Univerza v Ljubljani

Fakulteta za matematiko in fiziko

Teorija iz predavanj predmeta

ALGEBRA 1

Maja Levak

Predavatelj
Doc. dr. Klemen Šivic

Študijsko leto 2018/2019

Kazalo

1 VEKTORSKI PROSTOR $\mathbb{R}^3$

1.1 Koordinatni sistem

Model na množico $\mathbb{R}$ je številska premica ali realna os.

Premica na danem koordinatnem sistemu: na premici izberemo točko 0 (izhodišče) in 1 (enota). Običajno je 1 desno od 0. Vsaki točki T na številski premici lahko priredimo neko realno število $x \in \mathbb{R}$. Če je T desno od 0, točki priredimo razdaljo te točke od izhodišča. Če je T levo od 0, priredimo nasprotno vrednost razdalje te točke od izhodišča. Izhodišču priredimo 0. Ta preslikava je bijekcija iz številske premice v množico $\mathbb{R}$, zato številsko premico identificiramo z realnimi števili.

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y); x, y \in \mathbb{R}\}$$
$$= \text{množica urejenih parov realnih števil.}$$

Model na $\mathbb{R}^2$ je ravnina z danim koordinatnim sistemom. Koordinatni sistem določata dve pravokotni številski premici, tako, da se sekata v izhodiščih obeh premic. Obe številski premici poimenujemo **koordinatni osi**. Običajno si enici izberemo desno od izhodišča in nad njim. Vodoravni osi rečemo **abscisna** ali x**-os**, navpični pa **ordinatna os** ali y**-os**. Tak koordinatni sistem imenujemo **pozitivno orientiran**. Če pozitivni poltrak x-osi zavrtimo za pozitivni kot 90 stopinj (v nasprotni smeri urinega kazalca), dobimo pozitivni poltrak.

Imenujemo poljubno točko v ravnini. Premica skozi T, vzporedna y-osi, seka x-os v natanko eni točki, ki ustreza natančno določenimu realnemu številu x. Podobno vodoravna premica. Skozi T seka y-os v natančno eni točki, ki ustreza natančno določenemu številu y. Točki T smo priredili urejen par (x, y). Preslikava, ki točki T priredi urejen par (x, y) je **bijekcija iz ravnine v** $\mathbb{R}^2$. Zato ravnino identificiramo z $\mathbb{R}^2$. Številoma x in y pravimo **koordinati** točke T in pišemo $T(x, y)$.

Razdalja med točkama $T_1(x_1, y_1)$ in $T_2(x_2, y_2)$:

$$d(T_1, T_2) = \sqrt[2]{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

Množica vseh urejenih trojic realnih števil:

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z); x, y, z \in \mathbb{R}\}$$

Model za $\mathbb{R}^3$ je prostor z danim koordinatnim sistemom. Sestavljajo ga tri pravokotne številske premice, ki se sekajo v eni točki, ki je izhodišče vseh treh številskih premic. Temu presečišču pravimo **koordinatno izhodišče**, številske premice pa so **koordinatne osi**: x-os, y-os, z-os.

Dogovor: uporabljamo pozitivno orientiran koordinatni sistem. Če iz enote na z-osi pogledamo na xy-ravnine (to je ravnina, določena z x-osjo in y-osjo), vidimo pozitivno orientiran koordinatni sistem v ravnini. Če x-os zavrtimo za pozitivni kot 90 stopinj, dobimo y-os.

Definirajmo preslikavo iz $\mathbb{R}$ v prostor. Točko T dobimo tako, da gremo od izhodišča po x-osi za x, po premici vzporedni y-osi za y in po premici vzporedni z-osi za z. Števila x, y, z v urejeni trojici (x, y, z) so enolično določene s točko T. Npr. z dobimo kot presečišče z-osi z ravnino skozi točko T, ki je vzporedna xy-ravnini. To pomeni, da je konstruirana preslikava, ki trojici (x, y, z) priredi točko T, bijekcija iz $\mathbb{R}$ v prostor. Prostor z danim koordinatnim sistemom zato identificiramo z $\mathbb{R}^3$. Pišemo $T(x, y, z)$ in številom x, y, z pravimo **koordinate** točke T.

Razdalja med $T_1(x_1, y_1, z_1)$ in $T_2(x_2, y_2, z_2)$:

$$d(T_1, T_2) = \sqrt[2]{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2}$$

Na $\mathbb{R}^3$ imamo dve operaciji:

- Seštevanje po komponentah:

$$(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 + z_2)$$

- Množenje s skalarji (notranja operacija):

$$\lambda \in \mathbb{R}, (x, y, z) \in \mathbb{R} \Rightarrow \lambda(x, y, z) = (\lambda x, \lambda y, \lambda z)$$

  Množenje s skalarji je definirano po komponentah.

1.2 Vektorji

V fiziki pogosto uporabljamo količine, ki imajo poleg velikosti tudi smer (hitrost, sila ...).

Definicija. *Naj bo $a = (x, y, z) \in \mathbb{R}$ poljubna točka.* ***Krajevni vektor*** *točke a je usmerjena daljica od koordinatnega izhodišča do točke a. Oznaka: $\vec{a} = (x, y, z)$.*

Koordinate krajevnega vektorja so enake koordinatam končne točke. Zato $\mathbb{R}^3$ lahko identificiramo z množico vseh krajevnih vektorjev v prostoru.

Definicija. ***Vektor*** *$\vec{a} = (x, y, z)$ je množica vseh usmerjenih daljic, ki jih dobimo z vzporednim premikom krajevnega vektorja $\vec{a} = (x, y, z)$.*

Opomba: Natančno bomo pogosto rekli, da je vektor usmerjena daljica. Dve usmerjeni daljici določata isti vektor, če sta vzporedni, enako dolgi in kažeta v isto smer. Nenatančno bomo usmerjeni daljici od točke A do točke B pogosto rekli kar **vektor** od A do B in jo označili z $\overrightarrow{AB}$. vsakemu krajevnemu vektorju ustreza natanko en vektor oz. vektor je enolično določen z ustreznim krajevnim vektorjem. Vemo pa, da je vsak krajevni vektor enolično določen s svojo končno točko in da lahko prostor identificiramo z množico $\mathbb{R}$. Geometrijski pomen množice $\mathbb{R}$ je množica vektorjev.

Na $\mathbb{R}^3$ smo definirali seštevanje in množenje s skalarji. Kako se to prenese na množico vektorjev?

- **Množenje s skalarjem**: Če je α pozitiven, je usmerjena daljica določena z vektorjem $\alpha\vec{a}$, vzporedno usmerjeni daljici, določeni z vektorjem a, ∞- krat daljša in kaže v isto smer. Če je α negativen, je usmerjena daljica, določena z vektorjem $\alpha\vec{a}$, vzporedna usmerjeni daljici, določeni z vektorjem $\vec{a}$, (-α)-krat daljša in kaže v nasprotno smer. Če vzamemo dve enako dolgi usmerjeni daljici, ki kažeta v isto smer, in ju pomnožimo z istim skalarjem, spet dobimo enako dolgi, vzporedno usmerjeni daljici, ki kažeta v isto smer. Zato je množenje vektorja s skalarjem dobro definirano. S skalarjem lahko množimo kjerkoli v prostoru.

- **Seštevanje**: Če imata vektorja $\vec{a_1}$ in $\vec{a_2}$ skupni začetek, vsaka $\vec{a_1} + \vec{a_2}$ poteka od skupnega začetka do četrtega oglišča paralelograma, določenega z usmerjenima daljicama $\vec{a_1}$ in $\vec{a_2}$. Če usmerjeni daljici, ki določata vektorja $\vec{a_1}$ in $\vec{a_2}$, vzporedno premaknemo, tako da imata skupni začetek, se tudi diagonala paralelograma vzporedno premakne. Zato je seštevanje vektorjev dobro definirano. Seštevamo lahko kjerkoli v prostoru.

Odštevanje vektorjev definiramo s predpisom: $\vec{a} - \vec{b} = \vec{a} + (-\vec{b})$. Vektorje odštevamo po komponentah.

- Vektor $\vec{O} = (0,0,0)$ imenujemo **ničelni vektor**. Določen je z vsako usmerjeno daljico, ki se začne in konča v isti točki.
- Vektor $-\vec{a} = (-x, -y, -z)$ imenujemo **nasprotni vektor** vektorja $\vec{a} = (x, y, z)$.
- Če je $\vec{a}$ določen z usmerjeno daljico od A do B, je $-\vec{a}$ določen z usmerjeno daljico od B do A. Pišemo: $-\overrightarrow{AB} = \overrightarrow{BA}$.

1.2.1 Lastnosti računanja z vektorji

- Komutativnost
- Asociativnost
- $\vec{O} + \vec{a} = \vec{a} + \vec{O} = \vec{a}$
- $\vec{a} + (-\vec{a}) = -\vec{a} + \vec{a} = \vec{O}$
- Distributivnost $(\alpha + \beta)\vec{a} = \alpha\vec{a} + \beta\vec{a}, \alpha(\vec{a} + \vec{b}) = \alpha\vec{a} + \alpha\vec{b}$
- $(\alpha\beta)\vec{a} = \alpha(\beta\vec{a})$
- $1 \cdot \vec{a} = \vec{a}$

Definicija. *Naj bodo $\vec{a_1}, \vec{a_2}, \vec{a_3}, \dots, \vec{a_n}$ poljubni vektorji. Vsak vektor oblike $\alpha_1\vec{a_1} + \alpha_2\vec{a_2} + \dots + \alpha_n\vec{a_n}$ kjer so $\alpha_1, \dots, \alpha_n \in \mathbb{R}$, imenujemo **linearna kombinacija** vektorjev $\vec{a_1}, \dots, \vec{a_n}$.*

Definicija. *Vektorji $\vec{a_1}, \dots, \vec{a_n}$ so **linearno odvisni** kadar lahko vsaj enega od njih izrazimo kot linearno kombinacijo ostalih. Vektorji so **linearno neodvisni**, kadar niso linearno odvisni (vektorji so torej linearno neodvisni, kadar nobenega od njih ne moremo izraziti kot linearno kombinacijo ostalih). En vektor je linearno odvisen, kadar je ničelni vektor. Dva vektorja $\vec{a}$ in $\vec{b}$ sta linearno odvisna, kadar je $\vec{a} = \alpha\vec{b}$ za nek $\alpha \in \mathbb{R}$ ali $\vec{b} = \beta\vec{a}$ za nek $\beta \in \mathbb{R}$.*

Vektorja $\vec{a}$ in $\vec{b}$ sta linearno odvisna natanko takrat, ko pripadajoča krajevna vektorja ležita na isti premici (sta kolinearna). Ekvivalentno, poljubni usmerjeni daljici, ki določata vektorja $\vec{a}$ in $\vec{b}$, sta vzporedni.

