ in za $\forall u \in U$ velja $-u \in U$,
- $\forall u \in U,\ \forall \alpha \in \mathbb{F}$ velja $\alpha u \in U$.

Po prejšnji trditvi je zadosti preveriti, da za $\forall u_1, u_2$ velja $u_1 + u_2 \in U$ in za $\forall u \in U,\ \alpha \in \mathbb{F}$ velja $\alpha u \in U$.

Trditev 3.2. *Naj bo V vektorski prostor nad $\mathbb{F}$ in $U \subseteq V,\ U \neq \emptyset$. Potem je U vektorski podprostor V natanko tedaj, ko za $\forall u_1, u_2 \in U,\ \forall \alpha_1, \alpha_2 \in \mathbb{F}$ velja $\alpha_1 u_1 + \alpha_2 u_2 \in U$.*

Dokaz. ($\Rightarrow$) Denimo, da je $U \leq V$; potem za $\forall u_1, u_2 \in U, \forall \alpha_1, \alpha_2 \in \mathbb{F}$ velja $\alpha_1 u_1 \in U$ in $\alpha_2 u_2 \in U$. Ker je U zaprt za $+$, velja tudi $\alpha_1 u_1 + \alpha_2 u_2 \in U$.

($\Leftarrow$) Denimo, da velja $\forall u_1, u_2 \in U,\ \forall \alpha_1, \alpha_2 \in \mathbb{F} : \alpha_1 u_1 + \alpha_2 u_2 \in U$. Potem velja tudi

- $\forall u_1, u_2 \in U :\ 1 \cdot u_1 + 1 \cdot u_2 = u_1 + u_2 \in U$
- $\forall u_1, u_2 \in U,\ \forall \alpha_1 \in \mathbb{F} :\ \alpha_1 u_1 + 0 \cdot u_2 = \alpha_1 u_1 \in U$

in od tod sledi $U \leq V$. □

Opomba. Vsak podprostor U vektorskega prostora V vsebuje ničelni vektor. To sledi, ker za poljuben $x \in U$ velja $0 \cdot x \in U$.

Zgled 3.3. *Naj bo V vektorski prostor nad $\mathbb{F}$. Potem sta V (celotni vektorski prostor) in $\{0\}$ (trivialni podprostor) oba podprostora V. To velja zato, ker je vsaka linearna kombinacija ničelnega vektorja kar ničelni vektor sam.*

Zgled 3.4. *Navedimo nekaj podprostorov vektorskega prostora $\mathbb{R}^3$. Eden izmed njih je na primer kar $\{0\}$, oziroma trivialni podprostor. Izberimo si nek neničeln vektor $u \in \mathbb{R}^3$. Potem je*

$$U_1 = \{\alpha \cdot u : \alpha \in \mathbb{R}\}$$

podprostor v $\mathbb{R}^3$, hkrati pa tudi množica vseh točk, ki ležijo na premici s smernim vektorjem u, ki poteka skozi izhodišče. Denimo, da podprostor U_1 vsebuje tudi vektor $v \in \mathbb{R}^3$, ki ne leži na tej premici. Tako dobimo podprostor

$$U_2 = \{\alpha u + \beta v : \alpha, \beta \in \mathbb{R}\},$$

ki predstavlja ravnino, ki poteka skozi izhodišče. Ta postopek lahko naredimo še enkrat z vektorjem w, ki ne leži na tej ravnini. Tako dobimo podprostor

$$U_3 = \{\alpha u + \beta v + \gamma w : \alpha, \beta, \gamma \in \mathbb{R}\} = \mathbb{R}^3.$$

Torej smo pokazali, da je vsak podprostor $\mathbb{R}^3$ natanko eden izmed naslednjih objektov:

- *trivialni oziroma ničelni podprostor,*
- *premica, ki poteka skozi koordinatno izhodišče,*
- *ravnina, ki poteka skozi koordinatno izhodišče ali*
- *celoten prostor $\mathbb{R}^3$.*

Zgled 3.5. *Naj bo $\mathbb{F}$ polje in množica $\mathbb{F}^{\mathbb{F}} = \{$vse funkcije $\mathbb{F} \to \mathbb{F}\}$. Potem sta podprostora tudi $\mathbb{F}[x]$ (prostor vseh polinomov s koeficienti iz $\mathbb{F}$) in $\mathbb{F}_n[x]$ (prostor vseh polinomov stopnje največ n). $\mathbb{F}[x]$ je vektorski podprostor v $\mathbb{F}^{\mathbb{F}}$, ker je za poljubne $p, q \in \mathbb{F}[x]$ in $\alpha, \beta \in \mathbb{F}$ tudi $(\alpha p + \beta q)(x)$ polinom v x s koeficienti iz $\mathbb{F}$, torej velja $\alpha b + \beta q \in \mathbb{F}[x]$. Z enakim argumentom dokažemo tudi, da je $\mathbb{F}_n[x]$ je podprostor v $\mathbb{F}[x]$.*

Zgled 3.6. *Naj bo $X \subseteq \mathbb{R}$ interval na realni osi. Potem je $C(X) = \{f \in \mathbb{R}^X : f \text{ zvezna na } X\}$ vektorski podprostor v $\mathbb{R}^X$ (glej zapiske: analiza 1).*

3.1 Kvocientni prostori

Naj bo V vektorski prostor nad $\mathbb{F}$, U pa podprostor v V. Na množici V definiramo naslednjo relacijo: vektorja $x, y \in V$ sta v relaciji $x \sim y$ natanko tedaj, ko $x - y \in U$.

Trditev 3.3. *Relacija $\sim$ je ekvivalenčna na V:*

1. *Refleksivnost: za $\forall x \in V$ velja $x - x = 0 \in U$, torej velja $x \sim x$*
2. *Simetričnost: za $\forall x, y \in V$ velja $x - y \in U \implies y - x \in U$, torej velja $x \sim y \implies y \sim x$.*
3. *Tranzitivnost: za $\forall x, y, z \in V$ velja $x - y \in U \wedge y - z \in U \implies x - z \in U$.*

Definicija 3.3. Množico $V/_\sim$ običajno označujemo z $V/_U$. Njeni elementi so

$$\begin{aligned} v \in V: \ [v] &= \{x \in V : x \sim v\} \\ &= \{x \in V : x - v \in U\} \\ &= \{x \in V : x - v = u : u \in U\} \\ &= \{x \in V : x = v + u : u \in U\} \\ &\overset{\text{OZNAKA}}{=:} v + U \end{aligned}$$

To je levi odsek vektorja v glede na U.

Izrek 3.4.

Naj bo V vektorski prostor nad $\mathbb{F}$ in $U \leq V$. Potem $V/_U$ postane vektorski prostor nad $\mathbb{F}$ z naslednjim seštevanjem in množenjem s skalarjem:

$$\begin{aligned} (v_1 + U) + (v_2 + U) &\overset{DEF}{=} (v_1 + v_2) + U \\ \alpha \cdot (v + U) &\overset{DEF}{=} \alpha v + U \end{aligned}$$

$V/_U$ je kvocientni prostor prostora V glede na U.

Dokaz. Ključno je preveriti, da sta seštevanje in množenje s skalarjem dobro definirana: najprej moramo dokazati, da za vse $v_1 \sim x_1,\ v_2 \sim x_2$ velja

$$[v_1] + [v_2] = [x_1] + [x_2]?$$

Preveriti moramo, če velja $[v_1 + v_2] = [x_1 + x_2]$ oziroma $v_1 + v_2 \sim x_1 + x_2$. Ker vemo, da velja $v_1 \sim x_1,\ v_2 \sim x_2$, mora veljati tudi $v_1 - x_1 \in U,\ v_2 - x_2 \in U$. Sedaj lahko zapišemo

$$(v_1 + v_2) - (x_1 + x_2) = (v_1 - x_1) + (v_2 - x_2) \in U$$

in zato velja $[v_1 + v_2] = [x_1 + x_2]$. Torej je seštevanje dobro definirano. Dokazati moramo še, da za $v \sim x$ velja $[\alpha v] = [\alpha x]$. Zaradi $v \sim x$ velja

$$\alpha v - \alpha x = \alpha(v - x) \in U$$

in res sledi $[\alpha v] = [\alpha x]$. Torej je tudi množenje s skalarjem dobro definirano. Aksiomi vektorskih prostorov sledijo iz tega, da je V vektorski prostor. □

Zgled 3.7. *Naj bo vektorski prostor V in U ravnina $z = 0$; $U \leq V$. Elementi ${}^{V}/_{U}$ so:*

$$v \in \mathbb{R}^3 : \ v + U = \{v + u : u \in U\},$$

torej je to ravnina, ki gre skozi točko s krajevnim vektorjem v in je vzporedna ravnini U.

Definicija 3.4. Naj bo V vektorski prostor nad $\mathbb{F}$ in V_1, V_2 podprostora v V. Potem označimo

$$V_1 + V_2 = \{v_1 + v_2 : \ v_1 \in V_1, \ v_2 \in V_2\}$$

in tej množici pravimo vsota podprostorov V_1 in V_2.

Trditev 3.5. *Naj bo V vektorski prostor nad $\mathbb{F}$ in $V_1, V_2 \leq V$. Potem sta tudi $V_1 \cap V_2$ in $V_1 + V_2$ podprostora prostora V.*

Dokaz. Dokažimo najprej $V_1 \cap V_2 \leq V$. Vzemimo $x, y \in V_1 \cap V_2$ in $\alpha, \beta \in \mathbb{F}$; sledi

$$\begin{aligned} x \in V_1 \text{ in } y \in V_1 &\implies \alpha x + \beta y \in V_1 \\ x \in V_2 \text{ in } y \in V_2 &\implies \alpha x + \beta y \in V_2 \end{aligned}$$

Torej velja $\alpha x + \beta y \in V_1 \cap V_2$. Sedaj dokažimo še $V_1 + V_2 \leq V$. Vzemimo $x, y \in V_1 + V_2$ in $\alpha, \beta \in \mathbb{F}$:

$$\begin{aligned} x &= v_1 + v_2, \ v_1 \in V_1, \ v_2 \in V_2, \\ y &= w_1 + w_2, \ w_1 \in V_1, \ w_2 \in V_2. \end{aligned}$$

Sedaj pa lahko izrazimo linearno kombinacijo teh vektorjev in dobimo

$$\alpha x + \beta y = \alpha(v_1 + v_2) + \beta(w_1 + w_2) = \underbrace{(\alpha v_1 + \beta w_1)}_{\in V_1} + \underbrace{(\alpha v_2 + \beta w_2)}_{\in V_2} \in V_1 + V_2 \qquad \square$$

Trditev 3.6. *DN: $V_1 \cup V_2$ je podprostor v $U \Leftrightarrow V_1 \subseteq V_2$ ali $V_2 \subseteq V_1$*

Dokaz. Dokaz v levo je očiten. Dokazali bomo kontrapozicijo implikacije v desno: predpostavimo, da ne velja $V_1 \subseteq V_2$ ali $V_2 \subseteq V_1$. Potem obstajata $x \in V_1 \setminus V_2$ in $y \in V_2 \setminus V_1$. Od tod sledi, da velja $x + y \notin V_1$ in $x + y \notin V_2$. To pa pomeni, da za $x, y \in V_1 \cup V_2$ velja $x + y \notin V_1 \cup V_2$, torej $V_1 \cup V_2$ ni vektorski prostor. $\square$

Opomba. Podobno lahko definiramo vsoto več podprostorov v V:

$$V_1 + V_2 + \cdots + V_n = \{v_1 + v_2 + \cdots + v_n : v_1 \in V_1, \ v_2 \in V_2, \ldots, v_n \in V_n\}$$

Definicija 3.5. Naj bo V vektorski prostor in $V_1, V_2 \leq V$. Pravimo, da je V direktna vsota podprostorov V_1, V_21, če velja:

1. $V = V_1 + V_2$
2. $V_1 \cap V_2 = \{0\}$

To označimo $V_1 \oplus V_2$.

Zgled 3.8. *Naj bo vektorski prostor $V = \mathbb{R}^3$ in V_1, V_2 podprostora, kjer je V_1 ravnina $z = 0$ in V_2 premica $x = y = 0$. Potem velja $\mathbb{R}^3 = V_1 \oplus V_2$.*

Definicija 3.6. Naj bo V vektorski prostor nad $\mathbb{F}$ in $V_1, V_2, \ldots, V_n \leq V$. Pravimo, da je V direktna vsota podprostorov $V_1, V_2, \ldots, V_n$, če:

1. $V = V_1 + V_2 + \cdots + V_n$
2. $\forall i = 1, 2, \ldots, n : V_i \cap (V_1 + V_2 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_n) = \{0\}$

To označimo kot $V = V_1 \oplus V_2 + \oplus \cdots \oplus V_n$.

Izrek 3.7.

Naj bo V vektorski prostor nad $\mathbb{F}$ in $V_1, V_2 \leq V$. Potem velja $V = V_1 \oplus V_2$ natanko tedaj, ko se da za vsak $v \in V$ na enoličen način zapisati kot $v = v_1 + v_2$; $v_1 \in V_1,\ v_2 \in V_2$.

Dokaz. Dokaz implikacije v desno ($\Rightarrow$). Denimo, da je $V = V_1 \oplus V_2$. Naj bo $v = v_1 + v_2 = w_1 + w_2$ za neke $v_1, w_1 \in V_1,\ v_2, w_2 \in V_2$. Torej velja:

$$\underbrace{v_1 - w_1}_{\in V_1} = \underbrace{v_2 - v_2}_{\in V_2}$$

in iz predpostavke $V_1 \cap V_2 = \{0\}$ sledi $v_1 - w_1 = 0$ in $v_2 - w_2 = 0$. Torej je $v_1 = w_1,\ v_2 = w_2$ in zapis je enoličen.

Dokaz implikacije v levo ($\Leftarrow$). Denimo, da se da vsak $v \in V$ na enoličen način zapisati kot vsoto $v = v_1 + v_2$; $v_1 \in V_1,\ v_2 \in V_2$. Očitno je, da velja $V = V_1 + V_2$. Dokazati moramo še, da velja $V_1 \cap V_2 = \{0\}$. Vzemimo nek $x \in V_1 \cap V_2$; $x \in V_1$ in $x \in V_2$. Opazimo, da lahko x zapišemo kot

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

in x smo zapisali na dva načina kot $x = v_1 + v_2$. Ker je po predpostavki zapis enoličen, sledi $x = 0$. □

3.2 Homomorfizmi vektorskih prostorov

Definicija 3.7. Naj bosta U in V vektorska prostora nad poljem $\mathbb{F}$. Za preslikavo $A : U \to V$ pravimo, da je homomorfizem vektorskih prostorov oz. linearna preslikava, če velja:

1. $\forall u_1, u_2 \in U :\ A(u_1 + u_2) = A(u_1) + A(u_2)$ – aditivnost
2. $\forall u \in U : A(\alpha u) = \alpha A(u),\ \forall \alpha \in \mathbb{F}$ – homogenost

Oznaka: $A(u)$ krajše pišemo kot Au.

Zgled 3.9. *Preslikava $A : \mathbb{R}^3 \to \mathbb{R}^2$, $A(x, y, z) = (x, y)$ je linearna. Dokažimo aditivnost in homogenost.*

1. Aditivnost:

$$A\left(\begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} + \begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix}\right) = A\begin{bmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 \end{bmatrix} = \begin{bmatrix} x_1 + x_2 \\ y_1 + y_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} + \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = A\begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} + A\begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix}$$

2. Homogenost:

$$A\left(\alpha \begin{bmatrix} x \\ y \\ z \end{bmatrix}\right) = \begin{bmatrix} \alpha x \\ \alpha y \end{bmatrix} = \alpha \begin{bmatrix} x \\ y \end{bmatrix} = \alpha A \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

Zgled 3.10. *Vzemimo za vektorski prostor $R_n[x]$ in preslikavo $D : R_n[x] \to R_{n-1}[x],\ Dp = p'$. Dokažimo, da je D linearna preslikava.*

1. *Aditivnost:* $D(p+q) = (p+q)' = p' + q' = Dp + Dq$
2. *Homogenost:* $\forall \alpha \in \mathbb{R} :\ D(\alpha p) = (\alpha p)' = \alpha p' = \alpha Dp$

Definicija 3.8. Naj bosta U in V vektorska prostora nad $\mathbb{F}$. Množico vseh linearnih prslikav $U \to V$ označimo z $Hom_{\mathbb{F}}(U, V)$.

Definicija 3.9. Naj bo $A : U \to V$ linearna preslikava.

1. A je monomorfizem, če je injektivna.
2. A je izomorfizem, če je bijektivna.
3. A je epimorfizem, če je surjektivna.

Definicija 3.10. Linearnim preslikavam $A : U \to U$ pravimo endomorfizmi prostora U. Množico endomorfizmov prostora U označimo kot $End_{\mathbb{F}}(U) = Hom_{\mathbb{F}}(U, U)$

Definicija 3.11. Za vektorska prostora U in V nad $\mathbb{F}$ pravimo, da sta izomorfna, če obstaja izomorfizem $A : U \to V$. To označimo kot $U \cong V$.

Opomba. Če je $A : U \to V$ izomorfizem vektorskih prostorov, potem je $A^{-1} : V \to U$ tudi izomorfizem vektorskih prostorov.

Dokaz. Dokazati moramo, da je preslikava $A^{-1} : V \to U$ linearna.

1. Aditivnost: za poljubna $v_1, v_2 \in V$ velja $A^{-1}v_1 = u_1$ in $A^{-1}v_2 = u_2$ natanko tedaj, ko je $Au_1 = v_1$ in $Au_2 = v_2$. Od tod pa sledi $v_1 + v_2 = Au_1 + Au_2 \overset{\text{adit. A}}{=} A(u_1 + u_2)$ in
$$A^{-1}(v_1 + v_2) = u_1 + u_2 = A^{-1}v_1 + A^{-1}v_2.$$
2. Homogenost: za poljuben $v \in V$ velja $A^{-1}v = u$ natanko tedaj, ko je $Au = v$. Sedaj pa za $\forall \alpha \in \mathbb{F}$ velja $\alpha v = \alpha Au = A(\alpha u)$ in $A^{-1}(\alpha v) = \alpha u = \alpha A^{-1}v$. □

Naj bosta U in V vektorska prostora nad $\mathbb{F}$ in množica

$$Hom_{\mathbb{F}}(U, V) = \{\text{vse lin. preslikave } A : U \to V\}$$

Na $Hom_f(U, V)$ definiramo seštevanje in množenje s skalarjem. Naj bodo $A, B \in Hom_{\mathbb{F}}(U, V)$ in $\alpha \in \mathbb{F}$. Potem definiramo preslikavo $(A + B) : U \to V$ kot $(A + B)u = Au + Bu$ in preslikavo $(\alpha A) : U \to V$ kot $(\alpha A)u = \alpha \cdot Au$. Hitro sledi, da sta tako definirani preslikavi $(A + B)$ in (αA) prav tako linearni za $A, B \in Hom_{\mathbb{F}}(U, V)$.

Trditev 3.8. *Ob zgornjih definicijah $Hom_{\mathbb{F}}(U, V)$ postane vektorski prostor nad $\mathbb{F}$.*

Dokaz. Dokazati moramo vseh 5 aksiomov. Najprej dokažimo, da je $Hom_{\mathbb{F}}(U, V)$ Abelova grupa

za seštevanje. Začnimo z asociativnostjo: ta sledi iz tega, da za $\forall A, B, C \in Hom_{\mathbb{F}}(U, V)$ velja

$$\begin{aligned}\forall u \in U: \ ((A+B)+C)(u) &= (A+B)(u) + C(u) \\ &= (A(u) + B(u)) + C(u) \\ &\overset{\text{V vekt. pr.}}{=} A(u) + (B(u) + C(u)) \\ &= A(u) + (B+C)(u) \\ &= (A + (B+C))(u).\end{aligned}$$

Podoben sklep ponovimo še za komutativnost, ki sledi iz tega, da za $\forall A, B \in Hom_{\mathbb{F}}(U, V)$ velja

$$\begin{aligned}\forall u \in U: \ (A+B)(u) &= A(u) + B(u) \\ &\overset{\text{V. vekt. pr.}}{=} B(u) + A(u) \\ &= (B+A)(u).\end{aligned}$$

Za enoto vzamemo tako preslikavo $E : U \to V$, da velja $\forall v \in U : E(v) = 0$ in ta preslikava je očitno linearna. Prav tako za $\forall A \in Hom_{\mathbb{F}}(U, V)$ obstaja taka preslikava $(-A) : U \to V$, da za $\forall u \in U$ velja $(-A)(u) = -A(u)$. Taka preslikava je prav tako linearna in inverz od A.Torej smo dokazali prvi aksiom vektorskih prostorov. Preostale 4 aksiome pokažemo tako, da si izberemo poljubne $A, B \in Hom_{\mathbb{F}}(U, V)$, $\alpha, \beta \in \mathbb{F}$ in opazimo, da za $\forall u \in U$ naslednje:

- $((\alpha+\beta)A)(u) = (\alpha+\beta)A(u) \overset{\text{V vekt. pr.}}{=} \alpha A(u) + \beta A(u)$,
- $(\alpha(A+B))(u) = \alpha(A+B)(u) = \alpha(A(u) + B(u)) \overset{\text{V vekt. pr.}}{=} \alpha A(u) + \alpha B(u)$,
- $(\alpha(\beta A))(u) = \alpha(\beta A)(u) = \alpha(\beta A(u)) \overset{\text{V vekt. pr.}}{=} (\alpha\beta)A(u) = ((\alpha\beta)A)(u)$,
- $(1 \cdot A)(u) = 1 \cdot A(u) \overset{\text{V vekt. pr.}}{=} A(u)$.

Vsak izmed teh točk pa ravno ustreza enemu od aksiomov, ki smo jih želeli dokazati. □

Oglejmo si sedaj še primer, ko sta $A \in Hom_{\mathbb{F}}(U, V)$ in $B \in Hom_{\mathbb{F}}(V, W)$.

Trditev 3.9. *Če sta $A \in Hom_{\mathbb{F}}(U, V)$ in $B \in Hom_{\mathbb{F}}(V, W)$, potem je $B \circ A \in Hom_{\mathbb{F}}(U, W)$.*

Dokaz. Dokažimo aditivnost in homogenost:

1. Aditivnost:

$$\begin{aligned}(B \circ A)(u_1 + u_2) &= B(A(u_1 + u_2)) \\ &= B(Au_1) + B(Au_1) \\ &= (B \circ A)u_1 + (B \circ A)u_2\end{aligned}$$

2. Homogenost:

$$\begin{aligned}(B \circ A)(\alpha u) &= B(A(\alpha u)) \\ &= B(\alpha A u) \\ &= \alpha B(Au) \\ &= \alpha(B \circ A)(u)\end{aligned}$$

□

Kompozitum je operacija na $End_{\mathbb{F}}(U)$. Na $End_{\mathbb{F}}(U)$ imamo torej operacijo seštevanja, operacijo kompozituma (oznaka: $A \cdot B = A \circ B$) in množenje s skalarjem.

Definicija 3.12. Naj bo A neprazna množica in $\mathbb{F}$ polje. Recimo, da imamo na A operaciji seštevanja in produkta in recimo, da imamo še množenje s skalarjem $\mathbb{F} \times A \to A,\ (\alpha, a) \to \alpha a$. Pravimo, da je A algebra nad poljem $\mathbb{F}$, če velja:

1. A za seštevanje in množenje s skalarjem je vektorski prostor nad $\mathbb{F}$
2. $(A, +, \cdot)$ je kolobar
3. $\forall a, b \in A, \forall \alpha \in \mathbb{F} :\ \alpha(a \cdot b) = (\alpha a) \cdot b = a \cdot (\alpha b)$

Trditev 3.10. *$End_{\mathbb{F}}(U)$ s takim seštevanjem, množenjem s skalarjem in množenjem je algebra nad $\mathbb{F}$.*

Dokaz. Dokažimo vse tri točke:

1. $End_{\mathbb{F}}(U) = Hom_{\mathbb{F}}(U, U)$ je vektorski prostor
2. $(End_{\mathbb{F}}(U), +, \cdot)$ je kolobar, saj je $(End_{\mathbb{F}}(U), +)$ Abelova grupa in kompozitum asociativen. Preveriti moramo še levo in desno ditributivnost. Za $\forall A, B, C \in End_{\mathbb{F}}(U)$ velja

$$\begin{aligned} \forall u \in U : (A \cdot (B + C))(u) &= A((B + C)u) \\ &= A(Bu + Cu) \\ &= A(Bu) + A(Cu) \\ &= (A \cdot B)(u) + (A \cdot C)(u) \\ &= (AB + AC)(u) \end{aligned}$$

   in od tod sledi $A(B + C) = AB + AC$. Sedaj pa še druga distributivnost:

$$\begin{aligned} \forall u \in U : ((B + C) \cdot A)(u) &= (B + C)(Au) \\ &= B(Au) + C(Au) \\ &= (B \cdot A)(u) + (C \cdot A)(u) \\ &= (BA + CA)(u). \end{aligned}$$

3. $\forall A, B \in End_{\mathbb{F}}(U),\ \forall \alpha \in \mathbb{F}$ velja

$$\begin{aligned} \forall u \in U :\ (\alpha(A \cdot B))(u) &= \alpha(A \cdot B)(u) \\ &= \alpha A(B(u)) \\ &= (\alpha A)(B(u)) \\ &= ((\alpha A) \cdot B)(u) \end{aligned}$$

   Podobno pa velja tudi:

$$\begin{aligned} \forall u \in U :\ (\alpha(A \cdot B))(u) &= \alpha(A \cdot B)(u) \\ &= \alpha A(B(u)) \\ &\overset{\text{A lin.}}{=} A(\alpha B(u)) \\ &= A((\alpha B)u) \\ &= (A \cdot (\alpha B))(u) \end{aligned}$$

□

Trditev 3.11. *Naj bo $A : U \to V$ linearna preslikava. Potem je $A0_U \to 0_V$.*

Dokaz. Uporabimo enak sklep, kot smo ga že dvakrat (glej 2.6):

$$A0_U = A(0_U + 0_U) \overset{\text{aditivnost}}{=} A0_U + A0_U.$$

Ker je $(V, +)$ Abelova grupa, iz tega ponovno sledi $A0_U = 0_V$ in smo dokazali. □

3.3 Jedro in slika linearne preslikave

Definicija 3.13. Naj bo $A : U \to V$ linearna preslikava. Jedro in slika linearne preslikave sta definirana kot $\ker A = \{u \in U : Au = 0\}$ in $\operatorname{im} A = \{Au : u \in U\}$.

Izrek 3.12.

Naj bo $A : U \to V$ linearna. Potem je $\ker A$ podprostor v U in $\operatorname{im} A$ podprostor v V.

Dokaz. Dokažimo to trditev za $\ker A$ in $\operatorname{im} A$.

1. Vemo, da velja $0 \in \ker A$, zato je $\ker A \neq \emptyset$. Vzemimo $u_1, u_2 \in \ker A,\ \alpha, \beta \in \mathbb{F}$. Potem sledi
$$A(\alpha u_1 + \beta u_2) = \alpha A u_1 + \beta A u_2 = \alpha \cdot 0 + \beta \cdot 0 = 0,$$
torej $\alpha u_1 + \beta u_2 \in \ker A$ in smo pokazali, da je $\ker A$ podprostor U.
2. Očitno je $\operatorname{im} A$ neprazna. Vzemimo $v_1, v_2 \in \ker A,\ \alpha, \beta \in \mathbb{F}$. Potem obstajata $u_1, u_2 \in U$, da je $v_1 = Au_1$ in $v_2 = Au_2$ ter od tod sledi
$$\alpha v_1 + \beta v_2 = \alpha A u_1 + \beta A u_2 = A(\alpha u_1 + \beta u_2) \in \operatorname{im} A.$$ □

Trditev 3.13. *Naj bo $A : U \to V$ linearna preslikava.*

1. *A je injektivna natanko tedaj, ko je $\ker A = \{0\}$*
2. *A je surjektivna natanko tedaj, ko je $\operatorname{im} A = V$*

Dokaz. Osredotočili se bomo na točko (1), saj točka (2) sledi direktno iz definicije surjektivnosti. Dokažimo najprej implikacijo v desno ($\Rightarrow$). Recimo, da je A injektivna. Vzemimo poljuben $x \in \ker A$:
$$Ax = 0 = A0 \overset{\text{A inj.}}{\Longrightarrow} x = 0$$
in od tod sledi $\ker A = \{0\}$. Dokažimo sedaj trditev še v obratno smer ($\Leftarrow$). Recimo, da velja $\ker A = \{0\}$. Potem za poljubna $x, y \in U$ velja:
$$Ax = Ay \implies Ax - Ay = 0 \implies A(x - y) = 0 \implies x - y = 0$$
in A je injektivna. □

Izrek 3.14 (1. Izrek o izomorfizmu**).**

Naj bo $A : U \to V$ linearna preslikava. Potem je
$$U/_{\ker A} \cong \operatorname{im} A$$

Dokaz. Definirajmo preslikavo $B : U/_{\ker A} \to \operatorname{im} A$ kot $B(u + \ker A) \overset{\text{DEF}}{=} Au$. Dokazati moramo, da je ta preslikava dobro definirana, linearna in bijektivna. Pri dobri definiranosti moramo dokazati, da iz $u + \ker A = u_1 + \ker A$ sledi $Au = Au_1$. To hitro velja zaradi
$$\begin{aligned} u - u_1 \in \ker A &\implies A(u - u_1) = 0 \\ &\implies Au - Au_1 = 0. \end{aligned}$$

Linearnost B dokažemo s tem, da preverimo aditivnost in homogenost preslikave. Za $u, u_1 \in U$ je:

$$\begin{aligned} B((u + \ker A) + (u_1 + \ker A)) &= B((u_1 + u_2) + \ker A) \\ &= A(u_1 + u_2) \\ &= Au_1 + Au_2 \\ &= B(u_1 + \ker A) + B(u_2 + \ker A). \end{aligned}$$

Podobno tudi za $\forall \alpha \in \mathbb{F},\ \forall u \in U$ velja:

$$\begin{aligned} B(\alpha(u + \ker A)) &= B(\alpha u + \ker A) \\ &= A(\alpha u) \\ &= \alpha A u \\ &= \alpha B(u + \ker A) \end{aligned}$$

Sedaj opazimo, da za poljuben $v \in \operatorname{im} A$ obstaja $u \in U$, da je $v = Au = B(u + \ker A)$, od koder sledi surjektivnost preslikave B. Preostane nam le še injektivnost B. Dovolj je pokazati $\ker B = \{0 + \ker A\}$. Vzemimo $u + \ker A \in \ker B$. Potem je

$$\begin{aligned} Au = 0 &\implies u \in \ker A \\ &\implies u - 0 \in \ker A \\ &\implies u + \ker A = 0 + \ker A \end{aligned}$$

□

Opomba. Kadar dokazujemo ${}^{U}\!/_{U_1} \cong V$, lahko uporabimo 1. izrek o izomorfizmu: konstruiramo linearno preslikavo $A : U \to V$, da bo $\operatorname{im} A = V$ in $\ker A = U_1$. Po prvem izreku o izomorfizmu od tod sledi želena zveza.

Izrek 3.15 (2. izrek o izomorfizmu)**.**

Naj bosta V_1 in V_2 podprostora vektorskega prostora V. Potem je

$$(V_1 + V_2)/V_1 \cong V_2/(V_1 \cap V_2).$$

Dokaz. Definirajmo preslikavo $A : V_2 \to {}^{(V_1 + V_2)}\!/_{V_1}$ kot $Av_2 = v_2 + V_1$. Ta preslikava je očitno linearna. Sedaj moramo dokazati

1. $\operatorname{im} A = (V_1 + V_2)/V_1$: vzemimo poljuben $x \in (V_1 + V_2)/V_1$. Sedaj velja:

$$x = \underbrace{v_1}_{\in V_1} + \underbrace{v_2}_{\in V_2} + V_1 = v_2 + V_1 = Av_2$$

2. $\ker A = V_1 \cap V_2$: vzemimo poljuben $x \in \ker A$. Sedaj velja:

$$\begin{aligned} A\underbrace{v_2}_{\in V_2} = 0 + V_1 &\iff v_2 + V_1 = 0 + V_1 \\ &\iff v_2 - 0 \in V_1 \\ &\iff v_2 \in V_1 \end{aligned}$$

Preostalo velja po 1. izreku o izomorfizmu. □

Izrek 3.16 (3. izrek o izomorfizmu)**.**

Naj bodo $U \leq V \leq W$ vektorski prostori. Potem je V/U podprostor v W/U in velja

$$(W/U)\Big/(V/U) \cong W/V$$

Dokaz. Najprej dokažimo, da je V/U podprostor W/U. Dokazali smo že, da sta V/U in W/U vektorska prostora in očitno velja $V/U \subseteq W/U$. Naj bosta $v_1+U,\ v_2+U \in V/U$ in $\alpha, \beta \in \mathbb{F}$. Sedaj velja:

$$\begin{aligned}\alpha(v_1+U)+\beta(v_2+U) &= (\alpha v_1+U)+(\beta v_2+U)\\ &= (\alpha v_1+\beta v_2)+U\\ &\overset{\text{V vekt. pr.}}{\in} V/U\end{aligned}$$

in s tem smo dokazali, da je V/U podprostor W/U. Sedaj moramo dokazati, da $(W/U)\Big/(V/U)$ vsebuje iste elemente kot W/V. Vzemimo poljuben element $x \in (W/U)\Big/(V/U)$. Sedaj velja:

$$\begin{aligned}x \in (W/U)\Big/(V/U) &\iff x = (\overbrace{w}^{\in W}+U)+V/U\\ &\iff x = \{(w+u_1)+(v+u_2):\ v\in V, u_1,u_2\in U\}\\ &\iff x = \{w+(v+u_1+u_2):\ v\in V, u_1,u_2\in U\}\\ &\iff x = \{w+v':\ v'\in V\}\\ &\iff x = w+V \iff x \in W/V\end{aligned}$$

Peostane nam še, da dokažemo, da med $(W/U)\Big/(V/U)$ in W/V obstaja izomorfizem. Za to uporabimo izrek (3.15) in vstavimo: $V_1 = V/U$ in $V_2 = W/U$ (oba podprostora $V = W/U$) in od tod sledi formula: $(W/U)\Big/(V/U) \cong W/V$. □

3.4 Končnorazsežni vektorski prostori

Definicija 3.14. Naj bo V vektorski prostor nad $\mathbb{F}$ in X naj bo neprazna podmnožica v V. Definirajmo

$$Lin\ X = \{\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_kx_k:\ k\geq 1,\ \alpha_1,\alpha_2,\ldots,\alpha_k\in\mathbb{F},\ x_1,x_2,\ldots,x_k\in X\}.$$

Množici $Lin\ X$ pravimo linearna ogrinjača množice X.

Trditev 3.17. *Naj bo X podmnožica vektorskega prostora V. Potem je $Lin\ X$ najmanjši vektorski podprostor v V, ki vsebuje množico X:*

1. *Če je $U \leq V$ in $X \subseteq U$, potem je $Lin\ X \subseteq U$*
2. *$Lin\ X$ je podprostor v V, ki vsebuje X.*

Dokaz. Dokažimo obe točki:

1. Denimo, da velja $U \leq V$ in $X \subseteq U$. Potem za nek $y \in Lin\ X$, $y = \alpha_1x_1+\cdots+\alpha_kx_k$, velja:

$$x_1,\ldots x_k \in X \subseteq U \overset{\text{U podprostor}}{\Longrightarrow} y \in U$$

2. Očitno velja $X \subseteq LinX$. Dokazati moramo, da je $LinX$ vektorski podprostor v V. To je očitno, saj je linearna kombinacija dveh linearnih kombinacij vektorjev iz X prav tako linearna kombinacija vektorjev iz X. □

Definicija 3.15. Naj bo V vektorki prostor in X neprazna množica v V. Pravimo, da je X ogrodje za V, če $Lin\ X = V$. To pomeni, da je vsak $v \in V$ linearna kombinacija nekih vektorjev iz X.

Definicija 3.16. Vektorski prostor je končnorazsežen, če ima kakšno končno ogrodje, tj. obstaja končna množica $X \subseteq V$, da velja $Lin\ X = V$.

Zgled 3.11. *Naj bo $V = \mathbb{R}^3$. Množica*

$$X = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$$

je ogrodje $\mathbb{R}^3$. $\mathbb{R}^3$ je torej končnorazsežen vektorski prostor

Zgled 3.12. *$\mathbb{F}^n$ je prav tako končnorazsežen vektorski prostor nad $\mathbb{F}$:*

$$\mathbb{F}^n = Lin \left\{ \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \right\}$$

Zgled 3.13. *Vektorski prostor $\mathbb{F}[X]$ (vsi polinomi s koeficienti iz $\mathbb{F}$) ni končnorazsežen. Takšne vektorske prostora bomo obravnavali naslednje leto pri algebri 2.*

Zgled 3.14. *Vektorski prostor $\mathbb{F}_n[X]$ pa je končnorazsežen vektorski prostor. Njegovo ogrodje je na primer:*

$$\mathbb{F}_n[x] = Lin\ \{1, x, x^2, \ldots, x^n\}$$

Trditev 3.18. *Če je X ogrodje prostora V in $X \subseteq Y$, potem je tudi Y ogrodje prostora V (Y je množica vektorjev v V).*

Trditev 3.19. *Recimo, da je X ogrodje prostora V in recimo, da je $x \in X$ linearna kombinacija od x različnih vektorjev iz X. Potem je $X \setminus \{x\}$ tudi ogrodje prostora V.*

Definicija 3.17. Naj bo V vektorski prostor nad $\mathbb{F}$ in $\{v_1, v_2, \ldots, v_n\}$ množica vektorjev iz V. Pravimo, da so $v_1, v_2, \ldots, v_n$ linearno neodvisni, če iz enakosti

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0,\ \alpha_i \in \mathbb{F}$$

sledi

$$\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0.$$

Pravimo, da so $v_1, v_2, \ldots, v_n$ linearno neodvisni, če niso linearno odvisni.

Opomba. Kaj pomeni, da so $v_1, v_2, \ldots, v_n$ linearno odvisni? Na začetku smo že pokazali, da so ti vektorji linearno odvisni natanko tedaj, ko je vsaj eden izmed njih linearna kombinacija ostalih.

Definicija 3.18. Naj bo V vektorski prostor in $B = \{v_1, v_2, \ldots, v_n\}$ množica vektorjev iz V. Pravimo, da je B baza prostora V, če:

1. B je ogrodje V: $Lin\ B = V$
2. $v_1, v_2, \ldots, v_n$ so linearno neodvisni.

Opomba. Če ima nek vektorski prostor bazo, je ta prostor avtomatično končnorazsežen. Ali velja obratno: vsak končnorazsežen vektorski prostor ima bazo?

Izrek 3.20.

Vsak netrivialen končnorazsežen vektorski prostor ima bazo.

Dokaz. V naj bo končnorazsežen prostor in obstaja končna množica vektorjev $X = \{x_1, x_2, \ldots, x_n\}$, ki je ogrodje prostora V. Brez škode za splošnost so vsi vektorji v X različni od 0. Bazo B prostora V dobimo z algoritmom:

1. Ali so vektorji v ogrodju $X = \{v_1, v_2, \ldots, v_n\}$ linearno odvisni?
   - Če DA, potem je X baza prostora V.
   - Če NE, potem obstaja $v_i \in X$, ki ga lahko zapišemo kot linearno kombinacijo ostalih vektorjev iz X. Torej je tudi $X \setminus \{v_i\}$ ogrodje prostora V.
2. Postopek ponovimo z novim (zmanjšanim) ogrodjem prostora V.

Ta potopek ponavljamo, dokler ne dobimo množice linearno neodvisnih vektorjev B, ki je hkrati tudi ogrodje prostora V. Do tega pridemo v končno mnogo korakih, saj je množica X končna. □

3.5 Lastnosti baz končnorazsežnih prostorov

Trditev 3.21. *Naj bo $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ baza vektorskega prostora V. Potem se da vsak vektor $V \in V$ na enoličen način zapisati kot linearna kombinacija vektorjev iz B („vektorje razvijemo po bazi B“).*

Dokaz. Po definiciji lahko v zapišemo kot linearno kombinacijo vektorjev iz $\mathcal{B}$, saj je $\mathcal{B}$ ogrodje. Dokazati moramo enoličnost. Naj bo

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$
$$v = \beta_1 v_1 + \beta_2 v_2 + \cdots + \alpha_n v_n$$

Ti dve enačbi odštejemo in dobimo

$$(\alpha_1 - \beta_1)v_1 + (\alpha_2 - \beta_2)v_2 + \cdots + (\alpha_n - \beta_n)v_n = 0.$$

Ker so vektorji $v_1, v_2, \ldots, v_n$ linearno neodvisni, mora veljati

$$\alpha_1 = \beta_1, \alpha_2 = \beta_2, \ldots, \alpha_n = \beta_n,$$

torej je zapis enoličen. □

Lema 3.22. *Naj bo V vektorski prostor in $X = \{u_1, u_2, \ldots, u_m\}$ ogrodje V. Naj bo $Y = \{v_1, v_2, \ldots, v_n\}$ množica linearno neodvisnih vektorjev iz V. Potem je $n \leq m$.*

Dokaz. S protislovjem: recimo, da je $n > m$. Oglejmo si vektorje $X' = \{v_1, u_1, u_2, \ldots, u_m\}$. Množica X' je tudi ogrodje; iz nje po postopku iz prejšnjega dokaza odstranimo prvi u_i, ki je linearno odvisen od prejšnjih vektorjev (opomba: tak u_i obstaja, ker je v_1 neničeln in linearna kombinacija vektorjev iz X). Tako dobimo množico vektorjev

$$X'' = v_1, u_1', u_2', \ldots, u_{m-1}',$$

ki pa je ogrodje V. Postopek ponavljamo in vedno spet dobimo ogrodje prostora V. Po m korakih dobimo ogrodje

$$\overline{X} = \{v_1, v_2, \ldots, v_m\}.$$

Ker so vektorji $v_1, v_2, \ldots, v_n$ linearno neodvisni, je $\overline{X}$ baza prostora V. Od tod sledi, da se da vektor v_{m+1} zapisati kot linearna kombinacija vektorjev iz baze $\overline{X}$, kar pa je v protislovju s predpostavko, da so Y linearno neodvisna množica vektorjev. □

Posledica 3.23. *Naj bo V končnorazsežen vektorski prostor. Potem imajo vse baze isto moč.*

Dokaz. Recimo, da imamo bazi prostora

$$\mathcal{B}_1 = \{u_1, u_2, \ldots, u_m\}$$
$$\mathcal{B}_2 = \{v_1, v_2, \ldots, v_n\}$$

Ker je B_1 ogrodje in B_2 lin. neodvisna množica, po prejšnji lemi sledi $m \leq n$. Ta argument lahko tudi obrnemo in dobimo $n \leq m$. Od tod pa sledi $m = n$. □

Definicija 3.19. Naj bo V končnorazsežen vektorski prostor. Dimenzija prostora V je število vektorjev v neki poljubni bazi prostora V. Oznaka: $\dim V$.

Zgled 3.15. *Dokažimo, da je $\dim \mathbb{F}^n = n$. Vemo že, da velja*

$$\mathbb{F}^n = Lin\left\{ \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \right\}.$$

Torej je ta množica $e_1, e_2, \ldots, e_n$ linearno neodvisna (razmislek je preprost) in ogrodje prostora V, torej je baza. To je standardna baza prostora $\mathbb{F}^n$.

Zgled 3.16. *Dokažimo, da je $\dim \mathbb{F}_n[x] = n + 1$. Tudi pri tem primeru že vemo, da velja*

$$\mathbb{F}_n[x] = \{1, x, \ldots, x^n\}.$$

Trivialno je pokazati, da je tudi ta množica baza. Imenujemo jo standardna baza prostora $\mathbb{F}_n[x]$.

Trditev 3.24. *Recimo, da je V končno razsežen prostor in U podprostor v V. Recimo, da imamo bazo $\mathcal{B}$ podprostora U. Potem lahko množico $\mathcal{B}$ dopolnimo do baze celega prostora V.*

Dokaz. Naj bo $\mathcal{B} = \{u_1, u_2, \ldots, u_m\}$ baza prostora U. Če je $Lin\ \mathcal{B} = U = V$, potem je $\mathcal{B}$ baza prostora V. Sicer pa vzamemo poljuben neničeln vektor $v_1 \in V \setminus Lin\ \mathcal{B}$ in dobimo linearno neodvisno množico $\mathcal{B}_1 = \{u_1, u_2, \ldots, u_m, v_1\}$. Ta postopek ponovimo; konča se v končno mnogo korakih, ker je V končno razsežen prostor. Na koncu dobimo bazo

$$\mathcal{B}_k = \{u_1, u_2, \ldots, u_m, v_1, \ldots, v_k\}$$ □

Posledica 3.25. *Naj bo V končnorazsežen prostor,* $\dim V = n$. *Če je X podmnožica v V, ki vsebuje natanko n linearno neodvisnih vektorjev, je X že baza prostora V.*

Dokaz. Naj bo $U = Lin\ X$ in predpostavimo, da je $U \leq V$. X je baza prostora U, sestavljena iz n vektorjev. Po prejšnji trditvi lahko X dopolnimo do baze V, vendar pa od tod sledilo, da je $\dim V > n$, kar pa je v nasprotju s predpostavko. □

Posledica 3.26. *Naj bo V vektorski prostor nad $\mathbb{F}$ in* $\dim V = n$. *Potem je $V \cong \mathbb{F}^n$.*

Dokaz. V ima bazo, sestavljeno iz n vektorjev. Naj bo to $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$. Definiramo preslikavo $\Phi_{\mathcal{B}} : \mathbb{F}^n \to V$ s predpisom

$$\Phi_{\mathcal{B}} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$

Dokazali bomo, da je $\Phi_{\mathcal{B}}$ izomorfizem med $\mathbb{F}^n$ in V.

1. $\Phi_{\mathcal{B}}$ linearna: dokaz je trivialen.
2. $\Phi_{\mathcal{B}}$ injektivna: vzemimo $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \ker \Phi_{\mathcal{B}}$. Od tod sledi $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$. Ker pa so vektorji $v_1, v_2, \ldots, v_n$ linearno neodvisni, velja $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$. Torej je $\ker \Phi_{\mathcal{B}} = \{(0, 0, \ldots, 0)\}$.
3. $\Phi_{\mathcal{B}}$ surjektivna: vzemimo poljuben $v \in V$. Ker je $\mathcal{B}$ baza V, lahko v razvijemo po $\mathcal{B}$, kar pomeni, da $v \in \operatorname{im} \Phi_{\mathcal{B}}$. □

Izrek 3.27.

Naj bosta U in V končnorazsežna vektorska prostora nad $\mathbb{F}$. Potem sta U in V izomorfna natanko tedaj, ko $\dim U = \dim V$.

Dokaz. ($\Leftarrow$) Recimo, da $\dim U = \dim V = n$. Sledi, da imamo izomorfizma vektorskih prostorov $\Phi_{\mathcal{B}} : \mathbb{F}^n \to U$ in $\Phi_{\mathcal{C}} : \mathbb{F}^n \to V$. Potem je $\Phi_{\mathcal{C}} \Phi_{\mathcal{B}}^{-1}$ izomorfizem med U in V.

($\Rightarrow$) Dokažimo sedaj še v drugo smer. Naj bo $\dim U = n$ in baza za U $\mathcal{B} = \{u_1, u_2, \ldots, u_n\}$. Imamo izomorfizem $A : U \to V$. Trdimo, da je $\mathcal{C} = \{Au_1, Au_2, \ldots, Av_n\}$ baza V. Dokažimo, da je $\mathcal{C}$ ogrodje. Vzemimo $v \in V$. Ker je A bijekcija, obstaja $u \in U$, da je $Au = v$. Ker lahko vektor u razvijemo po bazi $\mathcal{B}$: $u = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$, lahko vektor v zapišemo kot

$$\begin{aligned} v = Au &= A(\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n) \\ &= \alpha_1 Au_1 + \alpha_2 Au_2 + \cdots + \alpha_n Au_n. \end{aligned}$$

Dokažimo še, da so vektorji iz $\mathcal{C}$ linearno neodvisni. Oglejmo si linearno kombinacijo teh vektorjev:

$$\begin{aligned}\alpha_1 Au_1 + \alpha_2 Au_2 + \cdots + \alpha_n Au_n = 0 &\implies A(\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n) = 0\\ &\implies \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n \in \ker A\\ &\overset{\text{A inj.}}{\implies} \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n = 0\end{aligned}$$

in ker so $u_1, u_2, \ldots, u_n$ linearno neodvisni, sledi $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$. □

Trditev 3.28. *Naj bo V končnorazsežen vektorski prostor in U podprostor v V. Potem obstaja podprostor $W \leq V$, da je $V = U \oplus W$.*

Dokaz. Izberimo neko bazo $\mathcal{B} = \{u_1, u_2, \ldots, u_m\}$. To bazo dopolnimo do baze V, ki jo označiumo s $\mathcal{C} = \{u_1, u_2, \ldots, u_m, w_1, w_2, \ldots, w_k\}$. Definiramo $W = Lin\ \{w_1, w_2, \ldots, w_k\}$, $W \leq V$. Trdimo, da je $V = U \oplus W$. Vemo, da lahko poljuben $v \in V$ razvijemo po bazi $\mathcal{C}$:

$$v = \underbrace{\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_m u_m}_{\in U} + \underbrace{\beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_k w_k}_{\in W},$$

torej $V = U + W$. Sedaj vzemimo $v \in U \cap W$, torej $v \in U$ in $v \in W$. Potem je $v = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_m u_m$ in $v = \beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_k w_k$. Torej velja

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n - \beta_1 w_1 - \beta_2 w_2 - \cdots - \beta_k w_k = 0.$$

Zaradi linearne neodvisnosti sledi $\alpha_1 = \cdots = \alpha_m = \beta_1 = \cdots = \beta_k = 0$. Zato je $v = 0$ in $U \cap W = \{0\}$. □

Trditev 3.29. *Naj bo V končnorazsežen prostor in $U \leq V$. Potem je*

$$\dim {}^{V}\!/_{U} = \dim V - \dim U.$$

Dokaz. Po prejšnji trditvi obstaja $W \leq V$, da je $V = U \oplus W$. Sedaj pa uporabimo 2. izrek o izomorfizmu, ki pravi, da za $V_1, V_2 \leq V$ velja

$$(V_1 + V_2)\,/_{V_2} \cong V_1 \Big/ (V_1 \cap V_2)\,.$$

Če vstavimo $V_1 = W$ in $V_2 = U$, dobimo

$${}^{V}\!/_{U} \cong W \Big/ \{0\} \cong W.$$

Torej $\dim {}^{V}\!/_{U} = \dim V - \dim U$. □

Trditev 3.30. *Naj bo V končnorazsežen vektorski prostor in $V_1, V_2 \leq V$. Potem*

$$\dim(V_1 + V_2) = \dim V_1 + \dim V_2 - \dim(V_1 \cap V_2).$$

Dokaz. To je direktna posledica prejšnje trditve in 2. izreka o izomorfizmu.

$$\begin{aligned}(V_1 + V_2)\,/_{V_2} \cong V_1 \Big/ (V_1 \cap V_2) &\implies \dim (V_1 + V_2)\,/_{V_2} = \dim V_1 \Big/ (V_1 \cap V_2)\\ &\implies \dim(V_1 + V_2) - \dim V_1 = \dim V_2 - \dim(V_1 \cap V_2)\end{aligned}$$ □

Posledica 3.31. *Za končnorazsežna vektorska prostora V_1, V_2 velja* $\dim(V_1 \oplus V_2) = \dim V_1 + \dim V_2$.

Trditev 3.32. *Naj bosta U in V končnorazsežna vektorska prostora nad $\mathbb{F}$ in $A : U \to V$ linearna preslikava. Potem velja* $\dim \ker A + \dim \operatorname{im} A = \dim U$.

Dokaz. To je direktna posledica 1. izreka o izomorfizmu. □

Opomba.

1. Trditev 3.30 lahko dokažemo tako, da izberemo bazo prostora $V_1 \cap V_2$, jo razširimo do baz V_1 in V_2 in pokažemo, da je unija dobljenih baz baza za prostor $V_1 + V_2$.
2. Trditev 3.32 lahko dokažemo tako, da vzamemo bazo $\ker A$, jo dopolnimo do baze U in dokažemo, da dodane bazne vektorje A preslika v bazo $\operatorname{im} A$.

Definicija 3.20. Naj bo $A : U \to V$ linearna preslikava. Številu $r(A) = \text{rang}A = \dim \operatorname{im} A$ pravimo rang linearne preslikave A.

4 Linearne preslikave med končnorazsežnimi vektorskimi prostori in matrike

Naj bosta U, V vektorska prostora nad $\mathbb{F}$.[1] Naj bo $\mathcal{B} = \{u_1, u_2, \ldots, u_n\}$ baza U in $\mathcal{C} = \{v_1, v_2, \ldots, v_m\}$ baza V. Naj bo $A : U \to V$ linearna preslikava.

Trditev 4.1. *Preslikava A je enolično določena s slikami baznih vektorjev iz $\mathcal{B}$.*

Dokaz. Vektorje $Au_1, Au_2, \ldots, Au_n$ poznamo. Vzemimo $u \in U$; u lahko na enoličen način razvijemo po $\mathcal{B}$ kot $u = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$. Od tod pa sledi

$$Au = A(\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n) = \alpha_1 Au_1 + \alpha_2 Au_2 + \cdots + \alpha_n Au_n \qquad \square$$

Sedaj vektorje $Au_1, Au_2, \ldots, Au_n$ razvijemo po bazi $\mathcal{C}$:

$$\begin{aligned} Au_1 &= \alpha_{11} v_1 + \alpha_{21} v_2 + \cdots + \alpha_{m1} v_m \\ Au_2 &= \alpha_{12} v_1 + \alpha_{22} v_2 + \cdots + \alpha_{m2} v_m \\ &\ldots \\ Au_n &= \alpha_{1n} v_1 + \alpha_{2n} v_2 + \cdots + \alpha_{mn} v_m \end{aligned}$$

Skalarje, ki smo jih dobili, zložimo v tabelo, ki ji pravimo matrika, ki pripada linearni preslikavi A glede na bazi $\mathcal{B}$ in $\mathcal{C}$.

$$A_{\mathcal{C}\mathcal{B}} = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \ldots & \alpha_{mn} \end{bmatrix}$$

Terminologija: pravimo, da je ta matrika $m \times n$ matrika nad poljem $\mathbb{F}$.

$$[\alpha_{ij}]_{i=1,2,\ldots,m}^{j=1,2,\ldots,n} = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \ldots & \alpha_{mn} \end{bmatrix}$$

Matrike kot tabele označujemo z velikimi tiskanimi črkami. Nazadnje definirajmo še množico

$$\mathbb{F}^{m \times n} = \{\text{vse } m \times n \text{ matrike nad poljem } \mathbb{F}\}.$$

Zgled 4.1 (Poseben primer)**.** *Recimo, da imamo matriko $A \in \mathbb{F}^{m \times n}$. Potem ta matrika določa linearno preslikavo $A : \mathbb{F}^n \to \mathbb{F}^m$ na naslednji način. Izberemo standardno bazo $\mathbb{F}^n$: $\mathcal{S} = \{e_1, e_2, \ldots, e_n\}$. Potem definiramo, da je Ae_1 prvi stolpec matrike A, Ae_2 drugi stolpec matrike A in tako dalje. Seveda pa velja tudi obratno: naj bo $A : \mathbb{F}^n \to \mathbb{F}^m$ linearna preslikava in naj bosta $\mathcal{B}, \mathcal{C}$ zaporedoma standardni bazi prostorov $\mathbb{F}^n, \mathbb{F}^m$. Potem preslikava A nazaj določa matriko $A_{\mathcal{C}\mathcal{B}}$.*

Trditev 4.2. *Naj bosta U in V vektorska prostora nad $\mathbb{F}$, izberimo bazo $\mathcal{B} = \{u_1, u_2, \ldots, u_n\}$ za U in bazo $\mathcal{C} = \{v_1, v_2, \ldots, v_m\}$ za V. Potem je preslikava $\Phi_{\mathcal{C}\mathcal{B}} : Hom_{\mathbb{F}}(U, V) \to \mathbb{F}^{m \times n}$ s predpisom $\Phi_{\mathcal{C}\mathcal{B}}(A) = A_{\mathcal{C}\mathcal{B}}$ bijekcija.*

Dokaz. Dokazati moramo surjektivnost in injektivnost.

- Surjektivnost: vzemimo poljubno matriko $A \in \mathbb{F}^{m \times n}$, $A = [\alpha_{ij}]$. Vzemimo linearno preslikavo

[1] Dogovor: od tu naprej obravnavamo le končnorazsežne prostore.

$\mathcal{A} : U \to V$ s predpisom

$$\begin{aligned}\mathcal{A}u_1 &= \alpha_{11}v_1 + \alpha_{21}v_2 + \cdots + \alpha_{m1}v_m\\ \mathcal{A}u_2 &= \alpha_{12}v_1 + \alpha_{22}v_2 + \cdots + \alpha_{m2}v_m\\ &\cdots\\ \mathcal{A}u_n &= \alpha_{1n}v_1 + \alpha_{2n}v_2 + \cdots + \alpha_{mn}v_m.\end{aligned}$$

Potem je A matrika za $\mathcal{A}$ v bazah $\mathcal{B}$ in $\mathcal{C}$, torej velja $\mathcal{A}_{\mathcal{CB}} = A$ in posledično $\Phi_{\mathcal{CB}}(\mathcal{A}) = A$.

- Injektivnost: recimo, da sta $A : U \to V$ in $B : U \to V$ linearni preslikavi, za kateri velja $\Phi_{\mathcal{CB}}(A) = \Phi_{\mathcal{CB}}(B)$. Potem je $A_{\mathcal{CB}} = B_{\mathcal{CB}}$, od tod pa sledi, da velja

$$Au_1 = Bu_1,\ Au_2 = Bu_2, \ldots,\ Au_n = Bu_n.$$

Ker A in B slikata bazne vektorje iz baze $\mathcal{B}$ enako, sta nujno enaki in velja $A = B$. □

Na $\mathbb{F}^{m\times n}$ vpeljemo seštevanje in množenje s skalarjem (iz $\mathbb{F}$) na naslednji način. Naj bosta $A, B \in \mathbb{F}^{m\times n}$, $A = [\alpha_{ij}]$ in $B = [\beta_{ij}]$. Potem je $A + B \overset{\text{DEF}}{=} [a_{ij} + b_{ij}]$ in $\alpha A \overset{\text{DEF}}{=} [\alpha a_{ij}]$.

Opomba. Elemente $\mathbb{F}^n$ (stolpci dolžine n) lahko gledamo kot $n \times 1$ matrike. Seštevanje in množenje s skalarjem, ki smo ju definirali za matrike, se tu ujemata s seštevanjem in množenjem s skalarjem, ki smo ju definirali v $\mathbb{F}^n$

Trditev 4.3. *$\mathbb{F}^{m\times n}$ z zgornjim seštevanjem in množenjem s skalarjem postane vektorski prostor nad poljem $\mathbb{F}$.*

Dokaz. DN (aksiomi vektorskega prostora sledijo iz lastnosti polja $\mathbb{F}$). □

Trditev 4.4. *Definirajmo E_{ij} kot matriko $m \times n$, ki ima na (i, j)-tem mestu 1, povsod drugod pa 0 (pri tem indeks i teče po $1, \ldots, m$, indeks j pa po $1, \ldots, n$). Potem je*

$$\{E_{ij} :\ i = 1, \ldots, m,\ j = 1, \ldots, n\}$$

baza prostora $\mathbb{F}^{m\times n}$.

Opomba. Tej bazi se reče tudi standardna baza prostora $\mathbb{F}^{m\times n}$. Od tod sledi, da je $\dim \mathbb{F}^{m\times n} = m \cdot n$, torej $\mathbb{F}^{m\times n} \cong \mathbb{F}^{m\cdot n}$.

Izrek 4.5.

Naj bosta U, V končnorazsežna vektorska prostora nad $\mathbb{F}$, $\mathcal{B}$ naj bo baza U, $\mathcal{C}$ pa naj bo baza V. Potem je

$$\Phi_{\mathcal{CB}} : Hom_{\mathbb{F}}(U, V) \to \mathbb{F}^{m\times n}$$

s predpisom $A \mapsto A_{\mathcal{CB}}$ izomorfizem vektorskih prostorov.

Dokaz. Vemo že, da je $\Phi_{\mathcal{CB}}$ bijekcija. Dokazati moramo linearnost. Naj bosta $\mathcal{B} = \{u_1, u_2, \ldots, u_n\}$ in $\mathcal{C} = \{u_1, u_2, \ldots, u_m\}$ bazi prostorov U in V. Pokažimo, da je $\Phi_{\mathcal{CB}}$ aditivna: dokazujemo, da velja $(A + B)_{\mathcal{CB}} = A_{\mathcal{CB}} + B_{\mathcal{CB}}$. Sedaj velja

$$\begin{aligned}(A + B)u_1 &= Au_1 + Bu_1\\ &= \alpha_{11}v_1 + \alpha_{21}v_2 + \cdots + \alpha_{m1}v_m\\ &+ \beta_{11}v_1 + \beta_{21}v_2 + \cdots + \beta_{m1}v_m\\ &= (\alpha_{11} + \beta_{11})v_1 + (\alpha_{21} + \beta_{21})v_2 + \cdots + (\alpha_{m1} + \beta_m)v_m\end{aligned}$$

Torej je matrika za $A+B$ v bazah $\mathcal{B}$ in $\mathcal{C}$:

$$\begin{aligned}(A+B)_{\mathcal{C}\mathcal{B}} &= \begin{bmatrix} \alpha_{11}+\beta_{11} & \dots & \alpha_{1n}+\beta_{1n} \\ \vdots & & \vdots \\ \alpha_{m1}+\beta_{m1} & \dots & \alpha_{mn}+\beta_{mn} \end{bmatrix} \\ &= \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \dots & \alpha_{mn} \end{bmatrix} + \begin{bmatrix} \beta_{11} & \dots & \beta_{1n} \\ \vdots & & \vdots \\ \beta_{m1} & \dots & \beta_{mn} \end{bmatrix} \\ &= A_{\mathcal{C}\mathcal{B}} + B_{\mathcal{C}\mathcal{B}}\end{aligned}$$

Podobno se dokaže tudi homogenost $\Phi_{\mathcal{C}\mathcal{B}}$. □

Zgled 4.2 (Poseben primer)**.** *Imejmo linearno preslikavo $A : \mathbb{F}^n \to \mathbb{F}^m$. Za prostora $\mathbb{F}^n, \mathbb{F}^m$ izberimo standardni bazi $\mathcal{B} = \{e_1, e_2, \dots, e_n\}$ in $\mathcal{C} = \{e_1, e_2, \dots, e_m\}$. Preslikavi A priredimo matriko $A_{\mathcal{C}\mathcal{B}} = [\alpha_{ij}]$. Denimo, da je $x \in \mathbb{F}^n$ poljuben vektor, ki ga lahko razvijemo kot $x = \beta_1 e_1 + \beta_2 e_2 + \dots + \beta_n e_n$. Zanima nas, kam se preslika vektor Ax.*

$$\underbrace{\begin{bmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \dots & \alpha_{mn} \end{bmatrix}}_{A_{\mathcal{C}\mathcal{B}}} \underbrace{\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}}_{x} = \underbrace{\begin{bmatrix} \alpha_{11}\beta_1 + \dots + \alpha_{1n}\beta_n \\ \vdots \\ \alpha_{m1}\beta_1 + \dots + \alpha_{mn}\beta_n \end{bmatrix}}_{Ax}$$

Torej je i-ta komponenta Ax enaka skalarnemu produktu i-te vrstice matrike $A_{\mathcal{C}\mathcal{B}}$ in stolpca x.

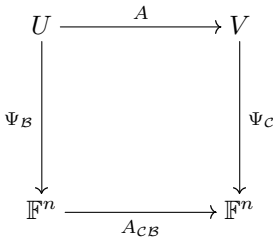
Definicija 4.1. Naj bo $A \in \mathbb{F}^{m\times n}$ in $x \in \mathbb{F}^n$. Produkt matrike A z vektorjem x je vektor Ax, ki ga dobimo na naslednji način: i-ta komponenta Ax je enaka skalarnemu produktu i-te vrstice A in stolpca x.

Zgled 4.3.

$$\begin{bmatrix} 2 & -1 \\ 3 & 0 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 2\cdot 7 - 1\cdot 8 \\ 3\cdot 7 + 0\cdot 8 \\ 4\cdot 7 + 5\cdot 8 \end{bmatrix} = \begin{bmatrix} 6 \\ 21 \\ 68 \end{bmatrix}$$

Opomba. Če je $A : \mathbb{F}^n \to \mathbb{F}^m$ in sta $\mathcal{B}$ in $\mathcal{C}$ standardni bazi, potem je $Ax = A_{\mathcal{C}\mathcal{B}}x$.