Naj bosta $\vec{a}$ in $\vec{b}$ linearno neodvisna krajevna vektorja. Vsak vektor oblike $\alpha\vec{a} + \beta\vec{b}$ leži v ravnini, ki jo določata $\vec{a}$ in $\vec{b}$. Velja tudi obratno: vsak vektor $\vec{c}$ na ravnini, določeni z $\vec{a}$ in $\vec{b}$, lahko zapišemo kot linearno kombinacijo $\vec{c} = \alpha\vec{a} + \beta\vec{b}$. Kako: premica, ki gre skozi konec $\vec{c}$-ja in je vzporedna vektorju $\vec{b}$, seka premico, določeno z vektorjem $\vec{a}$, v natančno eni točki, ki jo določa krajevni vektor $\alpha\vec{a}$ za nek $\alpha \in \mathbb{R}$. Podobno definiramo vektor $\beta\vec{b}$. Po definiciji seštevanja je $\vec{c} = \alpha\vec{a} + \beta\vec{b}$. Velja še več: α, β sta enolično določena s $\vec{c}$. Recemo, da je $\vec{c} = \alpha\vec{a} + \beta\vec{b}$ in $\vec{a'} \neq \vec{a}$ ali $\vec{b'} \neq \vec{b}$. Če je $\vec{a'} \neq \vec{a}$ je $\vec{a} = \frac{\beta'-\beta}{\alpha'-\alpha}\vec{b}$. Če je $\beta' \neq \beta$ pa je $\vec{b} = \frac{\alpha'-\alpha}{\beta'-\beta}\vec{a}$. V obeh primerih dobimo protislovje s tem, da sta $\vec{a}$ in $\vec{b}$ linearno neodvisna.

Ravnina, določena z linearno neodvisnima krajevnima vektorjema $\vec{a}$ in $\vec{b}$ je natanko množica vseh linearnih kombinacij $\alpha\vec{a} + \beta\vec{b}$, kjer sta $\alpha, \beta \in \mathbb{R}$.

Definicija. ***Baza ravnine*** *je množica, sestavljena iz dveh linearno neodvisnih vektorjev.*

Dokazali smo, da se da vsak vektor v ravnini na enoličen način zapisati kot linearni kombinaciji baznih elementov. Dokazali smo tudi, da so trije vektorji linearno odvisni natanko takrat, ko pripadajoči krajevni vektorji ležijo v isti ravnini.

Definicija. ***Baza prostora*** *je množica, sestavljena iz treh linearno neodvisnih vektorjev.*

Trditev. *Naj bo $\{\vec{a}, \vec{b}, \vec{c}\}$ baza prostora. Potem lahko vsak vektor $\vec{x} \in \mathbb{R}^3$ zapišemo kot linearno kombinacijo $\vec{x} = \alpha\vec{a} + \beta\vec{b} + \gamma\vec{c}$. Pri tem so α, β, γ enolično določeni z vektorjem $\vec{x}$.*

Trditev. *Vektorji $\vec{a}, \vec{b}, \vec{c}$ so linearno odvisni takrat, ko obstajajo $\alpha, \beta, \gamma \in \mathbb{R}$, ne vsi 0, da je $\alpha\vec{a} + \beta\vec{b} + \gamma\vec{c} = \vec{O}$. Vektorji $\vec{a}, \vec{b}, \vec{c}$ so torej linearno neodvisni, kadar velja sklep $\alpha\vec{a} + \beta\vec{b} + \gamma\vec{c} = \vec{O} \Rightarrow \alpha = \beta = \gamma = 0$ (oziroma edina linearna kombinacija, ki je 0, je tista, pri katerem so vsi koeficienti enaki 0, tj.* ***trivialna linearna kombinacija****).*

Definicija. ***Skalarni produkt*** *vektorjev $\vec{a_1} = (x_1, y_1, z_1)$ in $\vec{a_2} = (x_2, y_2, z_2)$ je število (skalar).*

$$\vec{a_1} \cdot \vec{a_2} = x_1x_2 + y_1y_2 + z_1z_2$$

Posledica. *Če je $\vec{a} = (x, y, z)$ potem je $x = \vec{a} \cdot \vec{i}, y = \vec{a} \cdot \vec{j}, z = \vec{a} \cdot \vec{k}$.*

Lastnosti skalarnega produkta:

- Komutativnost: $\vec{a} \cdot \vec{b} = \vec{b} \cdot \vec{a}$ za vsaka $\vec{a}, \vec{b} \in \mathbb{R}^2$
- Distributivnost: $\vec{a}(\vec{b} + \vec{c}) = \vec{a}\vec{b} + \vec{a}\vec{c}$ (in $(\vec{b} + \vec{c})\vec{a} = \vec{b}\vec{a} + \vec{c}\vec{a}$) za vse $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$
- Homogenost: $(\alpha\vec{a}) \cdot \vec{b} = \vec{a} \cdot (\alpha\vec{b}) = \alpha \cdot (\vec{a}\vec{b})$ za vse $\vec{a}, \vec{b} \in \mathbb{R}^2, \alpha \in \mathbb{R}$
- Pozitivna definitnost: $\vec{a} \cdot \vec{a} \geq 0$ za vsaka $\vec{a} \in \mathbb{R}^3$ in $\vec{a} \cdot \vec{a} = 0$ v primeru, ko je $\vec{a} = 0$.

Definicija. ***Dolžina*** *ali* ***normala vektorja*** $\vec{a}$ *je število* $||\vec{a}|| = |\vec{a}| = \sqrt{\vec{a} \cdot \vec{a}}$.

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

$$||\vec{a}|| = |\vec{a}| = \sqrt{\vec{a} \cdot \vec{a}} = \sqrt{x^2 + y^2 + z^2}$$

Običajno dobimo usmerjene daljice od $(0, 0, 0)$ do (x, y, z).

Izrek. $\vec{a} \cdot \vec{b} = |\vec{a}| \cdot |\vec{b}| \cdot cos\varphi$, *kjer je* φ *kot med usmerjenima daljicama, ki določata vektorja* $\vec{a}$ *in* $\vec{b}$ *in imata skupni začetek.*

Dogovor: Ničelni vektor je pravokoten na vsak vektor.

Posledica. *Če je* $\vec{a}$ *pravokoten na* $\vec{b}$, *potem velja, da je* $\vec{a} \cdot \vec{b} = 0$.

$$\vec{a} \perp \vec{b} \Rightarrow \vec{a} \cdot \vec{b} = 0$$

PRIMER:

- Ploščina trikotnika v ravnini $z = 0$.

  Imejmo vektorja $\vec{a_1} = (x_1, y_1, 0)$ in $\vec{a_2} = (x_2, y_2, 0)$. Zanima nas ploščina paralelograma, napetega na $\vec{a_1}$ in $\vec{a_2}$. Recimo, da par $(\vec{a_1}, \vec{a_2})$ pozitivno orientiran. Vektor $\vec{a_1}$ zavrtimo za 90 stopinj v pozitivni smeri in dobljeni vektor označimo z $\vec{a_1'}$.

  $$P = |\vec{a_1}| \cdot |\vec{a_2}| \cdot sin\varphi$$

  Če je par $(\vec{a_1}, \vec{a_2})$ negativno orientiran, dobimo

  $$P = -|\vec{a_1}| \cdot |\vec{a_2}| \cdot sin\varphi$$

  Naj bo Θ kot med vektorjema $\vec{a_2}$ in $\vec{a_1'}$. Potem je $\Theta = \frac{\pi}{2} - \varphi$, kadar je Θ med 0 stopinj in $\frac{\pi}{2}$, oziroma bo $\Theta = \varphi - \frac{\pi}{2}$, kadar bo φ med $\frac{\pi}{2}$ in π. V obeh primerih je $cos\Theta = cos(\frac{\pi}{2} - \varphi) = sin\varphi$.

  $$P = |\vec{a_1}| \cdot |\vec{a_2}| \cdot cos\Theta = |\vec{a_1'}| \cdot |\vec{a_2}| \cdot cos\Theta = \vec{a_1'} \cdot \vec{a_2}$$
  $$\vec{a_1} = |\vec{a_1}| \cdot (cos\delta, sin\delta)$$
  $$\vec{a_1'} = |\vec{a_1}|(cos(\delta + \frac{\pi}{2}), sin(\delta + \frac{\pi}{2}) = |\vec{a_1}|(-sin\delta, cos\delta) = (-y_1, x_1)$$
  $$\vec{a_1} = (x_1, y_1)$$
  $$P = (-y_1, x_1)(x_2, y_2) = -x_2 y_1 + x_1 y_2$$

Če je par $(\vec{a_1}, \vec{a_2})$ negativno orientiran, je $P = x_2y_1 - x_1y_2$.

Izraz $x_2y_1 - x_1y_2$ nam pove produkt ploščine in orientacije paralelograma, napetega na $\vec{a_1} = (x_1, y_1)$ in $\vec{a_2} = (x_2, y_2)$. Orientacija je $+1$, če je par (a_1, a_2) pozitivno orientiran, in je -1, če je negativno orientiran.

Izrazu $x_1y_2 - x_2y_1$ pravimo 2×2 **determinanta** in ga označimo:

$$\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}$$

Ugotovili smo, da bo determinanta enaka nič natanko takrat, kadar bosta vektorja (x_1, y_1) in (x_2, y_2) linearno odvisna.

1.3 Vektorski produkt

Motivacija: $\vec{M} = \vec{r} \times \vec{F}$. $|\vec{r}| \cdot |\vec{F}| \cdot sin\varphi$

Definicija. ***Vektorski produkt*** *vektorjev $\vec{a}$ in $\vec{b}$ je vektor $\vec{a} \times \vec{b}$ z naslednjimi lastnostmi:*

1. *$\vec{a} \times \vec{b} \perp \vec{a}$ in $\vec{a} \times \vec{b} \perp \vec{b}$*
2. *$|\vec{a} \times \vec{b}| = |\vec{a}| \cdot |\vec{b}| \cdot sin\varphi$ kjer je φ kot med usmerjenima daljicama, določenima z $\vec{a}$ in $\vec{b}$, ki imata skupen začetek (torej $|\vec{a} \times \vec{b}|$ je ploščina paralelograma, napetega na krajevna vektorja $\vec{a}$ in $\vec{b}$).*
3. *$(\vec{a}, \vec{b}, \vec{a} \times \vec{b})$ je pozitivno urejena trojica (to pomeni, če iz vrha $\vec{a} \times \vec{b}$ pogledamo na ravnino, določeno z $\vec{a}$ in $\vec{b}$, potem se $\vec{a}$ pri vrtenju za pozitiven kot med 0 in ϕ zavrti v večkratnik vetorja $\vec{b}$.*

Dogovor: Ničelni vektor je vzporeden vsakemu vektorju.

Posledica. $\vec{a} \times \vec{b} = 0 \Leftrightarrow \vec{a} || \vec{b}$

- Poiščimo formulo za vektorski produkt.

  $$\vec{a} = (a_1, a_2, a_3),\ \vec{b} = (b_1, b_2, b_3),\ \vec{a} \times \vec{b} = (c_1, c_2, c_3)$$

  Izračunajmo $\vec{c_3}$.

  $$\vec{c_3} = (\vec{a} \times \vec{b}) \cdot \vec{k}$$

  Naj bo ϑ kot med $\vec{a} \times \vec{b}$ in $\vec{k}$. Potem je

  $$\vec{c_3} = |\vec{a} \times \vec{b}| \cdot |\vec{k}| \cdot cos\vartheta$$

  (ta enačba predstavlja ploščino paralelograma napetega na $\vec{a}$ in $\vec{b}$).

  Vektorja $\vec{a}$ in $\vec{b}$ projiciramo na ravnino $z = 0$ in dobljena vektorja označimo z $\vec{a'}$ in $\vec{b'}$.

  Paralelogram, ki ga določata vektorja, ima oglišča $(0, 0, 0), (a_1, a_2, a_3), (b_1, b_2, b_3)$ in $(a_1 + b_1, a_2 + b_2, a_3 + b_3)$. Projekcije teh točk so $(0, 0, 0), (a_1, a_2, 0), (b_1, b_2, 0)$ in $(a_1 + b_1, a_2 + b_2, 0)$, ki spet tvorijo oglišča paralelograma. Zanima nas zveza med ploščinama paralelogramov $OBCA$ in $OB'C'A'$.

  ... nimam zapiskov ...

1.3.1 Lastnosti vektorskega produkta

1. Antikomutativnost: $\vec{a} \times \vec{b} = -\vec{b} \times \vec{a}$ za vsaka $\vec{a}, \vec{b} \in \mathbb{R}^3$

2. Distributivnost: $\vec{a} \times (\vec{b} + \vec{c}) = \vec{a} \times \vec{b} + \vec{a} \times \vec{c}$ in $(\vec{b} + \vec{c}) \times \vec{a} = \vec{b} \times \vec{a} + \vec{c} \times \vec{a}$ za vse $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$

3. Homogenost: $(\alpha\vec{a}) \times \vec{b} = \alpha(\vec{a} \times \vec{b})$ za vse $\vec{a}, \vec{b} \in \mathbb{R}^3$ in $\alpha \in \mathbb{R}$

1.4 Mešani produkt

Mešan produkt vektorjev $\vec{a}$, $\vec{b}$ in $\vec{c}$ je število $[\vec{a},\vec{b},\vec{c}] = (\vec{a}\times\vec{b})\cdot\vec{c}$.

$$\vec{a} = (a_1, a_2, a_3),\ \vec{b} = (b_1, b_2, b_3),\ \vec{a}\times\vec{b} = (c_1, c_2, c_3)$$

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

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

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

Geometrijska interpretacija: Paralelepiped je geometrijsko telo s tremi četvericami paroma vzporednih robov ("nagnjen kvader"). Določen je s tremi linearno neodvisnimi vektorji. Paralelepiped je poseben primer prizme, zato je $V = p\times v$.

Naj bo paralelepiped določen z vektorji $\vec{a},\vec{b},\vec{c}$ in naj bo φ kot med $\vec{c}$ in $\vec{a}\times\vec{b}$. φ je tudi kot med vektorjem $\vec{c}$ in višino.

$$v = |\vec{c}|\cdot cos\varphi$$

$$V = p\cdot v = |\vec{a}\times\vec{b}|\cdot|\vec{c}|\cdot|cos\varphi| = |(\vec{a}\times\vec{b})\cdot\vec{c}| = |[\vec{a},\vec{b},\vec{c}]|$$

Prostornina paralelepipeda je enaka absolutni vrednosti mešanega produkta. Predznak mešanega produkta nam pove orientacijo $[\vec{a},\vec{b},\vec{c}]\geq 0 \Leftrightarrow [\vec{a},\vec{b},\vec{c}]$ je pozitivno orientirana trojica ($\vec{c}$ "kaže gor" $\Leftrightarrow \varphi\in[0,\frac{\pi}{2}]$).

1.4.1 Lastnosti mešanega produkta

1. $[\vec{a}, \vec{b}, \vec{c}] = [\vec{b}, \vec{c}, \vec{a}] = -[\vec{a}, \vec{c}, \vec{b}]$ za vse $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$
2. Homogenost v vseh treh faktorjih: $\alpha[\vec{a}, \vec{b}, \vec{c}] = [\alpha\vec{a}, \vec{b}, \vec{c}] = [\vec{a}, \alpha\vec{b}, \vec{c}] = [\vec{a}, \vec{b}, \alpha\vec{c}]$
3. Distributivnost v vseh treh faktorjih

1.5 Dvojni vektorski produkt

$(\vec{a} \times \vec{b}) \times \vec{c} \perp \vec{a} \times \vec{b} \Rightarrow (\vec{a} \times \vec{b}) \times \vec{c}$ leži v ravnini, ki jo določata $\vec{a}$ in $\vec{b}$.

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

$(\vec{a} \times \vec{b}) \times \vec{c} \perp \vec{c} \Rightarrow (\alpha\vec{a} + \beta\vec{b}) \cdot \vec{c} = 0$

$\alpha\vec{a} \cdot \vec{c} = -\beta\vec{b} \cdot \vec{c}$

Če $\vec{c} \perp \vec{a}$ in $\vec{c} \perp \vec{b} \Rightarrow \vec{c} \,||\, \vec{a} \times \vec{b} \Rightarrow (\vec{a} \times \vec{b}) \times \vec{c} = \vec{O}$

Če $\vec{c} \not\perp \vec{a}$ ali $\vec{c} \not\perp \vec{b}$. $\exists\gamma: \;\; \alpha = \gamma(\vec{b} \cdot \vec{c}), \;\; \beta = -\gamma(\vec{a} \cdot \vec{c})$

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

Poračunamo npr. eno komponento in dobimo $\gamma = -1$.

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

$\vec{c}$ zamenjamo s $\vec{c} \times \vec{d}$:

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

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

$$(\vec{a} \times \vec{b}) \cdot (\vec{c} \times \vec{d}) = \begin{vmatrix} \vec{a}\vec{c} & \vec{a}\vec{d} \\ \vec{b}\vec{c} & \vec{b}\vec{d} \end{vmatrix}$$

Temu pravimo tudi **Lagrangeva identiteta**.

Poseben primer: $\vec{d} = \vec{b}$, $\vec{c} = \vec{a}$. Sledi $|\vec{a} \times \vec{b}^2| = |\vec{a}|^2 \cdot |\vec{b}|^2 - (\vec{a} \cdot \vec{b})^2$

2 ENAČBE PREMIC IN RAVNIN V $\mathbb{R}^3$

Imejmo ravnino Σ. Enačba ravnine Σ je taka enačba v spremenljivkah x, y, z, da velja:

- Točka $T(a, b, c)$ leži na ravnini Σ natanko tedaj, kadar trojica (a, b, c) zadošča enačbi.

Definicija. ***Normala ravnine*** *je vsak neničelni vektor, ki je pravokoten na ravnino.*

Več ravnin ima lahko isto normalo. Ravnine, ki imajo isto normalo, so **vzporedne**.

Ravnina je natančno določena s svojo normalo in eno točko na njej. Ta točka ni enolično določena z ravnino (lahko vzamemo poljubno točko). Tudi normala ni enolično določena (lahko jo pomnožimo s poljubnim neničelnim skalarjem).

- Imejmo ravnino Σ z normalno n in neko točko T_0 s krajevnim vektorjem $\vec{r_0}$ na njej. Iščemo enačbo ravnine Σ.

  Naj bo $\vec{r}$ krajevni vektor poljubne točke T.

  $$T \in \Sigma \Leftrightarrow T_0T = \vec{r} - \vec{r_0} \in \Sigma \Leftrightarrow \vec{r} - \vec{r_0} \perp (\vec{r} - \vec{r_0}) \cdot \vec{n} = 0$$

  $\vec{n}$ je vektor, ki je pravokoten na vse vektorje v ravnini.

  $(\vec{r} - \vec{r_0}) \cdot \vec{n} = 0$ je enačba ravnine Σ, ki ji pravimo **vektorska enačba ravnine**.

- Po komponentah

  $$((x, y, z) - (x_0, y_0, z_0)) \cdot (a, b, c) = 0$$
  $$ax - ax_0 + by - by_0 + cz - cz_0 = 0$$

  Označimo

  $$d = -ax_0 - by_0 - cz_0 = -n \cdot r_0$$

  (To je realno število, saj sta $\vec{r}$ in $\vec{r_0}$ znana).

  Dobili smo enačbo

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

- Vsako ravnino lahko zapišemo kot rešitev linearne enačbe

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

  Velja tudi obratno.

- Vsaka enačba oblike $ax + by + cz + d = 0$, kjer a, b, c, niso vsi 0, določa neko ravnino.

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

  Zaradi simetrije lahko predpostavimo, da je $a \neq 0$.
  Izberemo poljubna $y_0, z_0 \in \mathbb{R}$ in definirajmo $x_0 = \frac{by_0+cz_0+d}{a}$ in $r_0 = (x_0, y_0, z_0)$.

  Enačba ravnine z normalo n, ki poteka skozi točko s krajevnim vektorjem $\vec{r_o}$ je
  $$(\vec{r} - \vec{r_0}) \cdot \vec{n} = 0 \Leftrightarrow ax + by + cz = -a - \frac{by_0 + cz_0 + d}{a} + by_0 + cz_0$$

  To je naša prvotna enačba.

  Enačbi $ax + by + cz + d = 0$ po navadi rečemo **implicitna enačba ravnine**.

  Enačba ravnine ni enolično določena, ker si lahko izberemo drugo normalo ali drugo točko na ravnini. Določena je do množenja z neničelnim skalarjem natančno. Pogosto je ugodno, če ima normala dolžino 1. Zato normalo naravnamo tako, da namesto n vzamemo $\frac{n}{|\vec{n}|}$ kar je enotski vektor.
  $$|\vec{n}| = \sqrt{a^2 + b^2 + c^2}$$

  Dobimo enačbo
  $$\frac{ax}{\sqrt{a^2 + b^2 + c^2}} + \frac{by}{\sqrt{a^2 + b^2 + c^2}} + \frac{cz}{\sqrt{a^2 + b^2 + c^2}} + \frac{d}{\sqrt{a^2 + b^2 + c^2}} = 0$$

  Tej enačbi pravimo **normalna enačba ravnine**. Določena je do predznaka natančno.