Obravnavajmo splošen primer. Naj bo $A : U \to V$ linearna preslikava. Potem naj bodo množice $\mathcal{B} = \{u_1, u_2, \dots, u_n\}$, $\mathcal{C} = \{v_1, v_2, \dots, v_m\}$, $\mathcal{E} = \{e_1, e_2, \dots, e_n\}$ in $\mathcal{F} = \{f_1, f_2, \dots, f_m\}$ zaporedoma baze prostorov $U, V, \mathbb{F}^n, \mathbb{F}^m$. Ker je $\dim U = n$, imamo izomorfizem $\Phi_{\mathcal{B}} : \mathbb{F}^n \to U$ s predpisom $\Phi_{\mathcal{B}} e_i = u_i$ in inverzom $\Psi_{\mathcal{B}} : U \to \mathbb{F}^n$, $\Psi_{\mathcal{B}} u_i = e_i$. Podobno ($\dim V = m$) imamo tudi izomorfizem $\Phi_{\mathcal{C}} : \mathbb{F}^m \to V$ s predpisom $\Phi_{\mathcal{C}} f_i = v_i$ in inverzom $\Psi_{\mathcal{C}} : V \to \mathbb{F}^m$, $\Psi_{\mathcal{C}} v_i = f_i$.



Izrek 4.6.

Za tako definirane linearne preslikave velja $\Psi_{\mathcal{C}} \circ A = A_{\mathcal{CB}} \circ \Psi_{\mathcal{B}}$

Dokaz. Dokaz je očiten, če narišemo diagram preslikav in opazimo, da ta komutira. Bolj formalen dokaz pa je sledeč. Dokazati želimo, da velja $(\Psi_{\mathcal{C}} \circ A)u_i = (A_{\mathcal{CB}} \circ Psi_{\mathcal{B}})$ za $\forall i$. Označimo matriko

$$A_{\mathcal{CB}} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}.$$

Sedaj si bomo posebej ogledali obe strani enačbe in dokazali, da sta si med seboj enaki. Sedaj je:

$$\begin{aligned} (\Psi_{\mathcal{C}} \circ A)u_i &= \Psi_{\mathcal{C}}(Au_i) \\ &= \Psi_{\mathcal{C}}(a_{1i}v_1 + a_{2i}v_2 + \dots + a_{mi}v_m) \\ &= a_{1i}\Psi_{\mathcal{C}}v_1 + a_{2i}\Psi_{\mathcal{C}}v_2 + \dots + a_{mi}\Psi_{\mathcal{C}}v_m \\ &= a_{1i}f_1 + a_{2i}f_2 + \dots + a_{mi}f_m \end{aligned}$$

in dobimo i-ti stolpec matrike $A_{\mathcal{CB}}$. Na drugi strani enačbe pa dobimo

$$(A_{\mathcal{CB}} \circ \Psi_{\mathcal{B}})u_i = A_{\mathcal{CB}}(\Psi_{\mathcal{B}}u_i) = A_{\mathcal{CB}}(e_i),$$

kar je prav tako enako i-temu stolpcu $A_{\mathcal{CB}}$. □

Uporaba: naj bo $A : U \to V$, $\mathcal{B}$ baza za U in $\mathcal{C}$ baza za V. Naj bo $u \in U$ poljuben vektor. Potem je

$$\begin{aligned} (\Psi_{\mathcal{C}} \circ A)u = (A_{\mathcal{CB}} \circ \Psi_{\mathcal{B}})u &\implies \Psi_{\mathcal{C}}(Au) = A_{\mathcal{CB}}(\psi_{\mathcal{B}}u) \\ &\implies (Au)_{\mathcal{C}} = A_{\mathcal{CB}}u_{\mathcal{B}}, \end{aligned}$$

pri čemer smo z $u_{\mathcal{B}}$ označili stolpec v $\mathbb{F}^n$, ki pripada vektorju u glede na bazo $\mathcal{B}$.

Zgled 4.4. *Naj bo* $D : \mathbb{R}_3[x] \to \mathbb{R}_2[x]$ *linearna preslikava s predpisom* $Dp = p'$. *Kako lahko izračunamo* $D(1 + 2x + x^2)$*? V tem primeru je očitno, da je to kar*

$$D(1 + 2x + x^2) = (1 + 2x + x^2)' = 2x + 2.$$

Lahko pa to naredimo še na drug način. Izberemo standardno bazo $\mathcal{B} = \{1, x, x^2, x^3\}$ *prostora* $\mathbb{R}_3[x]$ *in standardno bazo* $\mathcal{B} = \{1, x, x^2\}$ *prostora* $\mathbb{R}_2[x]$. *Tako dobimo matriko*

$$D_{\mathcal{CB}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

Sedaj pa nam preostane le še, da izračunamo

$$(Dp)_{\mathcal{C}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \\ 0 \end{bmatrix},$$

kar ustreza $Dp = 2 + 2x$. *Pri tem zgledu smo pokazali, da se rezultat, ki ga dobimo z uporabo prejšnjega izreka ujema z dejanskim rezultatom.*

4.1 Množenje matrik

Definicija 4.2. Naj bo $A \in \mathbb{F}^{m\times n}$ in $B \in \mathbb{F}^{n\times p}$. Definiramo matriko $AB \in \mathbb{F}^{m\times p}$ na naslednji način: (i,j)-ti element matrike AB je skalarni produkt i-te vrstice A in j-tega stolpca matrike B.

Zgled 4.5 (Poseben primer)**.** *Za $A \in \mathbb{F}^{m\times n}$ in $B \in \mathbb{F}^{n\times 1}$ se AB ujema z definicijo AB-ja v primeru, ko množimo matriko z vektorjem.*

Zgled 4.6.

$$\begin{bmatrix} 2 & 1 & 3 \\ 4 & 0 & -2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 0 \\ 3 & 1 & 0 \\ 1 & 0 & 3 \end{bmatrix} = \begin{bmatrix} 8 & 5 & 9 \\ 2 & 8 & -6 \end{bmatrix}$$

Produkt matrike $A \in \mathbb{F}^{m\times n}$, $A = [a_{ij}]$ in $B \in \mathbb{F}^{n\times p}$ je matrika $AB \in \mathbb{F}^{m\times p}$, $AB = [c_{ij}]$, kjer je $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$.

Izrek 4.7.

Naj bosta $A : U \to V$ in $B : W \to U$ linearni preslikavi. Naj bo $\mathcal{B}$ baza U, $\mathcal{C}$ baza V in $\mathcal{D}$ baza W. Za linearno preslikavo $A \circ B : W \to V$ velja

$$(A \circ B)_{\mathcal{CD}} = A_{\mathcal{CB}} \cdot B_{\mathcal{BD}}.$$

Dokaz. Vzemimo, da je množica $\mathcal{B} = \{u_1, u_2, \ldots, u_n\}$ baza U, $\mathcal{C} = \{v_1, v_2, \ldots, v_m\}$ baza V in $\mathcal{D} = \{w_1, w_2, \ldots, w_p\}$ baza W. Naj bosta matriki $A_{\mathcal{CB}} = [a_{ij}]$ in $B_{\mathcal{BD}} = [b_{ij}]$. Če sedaj na dolgo razpišemo $(A \circ B)w_j$, dobimo, da je $j-$ti stolpec matrike $(A \circ B)_{\mathcal{CD}}$:

$$\begin{bmatrix} b_{1j}a_{11} + b_{2j}a_{12} + \cdots + b_{nj}a_{1n} \\ \vdots \\ b_{1j}a_{m1} + b_{2j}a_{12} + \cdots + b_{nj}a_{1n} \end{bmatrix} = j\text{-ti stolpec } A_{\mathcal{CB}} \cdot B_{\mathcal{BD}}$$ □

Posledica 4.8. *Za operacije z matrikami veljajo naslednje trditve:*

1. $A(B \cdot C) = (A \cdot B)C$ *za* $\forall A \in \mathbb{F}^{m\times n}, B \in \mathbb{F}^{n\times p}, C \in \mathbb{F}^{p\times r}$
2. $A(B + C) = AB + AC$ *za* $\forall A \in \mathbb{F}^{m\times n}, B, C \in \mathbb{F}^{n\times p}$
3. $(B + C)A = BA + CA$ *za* $\forall B, C \in \mathbb{F}^{m\times n}, A \in \mathbb{F}^{n\times p}$
4. $(\alpha A) \cdot B = A \cdot (\alpha B) = \alpha(AB)$ *za* $\forall \alpha \in \mathbb{F}, A \in \mathbb{F}^{m\times n}, B \in \mathbb{F}^{n\times p}$

Dokaz. Vse to sledi iz analognih lastnosti za linearne preslikave. □

4.2 Dualni prostor in dualna preslikava

Definicija 4.3. Naj bo V vektorski prostor nad poljem $\mathbb{F}$. Linearen funkcional je linearna preslikava $\phi : V \to \mathbb{F}$ (sliko elementa v pišemo kar kot $\phi(v)$).

Opomba. Polje $\mathbb{F}$ je tudi vektorski prostor nad $\mathbb{F}$: $\mathbb{F} = \mathbb{F}^1$.

Zgled 4.7. *Definiramo preslikavo* $\phi : \mathbb{R}_n[x] \to \mathbb{R}$ *kot* $\phi(p) = \int_0^1 p(x)dx$. *Najprej moramo dokazati, da je ta preslikava zares linearna:*

- $\phi(p+q) = \int_0^1 (p(x)+q(x))dx = \int_0^1 p(x)dx + \int_0^1 q(x)dx = \phi(p) + \phi(q)$
- $\phi(\alpha p) = \int_0^1 \alpha p(x)dx = \alpha \int_0^1 p(x)dx = \alpha\phi(p)$

Sedaj ko smo to dokazali, lahko izračunamo matriko za ϕ. *Baza* $\mathbb{R}_n[x]$ *je* $\mathcal{B} = \{1, x, \ldots, x^n\}$, *baza* $\mathbb{R}$ *pa* $\mathcal{C} = 1$. *Sedaj velja*

$$\phi(x^k) = \int_0^1 x^k dx = \frac{1}{k+1} = \frac{1}{k+1} \cdot 1$$

in matrika za ϕ *je* $\phi_{\mathcal{CB}} = \begin{bmatrix} 1 & \frac{1}{2} & \cdots & \frac{1}{n+1} \end{bmatrix}$.

Vzemimo množico linearnih funckionalov $\phi : V \to \mathbb{F}$, t.j. $Hom_{\mathbb{F}}(V, \mathbb{F})$. To množico krajše označimo z V^* in to je dualni prostor vektorskega prostora V. Omejimo se na primer $\dim V < \infty$.

Izrek 4.9.

Naj bo $\{v_1, v_2, \ldots, v_n\}$ *baza prostora* V. *Definiramo linearne funkcionale* $\phi_1, \phi_2, \ldots, \phi_n \in V^*$ *na naslednji način:*

$$\phi_i(v_j) = \begin{cases} 1: & i = j \\ 0: & \textit{sicer} \end{cases}$$

Potem je $\{\phi_1, \phi_2, \ldots, \phi_n\}$ *baza* V^*. *Tej bazi pravimo dualna baza baze* $\{v_1, v_1, \ldots, v_n\}$.

Dokaz. Dokazati moramo linearno neodvisnost in ogrodje.

1. Recimo, da je $\alpha_1\phi_1 + \alpha_2\phi_2 + \cdots + \alpha_n\phi_n = 0;\ \alpha_i \in \mathbb{F}$. Vzemimo vektor v_i:

$$(\alpha_1\phi_1 + \alpha_2\phi_2 + \cdots + \alpha_n\phi_n)(v_i) = (0)(v_i)$$
$$\alpha_1\phi_1(v_i) + \alpha_2\phi_2(v_i) + \cdots + \alpha_n\phi_n(v_i) = 0$$

   in od tod sledi, da je $\alpha_i = 0$ za $\forall i \in 1, 2, \ldots, n$.

2. Naj bo $\phi \in V^*$ poljuben. Trdimo, da velja

$$\phi = \phi(v_1)\phi_1 + \phi(v_2)\phi_2 + \cdots + \phi(v_n)\phi_n.$$

   To je res, saj se leva in desna stran ujemata v poljubnem vektorju $v_i,\ i = 1, 2, \ldots, n$. □

Posledica 4.10. $\dim V^* = \dim V$, *torej je* $V^* \cong V$.

Definicija 4.4. Naj bo V vektorski prostor in X neprazna množica v V. Definirajmo množico

$$X^0 = \{\phi \in V^* :\ \phi\big|_X = 0\}.$$

Množici X^0 pravimo anihilator množice X.

Trditev 4.11. *Če je* $X \subseteq V$, *potem je* X^0 *vektorski podprostor v* V^*.

Dokaz. Vzemimo $\phi, \psi \in X^0$ in $\alpha, \beta \in \mathbb{F}$. Za poljuben $x \in X$ velja $(\alpha\phi+\beta\psi)(x) = \alpha\phi(x)+\beta\phi(x) = 0$, torej $\alpha\phi + \beta\psi \in X^0$. □

Trditev 4.12. *Recimo* $V = U \oplus W$. *Potem je* $U^0 \cong W^*$ *in* $W^0 \cong U^*$.

Dokaz. Definirajmo $\Phi : U^0 \to W^*$, $\Phi(\phi) = \phi\big|_W$. Dokazati moramo, da je Φ izomorfizem, torej rabimo preveriti linearnost in bijektivnost preslikave Φ. Aditivnost sledi iz tega, da za za $\phi, \psi \in U^0$ velja

$$\Phi(\phi + \psi) = (\phi + \psi)\big|_W = \phi\big|_W + \psi\big|_W = \Phi(\phi) + \Phi(\psi).$$

Podobno dobimo homogenost, saj za $\phi \in U^0,\ \alpha \in \mathbb{F}$ velja

$$\Phi(\alpha\phi) = (\alpha\phi)\big|_W = \alpha\phi\big|_W = \alpha\Phi(\phi).$$

Sedaj naj bo $\phi \in \ker \Phi$. Potem je $\Phi(\phi) = 0$ oziroma $\phi\big|_W = 0$. Vemo pa že, da je $\phi\big|_U = 0$. Ker se vsak $v \in V$ da zapisati kot $v = u + w$, kjer je $u \in U$ in $w \in W$, sledi

$$\phi(v) = \phi(u + w) = \phi(u) + \phi(w) = 0 + 0 = 0.$$

ϕ je torej ničelni funkcional in $\ker \Phi = \{0\}$, s čimer smo dobili injektivnost. Preostane nam torej le še surjektivnost Φ: izberemo $\psi \in W^*$, $\psi : W \to \mathbb{F}$. Iščemo $\phi \in U^0$, da je $\Phi(\phi) = \psi$. Vsak $v \in V$ se da enolično zapisati kot $v = u + w$, kjer je $u \in U$ in $w \in W$. Ker velja

$$\phi(v) = \phi(u) + \phi(w) = 0 + \phi(w) = \psi(w),$$

zato definiramo $\phi(u + w) = \psi(w)$ in ta ϕ zadošča pogojem. □

Naj bo $A : U \to V$ linearna preslikava. Imamo preslikavo $A^* : V^* \to U^*$, dano s $A^*(\phi) = \phi A$. Potem je A^* dualna preslikava preslikave A.

Trditev 4.13. *A^* je linearna preslikava.*

Izrek 4.14.

Naj bo $A : U \to V$ linearna. Potem velja $\ker A^* = (\operatorname{im} A)^0$ *in* $\operatorname{rang} A^* = \operatorname{rang} A$.

Dokaz. Dokažimo posebej oba dela trditve.

1. Naj bo $\phi \in \ker A^*$. Potem velja

$$A^*(\phi) = 0 \iff \phi A = 0 \iff \phi(Au) = 0,\ \forall u \in U \iff \phi\big|_{\operatorname{im} A} = 0 \iff \phi \in (\operatorname{im} A)^0$$

2. Vemo, da je $\operatorname{im} A \leq V$. Obstaja podprostor $W \leq V$, da $V = W \oplus \operatorname{im} A$. Po prejšnji trditvi je $W^* \cong (\operatorname{im} A)^0 = \ker A^*$. Od tod sledi, da velja

$$\dim \ker A^* = \dim W^* = \dim W = \dim V - \dim \operatorname{im} A.$$

   Po drugi strani pa je $A^* : V^* \to U^*$ linearna, zato je $\dim \ker A^* + \dim \operatorname{im} A^* = \dim V^*$. Ko ti dve enačbi združimo, dobimo $\dim \operatorname{im} A^* = \dim \operatorname{im} A$. □

Denimo, da imamo preslikavo $A : U \to V$ in njeno dualno preslikavo $A^* : V^* \to U^*$ (to sta dualni bazi prostorov U^*, V^*). Naj bo množica $\mathcal{B} = \{u_1, u_2, \ldots, u_n\}$ baza U, $\mathcal{C} = \{v_1, v_2, \ldots, v_m\}$ baza V, $\mathcal{B}^* = \{\phi_1, \phi_2, \ldots, \phi_n\}$ baza U^* in $\mathcal{C}^* = \{\psi_1, \psi_2, \ldots, \psi_n\}$ baza V^*. V kakšni zvezi sta matriki $A_{\mathcal{C}\mathcal{B}} = [a_{ij}]$ in $A^*_{\mathcal{B}^*\mathcal{C}^*} = [b_{ij}]$? Oglejmo si najprej

$$\begin{aligned}(A^*\psi_j)u_i &= (b_{1j}\phi_1 + b_{2j}\phi_2 + \cdots + b_{nj}\phi_n)u_i \\ &= b_{1j}\phi_1(u_i) + b_{2j}\phi_2(u_i) + \cdots + b_{nj}\phi_n(u_i) = b_{ij}\end{aligned}$$

Po drugi strani pa je ta isti izraz enak

$$\begin{aligned}(A^*\psi_j)u_i &= \psi_j(Au_i)\\ &= \psi_j(a_{1i}v_1 + a_{2i}v_2 + \cdots + a_{mi}v_m)\\ &= a_{1i}\psi_j(v_1) + a_{2i}\psi_j(v_2) + \cdots + a_{mi}\psi_j(v_m) = a_{ji}\end{aligned}$$

Torej za vsak par (i,j) velja $b_{ij} = a_{ji}$.

Definicija 4.5. Naj bo $A \in \mathbb{F}^{m\times n}$. Transponiranka matrike A je matrika $A^\top \in \mathbb{F}^{n\times m}$, katere (i,j)- ti element je (j,i)- ti element matrike A.

Zgled 4.8.

$$A = \begin{bmatrix}2 & 1 & 3\\ 0 & -1 & 4\end{bmatrix} \qquad A^\top = \begin{bmatrix}2 & 0\\ 1 & -1\\ 3 & 4\end{bmatrix}$$

Sedaj pa smo že dokazali naslednji izrek:

Izrek 4.15.

Naj preslikavi $A : U \to V$ v bazah $\mathcal{B},\mathcal{C}$ prostorov U,V pripada matrika $A_{\mathcal{C}\mathcal{B}}$. Potem dualni preslikavi $A^* : V^* \to U^*$ v dualnih bazah $\mathcal{B}^*,\mathcal{C}^*$ prostorov U^*,V^* pripada matrika $A^*_{\mathcal{B}^*\mathcal{C}^*} = (A_{\mathcal{C}\mathcal{B}})^\top$.

Trditev 4.16. *Za transponiranke veljajo naslednje točke:*

1. $(A^\top)^\top = A,\ \forall A \in \mathbb{F}^{m\times n}$
2. $(A+B)^\top = A^\top + B^\top,\ \forall A,B \in \mathbb{F}^{m\times n}$
3. $(\alpha A)^\top = \alpha_i A^\top,\ \forall A \in \mathbb{F}^{m\times n}, \alpha \in \mathbb{F}$
4. $(AB)^\top = B^\top A^\top,\ \forall A \in \mathbb{F}^{m\times n}, B \in \mathbb{F}^{n\times p}$

4.3 Rang matrike

Naj bo $A \in \mathbb{F}^{m\times n}$ matrika in $A : \mathbb{F}^n \to \mathbb{F}^m$ njena ustrezna preslikava. Potem definiramo $\mathrm{rang}A$ matrike kot rang linearne preslikave $A : \mathbb{F}^n \to \mathbb{F}^m$. Po drugi strani pa

Trditev 4.17. *Naj bo $A : U \to V$ linearna preslikava, $\mathcal{B}$ baza U, $\mathcal{C}$ baza V in A-ju priredimo matriko $A_{\mathcal{C}\mathcal{B}}$. Potem je* $\mathrm{rang}A_{\mathcal{C}\mathcal{B}} = \mathrm{rang}A$.

Dokaz. Ponovno trditev hitro sledi iz komutativnega diagrama. Sicer pa velja

$$\Psi_{\mathcal{C}}(Au) = A_{\mathcal{C}\mathcal{B}}(\Psi_B u) \in \mathrm{im}\, A_{\mathcal{C}\mathcal{B}} \implies \Psi_{\mathcal{C}}(\mathrm{im}\, A) = \mathrm{im}\, A_{\mathcal{C}\mathcal{B}}.$$

in če je $\{x_1,\ldots,x_k\}$ baza $\mathrm{im}\, A$, potem je $\{\Psi_{\mathcal{C}}x_1,\ldots,\Psi_{\mathcal{C}}x_k\}$ baza $\Psi_{\mathcal{C}}(\mathrm{im}\, A)$. Od tod pa sledi

$$\mathrm{rang}A_{\mathcal{C}\mathcal{B}} = \dim \mathrm{im}\, A_{\mathcal{C}\mathcal{B}} = \dim \Psi_{\mathcal{C}}(\mathrm{im}\, A) = \dim \mathrm{im}\, A = \mathrm{rang}A. \qquad \square$$

Izpeljali bomo algoritem za računanje ranga matrike $A \in \mathbb{F}^{m\times n}$.

Definicija 4.6. Vrstični rang matrike A $\mathrm{rang}_v A$ je maksimalno število linearno neodvisnih vrstic matrike A. Stolpični rang matrike A $\mathrm{rang}_s(A)$ pa je maksimalno število linearno neodvisnih stolpcev matrike A.

Izrek 4.18.

Za poljubno matriko $A \in \mathbb{F}^{m\times n}$ *je* $\text{rang}_v(A) = \text{rang}_s(A) = \text{rang}A$.

Dokaz. Najprej bomo dokazali $\text{rang}_s A = \text{rang}A$. Z $A^{(i)} = Ae_i,\ i = 1, \ldots, n$ označimo i-ti stolpec matrike A. Vzemimo sedaj poljuben $x \in \text{im}\, A$, torej je $x = Ay$ za nek $y \in \mathbb{F}^n$. Ker lahko y zapišemo kot

$$\begin{aligned} y = \alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_n e_n &\implies x = \alpha_1 Ae_1 + \alpha_2 Ae_2 + \cdots + \alpha_n Ae_n \\ &\implies x = \alpha_1 A^{(1)} + \alpha_2 A^{(2)} + \cdots + \alpha_n A^{(n)}, \end{aligned}$$

mora veljati

$$\text{rang}A = \dim \text{im}\, A = \dim Lin\, \{A^{(1)}, A^{(2)}, \ldots, A^{(n)}\} = \text{rang}_s A.$$

Sedaj pa dokažimo še $\text{rang}_v A = \text{rang}A$. Vemo, da je $A : \mathbb{F}^n \to \mathbb{F}^m$ linearna preslikava in $A^* : (\mathbb{F}^m)^* \to (\mathbb{F}^n)^*$ njena dualna preslikava. Od tod sledi

$$\text{rang}A = \text{rang}A^* = \text{rang}A^\top = \text{rang}_s A^\top = \text{rang}_v A. \qquad \square$$

Naslednje transformacije matrike A ne spremenijo njenega ranga:

1. menjava stolpcev/vrstic,
2. množenje stolpca/vrstice z neničelnim skalarjem in
3. en stolpec/vrstico prištejemo k nekemu drugemu stolpcu/vrstici.

S temi transformacijami lahko vsako matriko spravimo v posebno obliko (row echelon form), od koder pa lahko izračunamo njen rang.

Zgled 4.9.

$$A = \begin{bmatrix} 1 & 6 & 7 & 12 \\ 2 & 5 & 8 & 11 \\ 3 & 4 & 9 & 10 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & \frac{13}{7} & \frac{6}{7} \\ 0 & 1 & \frac{6}{7} & \frac{13}{7} \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Rang matrike A *je* 2.

4.4 Sistemi linearnih enačb

Obravnavali bomo sisteme m enačb z n neznankami nad poljem $\mathbb{F}$. Naj bodo neznanke $x_1, x_2, \ldots, x_n$ in enačbe

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

Sestavimo matriko in vektorja

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix} \qquad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \qquad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

Sedaj lahko sistem zapišemo v matrični obliki $Ax = b$.

Zgled 4.10 (Poseben primer)**.** *Naj bo $b = 0$ oziroma $Ax = 0$. Temu pravimo tudi homogen sistem. Množica rešitev tega sistema je* $\ker A$*. Vemo že, da vedno velja* $0 \in \ker A$ *(trivialna rešitev). Sistem $Ax = 0$ pa ima tudi netrivilne rešitve natanko tedaj, ko je* $\ker A \neq 0$*. Recimo, da ima* $\ker A$ *bazo* $\{v_1, v_2, \ldots, v_k\}$*, kjer je* $k = n - \text{rang}A$*.* ***Torej ima*** $Ax = 0$ ***netrivialne rešitve natanko tedaj, ko je*** $\textbf{rang}A$ ***manjši od števila neznank.*** *Poljubna rešitev sistema $Ax = 0$ je oblike*

$$x = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k,$$

kjer so $\alpha_i \in \mathbb{F}$ poljubni. Temu pravimo k-parametrična rešitev.

Sedaj si oglejmo splošen primer $Ax = b$.

Izrek 4.19.

Če je $\tilde{x}$ neka rešitev sistema $Ax = b$, potem je množica vseh rešitev tega sistema enaka

$$\tilde{x} + \ker A = \tilde{x} + y : \ y \in \ker A.$$

Dokaz. Z R označimo množico rešitev sistema $Ax = b$. Predpostavimo, da je $\tilde{x} \in R$ in $A\tilde{x} = b$. Najprej rabimo dokazati, da je $\tilde{x} + \ker A \subseteq R$. Vzemimo $\tilde{x} + y$, $y \in \ker A$. Potem je

$$A(\tilde{x} + y) = A\tilde{x} + Ay = b + 0 = b \implies \tilde{x} + y \in R.$$

Sedaj rabimo dokazati še $R \subseteq \tilde{x} + \ker A$. Vzemimo $x \in R$, torej $Ax = b$. Sedaj velja

$$Ax - A\tilde{x} = 0 \implies x - \tilde{x} \in \ker A \implies x = \tilde{x} + \ker A \qquad \square$$

Kdaj je torej sistem $Ax = b$ rešljiv in kako v praksi poiščemo vse rešitve? Najprej napravimo razširjeno matriko sistema $\tilde{A} = \left[A\middle|b\right]$. Naslednje transformacije na $\tilde{A}$ ne spremenijo množice rešitev sistema:

1. menjava vrstic,
2. menjava stolpcev (POZOR: spremeni se vrstni red neznank),
3. vrstico lahko pomnožimo z neničelnim številom in
4. vrstici lahko prištejemo neko drugo vrstico.

S podobnim algoritmom kot pri iskanju ranga lahko transformiramo tudi matriko $\left[A\middle|b\right]$ v enako obliko, kot smo naredili v prejšnjem poglavju. Temu postopku rečemo Gaussova eliminacija. Matrika takšne oblike je rešljiva natanko tedaj, ko je v tistih vrsticah, kjer je matrika A ničelna, ničeln tudi stolpec b. Če je ta pogoj izpolnjen in je $r = \text{rang}A$, lahko spremenljivke $x_1, \ldots, x_r$ izrazimo s poljubnimi parametri $x_{r+1}, \ldots, x_n$ (teh je ravno $\dim \ker A$).

Izrek 4.20 (Kronecker-Capellijev izrek**).**

Sistem $Ax = b$ rešljiv natanko tedaj, ko je $\text{rang}\tilde{A} = \text{rang}A$.

Povzetek: $Ax = b$, $\tilde{A} = \left[A\middle|b\right]$

1. Če je $\text{rang}\tilde{A} \neq \text{rang}A$, sistem nima rešitev.
2. Če je $\text{rang}\tilde{A} = \text{rang}A$, sistem ima rešitve:
   - $\text{rang}\tilde{A} = \text{rang}A = n$, sistem ima natanko eno rešitev
   - $\text{rang}\tilde{A} = \text{rang}A < n$, sistem ima $(n - \text{rang}A)$-parametrično rešitev sistema

4.5 Endomorfizmi končnorazsežnih vektorskih prostorov in kvadratne matrike

Naj bo V končnorazsežen vektorski prostor nad $\mathbb{F}$ in $\dim V = n$. Spoznali smo že množico $End_{\mathbb{F}}$ (t.j. množica vseh linearnih preslikav $V \to V$) in dokazali, da je $End_{\mathbb{F}}(V)$ algebra nad $\mathbb{F}$. To pomeni, da je $End_{\mathbb{F}}(V)$:

- vektorski prostor,
- kolobar (množenje s kompozitumom)
- $\alpha(AB) = (\alpha A)B = A(\alpha B),\ \forall A, B \in End_{\mathbb{F}}(V), \alpha \in \mathbb{F}$

Izberemo bazo $\mathcal{B}$ prostora V; endomorfizmu $A : V \to V$ priredimo matriko $A_{\mathcal{BB}} \in \mathbb{F}^{n\times n}$ (kvadratna matrika). Imamo preslikavo $\Phi_{\mathcal{BB}} : End_{\mathbb{F}}(V) \to \mathbb{F}^{n\times n}$ s predpisom $\Phi_{\mathcal{BB}}(A) = A_{\mathcal{BB}}$. Pokazali smo že, da je $\Phi_{\mathcal{BB}}$ izomorfizem vektorskih prostorov. Na $\mathbb{F}^{n\times n}$ imamo poleg seštevanja in množenja s skalarji tudi operacijo množenja (= produkt matrik). S tem $\mathbb{F}^{n\times n}$ postane algebra nad $\mathbb{F}$.

Definicija 4.7. Naj bosta X, Y algebri nad $\mathbb{F}$. Homomorfizem algeber je preslikava $f : X \to Y$, za katero velja

1. f je linearna preslikava
2. f je homomorfizem kolobarjev

Izrek 4.21.

$\Phi_{\mathcal{BB}} : End_{\mathbb{F}}(V) \to \mathbb{F}^{n\times n}$ je izomorfizem algeber.

Dokaz. Vemo že, da je $\Phi_{\mathcal{BB}}$ izomorfizem vektorskih prostorov. Vzemimo $A, B \in End_{\mathbb{F}}(V)$: po izreku 4.7 velja

$$\Phi_{\mathcal{BB}}(A \cdot B) = (AB)_{\mathcal{BB}} = A_{\mathcal{BB}}B_{\mathcal{BB}} = \Phi_{\mathcal{BB}}(A)\Phi_{\mathcal{BB}}(B) \qquad \square$$

$End_{\mathbb{F}}(V)$ ima nevtralen element za množenje: preslikavo $id : V \to V$. Identična prelikava se preslika v $\Phi_{\mathcal{BB}}(id) = id_{\mathcal{BB}}$, t.j. „identična matrika“

$$id_{\mathcal{BB}} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix} = I.$$

Očitno je $id \circ A = A \circ id = A$. Od tod sledi $\Phi_{\mathcal{BB}}(id \cdot A) = \Phi_{\mathcal{BB}}(A \cdot id) = \Phi_{\mathcal{BB}}(A)$ in posledično $\Phi_{\mathcal{BB}}(id)\Phi_{\mathcal{BB}}(A) = \Phi_{\mathcal{BB}}(A)\Phi_{\mathcal{BB}}(id) = \Phi_{\mathcal{BB}}(A)$. Sedaj pa je $I \cdot A_{\mathcal{BB}} = A_{\mathcal{BB}} \cdot I = A_{\mathcal{BB}}$ oziroma za vsako matriko $A \in \mathbb{F}^{n\times n}$ velja $A \cdot I = I \cdot A = A$. Torej je I enota za množenje v $\mathbb{F}^{n\times n}$.

Definicija 4.8. Bijektivnim endomorfizmom vektorskega prostora V pravimo avtomorfizmi vektorskega prostora V. Definiramo

$$Aut_{\mathbb{F}} = \{ \text{ vse bijektivne preslikave } A : V \to V \ \}.$$

Očitno velja $id \in Aut_{\mathbb{F}}(V)$. Od tod pa sledi, da $Aut_{\mathbb{F}}$ ni vektorski prostor, saj nimamo niti aditivnosti niti homogenosti (res, tako $(id) + (-id)$ kot $0 \cdot id$ sta ničelni preslikavi, torej nista bijektivni in zato nista elementa $Aut_{\mathbb{F}}(V)$). Imamo pa operacijo produkta na $Aut_{\mathbb{F}}(V)$, saj je za $A, B \in Aut_{\mathbb{F}}(V)$ tudi $A \cdot B$ bijektivna preslikava $V \to V$.