2.1 Razdalja do ravnine

- Imejmo ravnino Σ z enačbo $(\vec{r} - \vec{r_0}) \cdot \vec{n} = 0$, kjer je $\vec{r_0} = (x_0, y_0, z_0)$ in $\vec{n} = (a, b, c)$ in točko T_1 s krajevnim vektorjem $\vec{r_1} = (x_1, y_1, z_1)$.

  Zanima nas razdalja med ravnino Σ in točko T_1.

  T_0 naj bo točka s krajevnim vektorjem $\vec{r_0}$.

  Naj bo $d = -\vec{n} \cdot \vec{r_0}$. Potem je $ax + by + cz + d = 0$ enačba ravnine.

  Naj bo Δ razdalja med T_1 in Σ.

  Naj bo φ kot med vektorjem $\overrightarrow{T_0T_1} = \vec{r_1} - \vec{r_0}$ in zveznico med T_1 in pravokotno projekcijo T_1 na Σ. Potem je $\Delta = |\vec{r_1} - \vec{r_0}| \cdot cos\varphi$.

  φ je tudi kot med $\vec{n}$ in $\vec{r_1} - \vec{r_0}$, če T_1 leži v istem polprostoru, ki ga določa ravnina Σ, kot kaže normala.

  Če je T_1 na drugi strani ravnine, je $T - \varphi$ kot med $\vec{n}$ in $\vec{r_1} - \vec{r_0}$.

  Če je T_1 na isti strani ravnine kot normala, je

  $$(\vec{r_1} - \vec{r_0}) \cdot \vec{n} = 0 = |\vec{n}| \cdot |\vec{r_1} - \vec{r_0}| \cdot cos\varphi$$

  Če je T_1 na drugi strani ravnine kot normala, pa je

  $$(\vec{r_1} - \vec{r_0}) \cdot \vec{n} = |\vec{n}| \cdot |\vec{r_1} - \vec{r_0}| \cdot cos(\pi - \varphi) = -|\vec{n}| \cdot |\vec{r_1} - \vec{r_0}| \cdot cos\varphi$$

  V vsakem primeru je

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

- Predznak skalarnega produkta $\vec{n} \cdot (\vec{r_1} - \vec{r_0})$ nam pove, na kateri strani ravnine leži točka T_1: Če je predznak pozitiven, T_1 leži na tisti strani, kamor kaže normala. Če pa je predznak negativen, potem točka T_1 leži na drugi strani.

- Po komponentah:

$$
\begin{aligned}
\frac{|\vec{n}\cdot(\vec{r_1}-\vec{r_0})|}{|\vec{n}|} &= \frac{|(a,b,c)\cdot(x_1-x_0,y_1-y_0,z_1-z_0)|}{\sqrt{a^2+b^2+c^2}} \\
&= \frac{|ax_1+by_1+cz_1-(ax_0+by_0+cz_0)|}{\sqrt{a^2+b^2+c^2}} \\
&= \frac{|ax_1+by_1+cz_1+d|}{\sqrt{a^2+b^2+c^2}}
\end{aligned}
$$

- Točka T_1 leži v ravnini $\Leftrightarrow \Sigma = 0$

  Razdalja med dvema ravninama je najkrajša razdalja med točko na prvi ravnini in točko na drugi ravnini. Če se ravnini sekata, je ta razdalja enaka nič. Če sta ravnini vzporedni, pa je razdalja med njima enaka razdalji med poljubno točko na prvi ravnini in drugo ravnino.

  Razdalja med ravnino in premico, ki jo seka, je enaka 0.

  Razdalja med ravnino in njej vzporedno premico pa je enaka razdalji med poljubno točko na premici in ravnino.

2.2 Enačba premice

Premico lahko gledamo kot presek dveh ravnin. Enačba premice p bo zato sistem dveh linearnih enačb v spremenljivkah x, y, z tako, da velja: točka $T(a, b, c,)$ leži na premici $p \Leftrightarrow$ trojica (a, b, c) ustreza obema enačbama.

Definicija. ***Smerni vektor premice*** *p je vsak neničelni vektor, ki je vzporeden premici p.*

Premica je enolično določena z nekim svojim smernim vektorjem in neko točko na njej.

Smerni vektor ni enolično določen s premico, ampak ga lahko pomnožimo s poljubnim neničelnim skalarjem.

- Naj bo p premica s smernim vektorjem $\vec{s}$ in točko T_0 na njej. $\vec{s} = (a, b, c)$, točka T_0 pa naj ima krajevni vektor $\vec{r_0} = (x_0, y_0, z_0)$. Naj bo $\vec{r} = (x, y, z)$ krajevni vektor poljubne točke T. Enačba premice p bo tako enačba, ki bo veljala natanko tedaj, kadar bo točka T_0 ležala na premici p.

  $$T \in p \Leftrightarrow \overrightarrow{T_0T} \mid\mid \vec{s} \Leftrightarrow \overrightarrow{T_0T} = \vec{r} - \vec{r_0} = \lambda\vec{s},\ \lambda \in \mathbb{R}$$

  $\vec{r} = \vec{r_0} + \lambda\vec{s},\ \lambda \in \mathbb{R}$ je **vektorska parametrična enačba premice**.

- Po komponentah

  $$(x, y, z) = (x_0, y_0, z_0) + \lambda(a, b, c)$$

  $$x = x_0 + \lambda a$$
  $$y = y_0 + \lambda b$$
  $$z = z_0 + \lambda c$$

  To je **parametrična enačba premice** (λ je parameter).

- Znebimo se parametra. Če je $abc \neq 0$, je $\lambda = \frac{x-x_0}{a} = \frac{y-y_0}{b} = \frac{z-z_0}{c}$

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

  To je **enačba premice**.

- Če je npr. $a = 0$ in $bc \neq 0$, je $x = x_0$ in $\lambda = \frac{y-y_0}{b} = \frac{z-z_0}{c}$. V tem primeru je enačba premice: $x = x_0, \frac{y-y_0}{b} = \frac{z-z_0}{c}$. Če je npr. $a = b$, je $c \neq 0$ in je enačba premice enaka $x = x_0, y = y_0$.

  Premica je enolično določena z dvema točkama na njej.

- Naj bosta A in B točki na premici p in naj bosta $\vec{r_A}$ in $\vec{r_B}$ njuna krajevna vektorja. Za točko na premici si lahko vzamemo A, za smerni vektor pa $\overrightarrow{AB} = \vec{r_B} - \vec{r_A}$. **Vektorska enačba premice** je torej

$$\vec{r} = \vec{r_A} + \lambda(\vec{r_B} - \vec{r_A}),\ \ \lambda \in \mathbb{R}$$

2.3 Razdalja do premice

- Imejmo premico p z enačbo $\vec{r} = \vec{r_0} + \lambda\vec{s},\ \lambda \in \mathbb{R}$, kjer je $\vec{r_0} = (x_0, y_0, z_0)$ in $\vec{s} = (a, b, c)$.

  Naj bo T_1 poljubna točka s krajevnim vektorjem $\vec{r_1} = (x_1, y_1, z_1)$. Zanima nas razdalja Δ med točko T_1 in premico p.

  Najbližja točka točki T_1, ki leži na premici p, je pravokotna projekcija točki T_1 na p.

  Naj bo φ kot med vektorjema $\vec{s}$ in $\overrightarrow{T_0T_1} = (\vec{r_1} - \vec{r_0})$.

$$\Delta = |\overrightarrow{T_0T_1}| \cdot sin\varphi \quad (= |\overrightarrow{T_0T_1}| \cdot sin(\pi - \varphi))$$

  Vemo, da je $|\vec{s} \times (\vec{r_1} - \vec{r_0})| = |\vec{s}| \cdot |\vec{r_1} - \vec{r_0}| \cdot sin\varphi$

$$\Delta = |\vec{r_1} - \vec{r_0}| \cdot sin\varphi = \frac{|\vec{s} \times (\vec{r_1} - \vec{r_0})|}{|\vec{s}|}$$

  PRIMER:

  - *Izračunaj razdaljo med točko* $A(1, 1, 1)$ *in premico z enačbo* $\frac{x}{2} = y + 12 = z = 1$

    1. $\vec{r_1} = (1, 1, 1)$, $\vec{r_0} = (0, -1, -1)$, $\vec{s} = (2, -2, 1)$
    2. $\vec{r_1} - \vec{r_0} = (1, 2, 2)$
    3. $\vec{s} \times (\vec{r_1} - \vec{r_0}) = (-6, -3, 6)$
    4. $\Delta = 3$

    Če se premici sekiata, je razdalja med njima enaka 0. Če sta premici vzporedni, je razdalja med njima enaka razdalji me poljubno točko na prvi premici in drugo premico.

2.4 Razdalja med mimobežnima premicama

- Imejmo premici p_1 in p_2 z enačbama $\vec{r} = \vec{r_1} + \lambda \vec{s_1},\ \lambda \in \mathbb{R}$ in $\vec{r} = \vec{r_2} + \lambda \vec{s_2},\ \lambda \in \mathbb{R}$.

  Predpostavimo, da $\vec{s_1}$ ni vzporedna z $\vec{s_2}$.

  T_1 naj bo točka s krajevnim vektorjem $\vec{r_1}$, T_2 pa točka s krajevnim vektorjem $\vec{r_2}$. Δ naj bo razdalja med p_1 in p_2 (najboljša razdalja med neko točko iz p_1 in neko točko iz p_2).

  q_2 naj bo premica skozi T_2, ki je vzporedna p_1, q_1 pa naj bo premica skozi T_1, ki je vzporedna p_1.

  Premici p_1 in q_1 določata ravnino Σ_1, premici p_2 in q_2 pa ravnino Σ_2. Ravnini sta vzporedni, saj obe vsebujeta nekolinearna vektorja $\vec{s_1}$ in $\vec{s_2}$.

  $p_1 \in \Sigma_1, p_2 \in \Sigma_2 \Rightarrow \Delta$ je večja ali enaka razdalji med ravninama Σ_1 in Σ_2 (minimum po večji množici je manjši ali enak minimumu po manjši množici).

  Q_1 naj bo presečišče p_1 in pravokotne projekcije p_2 na ravnino Σ_1.
  Q_2 pa naj bo presečišče p_2 in pravokotne projekcije p_1 na ravnino Σ_2.

$$
\begin{gathered}
|\overrightarrow{Q_1 Q_2}| \geq \Delta,\ \textit{po konstrukciji pa je}\ |\overrightarrow{Q_1 Q_2}| = d(\Sigma_1, \Sigma_2) \\
\Delta \leq |\overrightarrow{Q_1 Q_2}| = d(\Sigma_1, \Sigma_2) \leq d(\Sigma_1, \Sigma_2) \leq \Delta \Rightarrow \\
\Delta = |\overrightarrow{Q_1 Q_2}| = d(\Sigma_1, \Sigma_2) = d(T_2, \Sigma_1)
\end{gathered}
$$

  Za normalo na ravnino Σ_1 lahko vzamemo vektorski produkt $\vec{s_1} \times \vec{s_2}$.