Trditev 4.22. *$Aut_{\mathbb{F}}(V)$ je za operacijo $\cdot$ grupa.*

Dokaz. Očitno imamo asociativnost in enoto $id : V \to V$. Ker je poljubna $A \in Aut_{\mathbb{F}}(V)$ bijektivna, obstaja $A^{-1} : V \to V$, ki je tudi linearna, zato velja $A^{-1} \in Aut_{\mathbb{F}}(V)$. □

Trditev 4.23. *Naj bo $A : V \to V$ endomorfizem prostora[2] V. Naslednje trditve so ekvivalentne:*

1. *$A \in Aut_{\mathbb{F}}(V)$ (A je bijektivna),*
2. *A je surjektivna,*
3. *A je injektivna in*
4. *$\text{rang}A = n$*

Dokaz. Ekvivalenco teh izjav bomo dokazali s štirimi zaporednimi implikacijami.

- $(1 \Rightarrow 2)$ To je očitno.
- $(2 \Rightarrow 3)$ Predpostavimo, da je A surjektivna in potem je $\text{im}\, A = V$. Sedaj iz zveze $\dim \ker A + \dim \text{im}\, A = \dim V$ sledi $\dim \ker A = 0$ in A je injektivna.
- $(3 \Rightarrow 4)$ Ta trditev sledi iz iste zveze kot prej. Če je A injektivna, je $\dim \ker A = 0$ in $\dim \text{im}\, A = \text{rang}A = 0$.
- $(4 \Rightarrow 1)$ Ponovno uporabimo isto zvezo. □

Kako lahko $Aut_{\mathbb{F}}(V)$ povežemo z $n \times n$ matrikami? Če je $A \in Aut_{\mathbb{F}}(V)$, potem obstaja $B \in Aut_{\mathbb{F}}(V)$, da je $AB = BA = id$.

Definicija 4.9. Matrika $A \in \mathbb{F}^{n \times n}$ je obrnljiva, če obstaja $B \in \mathbb{F}^{n \times n}$, da je $A \cdot B = B \cdot A = I$. Če taka B obstaja, je enolično določena. Matriki B pravimo inverz matrike; $B = A^{-1}$.

Matrika

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{C}^{2 \times 2}$$

je obrnljiva natanko tedaj, ko je $ad - bc \neq 0$. V tem primeru je

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Opomba. Če za matriki $A, B \in \mathbb{F}^{n \times n}$ velja $AB = I$, potem je tudi $BA = I$. To sledi iz tega, da gledamo A in B kot linearni preslikavi $\mathbb{F}^n \to \mathbb{F}^n$. Ker je $AB = I$, je A surjektivna, od tod pa sledi, da je bijekcija in ima inverz $AC = CA = I$. Od tod pa sledi $B = C$.

Matrika A je obrnljiva natanko tedaj, ko je $\text{rang}A = n$ (n = velikost matrike). Inverz matrike A, če obstaja, lahko poiščemo s pomočjo Gaussove eliminacije.

4.6 Prehod med bazami

Recimo, da imamo linearno preslikavo $A : U \to V$ in U, V končnorazsežna prostora. Za U izberemo bazo $\mathcal{B}$, za V izberemo bazo $\mathcal{C}$ in dobimo matriko $A_{\mathcal{CB}}$. Recimo, da za U izberemo drugo bazo $\mathcal{B}'$ in za V drugo bazo $\mathcal{C}'$. S tem dobimo matriko $A_{\mathcal{C}'\mathcal{B}'}$. V kakšni zvezi sta $A_{\mathcal{CB}}$ in $A_{\mathcal{C}'\mathcal{B}'}$?

Predpriprava: vzemimo preslikavo $id : V \to V$. Izberimo bazo $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ in bazo $\mathcal{C} =$

[2]Pozor: tu je ključno, da velja $\dim V < \infty$

$\{w_1, w_2, \ldots, w_n\}$ prostora V. Kako izgleda matrika $(id)_{\mathcal{CB}}$?

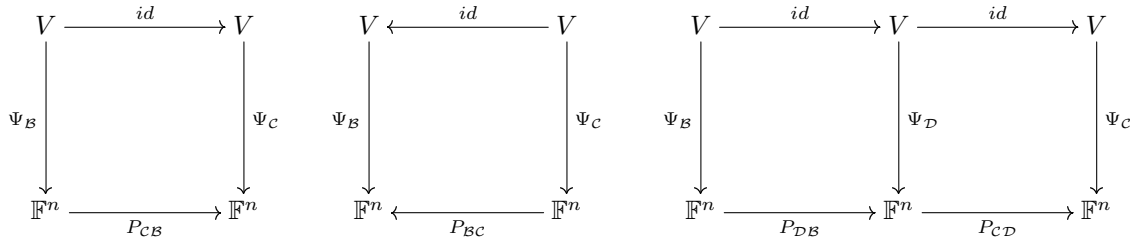
$$\begin{aligned} id(v_1) &= p_{11}w_1 + p_{21}w_2 + \cdots + p_{n1}w_n \\ id(v_2) &= p_{12}w_1 + p_{22}w_2 + \cdots + p_{n2}w_n \\ &\cdots \\ id(v_n) &= p_{1n}w_1 + p_{2n}w_2 + \cdots + p_{nn}w_n \end{aligned}$$

Tako dobimo prehodno matriko iz baze $\mathcal{B}$ v bazo $\mathcal{C}$:

$$(id)_{\mathcal{CB}} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & \vdots & & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{bmatrix} = P_{\mathcal{CB}}$$

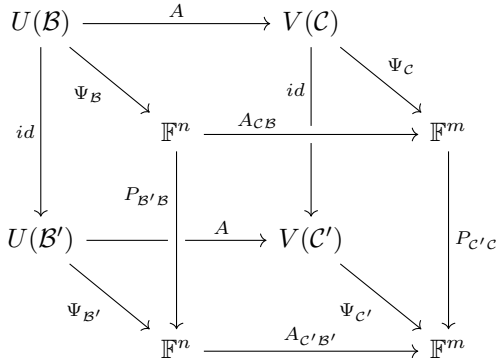
Trditev 4.24. *Naj bodo $\mathcal{B}, \mathcal{C}, \mathcal{D}$ baze vektorskega prostora V in $v \in V$. Potem veljajo naslednje točke:*

- $P_{\mathcal{CB}} v_{\mathcal{B}} = v_{\mathcal{C}}$
- *$P_{\mathcal{CB}}$ je obrnljiva matrika; $P_{\mathcal{CB}}^{-1} = P_{\mathcal{BC}}$*
- $P_{\mathcal{CD}} \cdot P_{\mathcal{DB}} = P_{\mathcal{CB}}$



Dokaz. Vse tri točke sledijo iz diagramov, ki komutirajo. □

Vrnimo se na osnovni problem.



Trditev 4.25. *Naj bo $A : U \to V$ linearna preslikava. Naj bosta $\mathcal{B}, \mathcal{B}'$ bazi prostora U in $\mathcal{C}, \mathcal{C}'$ bazi prostora V. Potem je $A_{\mathcal{CB}} = P_{\mathcal{CC}'} \cdot A_{\mathcal{C}'\mathcal{B}'} \cdot P_{\mathcal{B}'\mathcal{B}}$.*

Dokaz. Vzemimo poljuben $u \in U$. Sedaj velja

$$\begin{aligned} P_{\mathcal{C}\mathcal{C}'} \cdot A_{\mathcal{C}'\mathcal{B}'} \cdot P_{\mathcal{B}'\mathcal{B}} \cdot u_{\mathcal{B}} &= P_{\mathcal{C}\mathcal{C}'} \cdot A_{\mathcal{C}'\mathcal{B}'} \cdot u_{\mathcal{B}'} \\ &= P_{\mathcal{C}\mathcal{C}'}(Au)_{\mathcal{C}'} = (Au)_{\mathcal{C}} \\ &= A_{\mathcal{C}\mathcal{B}} \cdot u_{\mathcal{B}} \quad \forall u \end{aligned}$$

Če izberemo $u_{\mathcal{B}} = (1, 0, \ldots, 0)$, je prvi stolpec $P_{\mathcal{C}\mathcal{C}'} \cdot A_{\mathcal{C}'\mathcal{B}'} \cdot P_{\mathcal{B}'\mathcal{B}}$ enak prvemu stolpcu $A_{\mathcal{C}\mathcal{B}}$ in s podobnim argumentom to dokažemo za vse stolpce. Zato se matriki ujemata. □

Definicija 4.10. Naj bosta $A, B \in \mathbb{F}^{m\times n}$. Pravimo, da sta A in B ekvivalentni, če obstajata obrnljivi matriki $P \in \mathbb{F}^{m\times m}$ in $Q \in \mathbb{F}^{n\times n}$, da velja $B = PAQ$. To označimo $A \sim B$.

Opomba. Če linearni preslikavi priredimo matriko glede na različna para baz, sta ti matriki vedno ekvivalentni oziroma velja $A_{\mathcal{C}'\mathcal{B}'} \sim A_{\mathcal{C}\mathcal{B}}$.

Trditev 4.26. *Relacija $\sim$ je ekvivalenčna relacija na $\mathbb{F}^{m\times n}$.*

Dokaz. Po točkah dokazujemo refleksivnost, simetričnost in tranzitivnost.

1. Ker je $A = I_m A I_n$, je za vsak $A \in \mathbb{F}^{m\times n}$ $A \sim A$.
2. Naj bo $A \sim B$. Potem je $A = PAQ$, kjer sta P, Q obrnljivi. Od tod pa sledi $B = P^{-1}AQ^{-1}$ in torej velja tudi $B \sim A$.
3. Naj bosta $A \sim B$ in $B \sim C$. Potem je $B = PAQ$ in $C = RBS$, kjer so P, Q, R, S obrnljive. Potem je $C = RBS = (RP)A(QS)$ in ker je produkt dveh obrnljivih matrik tudi obrnljiva matrika ($(RP)^{-1} = P^{-1}R^{-1}$), je $A \sim C$. □

Lema 4.27. *Naj bo $A \in \mathbb{F}^{m\times n}$ in $P \in \mathbb{F}^{m\times m}$ ter $Q \in \mathbb{F}^{n\times n}$ obrnljivi matriki.*

- $\text{rang}PA = \text{rang}A$
- $\text{rang}AQ = \text{rang}A$
- *Če je $A \sim B$, potem je* $\text{rang}A = \text{rang}B$.

Dokaz. Dokažimo vsako točko posebej.

1. Matriki P in A gledamo kot linearni preslikavi. Naj bo $\{v_1, v_2, \ldots, v_r\}$ baza $\text{im}\, A$, $r = \text{rang}A$. Dokazati želimo, da je $\{Pv_1, Pv_2, \ldots, Pv_r\}$ baza $\text{im}\, PA$. Dokažimo najprej, da je ta množica vektorjev ogrodje. Vzemimo $x \in PA$. Potem obstaja y, da je

   $$\begin{aligned} x = PAy &= P(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r) \\ &= \alpha_1 Pv_1 + \alpha_2 Pv_2 + \cdots + \alpha_r Pv_r. \end{aligned}$$

   Sedaj pa dokažimo še linearno neodvisnost.

   $$\begin{aligned} \alpha_1 Pv_1 + \alpha_2 Pv_2 + \cdots + \alpha_r Pv_r = 0 &\implies P(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r) = 0 \\ &\implies \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r \in \ker P = \{0\} \\ &\implies \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r = 0 \\ &\implies \alpha_1, \alpha_2, \ldots, \alpha_r = 0 \end{aligned}$$

   in smo dokazali. Podobno velja tudi, da če sta $A \in \mathbb{F}^{m\times n}$ in $B \in \mathbb{F}^{n\times p}$, potem je $\text{rang}(AB) \leq rangB$ in $\text{rang}(AB) \leq \text{rang}A$.
2. Če je Q obrnljiva, je obrnljiva tudi $Q^\top$ in je $(Q^\top)^{-1} = (Q^{-1})^\top$.

   $$\text{rang}(AQ) = \text{rang}(AQ)^\top = \text{rang}(Q^\top A^\top) \overset{(a)}{=} \text{rang}A^\top = \text{rang}A.$$

3. Recimo $A \sim B$, potem obstajata obrnljivi matriki P, Q, tako da je $B = PAQ$. Od tod pa po točkah (a) in (b) sledi $\text{rang}B = \text{rang}A$. □

Lema 4.28. *Recimo, da je $A : U \to V$ linearna preslikava. Potem obstajata bazi $\mathcal{B}, \mathcal{C}$ za U, V, da je*

$$A_{\mathcal{C}\mathcal{B}} = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ & & \end{bmatrix}.$$

Dokaz. Naj bo $\{w_1, w_2, \ldots, w_k\}$ baza $\ker A$. To bazo dopolnimo do baze celotnega vektorskega prostora U, ki je $\mathcal{B} = \{u_1, u_2, \ldots, u_l, w_1, w_2, \ldots, w_k\}$. Trdimo, da je $\{Au_1, Au_2, \ldots, Au_l\}$ baza $\text{im}\, A$. Najprej bomo dokazali, da je ta množica ogrodje: izberemo $v \in \text{im}\, A$, torej obstaja $u \in U$, da je $v = Au$. Potem je

$$\begin{aligned} v = Au &= A(\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_l u_l + \beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_k w_k) \\ &= \alpha_1 Au_1 + \alpha_2 Au_2 + \cdots + \alpha_l Au_l \end{aligned}$$

Sedaj dokažimo še linearno neodvisnost: denimo, da je

$$\alpha_1 Au_1 + \alpha_2 Au_2 + \cdots + \alpha_l Au_l = 0 \implies A(\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_l u_l) = 0,$$

zato ga lahko razvijemo po bazi $\{w_1, w_2, \ldots, w_k\}$:

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_l u_l = \beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_k w_k.$$

Ker so ti vektorji linearno neodvisni, sledi $\alpha_i = 0, \ \forall i$ in $\beta_j = 0, \ \forall j$. Torej so $Au_1, Au_2, \ldots, Au_l$ linearno neodvisni. Sedaj bazo $\text{im}\, A$ dopolnimo do baze celotnega prostora V, ki jo označimo s $\mathcal{C} = \{Au_1, Au_2, \ldots, Au_l, v_1, v_2, \ldots, v_s\}$. Če sedaj poiščemo matriko $A_{\mathcal{C}\mathcal{B}}$, dobimo

$$A_{\mathcal{C}\mathcal{B}} = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ & & \end{bmatrix},$$

kjer je število enic enako rangu preslikave A. □

Izrek 4.29.

$m \times n$ matriki A in B sta ekvivalentni natanko tedaj, ko je $\text{rang}A = \text{rang}B$.

Dokaz. Izjava ($\Rightarrow$) sledi iz prve leme, zato je dovolj, da dokažemo le v smer ($\Leftarrow$). Naj velja predpostavka $\text{rang}A = \text{rang}B$. Matriki A in B gledamo kot linearni preslikavi $\mathbb{F}^n \to \mathbb{F}^m$. Po prejšnji lemi obstajata bazi $\mathcal{B}, \mathcal{B}'$ za $\mathbb{F}^n$ in $\mathcal{C}, \mathcal{C}'$ za $\mathbb{F}^m$, da je

$$A_{\mathcal{C}\mathcal{B}} = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ & & \end{bmatrix} \qquad B_{\mathcal{C}'\mathcal{B}'} = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ & & \end{bmatrix},$$

kjer je število enk enako $\text{rang}A = \text{rang}B$. Torej je

$$A \sim \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ & & \end{bmatrix} \qquad B \sim \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ & & \end{bmatrix}$$

in iz simetričnosti in tranzitivnosti relacije $\sim$ sledi $A \sim B$. □

Definicija 4.11. Naj bosta $A, B \in \mathbb{F}^{n\times n}$. Pravimo, da sta A in B podobni, če obstaja obrnljiva matrika $P \in \mathbb{F}^{n\times n}$, da je $B = P^{-1}AP$.

Opomba. Če je $A : V \to V$ in $\mathcal{B}, \mathcal{B}'$ bazi V, potem sta matriki $A_{\mathcal{B}\mathcal{B}}$ in $A_{\mathcal{B}'\mathcal{B}'}$ podobni. Hkrati pa velja, da če sta $A, B \in \mathbb{F}^{n\times n}$ podobni, sta tudi ekvivalentni.

Trditev 4.30. *Podobnost matrik je ekvivalenčna relacija na $\mathbb{F}^{n\times n}$.*

Opomba. Vsaka matrika je ekvivalentna matriki oblike

$$\begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ & & \end{bmatrix}.$$

Ni pa res, da je vsaka matrika podobna neki takšni matriki. Matrikam oblike

$$\begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}$$

pravimo diagonalne matrike. Izkazalo se bo, da niso vse matrike podobne diagonalnim matrikam.

4.7 Determinante kvadratnih matrik

Naj bosta U, V vektorska prostora nad $\mathbb{F}$. V polju $\mathbb{F}$ naj velja $1+1 \neq 0$ (primer, kjer to ne velja, je $\mathbb{Z}_2$).

Definicija 4.12. Preslikava $F : U^n \to V$ je n-linearna, če so linearne vse preslikave $U \to V$,

$$u \mapsto F(u_1, \ldots, u_{i-1}, u, u_{i+1}, \ldots, u_n)$$

za vsak $i \in \{1, 2, \ldots, n\}$ in vse $u_i \in U$. To pomeni, da je $F(u_1, \ldots, u_{i-1}, \alpha u + \beta\tilde{u}, u_{i+1}, \ldots, u_n) = \alpha F(u_1, \ldots, u_{i-1}, u, u_{i+1}, \ldots, u_n) + \beta F(u_1, \ldots, u_{i-1}, \tilde{u}, u_{i+1}, \ldots, u_n)$.

V algebri 1-linearnim preslikavam pravimo linearne, 2-linearnim preslikavam pa bilinearne preslikave.

Zgled 4.11. *Vzemimo $U, V = \mathbb{R}$ in preslikavo $F : \mathbb{R}^2 \to \mathbb{R}$ s predpisom $F(x, y) = xy$. Sedaj vidimo, da je*

$$\begin{aligned} F(\alpha x + \beta x', y) &= (\alpha x + \beta x')y \\ &= \alpha xy + \beta x'y \\ &= \alpha F(x, y) + \beta F(x', y). \end{aligned}$$

Podobno je $F(x, \alpha y + \beta y')$, torej je ta preslikava F preprost primer bilinearne preslikave.

Zgled 4.12. *Vzemimo vektorska prostora $U = \mathbb{R}^3, V = \mathbb{R}$ in definirajmo preslikavo $F : (\mathbb{R}^3)^2 \to \mathbb{R}$ s predpisom $F(\vec{a}, \vec{b}) = \vec{a} \cdot \vec{b}$. Trivialno je dokazati, da je F bilinearna preslikava.*

Definicija 4.13. Naj bo $F : U^n \to V$ n-linearna. Pravimo, da je F antisimetrična, če velja

$$F(u_1, \ldots, u_i, \ldots, u_j, \ldots, u_n) = -F(u_1, \ldots, u_j, \ldots, u_i, \ldots, u_n)$$

za vse $u_1, \ldots, u_n \in U$ in za vse pare $i, j, i \neq j$.

Zgled 4.13. *Naj bosta vektorska prostora $U, V = \mathbb{R}^3$ in preslikava $F : (\mathbb{R}^3)^2 \to \mathbb{R}^3$ s predpisom $F(\vec{a}, \vec{b}) = \vec{a} \times \vec{b}$. F je antisimetrična bilinearna preslikava.*

Zgled 4.14. *Vzemimo ponovno vektorska prostora $U = \mathbb{R}^3$ in $V = \mathbb{R}$. Potem definiramo preslikavo $F : (\mathbb{R}^3)^3 \to \mathbb{R}$ s predpisom $F(\vec{a}, \vec{b}, \vec{c}) = (\vec{a} \times \vec{b}) \cdot \vec{c}$. Ponovno je očitno, da je F antisimetrična trilinearna preslikava, od koder sledi geometrijska lastnost determinante.*

Trditev 4.31. *Naj bo $F : U^n \to V$ n-linearna antisimetrična preslikava. Naj bodo $u_1, u_2, \ldots, u_n \in U$ in recimo $u_i = u_j$ za neka $i \neq j$. Potem je $F(u_1, u_2, \ldots, u_n) = 0$.*

Dokaz. To sledi direktno iz antisimetričnosti.

$$F(u_1, \ldots, u_i, \ldots, u_i, \ldots, u_n) = -F(u_1, \ldots, u_i, \ldots, u_i, \ldots, u_n) \qquad \square$$

Trditev 4.32. *Naj bo $F : U^n \to V$ n-linearna antisimetrična preslikava. Potem*

$$F(u_1, \ldots, u_i, \ldots, u_j + \alpha u_i, \ldots, u_n) = F(u_1, \ldots, u_i, \ldots, u_j, \ldots, u_n).$$

Dokaz. Trditev ponovno sledi iz antisimetričnosti in prejšnje trditve.

$$\begin{aligned} F(u_1, \ldots, u_i, \ldots, u_j + \alpha u_i, \ldots, u_n) &= F(u_1, \ldots, u_i, \ldots, u_j, \ldots, u_n) \\ &\quad + \alpha F(u_1, \ldots, u_i, \ldots, u_i, \ldots, u_n) \\ &= F(u_1, \ldots, u_i, \ldots, u_j, \ldots, u_n) \end{aligned} \qquad \square$$

Omejili se bomo an primer $U = \mathbb{F}^n$, $V = \mathbb{F}$. Naj bo $F : (\mathbb{F}^n)^n \to \mathbb{F}$ n-linearna antisimetrična preslikava (funkcional). Elementi $(\mathbb{F}^n)^n$ so n-terice stolpcev dolžine n, ki jih lahko identificiramo z matrikami: za $A \in \mathbb{F}^{n \times n}$ je $F(A) = F(A^{(1)}, A^{(2)}, \ldots, A^{(n)})$. Naj bo $A = [a_{ij}]$. Potem je

$$\begin{aligned} F(A) = F(Ae_1, Ae_2, \ldots, Ae_n) &= F(a_{11}e_1 + a_{21}e_2 + \cdots + a_{n1}e_n, \ldots, a_{1n}e_1 + a_{2n}e_2 + \cdots + a_{nn}e_n) \\ &= \sum a_{i_1 1} a_{i_2 2} \ldots a_{i_n n} F(e_{i_1}, e_{i_2}, \ldots, e_{i_n}), \end{aligned}$$

kjer vsota teče o vseh izbirah paroma različnih $i_1, i_2, \ldots i_n$. Pri tem $i_1, i_2, \ldots, i_n$ določajo permutacijo

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}.$$

Vektorje $e_{i_1}, e_{i_2}, \ldots, e_{i_n}$ lahko znotraj $F(e_{i_1}, e_{i_2}, \ldots, e_{i_n})$ premešamo, vsaka zamenjava spremeni predznak. Premešajmo jih do vrstnega reda $e_{i_1}, e_{i_2}, \ldots, e_{i_n}$:

$$\begin{aligned} F(A) &= \sum_{\sigma \in S_n} sgn\ \sigma \cdot a_{\sigma(1)1} \cdot a_{\sigma(2)2} \ldots a_{\sigma(n)n} \cdot F(e_1, e_2, \ldots, e_n) \\ &= \sum_{\sigma \in S_n} sgn\ \sigma \cdot a_{\sigma(1)1} \cdot a_{\sigma(2)2} \ldots a_{\sigma(n)n} \cdot F(I) \end{aligned}$$

Definicija 4.14. Naj bo $A = [a_{ij}]$ matrika v $\mathbb{F}^{n\times n}$. Skalarju

$$\det A = \sum_{\sigma\in S_n} sgn\ \sigma \cdot a_{\sigma(1)1} \cdot a_{\sigma(2)2} \dots a_{\sigma(n)n}$$

pravimo determinanta matrike A.

Opomba. Če je $F : (\mathbb{F}^n)^n \to \mathbb{F}$ antisimetrična n-linearna preslikava in $A \in \mathbb{F}^{n\times n}$, je $F(A) = \det(A)F(I)$
To vsoto lahko zapišemo tudi drugače:

$$\begin{aligned}\det A &= \sum_{\sigma\in S_n} sgn\ \sigma \cdot a_{1\sigma^{-1}(1)} \cdot a_{2\sigma^{-1}(2)} \dots a_{n\sigma^{-1}(n)} \\ &= \sum_{\sigma\in S_n} sgn\ \sigma^{-1} \cdot a_{1\sigma(1)} \cdot a_{2\sigma(2)} \dots a_{n\sigma(n)}{}^{3} \\ &= \sum_{\sigma\in S_n} sgn\ \sigma \cdot a_{1\sigma(1)} \cdot a_{2\sigma(2)} \dots a_{n\sigma(n)}\end{aligned}$$

S tem smo pokazali, da velja $\det A = \det A^\top$. Determinanto matrike $A = [a_{ij}]$ označimo z

$$\det A = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

Determinanta $2x2$ matrike $A = [a_{ij}]$ je $\det A = a_{11}a_{22} - a_{12}a_{21}$, determinanta 3×3 matrike $[a_{ij}]$ pa je

$$\begin{aligned}\det A = {} & a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ & - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33}.\end{aligned}$$

Zgled 4.15. *Vzemimo preslikavo $F : (\mathbb{R}^3)^3 \to \mathbb{R}$ s predpisom $F(\vec{a}, \vec{b}, \vec{c}) = [\vec{a}, \vec{b}, \vec{c}]$. Pokazali smo že, da je F 3-linearna antisimetrična preslikava. Potem iz $F(A) = \det A \cdot F(I)$ sledi*

$$\begin{aligned}F(\vec{a}, \vec{b}, \vec{c}) &= \det A \cdot F((1,0,0),(0,1,0),(0,0,1)) \\ [\vec{a}, \vec{b}, \vec{c}] &= \det A \cdot [(1,0,0),(0,1,0),(0,0,1)] = \det A\end{aligned}$$

Determinanto lahko gledamo kot preslikavo $\det : \mathbb{F}^{n\times n} \to \mathbb{F}$. Oglejmo si nekatere njene lastnosti.

Izrek 4.33.

Preslikava $\det : \mathbb{F}^{n\times n} \to \mathbb{F}$ je n-linearen antisimetričen funkcional.

Dokaz. Naj bo $\det(A) = \det(A^{(1)}, A^{(2)}, \dots, A^{(n)})$, kjer je $A^{(i)}$ i-ti stolpec.

[3] Ko σ preteče cel S_n, tudi σ^{-1} preteče cel S_n.

1. Dokažimo aditivnost na prvem faktorju, enako sledi za ostale.

$$\begin{aligned}\det(B^{(1)}+C^{(1)},A^{(2)},\dots,A^{(n)}) &= \sum_{\sigma\in S_n} sgn\ \sigma\cdot(b_{\sigma(1)1}+c_{\sigma(1)1})\cdot a_{\sigma(2)2}\dots a_{\sigma(n)n}\\ &= \sum_{\sigma\in S_n} sgn\ \sigma\cdot b_{\sigma(1)1}\cdot a_{\sigma(2)2}\dots a_{\sigma(n)n}\\ &+ \sum_{\sigma\in S_n} sgn\ \sigma\cdot c_{\sigma(1)1}\cdot a_{\sigma(2)2}\dots a_{\sigma(n)n}\\ &= \det(B^{(1)},A^{(2)},\dots,A^{(n)})+\det(C^{(1)},A^{(2)},\dots,A^{(n)})\end{aligned}$$

2. Dokažimo homogenost na prvem faktorju, enako sledi za ostale

$$\begin{aligned}\det(\alpha A^{(1)},A^{(2)},\dots,A^{(n)}) &= \sum_{\sigma\in S_n} sgn\ \sigma\cdot(\alpha a_{\sigma(1)1})\cdot a_{\sigma(2)2}\dots a_{\sigma(n)n}\\ &= \alpha\sum_{\sigma\in S_n} sgn\ \sigma\cdot a_{\sigma(1)1}\cdot a_{\sigma(2)2}\dots a_{\sigma(n)n}\\ &= \alpha\det(A^{(1)},A^{(2)},\dots,A^{(n)})\end{aligned}$$

3. Dokažimo antisimetričnost z zamenjavo prvih dveh faktorjev:

$$\begin{aligned}\det(A^{(2)},A^{(1)},\dots,A^{(n)}) &= \sum_{\sigma\in S_n} sgn\ \sigma\cdot a_{\sigma(1)2}\cdot a_{\sigma(2)1}\dots a_{\sigma(n)n}\\ &= \sum_{\sigma'\in S_n} (-sgn\ \sigma')\cdot a_{\sigma'(1)1}\cdot a_{\sigma'(2)2}\dots a_{\sigma'(n)n}\\ &= -\det(A^{(1)},A^{(2)},\dots,A^{(n)})\end{aligned}$$

□

Opomba. Izrek v praksi pove:

- za vse stolpce in vrstice velja

$$\begin{vmatrix} b_{11}+c_{11} & a_{12} & \dots & a_{1n}\\ b_{21}+c_{21} & a_{22} & \dots & a_{2n}\\ \vdots & \vdots & & \vdots\\ b_{n1}+c_{n1} & a_{n2} & \dots & a_{nn}\end{vmatrix} = \begin{vmatrix} b_{11} & a_{12} & \dots & a_{1n}\\ b_{21} & a_{22} & \dots & a_{2n}\\ \vdots & \vdots & & \vdots\\ b_{n1} & a_{n2} & \dots & a_{nn}\end{vmatrix} + \begin{vmatrix} c_{11} & a_{12} & \dots & a_{1n}\\ c_{21} & a_{22} & \dots & a_{2n}\\ \vdots & \vdots & & \vdots\\ c_{n1} & a_{n2} & \dots & a_{nn}\end{vmatrix}$$

- za vse stolpce in vrstice velja

$$\begin{vmatrix} \alpha a_{11} & a_{12} & \dots & a_{1n}\\ \alpha a_{21} & a_{22} & \dots & a_{2n}\\ \vdots & \vdots & & \vdots\\ \alpha a_{n1} & a_{n2} & \dots & a_{nn}\end{vmatrix} = \alpha\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n}\\ a_{21} & a_{22} & \dots & a_{2n}\\ \vdots & \vdots & & \vdots\\ a_{n1} & a_{n2} & \dots & a_{nn}\end{vmatrix}$$

- če v matriki zamenjamo poljubna stolpca (ali vrstici), se spremeni predznak determinante matrike
- če ima matrika dva enaka stolpca ali vrstici, je njena deteminanta ničelna

Izrek 4.34.

Preslikava $\det:\mathbb{F}^{n\times n}\to\mathbb{F}$ *je multiplikativna: za poljubni* $A,B\in\mathbb{F}^{n\times n}$ *je* $\det(AB)=\det A\cdot\det B$.

Dokaz. Definirajmo preslikavo $F : \mathbb{F}^{n\times n} \to \mathbb{F}$ s predpisom

$$F(v_1, v_2, \ldots, v_n) = \det(Av_1, Av_2, \ldots, Av_n).$$

Trdimo, da je F n-linearna antisimetrična preslikava: n-linearnost sledi iz linearnosti A, antisimetričnost pa iz antisimetričnosti det. Potem sledi $F(B) = \det B \cdot F(I)$. Sedaj pa velja

$$\begin{aligned} F(I) = F(e_1, e_2, \ldots, e_n) &= \det(Ae_1, Ae_2, \ldots, Ae_n) \\ &= \det(A^{(1)}, A^{(2)}, \ldots, A^{(n)}) \\ &= \det A \end{aligned}$$

in s tem smo dobili $F(B) = \det A \cdot \det B$. Po drugi strani pa je

$$F(B) = F(B^{(1)}, B^{(2)}, \ldots, B^{(n)}) = \det(AB^{(1)}, AB^{(2)}, \ldots, AB^{(n)}) = \det(AB) \qquad \square$$

Definicija 4.15. Naj bo $A = [a_{ij}]$. Označimo z A_{ij} matriko, ki jo dobimo, če v A odstranimo i-to vrstico in j-ti stolpec. Definirajmo $\tilde{a}_{ij} = (-1)^{i+j} \det A_{ij}$. To je (i, j)-ti kofaktor matrike A.

Zgled 4.16. *Naj bo matrika*

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}.$$

Potem je njen $(2, 3)$-ti kofaktor enak

$$\tilde{a}_{23} = (-1)^{2+3} \det \begin{bmatrix} 1 & 2 \\ 7 & 8 \end{bmatrix} = -(1 \cdot 8 - 2 \cdot 7) = 6$$

Izrek 4.35.

Naj bo $A = [a_{ij}]$. Potem je za vsak i

$$\det A = \sum_{j=1}^{n} a_{ij}\tilde{a}_{ij} = \sum_{i=1}^{n} a_{ij}\tilde{a}_{ij}.$$

Zgled 4.17. *Kako to izgleda v praksi?*

$$\begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \ldots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} = a_{i1}\tilde{a}_{i1} + a_{i2}\tilde{a}_{i2} + \cdots + a_{in}\tilde{a}_{in}$$

To je razvoj determinante po i-ti vrstici. Enako lahko naredimo tudi po stolpcu.

Dokaz. Naj bo $A = [a_{ij}]$ in $A^{(j)}$ j-ti stolpec matrike A. Oglejmo si

$$\begin{aligned}\det(A^{(1)}, A^{(2)}, \ldots, A^{(n-1)}, e_n) &= \sum_{\sigma \in S_n} sgn\ \sigma \cdot a_{\sigma(1)2} \cdot a_{\sigma(2)1} \ldots a_{\sigma(n-1),n-1} \cdot * \\ &= \sum_{\sigma \in S_{n-1}} sgn\ \sigma \cdot a_{\sigma(1)2} \cdot a_{\sigma(2)1} \ldots a_{\sigma(n-1),n-1} \\ &= \det A_{nn} = \tilde{a}_{nn}\end{aligned}$$

Sedaj si oglejmo še:

$$\begin{aligned}\det(A^{(1)}, \ldots, A^{(j-1)}, \overbrace{e_i}^{j}, A^{(j+1)} \ldots, A^{(n)}) &= (-1)^{n-j} \det(A^{(1)}, \ldots, A^{(j-1)}, A^{(j+1)} \ldots, A^{(n)}, e_i) \\ &= (-1)^{n-j}(-1)^{n-i} \det A_{ij} \\ &= (-1)^{2n-j-i} \det A_{ij} \\ &= (-1)^{j+i} \det A_{ij} = \tilde{a}_{ij}\end{aligned}$$

Končno dobimo:

$$\begin{aligned}\det A &= \det(A^{(1)}, \ldots, A^{(j-1)}, A^{(j)}, A^{(j+1)} \ldots, A^{(n)}) \\ &= \det(A^{(1)}, \ldots, A^{(j-1)}, a_{1j}e_1 + a_{2j}e_2 + \cdots + a_{nj}e_n, A^{(j+1)} \ldots, A^{(n)}) \\ &= \sum_{i=1}^{n} a_{ij} \det(A^{(1)}, \ldots, A^{(j-1)}, e_i, A^{(j+1)} \ldots, A^{(n)}) = \sum_{i=1}^{n} a_{ij}\tilde{a}_{ij}\end{aligned}$$ □

Tehnike računanja determinant:

1. Če v matriki zamenjamo dve vrstici (ali stolpca), se novi matriki spremeni predznak determinante.
2. Če nek stolpec (ali vrstico) pomnožimo z neničelnim skalarjem α, je determinanta nove matrike pomnožena z α.
3. Če v matriki nekemu stolpcu (ali vrstici) prištejemo večkratnik nekega drugega stolpca (ali vrstice), se determinanta ne spremeni.

Od tod sledi, da pri računanju determinante lahko kombiniramo razvoj po vrstici (stolpcu) z Gaussovo eliminacijo.

Trditev 4.36. *Naj bo A $n \times n$ matrika, B pa $m \times m$ matrika. Potem je determinanta bločne matrike*

$$\det \begin{bmatrix} A & * \\ 0 & B \end{bmatrix} = \det A \cdot \det B.$$

Dokaz. Naredimo indukcijo po n.

- $n = 1$: potem je $A = [a]$ in z razvojem po prvem stolpcu dobimo

$$\det \begin{bmatrix} a & * \\ 0 & B \end{bmatrix} = a \cdot (-1)^{1+1} \det B = a \det B = \det[a] \cdot \det B = \det A \cdot \det B$$

- $n \to n+1$: z razvojem po prvem stolpcu dobimo

$$\begin{aligned}\det \begin{bmatrix} A & * \\ 0 & B \end{bmatrix} &= a_{11}(-1)^{1+1} \begin{bmatrix} A_{11} & * \\ 0 & B \end{bmatrix} + a_{21}(-1)^{2+1} \begin{bmatrix} A_{21} & * \\ 0 & B \end{bmatrix} + \cdots + a_{n1}(-1)^{n+1} \begin{bmatrix} A_{n1} & * \\ 0 & B \end{bmatrix} \\ &\overset{\text{(I.P.)}}{=} a_{11}(-1)^{1+1} \det A_{11} \cdot \det B + a_{21}(-1)^{2+1} \det A_{21} \cdot \det B + \cdots + \\ &+ a_{n1}(-1)^{n+1} \det A_{n1} \cdot \det B \\ &= \det B \left(a_{11}(-1)^{1+1} \det A_{11} + a_{21}(-1)^{2+1} \det A_{21} + \cdots + a_{n1}(-1)^{n+1} \det A_{n1} \right) \\ &= \det B \cdot \det A \end{aligned}$$

□

Posledica 4.37. *Če je A zgornjetrikotna matrika*

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ & a_{22} & \dots & a_{2n} \\ & & \ddots & \vdots \\ & & & a_{nn} \end{bmatrix},$$

potem je njena determinanta enaka $\det A = a_{11}a_{22}\dots a_{nn}$.

Posledica 4.38. *Če je A diagonalna matrika*

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

potem je njena determinanta enaka $\det A = a_{11}a_{22}\dots a_{nn}$.

4.8 Uporaba determinant

Definicija 4.16. Naj bo $A = [a_{ij}]$ $n \times n$ matrika. Potem matriki

$$\tilde{A} = \begin{bmatrix} \tilde{a}_{11} & \tilde{a}_{12} & \dots & \tilde{a}_{1n} \\ \vdots & \vdots & & \vdots \\ \tilde{a}_{n1} & \tilde{a}_{n2} & \dots & \tilde{a}_{nn} \end{bmatrix}$$

pravimo prirejenka matrike A.

Trditev 4.39. $A \cdot \tilde{A}^\top = \det A \cdot I$

Dokaz. Imamo produkt matrik

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \cdot \begin{bmatrix} \tilde{a}_{11} & \tilde{a}_{21} & \dots & \tilde{a}_{n1} \\ \vdots & \vdots & & \vdots \\ \tilde{a}_{1n} & \tilde{a}_{2n} & \dots & \tilde{a}_{nn} \end{bmatrix}.$$

Oglejmo si (i,j)-ti element matrike $A \cdot \tilde{A}^\top$. Če je $i = j$, potem je to

$$a_{i1}\tilde{a}_{i1} + a_{i2}\tilde{a}_{i2} + \cdots + a_{in}\tilde{a}_{in} = \det A.$$

Če pa je $i \neq j$, potem pa je

$$a_{i1}\tilde{a}_{j1} + a_{i2}\tilde{a}_{j2} + \cdots + a_{in}\tilde{a}_{jn},$$

kar pa razvoj determinante matrike, v katerem sta i-ta in j-ta vrstica enaki $(a_{i1}, a_{i2}, \dots, a_{in})$, taka matrika pa ima seveda ničelno determinanto. Torej je za $i \neq j$ $(i,j)-$ti element matrike $A \cdot \tilde{A}^\top$ enak 0. □

Izrek 4.40.

Naj bo A $n \times n$ matrika. Potem je A obrnljiva natanko tedaj, ko je $\det A \neq 0$.

Dokaz. ($\Rightarrow$) Denimo, da je A obrnljiva. Potem obstaja taka matrika B, da je $AB = BA = I$. Od tod pa sledi

$$AB = I \implies \det(AB) = \det I \implies \det A \cdot \det B = 1 \implies \det A \neq 0.$$

($\Leftarrow$) Denimo, da je $\det A \neq 0$. Potem velja

$$A \cdot \tilde{A}^\top = \det A \cdot I \implies A \cdot \frac{1}{\det A} \tilde{A}^\top = I.$$

Sledi, da je A obrnljiva in $A^{-1} = \frac{1}{\det A} \tilde{A}^\top$. □

Opomba. Determinanta matrike A^{-1} je $\det A^{-1} = \frac{1}{\det A}$

Izrek 4.41 (Cramerjevo pravilo)**.**

Naj bo $A \in \mathbb{F}^{n \times n}$ in $b \in \mathbb{F}^n$. Recimo, da je A obrnljiva. Označimo z A_i matriko, ki jo dobimo, če v matriki A i-ti stolpec zamenjamo s stolpcem b. Potem rešitve sistema $Ax = b$ dobimo iz formule $x_i = \frac{\det A_i}{\det A}$.

Dokaz. Naj bo x rešitev sistema $Ax = b$. Potem je $x = A^{-1}b = \frac{1}{\det A} \tilde{A}^\top b$ in njegova i-ta komponenta

$$x_i = \frac{1}{\det A}(\tilde{a}_{1i}b_1 + \tilde{a}_{2i}b_2 + \cdots + \tilde{a}_{ni}b_n) = \frac{1}{\det A} \det A_i.$$ □

Definicija 4.17. Naj bo V končnorazsežen vektorski prostor nad $\mathbb{F}$ in $A : V \to V$ linearna preslikava. Izberimo bazo $\mathcal{B}$ prostora V. Determinanta endomorfizma je $\det A \equiv \det A_{\mathcal{B}\mathcal{B}}$.

Opomba. Da bi dokazali, da je ta definicija res smiselna, moramo preveriti, da je neodvisna od izbire baze $\mathcal{B}$.

Trditev 4.42. *Če sta A, B podobni $n \times n$ matriki, je $\det A = \det B$.*

Dokaz. Po definiciji podobnosti obstaja obrnljiva matrika P, da je $B = PAP^{-1}$. Potem je

$$\begin{aligned} \det B = \det(PAP^{-1}) &= \det P \cdot \det A \cdot \det P^{-1} \\ &= \det P \cdot \det A \cdot \frac{1}{\det P} \\ &= \det A \end{aligned}$$ □

Posledica 4.43. *Definicija determinante endomorfizma je neodvisna od izbire baze.*

Definicija 4.18. Naj bo $A \in \mathbb{F}^{m \times n}$ in $1 \leq k \leq \min\{m, n\}$. Minor reda k je determinanta matrike, katere členi se nahajajo v izbranih k vrsticah in k stolpcih matrike A.

Zgled 4.18. *Vzemimo matriko*

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 3 & 2 \\ 1 & 0 & 2 & 5 \end{bmatrix}.$$

Eden izmed minorjev reda 2 *je*

$$\begin{vmatrix} 1 & 3 \\ 1 & 2 \end{vmatrix} = 1 \cdot 2 - 1 \cdot 3 = -1.$$

Opomba. V $m \times n$ matriki je $\binom{m}{k}\binom{n}{k}$ minorjev reda k.

Lema 4.44. *Naj bo A $m \times n$ matrika. Če so vsi minorji reda k enaki* 0*, potem so tudi vsi minorji reda $r > k$ enaki* 0*.*

Dokaz. Indukcija po r.

1. $r = k+1$: Minor reda $k+1$ je determinanta neke matrike $(k+1) \times (k+1)$, ki je sestavljena iz elementov A. Če to determinanto razvijemo po neki vrstici, dobimo „linearno kombinacijo“ minorjev reda k, ki so po indukcijski predpostavki ničelni. Torej je tudi vsak minor reda $k+1$ enak 0.
2. $r = k+2$: Enak razmislek. □

Izrek 4.45.

Naj bo A $m \times n$ matrika. Potem je rang$A$ *enak najvecji vrednosti k, za katero obstaja neničeln minor reda k.*

Dokaz. Recimo, da je rang$A = r$ in k red najvecjega neničelnega minorja.

1. $(r \geq k)$: Matrika A ima neničeln minor reda k. V A premešamo vrstice in stolpce tako, da elementi tega minorja ležijo v zgornjem levem kotu in tvorijo matriko B. Seveda pri tem ostane rang matrike A nespremenjen. M je $k \times k$ matrika, ki je obrnljiva in ima zato rang k. To pomeni, da so stolpci matrike B linearno neodvisni, zato so podaljšani stolpci tudi linearno neodvisni. Teh stolpcev je k, torej velja $k \leq r$.
2. $(r \leq k)$: Matrika A ima r linearno neodvisnih stolpcev. Stolpce v matriki lahko premešamo tako, da bodo ti stolpcih na prvih r mestih. Enako naredimo še z linearno neodvisnimi vrsticami, ki jih je prav tako r. Tako dobimo v zgornjem levem kvadratu matriko B velikosti $r \times r$, rang$A$ pa pri tem ostane nespremenjen. Ker so v B vrstice in stolpci linearno neodvisni, je B obrnljiva in $\det B \neq 0$. Torej je $\det B$ minor matrike A, neničeln in reda r. Po definiciji k je torej $k \leq r$ in sledi $k = r$. □

4.9 Lastne vrednosti in lastni vektorji endomorfizmov ter kvadratnih matrik

Definicija 4.19. Naj bo V[a] vektorki prostor nad $\mathbb{F}$ in $A : V \to V$ linearna preslikava. Za neničeln vektor $v \in V$ pravimo, da je lasten vektor endomorfizma A, če obstaja $\lambda \in \mathbb{F}$, da velja $Av = \lambda v$. Skalarju λ pravimo lastna vrednost preslikave A.

[a] V bo ponavadi končnorazsežen

Definicija 4.20. Naj bo $A \in \mathbb{F}^{n \times n}$. Pravimo, da je $v \in \mathbb{F}^n \setminus \{0\}$ lasten vektor matrike A, če obstaja $\lambda \in \mathbb{F}$, da velja $A \cdot v = \lambda \cdot v$. Skalarju λ pravimo lastna vrednost matrike A.

Recimo, da je $A : V \to V$, naj bo V lasten vektor za A z lastno vrednostjo λ, torej $AV = \lambda v$. Potem velja $Av - \lambda v = 0$, od koder pa sledi $(A - \lambda I)v = 0$. To pa pomeni, da je $v \in \ker(A - \lambda I)$. Velja pa tudi obratno: če izberemo $v \in \ker(A - \lambda I) \setminus \{0\}$, potem je $(A - \lambda I)v = 0$ in od tod sledi $Av = \lambda v$.

Sklep: lastni vektorji preslikave A za lastno vrednost λ so natanko neničelni vektorji iz $\ker(A - \lambda I)$. Vemo, da je λ lastna vrednost preslikave A natanko tedaj, ko velja $\ker(A - \lambda I) \neq \{0\}$. Od tod naprej pa sledi

$$\begin{aligned} \ker(A - \lambda I) \neq \{0\} &\iff A - \lambda I \text{ ni injektivna} \\ &\iff A - \lambda I \text{ ni bijektivna (torej ni obrnljiva)} \\ &\iff \det(A - \lambda I) = 0. \end{aligned}$$

Definicija 4.21. Če je λ lastna vrednost preslikave A, podprostoru $\ker(A - \lambda I)$ pravimo lastni podprostor za lastno vrednost λ.

Sedaj vemo, da so lastne vrednost rešitve enačbe $\det(A - \lambda I) = 0$ in lastni vektorji neničelni elementi $\ker(A - \lambda I)$. Izraz $\det(A - \lambda I)$ izgleda kot

$$A - \lambda I = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} - \begin{bmatrix} \lambda & & & \\ & \lambda & & \\ & & \ddots & \\ & & & \lambda \end{bmatrix} = \begin{bmatrix} a_{11} - \lambda & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - \lambda & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - \lambda \end{bmatrix},$$

torej je $\det(A - \lambda I)$ polinom v spremenljivki λ stopnje n.

Definicija 4.22. Polinomu $p_A(\lambda) = \det(A - \lambda I)$ pravimo karakteristični polinom preslikave oz. matrike A. Torej so lastne vrednosti kar ničle karakterističnega polinoma matrike.

Trditev 4.46. *Podobni matriki imata isti karakteristični polinom.*

Dokaz. Naj bosta A, B podobni matriki. Potem po definiciji obstaja obrnljiva matrika P, da je $B = PAP^{-1}$. Sedaj pa velja

$$\begin{aligned} p_B(\lambda) = \det(B - \lambda I) &= \det(PAP^{-1} - \lambda I) \\ &= \det(PAP^{-1} - \lambda PIP^{-1}) \\ &= \det(P(A - \lambda I)P^{-1}) \\ &= \det P \cdot \det(A - \lambda I) \cdot \det P^{-1} \\ &= \det(A - \lambda I) = p_A(\lambda) \end{aligned}$$

□

Definicija 4.23. Naj bo λ lastna vrednost preslikave (matrike) A.

- Vrednost $\dim \ker(A - \lambda I)$ imenujemo geometrijska večkratnost lastne vrednosti λ.
- Večkratnosti λ kot ničle karakterističnega polinoma pravimo algebraična večkratnost lastne vrednosti λ.

Zgled 4.19. *Oglejmo si matriko*

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Najprej izračunajmo lastne vrednosti te matrike s pomočjo karakterističnega polinoma.

$$p_A(\lambda) = \det(A - \lambda I) = \begin{vmatrix} -\lambda & 1 \\ -1 & -\lambda \end{vmatrix} = \lambda^2 + 1,$$

ta polinom pa nima realnih ničel. Če torej gledamo matriko A kot element $\mathbb{R}^{2\times 2}$, nima lastnih vrednosti. Če pa jo gledamo kot element $\mathbb{C}^{2\times 2}$, pa ima lastni vrednosti $\lambda_1 = i$ in $\lambda_2 = -i$.

Definicija 4.24.

1. Naj bo $A : V \to V$. Pravimo, da se da A diagonalizirati, če obstaja baza $\mathcal{B}$ prostora V, da je $A_{\mathcal{B}\mathcal{B}}$ diagonalna:
$$A_{\mathcal{B}\mathcal{B}} = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}.$$
2. Naj bo $A \in \mathbb{F}^{n\times n}$. Pravimo, da se da A diagonalizirati, če je podobna neki diagonalni matriki, tj. obstaja obrnljiva matrika P in diagonalna matrika D, da je $A = PDP^{-1}$.

Trditev 4.47. *Lastne vrednosti diagonalne matrike so ravno elementi na diagonali te matrike.*

Dokaz. Naj bo matrika D iz zgornje trditve
$$D = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}.$$
Potem je njen karakteristični polinom
$$p_D(\lambda) = \det(D - \lambda I) = \begin{vmatrix} \lambda_1 - \lambda & & & \\ & \lambda_2 - \lambda & & \\ & & \ddots & \\ & & & \lambda_n - \lambda \end{vmatrix} = (\lambda_1 - \lambda)(\lambda_2 - \lambda)\dots(\lambda_n - \lambda)$$
in ničle p_D so ravno $\lambda_1, \lambda_2, \dots, \lambda_n$. □

Izrek 4.48.

1. *$A : V \to V$ se da diagonalizirati natanko tedaj, ko obstaja baza prostora V, sestavljena iz lastnih vektorjev preslikave A.*
2. *$A \in \mathbb{F}^{n\times n}$ se da diagonalizirati natanko tedaj, ko obstaja baza prostora $\mathbb{F}^n$, sestavljena iz lastnih vektorjev matrike A.*

Dokaz. ($\Leftarrow$) Recimo, da bazo V lahko sestavimo iz lastnih vektorjev A. Naj bo to baza $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$, kjer so v_i lastni vektorji A. Potem velja $Av_1 = \lambda_1 v_1, Av_2 = \lambda_2 v_2, \dots, Av_n = \lambda_n v_n$. Sedaj pa je
$$A_{\mathcal{B}\mathcal{B}} = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}.$$

($\Rightarrow$) Denimo, da obstaja baza $\mathcal{B} = \{u_1, u_2, \ldots, u_n\}$, da je $A_{\mathcal{B}\mathcal{B}}$ diagonalna:

$$A_{\mathcal{B}\mathcal{B}} = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}.$$

To pa pomeni, da je $Au_1 = \lambda_1 u_1, Au_2 = \lambda_2 u_2, \ldots, Au_n = \lambda_n u_n$. $\mathcal{B}$ je torej baza, sestavljena iz lastnih vektorjev A. □

Opomba. Kako bi dokazali ta izrek še za matrike? Predpostavimo, da se $A \in \mathbb{F}^{n\times n}$ da diagonalizirati. Naj bo $A = PDP^{-1}$, kjer je D diagonalna in so njeni diagonalci $\lambda_1, \ldots, \lambda_n$, torej so to tudi lastne vrednosti A. A lahko gledamo kot matriko v standardni bazi: $A = A_{\mathcal{S}\mathcal{S}}$. Iz zgornje točke vemo, da lastni vektorji tvorijo bazo prostora $\mathbb{F}^n$, $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ in $D = A_{\mathcal{B}\mathcal{B}}$, torej smo dokazali. Obrat te trditve je očiten.

Opomba. Zakaj je dobro, če se da matrika diagonalizirati? Naj bo $A = PDP^{-1}$, kjer je

$$D = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}.$$

Če želimo sedaj izračunati A^k, kjer je $k \in \mathbb{N}$, lahko to storimo naslednje:

$$\begin{aligned} A^k &= \underbrace{A \cdot A \cdot \cdots \cdot A}_{k \text{ faktorjev}} \\ &= \underbrace{PDP^{-1} \cdot PDP^{-1} \cdot \cdots \cdot PDP^{-1}}_{k \text{ faktorjev}} \\ &= PD^kP^{-1} = P \begin{bmatrix} \lambda_1^k & & & \\ & \lambda_2^k & & \\ & & \ddots & \\ & & & \lambda_n^k \end{bmatrix} P^{-1} \end{aligned}$$

Opomba. Obstajajo kompleksne matrike, ki se ne dajo diagonalizirati. Primer take matrike je

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

To je zato, ker je 0 dvojna lastna vrednost te matrike. Lastni vektorji torej pripadajo $\ker(A - 0 \cdot I) = \ker A$. Ker pa je $\dim \ker A = 1$, ne moremo sestaviti baze prostora $\mathbb{C}^2$ iz lastnih vektorjev. Zato se tudi A ne da diagonalizirati.

Trditev 4.49. *Naj bo $A : V \to V$ linearna in $v_1, v_2, \ldots, v_m \in V$, za katere velja $Av_i = \lambda_i v_i$, $\lambda_i \in \mathbb{F}$ in $v_i \neq 0$. Naj bodo $\lambda_1, \lambda_2 \ldots, \lambda_n$ paroma različne vrednosti. Potem so $v_i, v_2, \ldots, v_n$ linearno neodvisni.*

Dokaz. Recimo, da to ni res. Naj bo K najmanjše tako število, da je v_k linearna kombinacija $v_1, v_2, \ldots, v_{k-1}$:

$$v_k = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{k-1} v_{k-1}.$$

Na obeh straneh te enačbe uporabimo preslikavo A in dobimo

$$\begin{aligned} Av_k &= \alpha_1 Av_1 + \alpha_2 Av_2 + \cdots + \alpha_{k-1} Av_{k-1} \\ \lambda_k v_k &= \alpha_1 \lambda_1 v_1 + \alpha_2 \lambda_2 v_2 + \cdots + \alpha_{k-1} \lambda_k v_{k-1} \end{aligned}$$

Hkrati pa lahko vrhnjo enačbo pomnožimo s λ_k in dobimo

$$\lambda_k v_k = \alpha_1 \lambda_k v_1 + \alpha_2 \lambda_k v_2 + \cdots + \alpha_{k-1} \lambda_k v_{k-1}.$$

Dobljeni enačbi sedaj lahko med seboj odštejemo in dobimo

$$0 = \alpha_1(\lambda_1 - \lambda_k) v_1 + \alpha_2(\lambda_2 - \lambda_k) v_2 + \cdots + \alpha_{k-1}(\lambda_{k-1} - \lambda_k) v_{k-1}.$$

Po izbiri k so $v_1, v_2, \ldots, v_{k-1}$ linearno neodvisni, zato imamo $\alpha_1(\lambda_1 - \lambda_k) = 0, \alpha_2(\lambda_2 - \lambda_k) = 0, \ldots, \alpha_{k-1}(\lambda_{k-1} - \lambda_k) = 0$. Ker so $\lambda_1, \lambda_2, \ldots, \lambda_k$ paroma različni, velja $\alpha_1 = \alpha_2 = \cdots = \alpha_{k-1} = 0$. To pa pomeni, da je $v_k = 0$ in pridemo v protislovje. □

4.10 Karakteristični in minimalni polinom

Karakteristični polinom matrike $A \in \mathbb{F}^{n \times n}$ je $p_A = \det(A - \lambda I)$. To je polinom stopnje n s koeficienti iz polja $\mathbb{F}$: $p_A(\lambda) = a_n \lambda^n + a_{n-1} \lambda^{n-1} + \cdots + a_1 \lambda + a_0,\ a_i \in \mathbb{F}$. V tem razdelku bomo posplošili pojem polinoma.

Definicija 4.25. Matrični polinom je izraz

$$p(\lambda) = A_k \lambda^k + A_{k-1} \lambda^{k-1} + \cdots + A_1 \lambda + A_0,$$

kjer so $A_0, A_1, \ldots, A_k$ $n \times n$ matrike nad $\mathbb{F}$. Če je $A_k \neq 0$, pravimo, da je p matrični polinom stopnje k.

Definicija 4.26. Če je $p(\lambda) = A_k \lambda^k + A_{k-1} \lambda^{k-1} + \cdots + A_1 \lambda + A_0,\ A_i \in \mathbb{F}^{n \times n}$ matrični polinom in $B \in \mathbb{F}^{n \times n}$, definiramo

$$p(B) = A_k B^k + A_{k-1} B^{k-1} + \cdots + A_1 B + A_0 I.$$

Zgled 4.20 (Poseben primer)**.** *Če gledamo običajen polinom $p(\lambda) = a_n \lambda^n + a_{n-1} \lambda^{n-1} + \cdots + a_1 \lambda + a_0,\ a_i \in \mathbb{F}$, ga lahko obravnavamo tudi kot matrični polinom:*

$$p(\lambda) = (a_n \cdot I)\lambda^n + (a_{n-1} \cdot I)\lambda^{n-1} + \cdots + (a_1 I)\lambda + a_0 I$$
$$p(B) = (a_n \cdot I)B^n + (a_{n-1} \cdot I)B^{n-1} + \cdots + (a_1 I)B + a_0 I$$

:

Opomba. Če so $A_0, \ldots, A_k$ $n \times n$ matrike in $p(\lambda) = A_k \lambda^k + A_{k-1} \lambda^{k-1} + \cdots + A_1 \lambda + A_0$, je

$$p(\lambda) = \begin{bmatrix} p_{11}(\lambda) & p_{12}(\lambda) & \ldots & p_{1n}(\lambda) \\ \vdots & \vdots & & \vdots \\ p_{n1}(\lambda) & p_{n2}(\lambda) & \ldots & p_{nn}(\lambda) \end{bmatrix},$$

kjer je $p_{ij}(\lambda)$ polinom stopnje $\leq k$. Podobno lahko naredimo tudi obratno: $n \times n$ matriko B, katere elementi so polinomi s koeficienti iz polja, potem lahko B razčlenimo na matrični polinom.

Definicija 4.27. Na množici matričnih polinomov, katerih koeficienti so matrike iz $\mathbb{F}^{n \times n}$, lahko definiramo seštevanje in množenje.

- $p(\lambda) = A_k \lambda^k + A_{k-1} \lambda^{k-1} + \cdots + A_1 \lambda + A_0$,
- $q(\lambda) = B_k \lambda^k + B_{k-1} \lambda^{k-1} + \cdots + B_1 \lambda + B_0$,
- $(p + q)(\lambda) = (A_k + B_k)\lambda^k + (A_{k-1} + B_{k-1})\lambda^{k-1} + \cdots + (A_1 + B_1)\lambda + (A_0 + B_0)$ in

- $(pq)(\lambda) = (A_k B_k)\lambda^{2k} + \cdots + (A_2 B_0 + A_1 B_1 + A_0 B_2)\lambda^2 + (A_1 B_0 + A_0 B_1)\lambda + (A_0 B_0)$

Definicija 4.28. Matrika $B \in \mathbb{F}^{n\times n}$ je ničla matričnega polinoma $p(\lambda)$, če velja $p(B) = 0$.

Izrek 4.50 (Bezout)**.**

Naj bo $A \in \mathbb{F}^{n\times n}$ in $p(\lambda)$ matrični polinom s koeficienti iz $\mathbb{F}^{n\times n}$ stopnje k. Potem obstajata matrični polinom $q(\lambda)$ stopnje $k-1$ in matrika $R \in \mathbb{F}^{n\times n}$, da velja $p(\lambda) = q(\lambda)\cdot(A - \lambda I) + R$. Pri tem sta $q(\lambda)$ in R enolično določena in je $R = p(A)$.

Dokaz. Izrek dokažemo tako, da primerjamo koeficiente polinomov na obeh straneh. Od tod je tudi razvidno, da sta $q(\lambda)$ in R enolično določena. □

Oglejmo si sedaj karakteristični polinom matrike A: $p_A(\lambda) = \det(A - \lambda I)$. Ta polinom lahko seveda gledamo tudi kot matrični polinom.

Izrek 4.51 (Cayley-Hamiltonov izrek)**.**

Naj bo $A \in \mathbb{F}^{n\times n}$. Potem je $p_A(A) = 0$.

Dokaz. Oglejmo si $\left(\widetilde{A - \lambda I}\right)^\top$. Elementi te matrike so kofaktorji matrike $A - \lambda I$ in so polinomi v spremenljivki λ. Torej je ta matrika v resnici matrični polinom in $\left(\widetilde{A - \lambda I}\right)^\top \cdot (A - \lambda I) = \det(A - \lambda I)\cdot I$. Opazimo, da je $p_A(\lambda) = \left(\widetilde{A - \lambda I}\right)^\top \cdot (A - \lambda I)$. Po drugi strani pa Bezoutov izrek implicira, da obstaja $q(x)$, da je $p_A(\lambda) = q(\lambda)(A - \lambda I) + p_A(A)$. Zaradi enoličnosti pa je $q(x) = \left(\widetilde{A - \lambda I}\right)^\top$ in $p(A) = 0$. □

Definicija 4.29. Naj bo $A \in \mathbb{F}^{n\times n}$. Polinom $m_A(\lambda)$ je minimalni polinom matrike A, če:

1. vodilni koeficient polinoma $m_A(\lambda)$ je 1.
2. $m_A(A) = 0$
3. za vsak neničeln polinom $q(\lambda)$ nižje stopnje je $q(A) \neq 0$.

Izrek 4.52.

Minimalni polinom matrike je enolično določen.

Dokaz. Recimo, da sta $m_1(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0$ in $m_2(\lambda) = \lambda^n + b_{n-1}\lambda^{n-1} + \cdots + b_1\lambda + b_0$ minimalna polinoma matrike A. Potem je razvidno, da je $r(\lambda) \equiv m_1(\lambda) - m_2(\lambda)$ polinom stopnje $< k$. Hkrati pa velja $r(A) = m_1(A) - m_2(A) = 0$, torej je zaradi minimalnosti $r(\lambda) \equiv 0$. To pa pomeni $m_1(\lambda) \equiv m_2(\lambda)$. □

Trditev 4.53. *Minimalni polinom matrike A vedno deli karakteristični polinom.*

Dokaz. Trditev hitro sledi iz Bezoutovega izreka in minimalnosti $m_A(\lambda)$. □

Preselimo se sedaj v primer $\mathbb{F} = \mathbb{C}$. Karakteristični polinom matrike A je oblike

$$p_A(\lambda) = (-1)^n(\lambda - \lambda_1)^{n_1}(\lambda - \lambda_2)^{n_2} \dots (\lambda - \lambda_k)^{n_k},$$

kjer so $\lambda_1, \lambda_2, \dots, \lambda_k$ lastne vrednosti matrike A. Minimalni polinom matrike A pa je oblike

$$m_A(\lambda) = (\lambda - \lambda_1)^{m_1}(\lambda - \lambda_2)^{m_2} \dots (\lambda - \lambda_k)^{m_k},$$

kjer velja $0 \leq m_i \leq n_i$ za vsak i. Izkazalo pa se bo, da velja tudi $m_i \geq 1$ za vsak i.

Izrek 4.54.

Minimalni polinom $m_A(\lambda)$ ima iste ničle kot $p_A(\lambda)$.