  Torej je:

$$
\Delta = \frac{|(\vec{r_2} - \vec{r_1}) \cdot (\vec{s_1} \times \vec{s_2})|}{|\vec{s_1} \times \vec{s_2}|} = \frac{|[\vec{r_2} - \vec{r_1}, \vec{s_1}, \vec{s_2}]|}{|\vec{s_1} \times \vec{s_2}|}
$$

  Premici p_1 in p_2 se sekata $\Leftrightarrow [\vec{r_2} - \vec{r_1}, \vec{s_1}, \vec{s_2}] = 0$.

3 OSNOVNE ALGEBRSKE STRUKTURE

3.1 Ponovitev preslikav

Preslikava $f : A \to B$ je predpis, ki vsakemu elementu množice A priredi natanko en element množice B. Elementu $a \in A$ priredimo element iz B, ki ga označimo z $f(a)$ in ga imenujemo **slika elementa** a.

Preslikavo preprosto imenujemo tudi funkcija, predvsem v primerih, če je B množica števil. Množico A imenujemo **domena** ali **definicijsko območje** preslikave, množico B pa **kodomena** ali **zaloga vrednosti** preslikave.

Zaloga vrednosti preslikave $f : A \to B$ je množica $Z_f = \{f(x), x \in A\}$
Preslikavo določajo domena, kodomena in funkcijski predpis.

Če imata dve preslikavi isti predpis, domeni ali kodomeni pa sta različni, sta preslikavi različni.

Naj bo $C \subseteq A$ in $D \subseteq B$ in predpostavimo, da je $f(x) \in D$ za nek $x \in C$. Potem lahko definiramo preslikavo $g : C \to D$ s predpisom $g(x) = f(x)$ za $x \in C$. Preslikavi g, določeni s tem predpisom, pravimo **zožitev preslikave** f **na množico** C in pišemo $g = f|_c$. Namesto $f|_c$ bomo mogoče včasih pisali kar f in takrat bo moralo biti iz konteksta jasno, da gre za zožitev. Preslikavi f pravimo **razširitev preslikave** g.

Preslikava $f : A \to B$ je **surjektivna**, kadar je $Z_f = B$. To pomeni, da je vsak element množice B slika nekega elementa iz A.

Preslikava $f : A \to B$ je **injektivna**, kadar za vsaka različna elementa $x, y \in A$ velja $f(x) \neq f(y)$. Ekvivalentno, f je injektivna, kadar velja implikacija $x, y \in A. f(x) = f(y) \Rightarrow x = y$.

Preslikava $f : A \to B$ je **bijektivna**, kadar je surjektivna in injektivna hkrati.

Množici A in B imata **isto moč**, kadar obstaja bijektivna preslikava med njima.

Če je preslikava $f : A \to B$ bijektivna, potem za vsak $y \in B$ obstaja enoličen $x \in A$, da je $f(x) = y$. Preslikava $G : B \to A$, definirana s predpisom $g(y) =$ tisti $x \in A$, za katerega je $f(x) = y$, se imenujemo **inverzna preslikava** preslikave f. Oznaka: f^{-1}. f^{-1} je bijektivna.

Naj bo $C \subseteq B$. Množico $f^{-1}(C) = \{x \in A; f(x) \in C\}$ imenujemo **praslika množice** C.

$$f^{-1}(C) \subseteq A$$

Če je $C = \{y\}$, potem pišemo $f^{-1}(y)$ namesto $f^{-1}(\{y\})$ in tej množici rečemo **praslika elementa** y. Oznaka $f^{-1}(y)$ ne pomeni, da ima preslikava inverz.

Oznaka za sliko množice $C \subseteq A$: $f(C) = \{f(x), x \in C\} \subseteq B$

Kompozitum preslikav $f : A \to B$ in $g : B \to C$ je preslikava $g \circ f : A \to C$ definirana s predpisom $(g \circ f)(x) = g(f(x))$ za vsak $x \in A$. Ekvivalentno, to je tista preslikava $g \circ f : A \to C$, za katero komutira diagram (če gremo na katerikoli način v smeri puščic, dobimo isti rezultat).

Identiteta množice A je preslikava $id_A : A \to A$, definirana s predpisom $id_A(x) = x$ za vsak $x \in A$.

- $f : A \to B \Rightarrow id_B \circ f, f \circ id_A = f$
- Če je $f : A \to B$ bijektivna, potem je $f \circ f^{-1} = id_B, f^{-1} \circ f = id_A$

Trditev. *Naj bosta $f : A \to B$ in $g : B \to C$ preslikavi. Potem velja:*

1) Če sta f in g injektivni, je $g \circ f$ injektiven

2) Če sta f in g surjektivni, je $g \circ f$ surjektiven

3) Če sta f in g bijektivni, je $g \circ f$ bijektiven in $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

4) Če je $g \circ f$ injektivna, je f injektivna

5) Če je $g \circ f$ surjektivna, je g surjektivna

Posledica. *$f : A \to B$ je bijektivna preslikava z inverzom $g : B \to A \Leftrightarrow f \circ g = id_B$ in $g \circ f = id_A$. V tem primeru je $g = f$.*

Graf preslikave $f : A \to B$ je množica $\Gamma(f) = \{(x, f(x)).x \in A\} \subseteq A \times B\}$

3.2 Operacije

Operacija na množici A je preslikava $A \times A \to A$, kjer $(x, y) \mapsto x \cdot y$. Natančneje, to je **dvočlena** (ali binarna) **notranja** operacija. Element $x \circ y$ običajno imenujemo **kompozitum elementov** x in y.

PRIMERI:

1. $(\mathbb{N}, \circ)$ je množenje ali seštevanje. Odštevanje ni operacija na $\mathbb{N}$. Na primer $1-2=-1$ ni element naravnih števil.
2. $(\mathbb{R}, \circ)$ je množenje ali seštevanje ali odštevanje. Deljenje ni operacija na $\mathbb{R}$. $\frac{1}{0}$ ni realno število.
3. $(\mathbb{R}^3, \circ)$ je seštevanje vektorjev ali vektorski produkt. Skalarni produkt ni operacija na $\mathbb{R}$, ker rezultat ni vektor.
4. Naj bo A neprazna množica in $F(A)$ množica vseh preslikav $A \to A$. Na $F(A)$ lahko definiramo operacijo $(f \circ g) \mapsto f \circ g$ običajen kompozitum preslikav $(f \circ g)(x) = f(g(x))$ za vsak $x \in A$

n-člena (ali n**-terna**) operacija na množici A je preslikava

$$\underbrace{A \times A \times A \times ... \times A}_{n} \to A$$

Preslikava $A \to A$ je **enočlena** operacija.

PRIMERI:

- Naslednik je enočlena operacija na $\mathbb{N}$.
- Nasprotno število je enočlena operacija na $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
- $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \ (a, b, c) \mapsto ab + c$ je tročlena operacija.
- Težišče treh točk v ravnini je tročlena operacija na $\mathbb{R}^2$.

Naj bosta A in R dve množici. **Zunanja** (linearna) **operacija** na množici A je preslikava $R \times A \to A$.

PRIMER:

- Množenje vektorja s skalarjem je preslikava

$$\begin{aligned} \mathbb{R} \times \mathbb{R} &\to \mathbb{R}^3 \\ (\alpha, \vec{x}) &\mapsto \alpha\vec{x} \end{aligned}$$

  Torej je to zunanja binarna operacija na $\mathbb{R}^3$.

Če je na množici A definirana vsaj ena notranja zunanja operacija, pravimo, da ima množica A **algebraično strukturo**.

Obravnavali bomo samo linearne operacije, najprej notranje, nato pa tudi zunanje.

Nekatere lastnosti operacij:

- Operacija $\circ$ na množici A je **asociativna**, kadar velja $(a \circ b) \circ c = a \circ (b \circ c)$, $\forall a, b, c \in A$
- Če je operacija asociativna, ima izraz $a \circ b \circ c$ smisel, saj ni odvisen od tega, kako postavimo oklepaje.

Trditev. *Če je operacija $\circ$ na množici A asociativna, potem je izraz $a_1 \circ a_2 \circ ... \circ a_n$, kjer so $a_1, ..., a_n \in A$, neodvisen od tega, kako postavimo oklepaje.*

Brez dokaza, lahko bi dokazali z indukcijo na n.

Posledica. *Če je operacija $\circ$ asociativna, je izraz $a_1 \circ a_2 \circ ... \circ a_n$ dobro definiran.*

Pri asociativnih operacijah oklepaje po navadi izpuščamo.

Operacija na množici A je **komutativna** kadar velja $a \circ b = b \circ a$, $\forall a, b \in A$. Če za elementa a in b velja $a \circ b = b \circ a$, pravimo, da elementa komutirata.

PRIMERI:

- Seštevanje in množenje števil sta komutativni in asociativni operaciji.
- Odštevanje ni komutativno in ni asociativno.

$$(a - (b - c) \neq (a - b) - c)$$

- Vektorski produkt ni komutativen in ni asociativen.

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

- Komponiranje funkcij je asociativno in v splošnem ni komutativno.

Naj bo $\circ$ operacija na množici A. Element $e \in A$ se imenuje **enota** ali **nevtralni element**, kadar velja $e \circ a = a \circ e = a$, $\forall a \in A$. Splošneje, če velja $e \circ a = a$, $\forall a \in A$, elementu e pravimo **leva enota**, če velja $a \circ e = a$, $\forall a \in A$, pa elementu e pravimo **desna enota**

PRIMERI:

- $(\mathbb{R}, +):\ 0$ je enota
- $(\mathbb{R}^3, \times)$: ni enote
- $(\mathbb{R}, \cdot):\ 1$ je enota
- $(F(A), \circ):\ id_A$ je enota
- $(\mathbb{C} \times \mathbb{C} \to \mathbb{C},\ (z, w) \mapsto z|w|$ vsako število po absolutni vrednosti enako 1, je desna enota.

Trditev. *Če obstajata leva enota e in desna enota f, potem sta enaki in $e = f$ je obojestranska enota.*

Dokaz. $e = ef = f$ (f je desna enota, e je leva enota)

□

Posledica. *Če obstaja (obojestranska) enota, je ena sama.*

Naj bo $\circ$ operacija na množici A, ki ima enoto $e \in A$. Naj bo $a \in A$. Če obstaja element $a \in A$, da je $a \circ a' = e$, potem elementu a' pravimo **desni inverz** elementa a. Če obstaja element $a'' \in A$, da je $a'' \circ a = e$, potem elementu a'' pravimo **levi inverz** elementa a. Če obstaja element $a''' \in A$, ki je hkrati levi in desni inverz elementa a, mu pravimo **inverz** elementa a in ga označimo z a^{-1}.