Dokaz. Minimalni polinom $m_A(\lambda)$ delimo z $\lambda - \lambda_i$. Dobimo $m_A(\lambda) = q(\lambda)(\lambda - \lambda_i) + m_A(\lambda_i)$. Radi bi dokazali, da je $m_A(\lambda_i) = 0$. Namesto λ vstavimo matriko A in dobimo

$$q(A)(A - \lambda_i I) + m_A(\lambda_i)I = m_A(A) = 0.$$

Ker je λ_i lastna vrednost A, obstaja $x \in \mathbb{C}^n \setminus \{0\}$, da je $Ax = \lambda_i x$. Sedaj našo enačbo pomnožimo z x na levi in dobimo

$$q(A)(A - \lambda_i I)x + m_A(\lambda_i)Ix = 0$$

in od tod hitro sledi $m_A(\lambda_i) = 0$. To velja za vsak i. □

Trditev 4.55. *Podobni matriki imata isti minimalni polinom.*

Dokaz. Naj bosta matriki A, B podobni in naj bo $B = P^{-1}AP$, kjer je P obrnljiva. Naj bo p tak polinom, da je

$$p(\lambda) = a_k\lambda^k + \dots + a_1\lambda + a_0,$$

kjer so $a_i \in \mathbb{F}$. Naj bo $p(A) = 0$. Potem velja tudi

$$\begin{aligned} p(B) = a_kB^k + \dots + a_1B + a_0 \cdot I &= a_k(P^{-1}AP) + \dots + a_1(P^{-1}AP) + a_0(P^{-1}IP) \\ &= P^{-1}\left(a_kA^k + \dots + a_1A + a_0I\right)P \\ &= P^{-1} \cdot p(A) \cdot P = 0. \end{aligned}$$

Podoben sklep velja tudi obratno: če je $p(B) = 0$, je tudi $P(A) = 0$. Torej je množica polinomov, ki uničijo A, enaka množici polinomov, ki uničijo B. Od tod pa hitro sledi (iz lastnosti minimalnega polinoma), da sta minimalna polinoma A in B enaka. □

Definicija 4.30. Naj bo $A : V \to V$. Minimalni polinom endomorfizma A je minimalni polinom matrike $A_{\mathcal{BB}}$, kjer je $\mathcal{B}$ poljubna baza prostora V.

5 Struktura endomorfizmov končnih vekt. prostorov nad $\mathbb{C}$

5.1 Korenski podprostori

Definicija 5.1. Naj bo $A : V \to V$. Podprostor $U \leq V$ je invarianten za A, če velja $A(U) \subseteq U$.

Opomba. Če je $A : V \to V$ in je podprostor U invarianten za A, potem zožitev A-ja na podprostor U slika v U; $A\big|_U$ je endomorfizem prostora U.

Denimo, da imamo linearno preslikavo $A : V \to V$ in $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$, kjer so $V_i \leq V$ in vsi V_i invariantni za A. Naj bo $\mathcal{B}_i$ baza podprostora V_i, kjer je $i = 1, \ldots, r$. Potem je $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \cdots \cup \mathcal{B}_r$ baza prostora V. Matrika preslikave A v bazi $\mathcal{B}$ je

$$A_{\mathcal{B}\mathcal{B}} = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{bmatrix}.$$

Pri tem je A_1 matrika $A\big|_{V_1}$ v bazi $\mathcal{B}_1$, A_2 matrika $A\big|_{V_2}$ v bazi $\mathcal{B}_2$ in tako dalje. Baze $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_r$ lahko konstruiramo tako, da bodo $A_1, A_2, \ldots, A_r$ zgornjetrikotne (Schurov izrek). Spomnimo se, da ima endomorfizem $A : V \to V$:

- karakteristični polinom $p_A(\lambda) = (-1)^n(\lambda - \lambda_1)^{n_1}(\lambda - \lambda_2)^{n_2} \ldots (\lambda - \lambda_k)^{n_k}$ in
- minimalni polinom $m_A(\lambda) = (\lambda - \lambda_1)^{m_1}(\lambda - \lambda_2)^{m_2} \ldots (\lambda - \lambda_k)^{m_k}$.

Pri tem za $\forall i$ velja $1 \leq m_i \leq n_i$.

Definicija 5.2. Podprostor $W_i = \ker(A - \lambda_i I)^{m_i}$ imenujemo korenski podprostor prostora V, ki pripada endomorfizmu A za lastno vrednost I.

Trditev 5.1. *Podprostori $W_1, W_2, \ldots, W_k$ so invariantni za A in velja $V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$.*

Dokaz. Dokažimo najprej, da je W_i invarianten za A. Naj bo $x \in W_i$. Potem je

$$(A - \lambda_i I)^{m_i}(Ax) = (A - \lambda_i I)^{m_i} Ax = A(A - \lambda_i I)^{m_i} x = 0$$

in $Ax \in \ker(A - \lambda_i I)^{m_i}$. Sedaj moramo še dokazati, da velja $V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$. Naj bo $x \in V$. Označimo $p_i(\lambda) = m_a(\lambda)(\lambda - \lambda_i)^{-m_i}$. Polinomi $p_1, p_2, \ldots, p_k$ nimajo skupne ničle in so zato tuji (največji skupni delitelj je konstantni polinom). Zato obstajajo kompleksni polinomi $q_1, q_2, \ldots, q_k$, da velja

$$p_1 q_1 + p_2 q_2 + \cdots + p_k q_k = 1.$$

Potem označimo $x_i = p_i(A)q_i(A)x$ in hitro sledi, da za $x_i, x_2, \ldots, x_k$ velja $x_i \in W_i$ in $x_1 + x_2 + \cdots + x_k = x$. Preostane nam še dokazati, da je ta zapis za x enoličen. Naj bo

$$\begin{aligned} x &= x_1 + x_2 + \cdots + x_k \\ x &= x_1' + x_2' + \cdots + x_k', \end{aligned}$$

za $x_i, x_i' \in W_i$. Označimo $y_i = x_i - x_i'$, $y_i \in W_i$ in sedaj je $y_i + y_2 + \cdots + y_k = 0$. Opazimo, da za $i \neq j$ velja $p_i(\lambda) = r_i(\lambda)(\lambda - \lambda_j)^{m_j}$ za nek polinom $r_i(\lambda)$, torej je $p_i(A)y_j = 0$ za $j \neq i$, od tod pa sledi, da je tudi $p_j(A)y_j = 0$. Sedaj pa dobimo

$$\begin{aligned} y_j = Iy_j &= \left(p_1(A)q_1(A) + p_2(A)q_2(A) + \cdots + p_k(A)q_k(A)\right) y_j \\ &= q_1(A)p_1(A)y_j + q_2(A)p_2(A)y_j + \cdots + q_k(A)p_k(A)y_j = 0 \end{aligned}$$

□

Oglejmo si sedaj zožitve endomorfizma A na korenske podprostore: $A_i = A\big|_{W_i} : W_i \to W_i$.

Trditev 5.2. *Ob zgornjih oznakah je* $p_{A_i}(\lambda) = \pm(\lambda - \lambda_i)^{n_i}$ *in* $m_{A_i}(\lambda) = (\lambda - \lambda_i)^{m_i}$.

Opomba. Zato se bomo v nadaljevanju omejili na endomorfizme z eno lastno vrednostjo.

Dokaz. Označimo zožitev identične preslikave $I : V \to V$ na podprostor W_i kot I_i. Ker je $W_i = \ker(A_i - \lambda_i I_i)^{m_i}$, je $(A_i - \lambda_i I_i)^{m_i} = 0$. Za polinom $q(\lambda) = (\lambda - \lambda_i)^{m_i}$ je $q(A_i) = 0$. Zato $m_{A_i}(\lambda)$ deli $q(\lambda)$ in $m_{A_i}(\lambda) = (\lambda - \lambda_i)^{s_i}$ za $1 \leq s_i \leq m_i$. Definiramo polinom

$$f(\lambda) = (\lambda - \lambda_1)^{s_1}(\lambda - \lambda_2)^{s_2} \dots (\lambda - \lambda_k)^{s_k}$$

in dokažimo, da za ta polinom velja $f(A) = 0$. Vzemimo $x \in V$. Ker je $V = W_1 \oplus W_2 \oplus \dots \oplus W_k$, lahko pišemo $x = x_1 + x_2 + \dots + x_k$, kjer je $x_i \in W_i$. Potem je

$$f(A)(x) = (A - \lambda_1 I)^{s_1}(A - \lambda_2 I)^{s_2} \dots (A - \lambda_k I)^{s_k}(x_1 + x_2 + \dots + x_k) = 0$$

in s tem smo dokazali $m_{A_i}(\lambda) = (\lambda - \lambda_i)^{m_i}$. Sedaj si oglejmo še karakteristični polinom A_i. Ta je očitno oblike $p_{A_i}(\lambda) = \pm(\lambda - \lambda_i)^{r_i}$. Dokazujemo, da je $r_i = n_i$. Vemo, da je

$$p_{A_i}(\lambda) = \det(A_i - \lambda I_i) = \pm(\lambda - \lambda_i)^{r_i}.$$

Sedaj pa se ponovno osredotočimo na celoten $p_A(\lambda)$:

$$\begin{aligned} p_A(\lambda) = p_{A_{\mathcal{BB}}}(\lambda) &= \begin{vmatrix} A_1 - \lambda I_1 & & & \\ & A_2 - \lambda I_2 & & \\ & & \ddots & \\ & & & A_k - \lambda I_k \end{vmatrix} \\ &= \det(A_1 - \lambda I_1)\det(A_2 - \lambda I_2)\dots\det(A_k - \lambda I_k) \\ &= \pm(\lambda - \lambda_1)^{r_1}(\lambda - \lambda_2)^{r_2}\dots(\lambda - \lambda_k)^{r_k}. \end{aligned}$$

Po drugi strani pa je $p_A(\lambda) = \pm(\lambda - \lambda_1)^{n_1}(\lambda - \lambda_2)^{n_2} \dots (\lambda - \lambda_k)^{n_k}$ in torej $n_i = r_i$. □

5.2 Endomorfizmi z eno samo lastno vrednostjo

Naj bo $A : V \to V$, A naj ima eno samo lastno vrednost ρ in naj bo $\dim V = n$. Karakteristični polinom je $p_A(\lambda) = (-1)^n(\lambda - \rho)^n$ in $m_A(\lambda) = (\lambda - \rho)^m$. Definirajmo $B = A - \rho I$. Potem je $p_B(\lambda) = (-1)^n\lambda^n$ in $m_B = \lambda^m$. Od tod sledi sklep, da je m tak, da velja $B^m = 0$ (B je nilpotenten) in $B^k \neq 0$ za $k < m$.

Trditev 5.3. *Velja*

$$\{0\} \subset \ker B \subset \dots \subset \ker B^m = V.$$

Dokaz. Dokažimo najprej, da za vsak i velja $\ker B^i \subseteq \ker B^{i+1}$. Naj bo $x \in \ker B^i$. Potem je $B^{i+1}x = B(B^i x) = 0$, torej $x \in \ker B^{i+1}$. Sedaj pa dokažimo še, da za noben i ne velja $\ker B^i \neq \ker B^{i+1}$. Denimo, da tak i obstaja. Potem lahko pokažemo, da velja $\ker B^{i+1} = \ker B^{i+2}$, kar pa vodi v protislovje. Res, vzemimo $x \in \ker B^{i+2}$. Torej $B^{i+1}(Bx) = 0$, zato $Bx \in \ker B^{i+1} = \ker B^i$, torej $B^{i+1}x = 0$ in smo pokazali želeno trditev. □

Trditev 5.4. *Velja:* $x \in \ker B^i \Leftrightarrow Bx \in \ker B^{i-1}$.

Definicija 5.3. Naj bo X neprazna množica vektorjev iz V. Pravimo, da je X i-linearno neodvisna, če velja:

- $X \subseteq \ker B^i$,
- vektorji iz X so linearno neodvisni in
- $LinX \cap \ker B^{i-1} = \{0\}$.

Trditev 5.5. *Če je množica X i-linearno neodvisna, je množica $BX = \{Bx : x \in X\}$ $(i-1)$-linearno neodvisna za $i \geq 2$.*

Dokaz. Iz prejšnje trditve sledi $BX \subseteq \ker B^{i-1}$. Dokažimo, da je BX linearno neodvisna. Naj bo $X = \{x_1, x_2, \ldots, x_k\}$ in $BX = \{Bx_1, Bx_2, \ldots, Bx_k\}$. Naj bo

$$\alpha_1 Bx_1 + \cdots + \alpha_k Bx_k = 0 \Leftrightarrow B(\alpha_1 x_1 + \cdots + \alpha_k x_k).$$

Potem je $\alpha_1 x_1 + \cdots + \alpha_k x_k \in \ker B \subseteq \ker B^{i-1}$, hkrati pa $\alpha_1 x_1 + \cdots + \alpha_k x_k \in LinX$. Ker pa je $\ker B^{i-1} \cap LinX = \{0\}$, sledi linearna nedvisnost. Sedaj dokažimo še tretjo lastnost $(i-1)$-linearne množice. Vzemimo $y \in LinBX \cap \ker B^{i-2}$. Potem je $y = \alpha_1 Bx_1 + \cdots + \alpha_k Bx_k$ in $B^{i-2}y = 0$. Od tod pa je

$$\begin{aligned} 0 = B^{i-2}y &= B^{i-2}\left(B\left(\alpha_1 x_1 + \cdots + \alpha_k x_k\right)\right) \\ &= B^{i-1}\left(\alpha_1 x_1 + \cdots + \alpha_k x_k\right) \end{aligned}$$

in ker je $\ker B^{i-1} \cap LinX = \{0\}$, je $\alpha_1 x_1 + \cdots + \alpha_k x_k = 0$ in sledi linearna neodvisnost. □

Sedaj bomo konstruirali posebno bazo prostora V, ki ji pravimo Jordanova baza endomorfizma B. Vemo, da je $\ker B^m = V$ in $\ker B^{m-1} \neq V$, torej je $\ker B^{m-1}$ pravi podprostor v V. Zato obstaja podprostor U_1 v V, da je $\ker B^{m-1} \oplus U_1$. Vzemimo poljubno bazo podprostora U_1: $\mathcal{U}_1 = \{u_1^{(1)}, \ldots, u_{s_1}^{(1)}\}$, kjer je $s_1 = \dim \ker B^m - \dim \ker B^{m-1}$. Trdimo, da je $\mathcal{U}_1$ m-linearno neodvisna. To je res, saj velja $\mathcal{U}_1 \subseteq \ker B^m = V$, $\mathcal{U}_1$ je linearno neodvisna in

$$Lin\, \mathcal{U}_1 \cap \ker B^{m-1} = U_1 \cap \ker B^{m-1} = \{0\}.$$

Zato je $B\mathcal{U}_1 = \{Bu_1^{(1)}, \ldots, Bu_{s_1}^{(1)}\}$ $(m-1)$-linearno neodvisna. Ta proces ponovimo še enkrat: $\ker B^{m-2}$ je pravi podprostor v $\ker B^{m-1}$, zato obstaja podprostor U_2, da bo $\ker B^{m-1} = \ker B^{m-2} \oplus U_2$. Brez škode za splošnost lahko bazo prostora U_2 sestavimo na naslednji način:

$$\mathcal{U}_2 = \{Bu_1^{(1)}, \ldots, Bu_{s_1}^{(1)}, \ldots\} = \{u_1^{(2)}, \ldots, u_{s_1}^{(2)}, \ldots, u_{s_2}^{(2)}\},$$

kjer je $s_2 = \dim \ker B^{m-1} - \dim \ker B^{m-2}$. Po konstrukciji je $\mathcal{U}_2$ $(m-1)$-linearno neodvisna. Postopek ponavljamo in dobimo $V = \ker B^m = \ker B^{m-1} \oplus U_1$, $\ker B^{m-1} = \ker B^{m-2} \oplus U_2$ in tako naprej do $\ker B = \{0\} \oplus U_2 = U_m$. Pri tem je baza U_i kar $\mathcal{U}_i = \{u_{s_1}^{(i)}, u_{s_1}^{(i)}, \ldots, u_{s_i}^{(i)}\}$. Hitro dokažemo tudi naslednjo trditev (nekoliko je treba paziti le pri enoličnosti zapisa).

Trditev 5.6. $V = U_1 \oplus U_2 \oplus \cdots \oplus U_m$.

Posledica 5.7. $\mathcal{U} = \mathcal{U}_1 \cup \mathcal{U}_2 \cup \cdots \cup \mathcal{U}_m$ *je baza prostora* V.

Definicija 5.4. Bazi $\mathcal{U}$ pravimo Jordanova baza endomorfizma B.

Matriko $J(B) = B_{\mathcal{U}\mathcal{U}}$ imenujemo Jordanova forma endomorfizma B. Vektorje Jordanove baze razvrstimo od $\mathcal{U}_m$ „navzgor“ (podrobneje: predavanja) in dobimo matriko $J(B)$, v kateri nastopajo bloki, imenovani Jordanove kletke.

Opomba. Velikost najvecje kletke je $m \times m$ in takih kletk je $s_1 = \dim \ker B^m - \dim \ker B^{m-1}$. Podobno je kletk velikosti $(n-1) \times (n-1)$ $s_2 - s_1 = 2\dim \ker B^{m-1} - \dim \ker B^m - \dim \ker B^{m-2}$. Podobno velja za vse ostale velikosti kletk, ki jih je vseh skupaj $s_m = \dim \ker B$.

Sedaj se vrnimo nazaj na endomorfizem $A = B + \rho I$. Za B imamo Jordanovo bazo U:

$$A_{\mathcal{U}\mathcal{U}} = (B + \rho I)_{\mathcal{U}\mathcal{U}} = B_{\mathcal{U}\mathcal{U}} + \rho I_{\mathcal{U}\mathcal{U}} = J(B) + \rho I.$$

Tako dobimo $J(A)$ oziroma Jordanovo formo endomorfizma A. Če imamo endomorfizem z več vrednosti, obravnavamo zožitve $A\big|_{W_i}$ na korenskih prostorih ($A\big|_{W_i}$ je endomorfizem z eno samo lastno vrednostjo).

Pri tem je A_i matrika za $A\big|_{W_i}$ v neki bazi W_i. Matrika za A v uniji baz je

$$A = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix}.$$

Definicija 5.5. Jordanova kanonična forma endomorfizma A je

$$J(A) = \begin{bmatrix} J(A_1) & & & \\ & J(A_2) & & \\ & & \ddots & \\ & & & J(A_k) \end{bmatrix}.$$

Opomba. Če je $A \in \mathbb{C}^{n\times n}$, lahko A gledamo kot endomorfizem $A : \mathbb{C}^n \to \mathbb{C}^n$. Jordanovi kanonični formi tega endomorfizma pravimo Jordanova kanonična forma matrike A. Če je $\mathcal{U}$ Jordanova baza, je $J(A) = A_{\mathcal{U}\mathcal{U}}$ in $A = A_{\mathcal{S}\mathcal{S}} = P_{\mathcal{S}\mathcal{U}} J(A) P_{\mathcal{U}\mathcal{S}}$, kjer so v stolpcih P vektorji iz $\mathcal{U}$.

5.3 Spektralna razčlenitev endomorfizma

Definicija 5.6. Preslikava $P : V \to V$ je projektor, če obstajata podprostora $V_1, V_2 \leq V$, da velja:

1. $V = V_1 \oplus V_2$,
2. $\forall x \in V_1 : \ Px = x$ in
3. $\forall x \in V_2 : \ Px = 0$.

Potem pravimo, da je P projektor na V_1 vzdolž V_2.

Trditev 5.8. *P je projektor natanko tedaj, ko velja $P^2 = P$. V tem primeru P projicira na* $\operatorname{im} P$ *vzdolž* $\ker P$.

Dokaz. ($\Rightarrow$) P naj bo projektor na V_1 vzdolž V_2, kjer je $V = V_1 \oplus V_2$. Vzemimo poljuben $v \in V$, ki se ga da na enoličen način zapisati kot $v = v_1 + v_2$, kjer $v_1 \in V_1$ in $v_2 \in V_2$. Potem je $Pv = v_1$ in posledično $P^2 v = v_1$ za $\forall v \in V$, torej je $P^2 = P$.

Sedaj pa dokažimo trditev še v drugo smer ($\Leftarrow$). Naj bo $P^2 = P$. Vzemimo $V_1 = \operatorname{im} P$ in $V_2 = \ker P$. Najprej moramo dokazati, da sploh velja $V = V_1 \oplus V_2$. To je res zato, ker lahko $v \in V$ zapišemo kot $v = Pv + (v - Pv)$ in zaradi $Pv = P^2 v$ je $P(v - Pv) = 0$, torej $v - Pv \in \ker P$. Sedaj si oglejmo še $v \in V_1 \cap V_2$. Ker je $v \in \operatorname{im} P$, je $v = Px$ za nek $x \in V$. Ker pa je tudi $v \in \ker P$, pa je $Pv = 0 \implies P^2 x = 0 \Rightarrow Px = 0$ in je $V_1 \cap V_2 = \{0\}$, kar smo želeli dokazati. Preostane le še, da pokažemo, da velja $Px = x$ za $x \in V_1$. To je res, ker je $x = Py$ za nek $y \in V$ in je $Px = P^2 y = Py = x$. □

Trditev 5.9. *Naj bo $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$. Naj bo P_i projektor na V_i vzdolž*

$$V_i' = V_1 \oplus \cdots \oplus V_{i-1} \oplus V_{i+1} \oplus \cdots \oplus V_k.$$

Potem velja $P_1 + P_2 + \cdots + P_k = I$ in $P_i P_j = 0$ za $i \neq j$.

Dokaz. Če nek $x \in V$ zapišemo kot $x = v_1 + v_2 + \cdots + v_k$, $v_i \in V_i$, potem hitro sledi

$$(P_1 + P_2 + \cdots + P_k)x = v_1 + v_2 + \cdots + v_k = x.$$

Podoben sklep naredimo tudi pri drugi točki. Ponovno zapišemo $x = v_1 + v_2 + \cdots + v_k$ in od tod

$P_iP_jx = P_iv_j = 0$, ker je $i \neq j$. □

Trditev 5.10. *Naj bo P projektor, A endomorfizem prostora V. Recimo, da sta* $\ker P$ *in* $\operatorname{im} P$ *invariantna za A. Potem je $AP = PA$.*

Dokaz. Naj bo $V = \operatorname{im} P \oplus \ker P$. Potem za nek $v \in V$, $v = v_1 + v_2$, kjer $v_1 \in \operatorname{im} P$ in $v_2 \in \ker P$, velja:

- $(AP)v = A(Pv) = A(P(v_1 + v_2)) = A(Pv_1 + Pv_2) = Av_1$ in
- $(PA)v = P(Av) = P(A(v_1 + v_2)) = P(Av_1 + Av_2) = Av_1$. □

Sedaj naj bo A endomorfizem $V \to V$ nad $\mathbb{C}$. Njegov minimalni polinom je

$$m_A(\lambda) = (\lambda - \lambda_1)^{m_1}(\lambda - \lambda_2)^{m_2} \dots (\lambda - \lambda_k)^{m_k}.$$

Korenski podprostori so $W_i = \ker(A - \lambda_i)^{m_i}$ in $V = W_1 \oplus W_2 \oplus \cdots \oplus W_n$. Naj bo P_i projektor na W_i vzdolž W_i'. Vemo že, da je $P_1 + P_2 + \cdots + P_k = I$ in P_iP_j za $i \neq j$. Dokazali smo že, da sta W_i in W_i' (torej $\operatorname{im} P_i$ in $\ker P_i$) invariantna za A, torej je $AP_i = P_iA$. Sedaj definirajmo $N_i = (A - \lambda_i I)P_i$.

Trditev 5.11. *Ob zgornji definiciji veljajo naslednje točke:*

- $N_iP_i = P_iN_i = N_i$,
- $N_iP_j = P_jN_i = 0$ *za* $i \neq j$,
- $N_i^{m_i} = 0$, $N_i^{m_i-1} \neq 0$,
- $N_iN_j = 0$ *za* $i \neq j$ *in*
- $(\lambda_iP_i + N_i)(\lambda_jP_j + N_j) = 0$ *za* $i \neq j$.

Dokaz. Dokaz teh točk je preprost (peta točka sledi iz direktnega računa in uporabe prve, druge in četrte točke). □

Sedaj se vrnimo na $A : V \to V$. Vemo, da je

$$A = AI = A(P_1 + P_2 + \cdots + P_k) = AP_1 + AP_2 + \cdots + AP_k.$$

Pri tem P_i in AP_i slikata $V \to W_i$. Potem je zožitev N_i na W_i kar $N_i = (A - \lambda_i I)$ in $AP_i = (N_i + \lambda_i I)P_i$. Torej imamo

$$A = (N_1 + \lambda_1 I)P_1 + (N_2 + \lambda_2 I)P_2 + \cdots + (N_k + \lambda_k I)P_k,$$

kjer so $N_1, \dots, N_k$ nilpotentni endomorfizmi. Temu pravimo spektralna razčlenitev endomorfizma. Zgornjo enačbo lahko še naprej poenostavimo v

$$A = (N_1 + \lambda_1 P_1) + (N_2 + \lambda_2 P_2) + \cdots + (N_k + \lambda_k P_k).$$

Ta zapis je koristen, ker velja

$$A^n = (N_1 + \lambda_1 P_1)^n + (N_2 + \lambda_2 P_2)^n + \cdots + (N_k + \lambda_k P_k)^n.$$

Zgled 5.1. *Če trditev, ki smo jo izpeljali, uporabimo na Jordanovi formi matrike A, dobimo*

$$A^n = (N_1 + \lambda_1 P_1)^n + \cdots = \begin{bmatrix} J_1^n & & & \\ & J_2^n & & \\ & & \ddots & \\ & & & J_l^n \end{bmatrix}.$$

Sklep: *če potenciramo Jordanovo formo, lahko potenciramo vsako kletko posebej.*

5.4 Funkcije matrik in endomorfizmov

Naj bo A poljubna matrika $n \times n$ nad $\mathbb{C}$. Motivirajmo izraz za potenčno funkcijo matrike oziroma A^n. Naj bo A podobna Jordanovi formi, torej $A = PJ(A)P^{-1}$. Potem je $A^n = PJ(A)^n P^{-1}$. Zgoraj smo pokazali, da je potenca Jordanove forme matrike preprosto potenca vsake kletke posebej. Zadošča torej izračunati potenco Jordanove kletke

$$J = \begin{bmatrix} \rho & 1 & & \\ & \rho & \ddots & \\ & & \ddots & 1 \\ & & & \rho \end{bmatrix}.$$

Za to kletko naredimo spektralni razcep in dobimo $J = \rho I + N$, ker je $P = I$ in

$$N = \begin{bmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix}.$$

Sedaj imamo $J^n = (N + \rho I)^n = \sum_{k=0}^{n} \binom{n}{k} \rho^{n-k} N^k$. Pri potenciranju matrike N se diagonala „premika“ navzgor. Tako dobimo

$$J^n = \begin{bmatrix} \binom{n}{0}\rho^n & \binom{n}{1}\rho^{n-1} & \cdots & \\ & \binom{n}{0}\rho^n & \ddots & \vdots \\ & & \ddots & \binom{n}{1}\rho^{n-1} \\ & & & \binom{n}{0}\rho^n \end{bmatrix}.$$

Sedaj lahko poskusimo ta izraz uporabiti za polinom matrike $p(A)$. Res, za $A = P \cdot J(A) \cdot P^{-1}$ velja $p(A) = Pp(J(A))P^{-1}$ in $p(J(A))$ je $J(A)$, kjer so vsi Jordanski bloki dani v polinom p. Problem nastane, ker je polinom Jordanove kletke zelo težavno izračunati na enak način kot zgoraj. Očitno potrebujemo nov način.

Trik: polinom $p(\lambda) = \alpha_n \lambda^n + \alpha_{n-1}\lambda^{n-1} + \cdots + \alpha_1 \lambda + \alpha_0$ napišemo kot linearno kombinacijo potenc $(\lambda - \rho)$ s pomočjo Taylorjevega polinoma p okoli točke ρ. Tako dobimo

$$p(\lambda) = p(\rho) + \frac{p'(\rho)}{1!}(\lambda - \rho) + \cdots + \frac{p^{(n)}(\rho)}{n!}(\lambda - \rho)^n.$$

S pomočjo te formule pa lahko izračunamo polinom Jordanove kletke:

$$p(J) = \begin{bmatrix} p(\rho) & \frac{p'(\rho)}{1!} & \cdots & \\ & p(\rho) & \ddots & \vdots \\ & & \ddots & \frac{p'(\rho)}{1!} \\ & & & p(\rho) \end{bmatrix}.$$

Če hočemo snov, ki smo jo izpeljali v tem sklopu, posplošiti na funkcije, moramo uporabiti snov analize.

Naj bo f neka funkcija, ki je zadostikrat odvedljiva okoli neke točke $x = \rho$. Potem to funkcijo v okolici te točke lahko aproksimiramo s Taylorjevim polinomom okoli točke ρ:

$$f(x) = f(\rho) + \frac{f'(\rho)}{1!}(x - \rho) + \cdots + \frac{f^{(n)}(\rho)}{n!}(x - \rho)^n + R_n(x).$$

Pri mnogo funkcijah, s katerimi se pogosto srečujemo, velja $\lim_{n\to\infty} R_n(x) = 0$. Če je funkcija neskončnokrat odvedljiva okoli točke ρ, jo lahko zapišemo s Taylorjevo vrsto:

$$f(x) = f(\rho) + \frac{f'(\rho)}{1!}(x - \rho) + \frac{f^{(2)}(\rho)}{2!}(x - \rho)^2 + \dots$$

Naj bo $A = PJ(A)P^{-1}$ in f m_i-krat odvedljiva v okolici λ_i, kjer je m_i velikost največje Jordanske kletke z lastno vrednostjo λ_i. Sedaj definiramo $f(A) = Pf(J(A))P^{-1}$, pri čemer je

$$f(J(A)) = \begin{bmatrix} f(J_1) & & & \\ & f(J_2) & & \\ & & \ddots & \\ & & & f(J_k) \end{bmatrix}$$

in funkcija pojamezne Jordanske kletke

$$f(J) = \begin{bmatrix} f(\rho) & \frac{f'(\rho)}{1!} & \cdots & \\ & f(\rho) & \ddots & \vdots \\ & & \ddots & \frac{f'(\rho)}{1!} \\ & & & f(\rho) \end{bmatrix}.$$

Zgled 5.2. *Naj bo matrika*

$$A = \begin{bmatrix} 2 & 1 & & & & \\ & 2 & 1 & & & \\ & & 2 & & & \\ & & & 3 & 1 & \\ & & & & 3 & \\ & & & & & 4 \end{bmatrix}.$$

Potem je

$$\sin A = \begin{bmatrix} \sin 2 & \frac{\cos 2}{1!} & -\frac{\sin 2}{2!} & & & \\ & \sin 2 & \frac{\cos 2}{1!} & & & \\ & & \sin 2 & & & \\ & & & \sin 3 & \frac{\cos 3}{1!} & \\ & & & & \sin 3 & \\ & & & & & \sin 4 \end{bmatrix}.$$

6 Vektorski prostori s skalarnim produktom

Naj bo V vektorski prostor nad $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$.

Definicija 6.1. Skalarni produkt na V je preslikava $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}$, ki preslika $(u, v) \to \langle u, v \rangle$ in zadošča naslednjim zahtevam:

- $\forall x \in V : \ \langle x, x \rangle \geq 0$ in $\langle x, x \rangle = 0 \iff x = 0$,
- $\forall x, y, z \in V : \ \langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$,
- $\forall x, y \in V, \forall \alpha \in \mathbb{F} : \ \langle \alpha x, y \rangle = \alpha \langle x, y \rangle$ in
- $\forall x, y \in V : \ \langle x, y \rangle = \overline{\langle y, x \rangle}$.

Zgled 6.1. *Oglejmo si nekaj zgledov standardnih skalarnih produktov v znanih vektorskih prostorih.*

- $V = \mathbb{R}^n$, $\langle (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \rangle = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$,
- $V = \mathbb{C}^n$, $\langle (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \rangle = x_1 \overline{y_1} + x_2 \overline{y_2} + \cdots + x_n \overline{y_n}$,
- $V = C([a, b])$ *nad* $\mathbb{R}$, $\langle f, g \rangle = \int_a^b f(x) g(x) \, dx$
- $V = C([a, b])$ *nad* $\mathbb{C}$, $\langle f, g \rangle = \int_a^b f(x) \overline{g(x)} \, dx$

Posledica 6.1. *Naj bo $\langle \cdot, \cdot \rangle$ skalarni produkt na V. Potev velja aditivnost in poševna homogenost na drugem faktorju. Prav tako velja $\langle 0, y \rangle$ za vsak $y \in V$.*

Definicija 6.2. Naj bo V vektorski prostor s skalarnim produktom in $x \in v$. Potem predpis $\|x\| = \sqrt{\langle x, x \rangle}$ imenujemo norma vektorja x.

Izrek 6.2 (Neenakost Cauchy-Schwarz-Bunjakowskega)**.**

Naj bo V vektorski prostor s skalarnim produktom in $x, y \in V$. Potem velja $|\langle x, y \rangle| \leq \|x\| \|y\|$. Enačaj velja natanko tedaj, ko sta vektorja x in y linearno odvisna.

Dokaz. Oglejmo si

$$\begin{aligned} \|\langle y, y \rangle x - \langle x, y \rangle y\|^2 &= \langle \langle y, y \rangle x - \langle x, y \rangle y, \langle y, y \rangle x - \langle x, y \rangle y \rangle \\ &= \langle y, y \rangle \overline{\langle y, y \rangle} \langle x, x \rangle - \langle y, y \rangle \overline{\langle x, y \rangle} \langle x, y \rangle \\ &- \langle x, y \rangle \overline{\langle y, y \rangle} \langle y, x \rangle + \langle x, y \rangle \overline{\langle x, y \rangle} \langle y, y \rangle \\ &= \|y\|^4 \|x\|^2 - \|y\|^2 |\langle x, y \rangle|^2 \\ &= \|y\|^2 \left(\|y\|^2 \|x\|^2 - |\langle x, y \rangle|^2 \right) \end{aligned}$$

in ker je leva stran te neenakosti večja ali enaka nič, je $\|y\|^2 \|x\|^2 \geq |\langle x, y \rangle|^2$. Hitro sledi, da velja enakost natanko tedaj, ko je $x = \alpha y$. □

Opomba. V vektorskem prostoru $\mathbb{C}^n$ se ta neenakost prevede v Cauchy-Schwartzevo neenakost:

$$|x_1 \overline{y_1} + x_2 \overline{y_2} + \cdots + x_n \overline{y_n}| \leq \sqrt{|x_1|^2 + |x_2|^2 + \cdots + |x_n|^2} \sqrt{|y_1|^2 + |y_2|^2 + \cdots + |y_n|^2}.$$

V prostoru $C([a, b])$ nad $\mathbb{R}$ pa se to prevede na neenakost Bunjakowskega:

$$\left| \int_a^b f(x) g(x) \, dx \right| \leq \sqrt{\int_a^b f(x)^2 \, dx} \sqrt{\int_a^b g(x)^2 \, dx}.$$

Trditev 6.3 (Lastnosti norme)**.** *Naj bo V vektorski prostor s skalarnim produktom. Potem velja:*

- $\|x\| \geq 0$ *in* $\|x\| = 0 \iff x = 0$,
- $\|\alpha x\| = |\alpha|\|x\|$ *za* $\forall x \in V,\ \forall \alpha \in \mathbb{F}$ *in*
- $\|x + y\| \leq \|x\| + \|y\|$ *za* $\forall x, y \in V$ *(trikotniška neenakost).*

Dokaz. Dokažimo tretjo točko.

$$\begin{aligned}
\|x+y\|^2 &= \langle x+y, x+y\rangle \\
&= \|x\|^2 + \langle x, y\rangle + \overline{\langle x, y\rangle} + \|y\|^2 \\
&= \|x\|^2 + 2\Re\langle x, y\rangle + \|y\|^2 \\
&\leq \|x\|^2 + 2|\langle x, y\rangle| + \|y\|^2 \\
&\leq \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 \\
&= (\|x\| + \|y\|)^2.
\end{aligned}$$

□

Definicija 6.3. Naj bo V poljuben vektorski prostor. Norma na V je preslikava $\|\cdot\| : V \to \mathbb{F}$ s predpisom $x \to \|x\|$, ki zadošča lastnostim:

- $\|x\| \geq 0$ in $\|x\| = 0 \iff x = 0$,
- $\|\alpha x\| = |\alpha|\|x\|$ za $\forall x \in V,\ \forall \alpha \in \mathbb{F}$ in
- $\|x + y\| \leq \|x\| + \|y\|$ za $\forall x, y \in V$.

Pravimo, da je V normiran prostor.

Definicija 6.4. Naj bo V normiran prostor in $x, y \in V$. Razdalja med x in y je $d(x, y) = \|x - y\|$.

6.1 Ortogonalnost

Naj bo V vektorski prostor s skalarnim produktom.

Definicija 6.5. $u, v \in V$ sta ortogonalna, če $\langle u, v\rangle = 0$.

Definicija 6.6. Kot med vektorjema u in v je definiran s predpisom $\cos\phi = \Re\left(\frac{\langle u,v\rangle}{\|u\|\|v\|}\right)$.

Opomba. Pojem kota je dobro definiran zaradi Cauchy-Schwartzeve neenakosti.

Trditev 6.4. *Če so $v_1, v_2, \ldots, v_k$ neničelni paroma pravokotni vektorji, potem so linearno neodvisni.*

Dokaz. Naj bo $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = 0$. To enakost skalarno pomnožimo z v_i in dobimo $\alpha_i \langle v_i, v_i\rangle = 0$. Od tod pa sledi $\alpha_i = 0$. □

Posledica 6.5. *Če je* $\dim V = n$*, ima vsaka množica neničelnih paroma pravokotnih vektorjev kvečjemu n elementov.*

Vprašanje: ali za V lahko najdemo ortogonalno bazo, t.j. bazo, sestavljeno iz paroma pravokotnih vektorjev?

Definicija 6.7. Naj bo X podmnožica v V. Pravimo, da je X ortogonalna množica, če velja: $\forall x, y \in X, x \neq y : \langle x, y \rangle = 0$.

Definicija 6.8. Naj bo X podmnožica v V. Pravimo, da je X ortonormirana množica, če je ortogonalna in za $\forall x \in X$ velja $\|x\| = 1$.

Opomba. Vektor $x \in V, x \neq 0$ normiramo tako, da ga pomnožimo s skalarjem $\frac{1}{\|x\|}$.

Izrek 6.6.

Recimo, da so $v_1, v_2, \ldots, v_k$ linearno neodvisni vektorji v V. Potem obstajajo paroma ortogonalni vektorji $u_1, u_2, \ldots, u_k$, da velja $Lin\{u_1, u_2, \ldots, u_k\} = Lin\{v_1, v_2, \ldots, v_k\}$. Dosežemo lahko, da so $u_1, u_2, \ldots, u_n$ ortonormirani.

Gram-Schmidtova ortogonalizacija. Za primer $k = 1$ lahko vzamemo $u_1 = v_1$, za primer $k = 2$ pa $u_1 = v_1$ in $u_2 = v_2 - \frac{\langle v_2, u_1 \rangle}{\langle u_1, u_1 \rangle} u_1$ in u_2 je linearno neodvisen od u_1 in je nanj pravokoten, kar hitro sledi iz direktnega računa. Sedaj vzemimo splošen primer in naredimo indukcijo po k. Naj trditev velja za $k - 1$ vektorjev. Vzemimo $v_1, v_2, \ldots, v_k$. Po indukcijski predpostavki obstajajo paroma pravokotni vektorji $u_1, u_2, \ldots, u_{k-1}$, da bo $Lin\{u_1, u_2, \ldots, u_{k-1}\} = Lin\{v_1, v_2, \ldots, v_{k-1}\}$. Potem definiramo

$$u_k = v_k - \frac{\langle v_k, u_1 \rangle}{\langle u_1, u_1 \rangle} u_1 - \frac{\langle v_k, u_2 \rangle}{\langle u_2, u_2 \rangle} u_2 - \cdots - \frac{\langle v_k, u_{k-1} \rangle}{\langle u_{k-1}, u_{k-1} \rangle} u_{k-1}$$

in hitro sledi, da u_k ustreza vsem zahtevanim lastnostim. □

Posledica 6.7. *Vsak končnorazsežev vektorski prostor s skalarnim produktom ima ortonormirano bazo.*

Trditev 6.8. *Naj bo $\{u_1, u_2, \ldots, u_n\}$ ortonormirana baza vektorskega prostora V in $v \in V$. Potem*

$$v = \langle v, u_1 \rangle u_1 + \langle v, u_2 \rangle u_2 + \cdots + \langle v, u_n \rangle u_n$$

in $\langle v, u_i \rangle$ je Fourierov koeficient pri u_i.

Definicija 6.9. Naj bosta V_1 in V_2 vektorska prostora nad $\mathbb{F}$ s skalarnima produktoma $\langle \cdot, \cdot \rangle_1$ in $\langle \cdot, \cdot \rangle_2$. Izomorfizem vektorskih prostorov s skalarnim produktom je preslikava $A : V_1 \to V_2$, za katero velja:

- A je izomorfizem običajnih vektorskih prostorov in
- $\forall x, y \in V_1 : \langle Ax, Ay \rangle_2 = \langle x, y \rangle_1$.

Izrek 6.9.

Naj bo V vektorski prostor s skalarnim produktom in $\dim V = n$. Potem je V izomorfen (v smislu izomorfizma vektorskih prostorov s skalarnim produktom) $\mathbb{F}^n$ z običajnim skalarnim produktom.

Dokaz. Za V izberemo ON bazo $\{v_1, v_2, \ldots, v_n\}$. Naj bo $A : \mathbb{F}^n \to V$ preslikava s predpisom $(\alpha_1, \ldots, \alpha_n) \to \alpha_1 v_1 + \cdots + \alpha_n v_n$. Vemo že, da je A izomorfizem običajnih vektorskih prostorov. Označimo s $\langle \cdot, \cdot \rangle_1$ skalarni produkt v $\mathbb{F}^n$ in s $\langle \cdot, \cdot \rangle_2$ skalarni produkt v V. Naj bosta $x = (x_1, x_2, \ldots, x_n)$ in $y = (y_1, y_2, \ldots, y_n)$. Potem je

$$\langle Ax, Ay \rangle_2 = \langle x_1 v_1 + x_2 v_2 + \cdots + x_n v_n, y_1 v_1 + y_2 v_2 + \cdots + y_n v_n \rangle_2 = x_1 \overline{y_1} + x_2 \overline{y_2} + \cdots + x_n \overline{y_n} = \langle x, y \rangle_1.$$

□

Definicija 6.10. Naj bo V vektorski prostor s skalarnim produktom in X ter Y neprazni podmnožici v V. Pravimo, da sta X in Y ortogonalni ($X \perp Y$), če velja $\langle x, y\rangle = 0$ za $\forall x \in X,\ \forall y \in Y$.

Trditev 6.10. *Če je $X \perp Y$, je tudi $LinX \perp LinY$.*

Dokaz. Vzemimo $v \in LinX$ in $u \in LinY$. Naj bo $v = \alpha_1 x_1 + \cdots + \alpha_k x_k$ in $u = \beta_1 y_1 + \cdots + \beta_l y_l$. Potem je

$$\langle u, v\rangle = \alpha_1\overline{\beta_1}\langle x_1, y_1\rangle + \alpha_1\overline{\beta_2}\langle x_1, y_2\rangle + \cdots = 0. \qquad \square$$

Definicija 6.11. Naj bo V vektorski prostor s skalarnim produktom in $V_1, V_2, \ldots, V_k$ podprostori v V. Vsota $V_1 + V_2 + \cdots + V_k$ je pravokotna vsota, če velja $V_i \perp V_j$ za vse $i \neq j$.

Trditev 6.11. *Ob zgornjih oznakah, če je $V_1 + V_2 + \cdots + V_k$ pravokotna vsota, je avtomatično direktna vsota.*

Dokaz. Naj bo $U = V_1 + V_2 + \cdots + V_k$. Recimo, da $u \in U$ lahko zapišemo kot $u = v_1 + v_2 + \cdots + v_k$ in $u = w_1 + w_2 + \cdots + w_k$, kjer $v_i, w_i \in U$. Potem je

$$(v_1 - w_1) + (v_2 - w_2) + \cdots + (v_k - w_k) = 0.$$

To enakost skalarno pomnožimo s $v_i - w_i$ in dobimo $0 = \langle v_i - w_i, v_i - w_i\rangle$, torej $v_i - w_i = 0$ in zapis je enoličen. $\square$

Definicija 6.12. Naj bo V vektorski prostor s skalarnim produktom in X neprazna množica v V. Množici $X^\perp = \{x \in V \,|\, \langle v, x\rangle = 0,\ \forall x \in X\}$ pravmo ortogonalni komplement množice X v V.

Trditev 6.12. *Ob zgornjih oznakah je $X^\perp$ vedno podprostor v V.*

Dokaz. Dokaz je trivialen. $\square$

Trditev 6.13. *Naj bo $\{v_1, v_2, \ldots, v_n\}$ ON baza prostora V in naj bosta $V_1 = Lin\{v_1, \ldots, v_k\}$ ter $V_2 = Lin\{v_{k+1}, \ldots, v_n\}$. Potem je $V = V_1 \oplus V_2$ (pravokotna vsota) in $V_1^\perp = V_2$, $V_2^\perp = V_1$.*

Dokaz. Dokaz je ponovno očiten. $\square$

Izrek 6.14.

Naj bo V vektorski prostor s skalarnim produktom in U podprostor v V. Potem je $V = U \oplus U^\perp$ (pravokotna vsota) in $(U^\perp)^\perp = U$.

Dokaz. Za U izberimo ortonormirano bazo $\{u_1, \ldots, u_m\}$ in to bazo dopolnimo do baze V. Dobljeno bazo z Gram-Schmidtovim postopkom pretvorimo v ON bazo V: $\{u_1, \ldots, u_m, v_1, \ldots, v_k\}$. Sedaj je $U = Lin\{u_1, \ldots, u_m\}$ in $\tilde{U} = Lin\{v_1, \ldots, v_k\}$. Po prejšnji trditvi je $V = U \oplus \tilde{U}$, $U^\perp = \tilde{U}$ in $(\tilde{U})^\perp = U$. Od tod pa sledijo želene zveze. $\square$

Trditev 6.15. *Naj bo V vektorski prostor s skalarnim produktom, $u, v \in V$ naj bosta pravokotna. Potem je $\|u + v\|^2 = \|u\|^2 + \|v\|^2$ (Pitagorov izrek).*

Dokaz.

$$\|u+v\|^2 = \langle u+v, u+v\rangle = \langle u,u\rangle + \langle v,v\rangle = \|u\|^2 + \|v\|^2. \qquad \square$$

6.2 Pravokotne projekcije

Naj bo V vektorski prostor s skalarnim produktom. Če je U podprostor v V, potem je $V = U \oplus U^\perp$.

Definicija 6.13. Projektorju $P : V \to V$ na U vzdolž $U^\perp$ pravimo pravokotni projektor na podprostor U.

Opomba. Naj bo P pravokoten projektor na U. Izberimo ON bazo U: $\{u_1, \ldots, u_m\}$. To bazo dopolnimo do ON baze V: $\{u_1, \ldots, u_m, v_1, \ldots, V_k\}$. Vzemimo poljuben $x \in V$. Razvijemo ga po tej bazi in dobimo

$$x = \langle x, u_1\rangle u_1 + \cdots + \langle x, u_m\rangle u_m + \langle x, v_1\rangle v_1 + \cdots + \langle x, v_k\rangle v_k.$$

Od tod sledi, da je $Px = \langle x, u_1\rangle u_1 + \cdots + \langle x, u_m\rangle u_m$.

Izrek 6.16.

Če je P pravokotni projektor na podprostor U in $v \in V$, potem je Pv tisti vektor v U, ki je najbližji vektorju v (glede na razdaljo $d(x,y) = \|x-y\|$). Torej velja $\|v - Pv\| = \min_{u\in U} \|v-u\|$.

Dokaz. Naj bo $v \in V$ in poljuben $u \in U$. Potem velja $v - Pv \in U^\perp$ ter $Pv - u$ (glej: spektralna razčlenitev endomorfizma). Potem je

$$\begin{aligned}\|v-u\|^2 &= \|v - Pv + Pv - u\|^2 \\ &= \|v-Pv\|^2 + \|Pv-u\|^2 \\ &\geq \|v-Pv\|^2\end{aligned}$$

in enakost velja natanko tedaj, ko je $u = Pv$. $\square$

6.3 Adjungiran prostor

Naj bo V vektorski prostor s skalarnim produktom nad $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Vemo že, da je V^* dualni prostor, t.j. prostor vseh funkcionalov $f : V \to \mathbb{F}$. Sedaj si oglejmo preslikavo $\phi_Z : V \to \mathbb{F}$ s predpisom $\phi_z(v) = \langle v, z\rangle$ za $z \in V$. Vemo, da je skalarni produkt aditiven in homogen v prvem faktorju, zato je ϕ_z res linearen funkcional. Sedaj pa se zdi „naravno“ definirati preslikavo $\Phi : V \to V^*$ s predpisom $z \to \phi_z$. Oglejmo si lastnosti te preslikave: hitro sledi, da je Φ aditivna in poševno homogena (t.j. $\Phi(\alpha z) = \overline{\alpha}\Phi(z)$).

Izrek 6.17 (Rieszov izrek)**.**

Preslikava Φ je bijektivna (poševni izomorfizem) prostorov V in V^*.

- *Za vsak funkcional $\phi : V \to \mathbb{F}$ obstaja tak vektor $z \in V$, da je $\phi = \phi_z$.*
- *Vektor iz prve točke je natanko določen in mu pravimo Rieszov vektor.*

Dokaz. Dokažimo najprej enoličnost. Denimo, da je $\phi_z = \phi_w$, torej $\phi_z(w) = \phi_w(v)$ za $\forall v \in V$. Ker za vsak $v \in V$ velja $\langle v, z\rangle = \langle v, w\rangle$, je prav tako $\langle v, z-w\rangle = 0$ za vse $v \in V$. Sedaj pa lahko vzamemo $v = z - w$ in dobimo $z - w = 0$, torej imamo res enoličnost.

Sedaj vzemimo poljuben funkcional $\phi : V \to \mathbb{F}$ in za V izberimo ON bazo $\{e_1, e_2, \ldots, e_n\}$. Naj bo $v \in V$. Potem v razvijemo po ON bazi in dobimo $v = \langle v, e_1\rangle e_1 + \cdots + \langle v, e_n\rangle e_n$. Če sedaj na tem

vektorju uporabimo funkcional ϕ, dobimo

$$\phi(v) = \langle v, \underbrace{\overline{\phi(e_1)}e_1 + \cdots + \overline{\phi(e_n)}e_n}_{z} \rangle = \phi_z(v). \qquad \square$$

Sedaj naj bosta U, V prostora s skalarnima produktoma $\langle \cdot, \cdot \rangle_U$ in $\langle \cdot, \cdot \rangle_V$ ter $A : U \to V$ linearna preslikava. Konstruirali bomo adjungirano preslikavo A^* (pozor: dualno preslikavo, ki smo jo do sedaj označevali s A^*, bomo od tod naprej označili s A^d). Vzemimo $v \in V$ in si oglejmo linearen funkcional $\phi : U \to \mathbb{F}$, dan s predpisom $\phi(u) = \langle Au, v \rangle_V$. Po Rieszovem izreku obstaja enolično določen $x \in U$, da je $\langle Au, v \rangle_V = \phi(u) = \langle u, x \rangle_U$ za $\forall u \in U$. Zaradi enoličnosti x lahko definiramo preslikavo $A^* : V \to U$ s predpisom $v \mapsto x$, torej $x = A^* v$. Potem velja $\langle Au, v \rangle_V = \langle u, A^* v \rangle_U$ za $\forall u \in U,\ \forall v \in V$.

Definicija 6.14. Preslikavi A^* pravimo adjungirana preslikava linearne preslikave A.

Trditev 6.18. *Preslikava A^* je linearna.*

Dokaz. Dokažimo aditivnost. Naj bosta $v_1, v_2 \in V$. Potem je

$$\begin{aligned} \langle u, A^*(v_1 + v_2) \rangle &= \langle Au, v_1 + v_2 \rangle \\ &= \langle Au, v_1 \rangle + \langle Au, v_2 \rangle \\ &= \langle u, A^* v_1 \rangle + \langle u, A^* v_2 \rangle \\ &= \langle u, A^* v_1 + A^* v_2 \rangle. \end{aligned}$$

Ker velja $\langle u, \rangle = \langle u, \rangle$ za $\forall u \in U$, lahko naredimo enak sklep kot v dokazu Rieszovega izreka in zaključimo, da je $A^*(v_1 + v_2) = A^* v_1 + A^* v_2$. $\square$

Trditev 6.19. *Naj bosta U in V vektorska prostora s skalarnim produktom.*

- *Če $A, B : U \to V$, potem $(A + B)^* = A^* + B^*$.*
- *Če $A : U \to V$ in $\alpha \in \mathbb{F}$, potem $(\alpha A)^* = \overline{\alpha} A^*$.*
- *Če $A : U \to V$, potem $(A^*)^* = A$.*
- *Naj bo $I : U \to U$ identična preslikava. Potem je $I^* = I$.*
- *Recimo $A : U \to V$, $B : V \to W$. Potem $(BA)^* = A^* B^*$.*

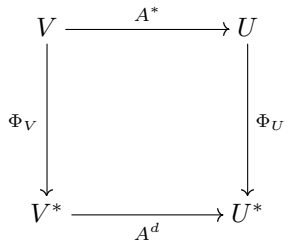
Dokaz. Dokažimo peto točko. Naj bo $A : U \to V$, $B : V \to W$ in $BA : U \to W$. Potem so $A^* : V \to U$, $B^* : W \to V$ in $(BA)^* : W \to U$. Izberimo poljuben $u \in U$ ter $w \in W$. Od tod sledi

$$\begin{aligned} \langle (BA)u, w \rangle_W &= \langle B(Au), w \rangle_W \\ &= \langle Au, B^* w \rangle_V \\ &= \langle u, A^* B^* w \rangle_U \end{aligned}$$

in je $(BA)^* w = A^* B^* w$, $\forall w \in W$. Zato je $(BA)^* = A^* B^*$. $\square$

6.4 Povezava med dualno in adjungirano preslikavo

Naj bosta U, V prostora s skalarnima produktoma in $A : U \to V$ linearna preslikava. Potem imamo adjungirano preslikavo $A^* : V \to U$, dualno preslikavo $A^d : V^* \to U^*$ in poševna izomorfizma $\Phi_U : U \to U^*$ ter $\Phi_V : V \to V^*$. Diagram teh štirih preslikav komutira.



Izrek 6.20.

$\Phi_U \circ A^* = A^d \circ \Phi_V$.

Dokaz. Vzemimo $v \in V$. Potem je $\Phi_U \circ A^*(v) = \Phi_U(A^*v) = \phi_{A^*v}$. Za poljuben $u \in U$ je $\phi_{A^*v}(u) = \langle u, A^*v\rangle_U = \langle Au, v\rangle_V$. Sedaj pa si oglejmo enačbo še z druge strani: $(A^d \circ \Phi_V)v = A^d(\phi_v) = \phi_v \circ A$ in za poljuben $u \in U$ je $(\phi_v \circ A)u = \phi_v(Au) = \langle Au, v\rangle_V$. Torej je $(\Phi_U \circ A^*)v = (A^d \circ \Phi_V)v$, $\forall v \in V$, zato sledi trditev. □

Trditev 6.21. *Če je $\{v_1, \ldots, v_n\}$ ortonormirana prostora V, potem je $\{\Phi_V(v_1), \ldots, \Phi_V(v_n)\}$ njena dualna baza.*

Dokaz.

$$\Phi_V(v_i)(v_j) = \phi_{v_i}(v_j) = \langle v_j, v_i\rangle = \begin{cases} 1: & i = j \\ 0: & i \neq j \end{cases}.$$

□

6.5 Matrika adjungirane preslikave

Naj bo $A : U \to V$ in njena adjungirana preslikava $A^* : V \to U$. Naj bo $\mathcal{B}$ baza U, $\mathcal{C}$ baza V in $A_{\mathcal{CB}}$ matrika za A v teh dveh bazah. Kakšna pa je matrika adjungirane preslikave $A^*_{\mathcal{BC}}$?

Izrek 6.22.

Naj bo $A : U \to V$ linearna preslikava in $\mathcal{B}$,$\mathcal{C}$ zaporedoma ortonormirani bazi prostorov U in V. Potem je

$$A^*_{\mathcal{BC}} = \overline{A_{\mathcal{CB}}}^{\top} = A^{\mathsf{H}}_{\mathcal{CB}}.$$

Dokaz. Naj bo $\mathcal{B} = \{u_1, u_2, \ldots, u_n\}$ ortonormirana baza U in $\mathcal{C} = \{v_1, v_2, \ldots, v_m\}$ ortonormirana baza V. Če Au_1 razvijemo po bazi $\mathcal{C}$, dobimo

$$Au_1 = \langle Au_1, v_1\rangle_V v_1 + \cdots + \langle Au_m, v_m\rangle_V v_m$$

in (i,j)-ti element matrike je $a_{ij} = \langle Au_j, u_i\rangle_V$. Sedaj razvijemo vektor A^*v_1 v bazi $\mathcal{B}$ in dobimo, da je (i,j)-ti element matrike $A^*_{\mathcal{BC}}$ $b_{ji} = \langle A^*v_j, u_i\rangle_U$ in takoj sledi, da je $a_{ij} = \overline{b_{ji}}$. □

Opomba. Naj bo A endomorfizem vektorkega prostora V in $\mathcal{B}$ njegova poljubna (ne nujno ortonormirana) baza. Potem je matrika $A^*_{\mathcal{BB}}$ podobna matriki $(A_{\mathcal{BB}})^{\mathsf{H}}$ (vaje: Gramova matrika).

7 Endomorfizmi prostorov s skalarnim produktom

Naj bo $A : V \to V$, kjer je V prostor s skalarnim produktom. Vemo, da ima A v neki bazi matriko $J(A)$ (Jordanova forma).

Izrek 7.1 (Schurov izrek)**.**

Za $A : V \to V$ obstaja ortonormirana baza $\mathcal{B}$, da bo $A_{\mathcal{B}\mathcal{B}}$ zgornjetrikotna.

Ideja dokaza. Gram-Schmidtov postopek uporabimo kar na Jordanovi bazi in uporabimo dejstvo, da so linearne ogrinjače prvih k vektorjev iz Jordanske baze invariantne za A. □

Opomba. Naj bo $A : V \to V$. Denimo, da se da A diagonalizirati v ortonormirani bazi $\mathcal{B}$. Potem je $A_{\mathcal{B}\mathcal{B}} \cdot A^{\mathsf{H}}_{\mathcal{B}\mathcal{B}} = A^{\mathsf{H}}_{\mathcal{B}\mathcal{B}} \cdot A_{\mathcal{B}\mathcal{B}}$ in posledično $AA^* = A^*A$.

7.1 Normalni endomorfizmi (operatorji) in matrike

Naj bo V vektorski prostor s skalarnim produktom.

Definicija 7.1. Preslikava $A : V \to V$ je normalna, če velja $AA^* = A^*A$.

Definicija 7.2. Matrika $A \in \mathbb{F}^{n\times n}$ je normalna, če $AA^{\mathsf{H}} = A^{\mathsf{H}}A$.

Opomba. Če obstaja ortonormirana baza, sestavljena iz lastnih vektorjev, potem je A normalna. Kasneje bomo spoznali, da ta trditev velja tudi v nasprotno smer.

Trditev 7.2. *A je normalna preslikava natanko tedaj, ko velja $\langle Ax, Ay\rangle = \langle A^*x, A^*y\rangle$ za $\forall x, y \in V$.*

Dokaz. Dokažimo to trditev v levo ($\Leftarrow$). Naj velja zgornja enakost in naj bosta $x, y \in V$ poljubna. Potem je $\langle A^*Ax, y\rangle = \langle AA^*x, y\rangle$ in to velja $\forall x, y \in V$. Zato je $A^*Ax = AA^*$ za $\forall x \in V$, torej $AA^* = A^*A$. □

Posledica 7.3. *Če je A normalna, velja $\|Ax\| = \|A^*x\|$, $\forall x \in V$ in $\ker A = \ker A^*$.*

Trditev 7.4. *Naj bo $A : V \to V$ normalen in $v \in V$ lastni vektor preslikave A za lastno vrednost λ. Potem je v tudi lasten vektor za A^* z lastno vrednostjo $\overline{\lambda}$.*

Dokaz. Dokazali bomo, da je $A - \lambda I$ normalna in nato uporabili prejšnjo posledico. Oglejmo si

$$\begin{aligned}(A-\lambda I)(A-\lambda I)^* &= (A-\lambda I)(A^*-\overline{\lambda}I)\\ &= AA^* - \overline{\lambda}I - \lambda A^* + \lambda\overline{\lambda}\lambda I\\ &= A^*A - \overline{\lambda}A - \lambda A^* + \lambda\overline{\lambda}I\\ &= (A-\lambda I)^*(A-\lambda I).\end{aligned}$$

Po prejšnji posledici velja $\ker(A-\lambda I) = \ker(A-\lambda I)^* = \ker(A^*-\overline{\lambda}I)$, torej za $v \in \ker(A-\lambda I)$ velja $A^*v = \overline{\lambda}$. □

Trditev 7.5. *Naj bo $A : V \to V$ normalna in λ_1, λ_2 različni lastni vrednosti, v_1 in v_2 pa pripadajoča lastna vektorja. Potem $v_1 \perp v_2$.*

Dokaz. Naj bo $Av_1 = \lambda_1 v_1$ in $Av_2 = \lambda_2 v_2$. Potem je

$$\begin{aligned}\lambda_1\langle v_1, v_2\rangle &= \langle Av_1, v_2\rangle \\ &= \langle v_1, A^* v_2\rangle \\ &= \langle v_1, \overline{\lambda_2} v_2\rangle \\ &= \lambda_2\langle v_1, v_2\rangle\end{aligned}$$

in ker je $\lambda_1 \neq \lambda_2$, je $\langle v_1, v_2\rangle = 0$. □

Trditev 7.6. *Naj bo $A : V \to V$ poljubna linearna preslikava in $U \leq V$. Potem je U invarianten za A natanko tedaj, ko je $U^\perp$ invarianten za A^*.*

Dokaz. Dokažimo to trditev v desno smer ($\Rightarrow$). Naj bo U invarianten za A in vzemimo poljubna $x \in U$ ter $y \in U^\perp$. Potem je $Ax \in U$ in $y \in U^\perp$, zato $\langle Ax, y\rangle = 0 \implies \langle x, A^* y\rangle$. Ker to velja za $\forall x \in U$, $\forall y \in U^\perp$, potem je $A^* y \in U^\perp$ za $\forall y \in U^\perp$, je $U^\perp$ invarianten za A^*. Pri dokazu v obratno smer ponovimo ta sklep. □

Izrek 7.7.

Naj bo $A : V \to V$ normalna preslikava. Potem obstaja ortonormirana baza V, sestavljena iz lastnih vektorjev preslikave A (nad $\mathbb{C}$).

Dokaz. Dokaz bo potekal z indukcijo. Za bazni primer vzemimo, da je $\dim V = 1$. Potem seveda obstaja ortonormirana baza V, sestavljena iz lastnih vektorjev preslikave A. Sedaj naj bo $\dim V = n$. Karakteristični polinom A ima vsaj eno ničlo nad $\mathbb{C}$, naj bo to λ_1. Naj bo λ_1 lastna vrednost A z lastnim vektorjem v_1, torej $Av_1 = \lambda_1 v_1$ in posledično $A^* v_1 = \overline{\lambda_1} v_1$. To pomeni, da je $U = Lin\{v_1\}$ invarianten za A in A^*, torej je $U^\perp$ invarianten za A in A^*. Sedaj si oglejmo zožitev $A\big|_{U^\perp} : U^\perp \to U^\perp$. Ta preslikava je prav tako normalna. Ker pa je $\dim U^\perp = n - 1$, lahko po indukcijski prepostavki najdemo ortonormirano bazo $U^\perp$, sestavljeno iz lastnih vektorjev $A\big|_{U^\perp}$ (torej lastnih vektorjev A): $\mathcal{B}' = \{u_1, \ldots, u_{n-1}\}$. Sedaj pa vzamemo $\mathcal{B} = \{v_1, u_1, \ldots, u_{n-1}\}$ in če v_1 normiramo, dobimo ortonormirano bazo V. □

7.2 Sebiadjungirani endomorfizmi in hermitske oziroma simetrične matrike

Definicija 7.3. Preslikava $A : V \to V$ je sebiadjungirana, če velja $A^* = A$.

Definicija 7.4. Matrika $A \in \mathbb{C}^{n\times n}$ je hermitska, če $A^{\mathsf{H}} = A$.

Definicija 7.5. Matrika $A \in \mathbb{R}^{n\times n}$ je simetrična, če $A^\top = A$.

Opomba. Če je A sebiadjungirana, je seveda tudi normalna.