PRIMERI:

- $(\mathbb{R}, +):\ -a$ je inverz od a
- $(\mathbb{R}, \cdot):\ \frac{1}{a}$ je inverz od a, obstaja le za $a \neq 0$
- $F(A)$: inverzi v splošnem ne obstajajo, $f \in F(A)$ ima inverz natanko tedaj, kadar je f bijektivna (in inverz je v tem primeru običajen inverz funkcije)

Trditev. *Naj bo $\circ$ asociativna operacija in naj bo a' levi inverz elementa a, a'' pa naj bo desni inverz elementa a. Potem je $a'' = a'$ in to je inverz elementa a.*

Dokaz. $a' = a' \circ e = a' \circ (a \circ a'') = (a' \circ a) \circ a'' = e \circ a'' = a''$

□

Posledica. *Če je $\circ$ asociativna operacija na množici A in obstaja inverz elementa $a \in A$, potem je ta inverz en sam.*

3.3 Grupe

Grupoid je neprazna množica z notranjo binarno operacijo.

Grupoid, v katerem je operacija asociativna, se imenuje **polgrupa**.

Monoid je polgrupa, v kateri obstaja enota za operacijo.

Grupoid, polgrupa, monoid so določeni z množico A in opracijo $\circ$ na njej. Pišemo $(A, \circ)$. Če bo jasno, za katero operacijo gre, bomo pogosto namesto $(A, \circ)$ pisali kar A.

PRIMERI:

- $(\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ so polgrupe. Razen $(\mathbb{N}, +)$ so tudi monoidi, enota je 0
- $(\mathbb{N}, \cdot), (\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$ so monoidi z enoto 1
- $(\mathbb{Z}, -)$ je samo grupoid, enako $(\mathbb{R}^3, \times)$
- $(F(A), \cdot)$ je monoid z enoto id_A

Trditev. *Naj bo $(A, \circ)$ monoid z enoto e in naj bosta $a, b \in A$ obrnljiva elementa. Potem je element $a \circ b$ tudi obrnljiv in velja $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.*

Obrnljiv element monoida je element, ki ima inverz.

Dokaz.

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

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

Dokazali smo, da je $b^{-1} \circ a^{-1}$ res inverz elementa $a \circ b$.

Definicija. ***Grupa*** *je monoid, v katerem je vsak element obrnljiv.*

Množica G z operacijo $\circ$ je torej grupa, kadar:

1. Asociativnost: $(a \circ b) \circ c = a \circ (b \circ c),\ \forall a, b, c \in G$
2. Obstaja (enoličen element) $e \in G$ (enota), da je $a \circ a = e \circ a = a,\ \forall a \in G$
3. Za vsak $a \in G$ obstaja (enoličen) element $a^{-1} \in G$, da je $a \circ a^{-1} = a^{-1} \circ a = e$. Pri tem je a^{-1} inverz elementa a.

PRIMERI:

- $(\mathbb{C}, +), (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ so grupe, enota je 0, inverz elementa a je $-a$
- $(\mathbb{C}, \cdot), (\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$ niso grupe, ker 0 nima inverza
- $(\mathbb{C}\backslash\{0\}, \cdot), (\mathbb{Q}\backslash\{0\}, \cdot), (\mathbb{R}\backslash\{0\}, \cdot)$ so grupe, enota je 1, inverz od a je $\frac{1}{a}$
- $(\mathbb{Z}\backslash\{0\}, \cdot)$ ni grupa, ker npr. $\frac{1}{2} \notin \mathbb{Z}$
- Naj bo $A \neq \emptyset$ neprazna množica in $F(A)$ množica preslikav $A \to A$. Ali je $(F(A), \circ)$ grupa?

  Če ima A vsaj 2 elementa, $F(A)$ ni grupa. Naj bo $a \in A$ poljuben element in $f : A \to A$ preslikava, definirana s predpisom $f(x) = a$ za vsak $x \in A$. Dokažemo, da f ni obrnljiv v $F(A)$.

  Recimo, da obstaja $g \in F(A)$, da je $g \circ f = f \circ g = id_A$

  $$f \circ g = id_A$$

  $$f(g(x)) = x,\ \forall x \in A$$
  $$a = x,\ \forall x \in A$$

  To je protislovje, saj ima A vsaj 2 elementa. Torej $F(A)$ ni grupa.

- $A \neq \emptyset$. S $S(A)$ označimo množico vseh bijektivnih preslikav $A \to A$.

  Vemo, da je kompozitum bijekcij bijekcija, zato je $\circ$ notranja operacija na $S(A)$. Vemo tudi, da je kompozitum asociativen, id_A je enota za $\circ$, za inverzno preslikavo f^{-1} pa velja $f \circ f^{-1} = f^{-1} \circ f = id_A$ in $f^{-1} \in S(A)$. Torej je f^{-1} inverz elementa $f \in S(A) \Rightarrow S(A)$ je grupa.

V grupi običajno namesto $a \circ b$ pišemo kar $a \cdot b$ ali ab in operaciji rečemo *produkt*. Definiramo tudi $a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n}$, če je $n \in \mathbb{N}$ in $a \in G, a^0 = e,\ a^{-n} = (a^{-1})^n,\ \forall n \in \mathbb{N},\ a \in G$. Namesto e običajno pišemo kar 1.

Pravimo, da uporabljamo *multiplikativni zapis operacije* ($\cdot$ namesto $\circ$, 1 namesto e, potence a^n)

Grupo določa par $(G, \cdot)$ (oziroma $(G, \circ)$). Če je jasno, za katero operacijo gre, govorimo kar o grupi G.

Trditev. *V grupi G za vsak $a \in G$ in vsaka $m, n \in \mathbb{Z}$ velja $a^m \cdot a^n = a^{m+n}$ in $(a^m)^n = a^{mn}$.*

Brez dokaza. Dokažimo lahko z indukcijo na n za $n > 0$, za $n < 0$ pa upoštevamo definicijo inverza.

Posledica. $a^{-n} = (a^n)^{-1}$

Definicija. *G je **komutativna grupa** ali **Abelova grupa**, kadar velja $ab = ba$ za vsaka $a, b \in G$.*

V Abelovih grupah običajno uporabljamo aditivni zapis: namesto $\cdot$ pišemo $+$ in operaciji rečemo *seštevanje*, namesto 1 pišemo 0, namesto a^{-1} pišemo $-a$, namesto a^n pišemo na.

Posledica. *V komutativni grupi G za vsaka $a, b \in G$ in vsaka $m, n \in \mathbb{Z}$ velja: $ma + na = (m + n)a$, $n(ma) = mna$ in $n(a + b) = na + nb$. Če G komutativna, ne velja nujno $(ab)^n = a^n \cdot b^n$*

Trditev. *Naj bo G grupa in $a, b, c \in G$ taki elementi, da je $ac = bc$ ali $ca = cb$. Potem je $a = b$.*

Dokaz. Če je $ac = bc$, to enakost pomnožimo s c^{-1} z desne $\Rightarrow a = b$.

Če je $ca = cb$ pa enakost pomnožimo z c^{-1} z leve $\Rightarrow a = b$.

Pravimo, da v grupi lahko krajšamo.

A pozor: $ac = cb \neq a = b$.

$\square$

PRIMER:

- Če je G le polgrupa in ni grupa, trditev ne velja. Primer:

$$G = F(A),\ |A| \geq 2.\ f : A \to A \text{ je konstantna preslikava}$$
$$\Rightarrow f \circ g = f \circ h,\ \forall g, h \in F(A)$$
$$f(g(x)) = f(h(x)),\ \forall x \in A$$

Pri Logiki in množicah boste videli, da z leve lahko krajšamo natanko z injektivnimi preslikavami, z desne pa s surjektivnimi.

Končne grupe pogosto podamo s **tabelo množenja**. V prvi stolpec in prvo vrstico napišemo vse elemente grupe $x_1, \ldots, x_n$. Na križišču i-te vrstice in j-tega stolpca napišemo $x_i x_j$. Iz prejšnje trditve sledi, da se v nobeni vrstici in v nobenem stolpcu element ne ponovi. Grupa je komutativna natanko tedaj, ko je tabela množenja simetrična glede na glavno diagonalo.

Tabela 1: Tabela množenja

$\cdot$	x_1	x_2	x_3	$\cdots$	x_n
x_1	1	x_2	$\cdots$	$\cdots$	x_n
x_2	x_2	x_1^2	$\cdots$	$\cdots$	$x_2 x_n$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
x_n	x_n	$x_n x_2$	$\cdots$	$\cdots$	x_n^2

PRIMERI: Poiščimo vse tabele množenja za grupe majhnih moči.

- $|G| = 1$ Edina taka grupa je *trivialna grupa* $\{1\}$.
- $|G| = 2$

$\cdot$	1	a
1	1	a
a	a	1

$\Leftrightarrow$	T	F
T	T	F
F	F	T

$+$	0	1
0	0	1
1	1	0

Zadnja tabela skriva v sebi seštevanje po modolu 2.

Splošneje, naj bo $n > 1$ naravno število. Z $\mathbb{Z}_n$ označimo množico ostankov celih števil pri deljenju z n.

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

V $\mathbb{Z}_n$ definiramo seštevanje s predpisom $a+b =$ ostanek vsote števil a in b pri deljenju z n.

Na primer v $\mathbb{Z}_6$ je 3+5=2, ker da 8 ostanek 2 pri deljenju s 6.

Izkaže se, da je $(\mathbb{Z}, +)$ grupa, enota je 0, inverz od a je $n - a$.

"Edina" grupa moči 2 je $\mathbb{Z}_2$. Natančneje, rekli bomo, da so vse grupe moči 2 izomorfne $\mathbb{Z}_2$.

- $|G| = 3$

$\cdot$	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tako prva kot tudi druga tabela predstavljata grupo $\mathbb{Z}_3$.

- $|G| = 4$ Primer: $\exists a \in G: \ a^2 \neq 1$

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

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

Obe tabeli sta $\mathbb{Z}_4$.

- Primer: $\forall x \in G : x^2 = 1$

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

$+$	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(0,0)	(1,1)	(0,1)	(1,0)	(0,0)

Če pogledamo prvo tabelo, vidimo, da je to grupa $\mathbb{Z}_2 \times \mathbb{Z}_2$. Seštevamo po komponentah, vsako komponento po modulu 2.