Trditev 7.8. *Če je $A : V \to V$ sebiadjungirana, so vse lastne vrednosti preslikave A realne.*

Dokaz. Recimo $Av = \lambda v$, $v \neq 0$. Ker je A normalna, velja $A^* v = \overline{\lambda} v$. Od tod pa sledi $\lambda v = \overline{\lambda} v$, torej $\lambda \in \mathbb{R}$. □

Trditev 7.9. *Naj bo $A : V \to V$ sebiadjungirana. Če velja $\langle Av, v\rangle = 0$, $\forall v \in V$, potem je $A = 0$.*

Dokaz. Naj bosta $x, y \in V$ poljubna vektorja. Oglejmo si

$$\begin{aligned} 0 &= \langle A(x+y), (x+y)\rangle \\ &= \langle Ax + Ay, x + y\rangle \\ &= \langle Ax, x\rangle + \langle Ax, y\rangle + \langle Ay, x\rangle + \langle Ay, y\rangle \\ &= \langle Ax, y\rangle + \langle Ay, x\rangle \\ &= \langle Ax, y\rangle + \langle y, Ax\rangle \end{aligned}$$

in vstavimo $y = Ax$ ter dobimo $Ax = 0$ za vsak $x \in V$. □

Trditev 7.10. *Naj bo $A : V \to V$ poljubna linearna preslikava. Potem obstajata sebiadjungirani linearni preslikavi $B, C : V \to V$, da velja $A = B + iC$. Preslikavi B, C sta enolično določeni.*

Dokaz. Recimo, da obstajata $A = B + iC$. Potem je $A^* = B^* - iC^* = B - iC$. Tako dobimo $B = \frac{1}{2}(A + A^*)$ in $C = \frac{1}{2i}(A - A*)$. Torej če B in C obstajata, sta enolično določena. Sedaj vzemimo te dve formuli za B, C in hitro ugotovimo, da je $B^* = B$ ter $C^* = C$. □

Trditev 7.11. *Preslikava $A : V \to V$ je sebiadjungirana natanko tedaj, ko velja $\langle Ax, x\rangle \in \mathbb{R}$ za $\forall v \in V$.*

Dokaz. Najprej dokažimo trditev v desno ($\Rightarrow$). Naj bo $A = A^*$. Potem je $\langle Av, v\rangle = \langle v, A^*v\rangle = \langle v, Av\rangle = \overline{\langle Av, v\rangle}$. Torej je $\langle Av, v\rangle \in \mathbb{R}$.

Sedaj pa dokažimo trditev še v drugo smer ($\Leftarrow$): naj bo $\langle Av, v\rangle \in \mathbb{R}$ za $\forall v \in V$. Po prejšnji trditvi obstaja sebiadjungirani preslikavi B, C, da je $A = B + iC$. Potem je $\langle Av, v\rangle = \langle Bv, v\rangle + i\langle Cv, v\rangle$ za $\forall v \in V$. Ker velja $\langle Av, v\rangle, \langle Bv, v\rangle, \langle Cv, v\rangle \in \mathbb{R}$ (B in C sta sebiadjungirani), je $\langle Cv, v\rangle = 0$ za $\forall v \in V$. Ker pa je C sebiadjungirana, je $C = 0$ in $A = B$, kjer je B tudi sebiadjungirana. □

7.3 Unitarni endomorfizmi in unitarne ter ortogonalne matrike

Definicija 7.6. Naj bo $A : V \to V$. Pravimo, da je A unitarna, če velja $AA^* = A^*A = I$.

Definicija 7.7. Matrika $A \in \mathbb{C}^{n\times n}$ je unitarna, če velja $AA^{\mathsf{H}} = A^{\mathsf{H}}A = I$.

Definicija 7.8. Matrika $A \in \mathbb{R}^{n\times n}$ je ortogonalna, če velja $AA^\top = A^\top A = I$.

Opomba. Definirajmo $GL(V)$ kot množico obrnljivih linearnih preslikav $A : V \to V$. Potem je $GL(V)$ grupa za kompozitum – tej grupa pravimo splošna linearna grupa avtomorfizmov prostora V. Podobno definiramo $GL_n(\mathbb{F})$ za obrnljive matrike v $\mathbb{F}^{n\times n}$. Sedaj pa definirajmo še $U(V)$ kot množico vseh unitarnih preslikav $A : V \to V$. To je unitarna grupa in je podgrupa v $GL(V)$.

Trditev 7.12. *Za $A : V \to V$ so ekvivalentne naslednje trditve:*

1. *A je unitarna,*
2. *$\forall x, y \in V : \ \langle Ax, Ay\rangle = \langle x, y\rangle$ in*
3. *A je izometrija: $\forall x \in V : \ \|Ax\| = \|x\|$*

Dokaz. Dokažimo tretjo implikacijo ($3 \implies 1$). Naj bo $B = A^*A - I$. Očitno je $B^* = B$, torej je

B sebiadjungirana. Sedaj pa za poljuben $x \in V$ velja

$$\begin{aligned}\langle Bx, x\rangle &= \langle (A^*A - I)x, x\rangle \\ &= \langle A^*Ax, x\rangle - \langle x, x\rangle \\ &= \langle Ax, Ax\rangle - \langle x, x\rangle \\ &= \|Ax\|^2 - \|x\|^2 = 0.\end{aligned}$$

Ker je B sebiadjungirana in je za poljuben $x \in V$ $\langle Bx, x\rangle = 0$, je $B = 0$ in $AA^* = I$. □

Trditev 7.13. *Naj bo $A : V \to V$ unitarna preslikava in $\{v_1, \ldots, v_n\}$ ortonormirana baza prostora V. Potem je $\{Av_1, \ldots, Av_n\}$ ortonormirana baza V.*

Velja tudi obrat te trditve.

Trditev 7.14. *Naj bo $A : V \to V$ in $\{v_1, \ldots, v_n\}$ ortonormirana baza V. Denimo, da je tudi $\{Av_1, \ldots, Av_n\}$ ortonormirana baza V. Potem je A unitarna.*

Dokaz. Vzemimo poljuben $v \in V$. Vektor v lahko razvijemo po bazi $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$, kjer je $\alpha_i = \langle v, v_i\rangle$. Potem je:

- $\|v\|^2 = \langle v, v\rangle = \alpha_1\overline{\alpha_1} + \cdots + \alpha_n\overline{a_n}$,
- $\|Av\|^2 = \langle Av, Av\rangle = \alpha_1\overline{\alpha_1} + \cdots + \alpha_n\overline{a_n}\|v\|^2$.

Torej je A izometrija in je torej unitarna. □

Oglejmo si še lastne vrednosti unitarnih preslikav:

Izrek 7.15.

Naj bo $A : V \to V$ unitarna. Potem vse lastne vrednosti A ležijo na enotski krožnici v kompleksni ravnini.

Dokaz. Sledi direktno iz izometrije. □

Če si sedaj ogledamo še unitarne matrike ($A \in \mathbb{C}^{n\times n},\ AA^{\mathsf{H}} = I$), vidimo, da velja:

1. $A \in \mathbb{C}^{n\times n}$ je unitarna $\iff$ stolpci matrike A tvorijo ortonormirano bazo prostora $\mathbb{C}^n$ pri običajnem skalarnem produktu,
2. $A \in \mathbb{C}^{n\times n}$ je ortogonalna $\iff$ stolpci matrike A tvorijo ortonormirano bazo prostora $\mathbb{R}^n$ pri običajnem skalarnem produktu.

7.4 Unitarna podobnost matrik

Naj bo A $n \times n$ matrika nad $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Naj bo $\mathcal{B}$ ortonormirana baza prostor $\mathbb{F}^n$. Potem je $A = P_{\mathcal{SB}}A_{\mathcal{BB}}P_{\mathcal{SB}}$. Stolpci matrike $P_{\mathcal{SB}}$ so vektorji iz baze $\mathcal{B}$, torej je $P_{\mathcal{SB}}$ unitarna in velja $P_{\mathcal{BS}} = P_{\mathcal{SB}}^{-1} = P_{\mathcal{SB}}^{\mathsf{H}}$. Označimo $P = P_{\mathcal{SB}}$ in vidimo, da je $A = PBP^{\mathsf{H}}$.

Definicija 7.9. Naj bosta $A, B \in \mathbb{F}^{n\times n}$. Pravimo, da sta A in B unitarno podobni, če obstaja unitarna mtrika P, da je $A = PBP^{\mathsf{H}}$.

Trditev 7.16. *Relacija unitarne podobnosti matrik je ekvivalenčna relacija na $\mathbb{F}^{n\times n}$.*

Posledica 7.17. *Vsaka normalna matrika je unitarno podobna diagonalni matriki: če je A torej normalna, potem obstaja unitarna matrika P in diagonalna matrika D, da je $A = PDP^{\mathsf{H}}$.*

7.5 Pozitivno definitni endomorfizmi in matrike

Definicija 7.10. Naj bo $A : V \to V$ sebiadjungiran endomorfizem. Pravimo, da je A pozitivno definiten, če velja $\langle Av, v\rangle > 0$ za $\forall v \in V \setminus \{0\}$.

Opomba. Pozitiven semidefiniten endomorfizem definiramo podobno, le da je $\langle Av, v\rangle \geq 0$ za $\forall v \in V$. Podobna definicija velja tudi za kvadratne matrike.

Izrek 7.18.

Naj bo $A : V \to V$ sebiadjungiran endomorfizem. Potem je A pozitivno definiten natanko tedaj, ko so vse lastne vrednosti preslikave A pozitivne. Podobno velja, da je A pozitivno semidefiniten natanko tedaj, ko so vse lastne vrednosti A nenegativne.

Dokaz. ($\Rightarrow$) Naj bo A pozitivno definitna. Naj bo λ lastna vrednost in $v \in V$ pripadajoč lastni vektor: $Av = \lambda v$. Potem je $\langle Av, v\rangle > 0 \implies \lambda\langle v, v\rangle > 0$ in $\lambda > 0$.

($\Leftarrow$) Recimo, da so vse lastne vrednosti $\lambda_1, \ldots, \lambda_n$ preslikave A strogo pozitivne in $A = A^*$. Potem obstaja ortonormirana baza $\{v_1, \ldots, v_n\}$ lastnih vektorjev A, tako da je $Av_i = \lambda_i v_i$. Izberimo poljuben $v \in V \setminus \{0\}$ in ga razvijemo po bazi: $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$. Potem je $\langle Av, v\rangle = \lambda_1|\alpha_1|^2 + \cdots + \lambda_n|\alpha_n|^2 > 0$. □

Sedaj navedimo nekaj lastnosti pozitivno definitnih matrik. Naj bo $A \in \mathbb{F}^{n\times n}$ in $A^{\mathsf{H}} = A$. Recimo, da je A pozitivno definitna.

1. Vsi diagonalni elementi A so večji od 0.
2. $\det A > 0$.
3. Vse manjše kvadratne matrike znotraj A z robom v levem zgornjem kotu (označimo jih A_k) so tudi pozitivno definitne.
4. Če je A hermitska, je A pozitivno definitna natanko tedaj, ko za vse A_k velja $\det A_k > 0$.
5. Pozitivno definitnost lahko karakteriziramo tudi s pomočjo karakterističnega polinoma $p_A(\lambda) = a_n\lambda^n + \cdots + a_1\lambda + a_0$, kjer so ničle lastne vrednosti $\lambda_1, \ldots, \lambda_n$. Iz Vietovih formul sledi, potem velja $a_0 > 0,\ a_1 < 0,\ a_2 > 0, \ldots$

Izkaže se, da za zadnjo točko velja tudi obratna trditev.

Izrek 7.19.

Naj bo A hermitska matrika in $p_A(\lambda) = a_n\lambda^n + \cdots + a_1\lambda + a_0$ njen karakteristični polinom. A je pozitivno definitna natanko tedaj, ko je

$$a_0 > 0,\ a_1 < 0,\ a_2 > 0, \ldots$$

Dokaz. Dokažimo izrek v levo ($\Leftarrow$): naj velja $a_0 > 0,\ a_1 < 0,\ a_2 > 0, \ldots$. Ker je A hermitska, so njene lastne vrednosti realne. Izberimo poljubno realno število $\alpha \leq 0$. Potem je $a_i\alpha^i \geq 0$ za vse $i = 1, \ldots, n$ in $a_0 > 0$. Od tod sledi, da je $p_A(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 > 0$, torej so vse ničle polinoma (in hkrati lastne vrednosti) večje od 0. □

Opomba. Naj bo $A : V \to V$ sebiadjungirana. Potem preslikava $F : V \times V \to \mathbb{F}$ s predpisom $F(u, v) = \langle Au, v\rangle$ definira skalarni produkt na V natanko tedaj, ko je A pozitivno definitna (glej: vaje).

Definicija 7.11. Naj bo $A : V \to V$ sebiadjungiran endomorfizem. Pravimo, da je A negativno definiten, če velja $\langle Av, v\rangle < 0$ za $\forall v \in V \setminus \{0\}$.

Opomba. Negativno semidefiniten endomorfizem definiramo podobno, le da je $\langle Av, v\rangle \leq 0$ za $\forall v \in V$. Podobna definicija velja tudi za kvadratne matrike.

Trditev 7.20. *Endomorfizem $A : V \to V$ je negativno definiten natanko tedaj, ko je $-A$ pozitivno definiten.*

Od tod sledijo vse nadaljne lastnosti.

Izrek 7.21.

Naj bo $A : V \to V$ sebiadjungiran endomorfizem. Potem je A negativno definiten natanko tedaj, ko so vse lastne vrednosti preslikave A negativne. Podobno velja, da je A negativno semidefiniten natanko tedaj, ko so vse lastne vrednosti A nepozitivne.

Naj bo $A \in \mathbb{F}^{n\times n}$ in $A^{\mathsf{H}} = A$. Recimo, da je A negativno definitna.

1. Vsi diagonalni elementi A so manjši od 0.
2. $\det A > 0$.
3. Za vsak $k \leq n$ je matrika A_k negativno definitna.
4. Če je A hermitska, je A negativno definitna natanko tedaj, ko za vse A_k velja $\det A_k < 0$.

Izrek 7.22.

Naj bo A hermitska matrika in $p_A(\lambda) = a_n\lambda^n + \cdots + a_1\lambda + a_0$ njen karakteristični polinom. A je negativno definitna natanko tedaj, ko je

$$a_0 < 0,\ a_1 > 0,\ a_2 < 0, \ldots$$

8 Kvadratne forme

Vzemimo prostor $\mathbb{R}^n$ s standardnim skalarnim produktom.

Definicija 8.1. Naj bo $A \in \mathbb{R}^{n\times n}$ simetrična matrika (torej $A^\top = A$). Kvadratna forma, ki pripada matriki A, je preslikava $K : \mathbb{R}^n \to \mathbb{R}$ s predpisom $K(x) = \langle Ax, x\rangle$.

Zgled 8.1. *Oglejmo si splošen primer takšne kvadratne forme. Naj bo $A = [a_{ij}] \in \mathbb{R}^{n\times n}$, kjer velja $a_{ij} = a_{ji}$. Označimo standardno bazo prostora $\mathbb{R}^n$ kot $\{e_1, e_2, \ldots, e_n\}$. Sedaj vzemimo nek poljuben vektor $x \in \mathbb{R}^n$ in naj bo $x = (x_1, \ldots, x_n) = x_1e_1 + \cdots + x_ne_n$. Sedaj imamo*

$$\begin{aligned} K(x) = \langle Ax, x\rangle &= \langle A(x_1e_1 + \cdots + x_ne_n), x_1e_1 + \cdots + x_ne_n\rangle \\ &= \langle x_1Ae_1 + \cdots + x_nAe_n, x_1e_1 + \cdots + x_ne_n\rangle \\ &= \sum_{i,j=1}^{n} x_ix_j\langle Ae_i, e_j\rangle = \sum_{i,j=1}^{n} a_{ij}x_ix_j. \end{aligned}$$

Opomba. Splošna kvadratna forma je sestavljena iz čistih kvadratov x_i^2 in mešanih členov x_ix_j za $i \neq j$. Naš cilj bo spremeniti koordinate tako, da se znebimo mešanih členov.

Denimo, da imamo kvadratno formo $K : \mathbb{R}^n \to \mathbb{R}$ s predpisom $K(x) = \langle Ax, x\rangle$. A je simetrična matrika. Potem obstaja ortonormirana baza prostora $\mathbb{R}$, sestavljena iz lastnih vektorjev matrike A. Torej obstaja ortogonalna matrika P in diagonalna matrika D, da je $A = PDP^\top$. Potem velja

$$K(x) = \langle Ax, x\rangle = \langle PDP^\top x, x\rangle = \langle DP^\top x, P^\top x\rangle.$$

Tako dobimo kvadratno formo $\widetilde{K} : \mathbb{R}^n \to \mathbb{R}$ s predpisom $\widetilde{K}(y) = \langle Dy, y\rangle$. S spremembo koordinat $y = P^\top x$ dobimo (v novih koordinatah) kvadratno formo brez mešanih členov. P je ortogonalna matrika; njeni stolpci so ortonormirani lastni vektorji matrike A. Ker je Portogonalna, so osi v novem koordinatnem sistemu še vedno paroma pravokotne. Novi koordinatni sistem sestavljajo ortonormirani lastni vektorji A, tj. stolpci matrike P

Definicija 8.2. Naj bosta A, B simetrični matriki v $\mathbb{R}^{n\times n}$. Pravimo, da sta A in B kongruentni, če obstaja obrnljiva matrika P, da je $B = P^\top AP$.

Definicija 8.3. Kvadratni formi F in $\widetilde{F}$ sta kongruentni, če sta pripadajoči matriki kongruentni.

Opomba. Relacijo kongruence označimo s $B \overset{k}{\sim} A$ oziroma $\widetilde{F} \overset{k}{\sim} F$. Za to relacijo veljajo naslednje točke.

- Matrika P ni nujno ortogonalna.
- Relacija $\overset{k}{\sim}$ je ekvivalenčna relacija na množici vseh simetričnih $n \times n$ matrik.
- Vsaka simetrična matrika je kongruentna neki diagonalni matriki.
- Vsaka kvadratna forma je kongruentna neki kvadratni formi brez mešanih členov.

Izrek 8.1 (Sylvestrov izrek o vztrajnosti)**.**

Vsaka simetrična matrika je kongruentna matriki oblike

$$B = \begin{bmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & -1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & -1 & & & \\ & & & & & & 0 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 0 \end{bmatrix},$$

kjer je p število vrednosti 1 in q število vrednosti -1. Pri tem sta p in q neodvisna od izbire P iz definicije kongruentnosti, temveč sta enolično določena za vse matrike iz danega ekvivalenčnega razreda matrike glede na relacijo $\overset{k}{\sim}$.

Dokaz. Naj bo A $n \times n$ simetrična matrika. Vemo, da je $A = PDP^\top$, kjer je matrika

$$D = \begin{bmatrix} \lambda_1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & \lambda_p & & & & & & \\ & & & \lambda_{p+1} & & & & & \\ & & & & \ddots & & & & \\ & & & & & \lambda_{p+q} & & & \\ & & & & & & 0 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 0 \end{bmatrix}.$$

Pri tem so $\lambda_1, \ldots, \lambda_p$ pozitivne lastne vrednosti in $\lambda_{p+1}, \ldots, \lambda_{p+q}$ negativne lastne vrednosti. Sedaj naj bo

$$R = \begin{bmatrix} \sqrt{\lambda_1} & & & & & & & & \\ & \ddots & & & & & & & \\ & & \sqrt{\lambda_p} & & & & & & \\ & & & \sqrt{-\lambda_{p+1}} & & & & & \\ & & & & \ddots & & & & \\ & & & & & \sqrt{-\lambda_{p+q}} & & & \\ & & & & & & 1 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 1 \end{bmatrix}.$$

Opazimo, da je R obrnljiva in lahko zapišemo $D = RBR^\top$. Torej je $A \overset{k}{\sim} D$ in $D \overset{k}{\sim} B$, torej je zaradi tranzitivnosti tudi $A \overset{k}{\sim} B$.

Sedaj moramo dokazati še enoličnost p in q. Denimo torej, da je $A \overset{k}{\sim} B$ z vrednostima p, q in $A \overset{k}{\sim} C$ z vrednostima p', q'. Dokazujemo, da je $p = p'$ in $q = q'$. Dokazujemo s protislovjem. Brez škode za splošnost recimo, da je $p > p'$. Zaradi tranzitivnosti velja $B \overset{k}{\sim} C$, torej obstaja taka obrnljiva matrika P, da velja $B = P^\top CP$. Vzemimo podprostora $V_1 = Lin\{e_1, \ldots, e_p\}$ in

$V_2 = Lin\{P^{-1}e_p, \ldots, P^{-1}e_n\}$. Ker je $\dim V_1 + \dim V_2 = n+1$, mora veljati $\dim(V_1 \cap V_2) > 0$. Od tod sledi, da obstaja neničeln vektor $x \in V_1 \cap V_2$. Zapišimo

$$x = x_1e_1 + \cdots + x_pe_p = y_pP^{-1}e_p + \cdots + y_nP^{-1}e_n.$$

Potem velja $\langle Bx, x\rangle > 0$, po drugi strani pa

$$\langle Bx, x\rangle = \langle P^\top CPx, x\rangle = \langle CPx, Px\rangle < 0.$$

S predpostavko smo prišli v protislovje, torej mora veljati $p \le p'$. Zaradi simetrije je tudi $p' \le p$, torej velja $p = p'$. Ker je $\mathrm{rang}A = \mathrm{rang}B = \mathrm{rang}C$, velja $p + q = p' + q'$, torej je tudi $q = q'$. □

Posledica 8.2. *Vsaka kvadratna forma K je kongruentna kvadratni formi oblike*

$$\widetilde{K}(y) = y_1^2 + \cdots + y_p^2 - y_{p+1}^2 - \cdots - y_{p+q}^2.$$

Paru (p, q) pravimo signatura kvadratne forme K. Dve kvadratni formi sta kongruentni natanko tedaj, ko imata enaki signaturi.

Ugotovili smo že, da se lahko v kvadratni formi znebimo mešanih členov z uvedbo novih spremenljivk.

Zgled 8.2 (Lagrangeva metoda)**.** *Naj bo $K(x) = K(x_1, \ldots, x_n) = \sum_{i,j=1}^n a_{ij}x_ix_j$.*

- *Denimo, da obstaja i, da je $a_{ii} \neq 0$. Brez škode za splošnost naj bo kar $a_{11} \neq 0$. Potem je*

$$\begin{aligned} K(x_1, \ldots, x_n) &= a_{11}x_1^2 + 2a_{12}x_1x_2 + \cdots + 2a_{1n}x_1x_n + K_1(x_2, \ldots, x_n) \\ &= a_{11}\left(x_1^2 + 2\frac{a_{12}}{a_{11}}x_1x_2 + \cdots + 2\frac{a_{1n}}{a_{11}}x_1x_n\right) + K_1(x_2, \ldots, x_n) \\ &= a_{11}\left(x_1 + \frac{a_{12}}{a_{11}}x_2 + \cdots + \frac{a_{1n}}{a_{11}}x_n\right)^2 + \widetilde{K_1}(x_2, \ldots, x_n) \\ &= a_{11}y_1^2 + \widetilde{K_1}(x_2, \ldots, x_n). \end{aligned}$$

  Ta postopek rekurzivno nadaljujemo, doler ne dobimo izraz brez mešanih členov.
- *Denimo, da za vsak $i \le n$ velja $a_{ii} = 0$. Potem za vsak par različnih števil i, j, za katerega velja $a_{ij} \neq 0$, vpeljemo novi koordinati $y_i = x_i + x_j$ in $y_j = x_i - x_j$. Potem velja $2a_{ij}x_ix_j = \frac{a_{ij}}{2}(y_i^2 - y_j^2)$.*

8.1 Krivulje drugega reda

Definicija 8.4. Krivulja drugega reda je množica točk v $\mathbb{R}^2$, ki zadoščajo enačbi

$$ax^2 + 2bxy + cy^2 + dx + ey + f = 0,$$

kjer velja $a, b, c, d, e, f \in \mathbb{R}$.

Z diagonalizacijo se lahko v tej enačbi znebimo mešanih členov in tako v novih koordinatah dobimo enačbo

$$\lambda_1x^2 + \lambda_2y^2 + \delta x + \phi y + f = 0^4.$$

Potem lahko sistematično s premikom koordinat ugotovimo obliko krivulje, ki ustreza tej enačbi. Ta lahko opisuje stožnico (elipso, hiperbolo ali parabolo), premico, par premic, eno točko ali prazno množico. Izbiranje med temi možnostmi je trivialno.

[4] Koordinati x in y v tej enačbi se seveda razlikujeta od koordinat v začetni enačbi, vendar pa sta zaradi preglednosti napisani kot x, y in ne na primer x', y'.

8.2 Ploskve drugega reda

Definicija 8.5. Ploskev drugega reda je množica točk $(x, y, z) \in \mathbb{R}^3$, ki zadoščajo enačbi

$$ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz + gx + hy + iz + j = 0,$$

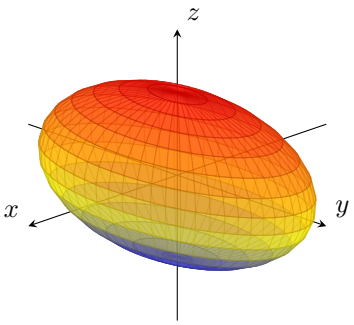
kjer so $a, \ldots, j \in \mathbb{R}$.

Kvadratni formi v enačbi priredimo simetrično matriko in z diagonalizacijo spremenimo koordinate. Tako dobimo enačbo

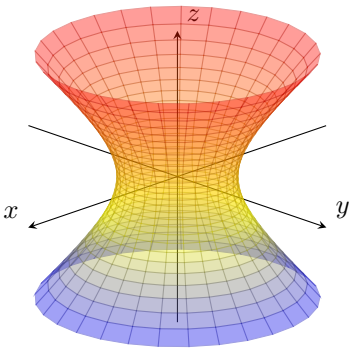
$$\lambda_1 x^2 + \lambda_2 y^2 + \lambda_3 z^2 + \alpha x + \beta y + \gamma z + j = 0.$$

Ponovno bomo obravnavali obliko ploskve, ki jo opiše ta enačba, glede na vrednosti koeficientov v njej.

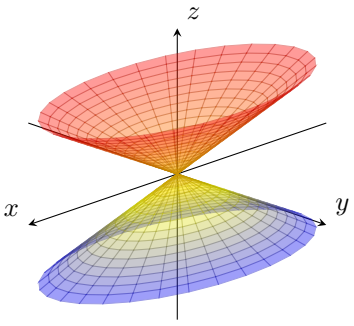
$\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} = 1$ Elipsoid

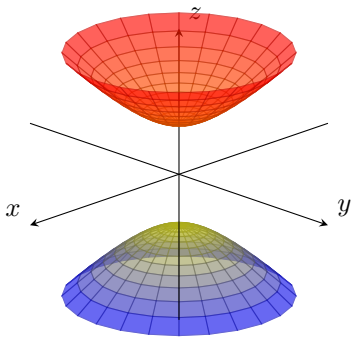
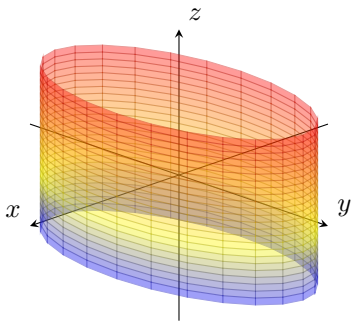
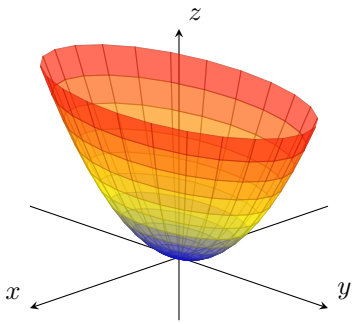
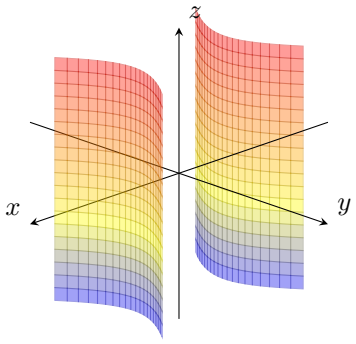


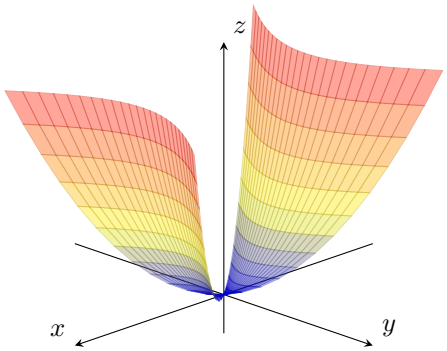
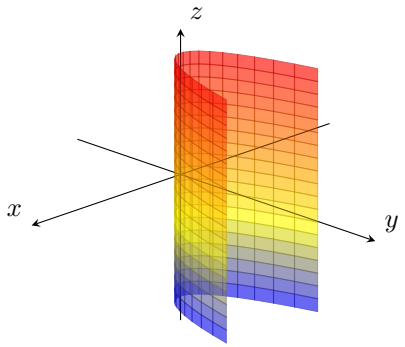
$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 1$ Enodelni eliptični hiperboloid



$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 0$ Eliptični stožec



$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = -1$	Dvodelni eliptični hiperboloid	
$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$	Eliptični valj	
$\frac{x^2}{a^2} + \frac{y^2}{b^2} = z$	Eliptični paraboloid	
$\frac{x^2}{a^2} - \frac{y^2}{b^2} = \pm 1$	Hiperbolični valj	

$\frac{x^2}{a^2} - \frac{y^2}{b^2} = \pm z$	Hiperbolični paraboloid	
$\frac{x^2}{a^2} = \pm y$	Parabolični valj	

Za zgled navedimo še nekaj primerov uporabe teorije za določanje vrste ploskve.

Zgled 8.3. *Kadar ima matrika A v kvadratni formi neničelne lastne vektorje, lahko hitro ugotovimo obliko ploskve s pomočjo lastnosti pozitivne definitnosti. Vzemimo enačbo $2x^2 + y^2 - 4xy - 4yz = 1$, ki ima matriko*

$$A = \begin{bmatrix} 2 & -2 & 0 \\ -2 & 1 & -2 \\ 0 & -2 & 0 \end{bmatrix}.$$

Potem velja:

- $\det A_1 = 2 > 0$
- $\det A_2 = \begin{vmatrix} 2 & -2 \\ -2 & 1 \end{vmatrix} = -2 < 0$
- $\det A = 2 \begin{vmatrix} 2 & 0 \\ -2 & -2 \end{vmatrix} = -8 < 0$

Ker velja $\det A < 0$, so bodisi vse lastne vrednosti A negativne bodisi je ena negativna in dve pozitivni. Če bi bile vse lastne vrednosti negativne, bi A bila negativno definitna in bi veljalo tudi $\det A_1 < 0$ in $\det A_2 < 0$. Ker to ni res, ima A eno negativno in dve pozitivni lastni vrednosti. Dana enačba torej predstavlja enodelni eliptični hiperboloid.

Zgled 8.4 (Uporaba Sylvestrovega izreka in Lagrangeve metode)**.** *Vzemimo enačbo $3x^2 + 2y^2 + 3z^2 - 2xy - 2yz - 2yz = 12$. Ta izraz lahko z Lagrangevo metodo napišemo kot kombinacijo*

kvadratov, in sicer $3(x-\frac{y}{3})^2+\frac{5}{3}(y-\frac{3}{5}z)^2+\frac{12}{5}z^2=12$. *Sedaj imamo*

$$D=\begin{bmatrix}3 & & \\ & \frac{5}{3} & \\ & & \frac{12}{5}\end{bmatrix},\quad P\begin{bmatrix}x\\y\\z\end{bmatrix}=\begin{bmatrix}x-\frac{y}{3}\\y-\frac{3}{5}z\\z\end{bmatrix},\quad P=\begin{bmatrix}1 & -\frac{1}{3} & 0\\0 & 1 & -\frac{3}{5}\\0 & 0 & 1\end{bmatrix},$$

kjer je matrika P *obrnljiva. Sedaj imamo* $\langle DP(x,y,z),P(x,y,z)\rangle=12$, *kar je ekvivalentno* $\langle P^\top DP(x,y,z),(x,y,z)\rangle=12$. *Ker je* D *kongruentna matriki identitete, je tudi* $P^\top DP$ *kongruentna matriki identitete. Zaradi enoličnosti so torej vse lastne vrednosti matrike* $P^\top DP$ *pozitivne in dana enačba predstavlja elipsoid.*