Poglejmo še drugo tabelo. To je res grupa, saj v splošnem velja: Če sta $(G, \circ)$ in $(H, *)$ grupi, potem je $G \times H$ grupa za operacijo $(a,b)(c,d) = (a \circ c, b * d)$. Enota: $(1_G, 1_H)$, inverz od (a,b) je (a^{-1}, b^{-1}).

- $|G| = 5$

Recimo najprej, da je $x^2 = 1$ za vsak $x \in G$. To pomeni: $\Rightarrow \exists a \in G : a^2 \neq 1$. BSŠ (brez škode za splošnost): $a^2 = b$.

$\cdot$	1	a	b	c	d
1	1	a	b	c	d
a	a	1	c	d	b
b	b	d	1	a	c
c	c	b	d	1	a
d	d	c	a	b	1

$\cdot$	1	a	b	c	d
1	1	a	b	c	d
a	a	b	c	d	1
b	b	c	d	1	a
c	c	d	1	a	b
d	d	1	a	b	c

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\mathbb{Z}_n$ je vedno komutativna grupa. Kartezični produkt komutativnih grup je komutativna grupa, če operacijo definiramo po komponentah. Iz tega sledi, da so vse grupe moči največ 5 komutativne.

Če pogledamo prvo tabelo, vidimo, da to ni grupa. Razlog, da to ni grupa: ker $(ab)d = cd = a \neq d = ac = a(bd)$. Preostali dve tabeli pa sta grupi $\mathbb{Z}_5$.

3.3.1 Grupe permutacij

Vemo že, da je množica $S(A)$ vseh bijektivnih preslikav $A \to A$ grupa za kompozitum. Če je A končna množica, bijektivno preslikavo $A \to A$ imenujemo **permutacija** množice A. Ko gledamo permutacije, elemente množice A lahko preimenujemo in se lastnosti permutacij ne spremenijo. Zato običajno vzamemo $A = \{1, \ldots, n\}$.

Grupa $(S(\{1, \ldots, n\}), \cdot)$ vseh permutacij množice $\{1, \ldots, n\}$ se imenuje **simetrična grupa reda** n. Oznaka: S_n. $|S_n| = n!$. Če je $n \geq 3$, S_n ni komutativna grupa.

Permutacijo $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ običajno zapišemo v obliki: $\pi = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{smallmatrix}\right)$

PRIMER:

- S_3 vsebuje permutacije $id = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right)$, $a = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$, $b = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$, $c = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$, $d = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right)$, $f = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$

  Operacija na S_n je običajen kompozitum preslikav $(\pi_1 \circ \pi_2)(x) = \pi_1(\pi_2(x))$, $\forall x \in \{1, \ldots, n\}$.

PRIMER:

- $a(b(1)) = a(2) = 3$,
  $a(b(2)) = a(1) = 1$,
  $a(b(3)) = a(3) = 2$,
  $\Rightarrow a \circ b = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right) = d$.

Tabela 2: Tabela za množenje za S_3

$\circ$	id	a	b	c	d	f
id	id	a	b	c	d	f
a	a	id	d	f	b	c
b	b	c	id	a	f	d
c	c	b	f	d	id	a
d	d	f	a	id	c	b
f	f	d	c	b	a	id

$$
\begin{aligned}
(a \circ c)(1) &= a(c(1)) = a(2) = 3 \\
(a \circ c)(2) &= a(c(2)) = a(3) = 2 \\
(a \circ c)(3) &= 1 \\
(c \circ a)(1) &= c(c(1)) = c(2) = 3 \\
(c \circ c)(2) &= c(c(2)) = c(3) = 1 \\
(c \circ c)(3) &= 2 \\
(c \circ a)(1) &= c(1) = 2 \\
(c \circ a)(2) &= c(3) = 1 \\
(c \circ a)(3) &= c(2) = 3 \\
d^2 &= (c^2)^2 = c^4 = c
\end{aligned}
$$

Tabela za množenje na S_3 ni simetrična glede na diagonalo, ker S_3 ni komutativn grupa.

Definicija. *Naj bodo $a_1, \dots, a_k \in \{1, \dots, n\}$ paroma različni. Permutacija $\sigma \in S_n$, za katero velja $\sigma(a_i) = a_{i+1}$ za $i = 1, \dots, k-1$, $\sigma(a_n) = a_1$ in $\sigma(a) = a$ za vse $a \in \{1, \dots, n\} \backslash \{a_1, \dots, a_n\}$, se imenuje **cikel dolžine** k. Oznaka: $\sigma = (a_1, a_2, \dots, a_k)$. Cikla $(a_1, \dots, a_k)$ in $(b_1, \dots, b_k)$ sta **disjunktna**, kadar sta množici $\{a_1, \dots, a_k\}$ in $\{b_1, \dots, b_k\}$ disjunktni. Disjunktna cikla vedno komutirata.*

Edini cikel dolžine 1 je identiteta. Cikel dolžine 2 se imenuje **transpozicija**.

PRIMER:

- $a = (2\ 3)$, $b = (1\ 2)$, $f = (1\ 3)$ so transpozicije v S_3, $c = (1\ 2\ 3)$ in $d = (1\ 3\ 2)$ pa sta 3-cikla v S_3.

Izrek. *Vsako permutacijo lahko zapišemo kot kompozitum disjunktnih ciklov. Ti cikli med seboj komutirajo in so do vrstnega reda s permutacijo enolično določeni.*

PRIMER:

- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 3 & 4 & 7 & 6 \end{pmatrix} = \begin{pmatrix} 1, 5, 4, 3 \end{pmatrix}\begin{pmatrix} 2 \end{pmatrix}\begin{pmatrix} 6, 7 \end{pmatrix}$

Cikle dolžine 1 v produktu (kompozitumu) običajno spuščamo, ker so enaki identiteti.

Dokaz. Disjunktni cikli vedno komutirajo, zato moramo dokazati le obstoj in enoličnost (do vrstnega reda natančno) razcepa permutacije na produkt (kompozitum) disjunktnih ciklov.

Obstoj: Obstoj bomo dokazali z indukcijo na n (n je moč množice, na kateri delujejo permutacije).

$$n = 1 : S_1 = \{id\}$$
$$n = 2 : S_2 = \{id, (1\ 2)\}$$
$$\text{Za } n \leq 2 \text{ izrek očitno velja.}$$

Naj bo $n \geq 3$ in predpostavimo, da izrek velja za vse permutacijske grupe S_m, kjer je $m < n$.

$\pi \in S_n$ naj bo poljubna premutacija.

Oglejmo si množico $\{1, \pi(1), \pi^2(1), \pi^3(1), \ldots\}$

$(\pi^2 = \pi \circ \pi,\ \pi^3 = \pi \circ \pi \circ \pi, \ldots)$

Ta množica je končna, saj je podmnožica množice $\{1, 2, \ldots, n\}$.

Zato obstajata k in l, $0 \leq l < k$, da je $\pi^k(1) = \pi^l(1)$.

Naj bo k najmanjši, za katerega tak l obstaja: $\pi^0(1) = 1 = id(1)$.

Dokažimo, da je $l = 0$.

Recimo, da je $l \geq 1$.

$\pi^2(l) = \pi^k(1)$ lahko na levi komponiramo s π^{-1}, ker je π bijekcija $\Rightarrow \pi^{l-1}(1) = \pi^{k-1}(1)$, $0 \leq l - 1 < k - 1$.

To je v protislovju z minimalnostjo k-ja. Torej je $l = 0$ in $\pi^k(1) = 1$.

Označimo $a_1 = 1,\ a_2 = \pi(1), \ldots, a_k = \pi^{k-1}(1)$.

Števila $a_1, \ldots, a_k$ so paroma različna in velja $\pi(a_i) = a_{i+1}$, za $i = 1, \ldots, k-1$ in $\pi(a_k) = a_1$.

Cikel $(a_1, \ldots, a_k)$ na množici $\{a_1, \ldots, a_k\}$ deluje enako kot permutacija π.

Definirajmo $\rho = (a_1, a_2, \ldots, a_k)^{-1} \circ \pi$.

Potem je $\rho(a_1) = a_1$ za vsak $i = 1, \ldots, k$. ρ lahko torej gledamo kot permutacijo množice $\{1, \ldots, n\} \backslash \{a_1, \ldots, a_k\}$.

Ta množica ima največ $n-1$ elementov, zato po indukcijski predpostavki ρ lahko zapišemo kot produkt dijskunktnih ciklov, ki ne vsebujejo elementov $a_1, \ldots, a_k$.

Potem pa tudi $\pi = (a_1, \ldots, a_n) = \rho$ lahko zapišemo kot produkt disjunktnih ciklov.

Enoličnost: Recimo, da je $\sigma_1\sigma_2\ldots\sigma_k = \rho_1\rho_2\ldots\rho_l = \pi$, kjer so σ disjunktni cikli in ρ_j disjunktni cikli.

Predpostavimo lahko, da je najmanjši element cikla vedno napisan na začetku.

Ker disjunktni cikli komutirajo, lahko predpostavimo tudi, da je najmanjši element σ_i manjši od najmanjšega elementa v σ_j, če je $i < j$, in isto velja za ρ_i in ρ_j.

$$\begin{aligned}
&\Rightarrow \sigma_1 = (1, a_1, \ldots, a_r),\ \rho_1 = (1, b_2, \ldots, b_s)\\
&\quad a_2 = \pi(1),\ a_3 = \pi(a_2) = \pi^2(1), \ldots, a_r = \pi^{r-1}(1),\\
&\quad a_2 = \pi(1),\ b_3 = (\pi^2(1), \ldots, b_s = \pi^{s-1}(1)\\
&\Rightarrow r = s\ in\ a = b\ za\ i = 2, \ldots, r-1 \Rightarrow \sigma_1 = \rho_1
\end{aligned}$$

Na nek način (oz. z indukcijo) dokažimo še $\sigma_2 = \rho_2, \ldots$ (in v posebnem primeru $l = k$).

□

Trditev. *Vsak cikel je produkt transpozicij.*

Dokaz. $(a_1, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \ldots (a_1, a_2)$.

□

Posledica. *Vsaka permutacija je produkt transpozicij.*

Zapis permutacije kot produkt transpozicij ni enoličen. Na primer, $id = (1\ 2)(1\ 2)$.

Definicija. *Za identiteto definiramo $s(id) = 1$. Če je σ cikel dolžine k, definiramo $s(\sigma) = (-1)^{k+1}$. Če je $\pi \in S_n$ poljubna permutacija, jo lahko zapišemo kot produkt disjunktnih ciklov $\pi = \sigma_1\sigma_2\ldots\sigma_m$.*

Definiramo $s(\pi) = s(\sigma_1)s(\sigma_2)\dots s(\sigma_m)$.

Ker je zapis permutacije kot produkt disjunktnih ciklov do vrstnega reda enoličen, je definicija števila $s(\pi)$ dobra. s je preslikava iz S_n v $\{-1, 1\}$.

$$\begin{aligned} s:\ S_n &\to \{-1, 1\} \\ \pi &\mapsto s(\pi) \end{aligned}$$

je dobro definirana preslikava.

Številu $s(\pi)$ pravimo **znak permutacije** π. Namesto $s(\pi)$ se včasih piše tudi $sgn(\pi)$.

PRIMER:

- $$\begin{aligned} s((1\ 3)(2\ 6\ 9\ 7)(4\ 5\ 8)) &= s((1\ 3))\ s((2\ 6\ 9\ 7))\ s((4\ 5\ 8)) \\ &= -1 \cdot (-1) \cdot 1 \\ &= 1 \end{aligned}$$

Znak vsake transpozicije je -1.

Trditev. *Če je $\tau \in S_n$ poljubna transpozicija in $\pi \in S_n$ poljubna permutacija, potem je $s(\tau\pi) = -s(\pi)$ $(= s(\tau)s(\pi))$.*

Dokaz.

<u>1. možnost</u>: Naj bo $\pi = \sigma_1 \dots \sigma_m$ zapis permutacije π kot produkt disjunktnih ciklov.

Znak permutacije $\sigma_1 \dots \sigma_m$ se seveda ne spremeni, če v ta produkt dodamo cikle dolžine 1. Zato lahko predpostavimo, da se vsako od števil pojavi (natanko enkrat) v kakšnem od ciklov σ.

Števili iz transpozicije τ sta lahko v enem ali dveh izmed ciklov σ.

? števili iz transpozicije τ sta v dveh ciklih. Lahko predpostavimo, da je $\tau = (a_1, b_1)$, $\sigma_n = (a_1, \dots, a_k)$ in $\sigma_2 = (b_1, \dots, b_l)$.

Potem je

$$\begin{aligned} s(\pi) &= s(\sigma_1)s(\sigma_2)\dots s(\sigma_m) \\ &= (-1)^{k+1} \dots (-1)^{l+1}\ s(\sigma_3)\dots s(\sigma_m) \\ &= (-1)^{?} s(\sigma_3)\dots s(\sigma_m) \\ \tau\pi &= (a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_l)\sigma_3 \dots \sigma_m \end{aligned}$$

To je zapis $\tau\pi$ na produkt disjunktnih ciklov, zato je $s(\tau\pi) = (-1)^{k+l+1}s(\sigma_3)\dots s(\sigma_m) =$ $= -s(\pi)$

<u>2. možnost</u>: Števili iz transpozicije τ sta v istem ciklu.

Predpostavimo lahko, da je $\tau = (a_1, a_k)$ in $\sigma_1 = (a_1, \dots, a_k, \dots, a_l)$.

Potem je

$$\begin{aligned} s(\pi) &= s(\sigma_1)\dots s(\sigma_m) \\ &= (-1)^{l+1}s(\sigma_2)\dots s(\sigma_m) \\ \tau\pi &= (a_1, a_2, \dots, a_{k-1})(a_k, a_{k+1}, \dots, a_l)\sigma_2\dots\sigma_m \end{aligned}$$

To je zapis $\tau\pi$ kot produkt disjunktnih ciklov, zato je

$$\begin{aligned} s(\tau\pi) &= (-1)^k(-1)^? s(\sigma_2)\dots s(\sigma_m) \\ &= (-1)^? s(\sigma_2)\dots s(\sigma_m) \\ &= -s(\pi) \end{aligned}$$

□

Posledica. *Če je $\pi = \tau_1 \dots \tau_m$, kjer so τ_i transpozicije, potem je*

$$s(\pi) = (-1)^m = \begin{cases} 1; & m \text{ sodo} \\ -1; & m \text{ liho} \end{cases}$$

Posledica. *Če sta π_1 in π_2 poljubni permutaciji, je $s(\pi_1\pi_2) = s(\pi_1)s(\pi_2)$*

Dokaz. Naj bo $\pi_1 = \tau_1 \dots \tau_k$ in $\pi_2 = \rho_1 \dots \rho_l$, kjer so τ_i in ρ_j transpozicije.

Potem je

$$\begin{aligned} s(\pi_1\pi_2) &= s(\tau_1 \dots \tau_k \rho_1 \dots \rho_l) \\ &= (-1)^{k+l} \\ &= (-1)^k(-1)^l \\ &= s(\pi_1)s(\pi_2) \end{aligned}$$

□

Posledica. *Iste permutacije ne moremo zapisati kot produkt sodega števila transpozicij in kot produkt lihega števila transpozicij.*

Dokaz. (POSLEDICE) Naj bo $\pi = \tau_1 \dots \tau_k = \rho_1 \dots \rho_l$, kjer so τ_i in ρ_j transpozicije. Znak permutacije π je po definiciji neodvisen od teh dveh zapisov, odvisen je le od permutacije. Po predprejšnji posledici je $s(\pi) = (-1)^k = (-1)^l \Rightarrow k$ in l sta obe sodi ali obe lihi

□

Definicija. *Permutaciji, ki jo napišemo kot produkt sodega števila transpozicij, pravimo* ***soda permutacija****, permutaciji, ki jo lahko zapišemo kot produkt lihega števila transpozicij, pa pravimo* ***liha permutacija****.*

Trditev. *Produkt sodih permutacij je soda permutacija, inverz sode permutacije je soda permutacija.*

Dokaz. Za produkt to že vemo, saj je $s(\pi_1\pi_2) = s(\pi_1)s(\pi_2)$.

Inverz: Naj bo $\pi = \tau_1 \dots \tau_m$, kjer so τ_i transpozicije.

Potem je $s(\pi) = (-1)^m$ in $\pi^{-1} = \tau_m^{-1} \dots \tau_1^1 = \tau_m \dots \tau_1$.

Torej je $s(\pi^{-1}) = (-1)^m = s(\pi)$.

Dokazali smo tudi, da je inverz lihe permutacije liha permutacija.

□

Naj A_n označuje množico sodih permutacij v S_n. Kompozitum sodih permutacij je soda permutacija (po prejšnji trditvi), torej je kompozitum notranja binarna operacija na množici A_n. Ta operacija je seveda asociativna. Identiteta, ki je enota za operacijo $\circ$, leži v A_n. Po prejšnji trditvi pa tudi inverz vsakega elementa iz A_n leži v A_n. Torej je A_n grupa za operacijo $\circ$. Rečemo ji **alternirajoča grupa reda** n.

Naj bo τ poljubna transpozicija. Potem je preslikava $\pi \mapsto \tau\pi$ bijekcija iz A_n v množico lihih permutacij v S_n.

Injektivnost: $\tau^{-1}: \ \tau\pi_1 = \tau\pi_2 \Rightarrow \pi_1 = \pi_2$

Surjektivnost: ρ liha permutacija $\Rightarrow$ def.: $\pi = \tau^{-1}\rho$ soda $\tau\pi = \tau\tau^{-1}\rho = \rho \Rightarrow$ $\Rightarrow A_n$ ima $\frac{n!}{2}$ elementov.

3.4 Podgrupe

Definicija. *Naj bo $(G, \cdot)$ grupa. Neprazna podmnožica $H \subseteq G$ je* ***podgrupa*** *grupe $(G, \cdot)$, kadar velja:*

(1) zaprtost za operacijo: če sta $x, y \in H$, mora biti $x \cdot y \in H$,

(2) zaprtost za invertiranje: če je $x \in H$, mora biti $x^{-1} \in H$

Trditev. *Naj bo H podgrupa grupe G in e enota grupa G. Potem je $e \in H$.*

Dokaz. $H \neq \emptyset \Rightarrow \exists a \in H$. Po (2) je $a' \in H$. Po (1) je $e = aa^{-1} \in H$.

□

Če je H podgrupa grupe $(G, \cdot)$, je množenje notranja binarna operacija na H, ki je asociativna, saj se asociativnost prenese iz G. H vsebuje tudi enoto in vse svoje inverze. Torej je $(H, \cdot)$ grupa.

PRIMER:

- $(\mathbb{Z}, +)$ je podgrupa v $(\mathbb{Q}, +)$, ta je pogrupa $(\mathbb{R}, +)$, ta je podgrupa $(\mathbb{C}, +)$
- $(\mathbb{Q}\backslash\{0\}, \cdot)$ je podgrupa $(\mathbb{R}\backslash\{0\}, \cdot)$, $(0, \infty)$ je podgrupa $(\mathbb{R}\backslash\{0\}, \cdot)$
- $(A_n, \circ)$ je podgrupa $(S_n, \circ)$
- Če je τ transpozicija, je $(\{id, \tau\}, \circ)$ podgrupa grupe $(S_n, \circ)$
- Vsaka grupa G, ki ima vsaj dva elementa, ima vsaj dve podgrupi: G - neprazna podgrupa in $\{e\}$ - trivialna podgrupa.

  Lahko se zgodi, da sta to edini podgrupi grupe G. Za primer lahko vzamemo $(\mathbb{Z}_p, +)$, kjer je p praštevilo.

Trditev. *Neprazna podmnožica H grupe $(G, \cdot)$ je podgrupa natanko takrat, ko velja $xy^{-1} \in H$, $\forall x, y \in H$.*

Dokaz.

$(\Rightarrow)$: H je podgrupa

Naj bosta $x, y \in H$ poljubna.

Ker je H podgrupa, po točki (2) in definiciji sledi $y^{-1} \in H$.

Po točki (1) je potem $xy^{-1} \in H$.

$(\Leftarrow)$:

Predpostavimo, da je velja $xy^{-1} \in H$ za vse $x, y \in H$. Radi bi dokazali, da je H zaprta za množenje in za invertiranje.

Naj bosta $x, y \in H$ poljubna.

Potem je $xx^{-1} \in H$.

Torej H vsebuje enoto e grupe G.

Potm pa velja tudi $x^{-1} = ex^{-1} \in H$, torej je H zaprta za invertiranje.

Enako velja tudi $y^{-1} \in H$.

Potem pa je $xy = x(y^{-1})^{-1} \in H$, torej je H zaprta za množenje.

$\square$

Posledica. *Naj bo $(G, +)$ aditivno pisana Abelova grupa. Potem je $\emptyset \neq H \subseteq G$ podgrupa grupe G natanko takrat, ko za vsaka $x, y \in H$ velja $x - y \in H$ (zaprtost za odštevanje).*

Trditev. *Presek poljubne družine podgrup je podgrupa.*

Dokaz. Naj bo $\{H_j\}_{j\in J}$ družina podgrup grupe G (J je poljubna indeksna množica) in naj bo $H = \bigcap_{j\in J} H_j$.

Naj bosta $x, y \in H$ poljubna.

Potem sta $x, y \in H_j$ za vsak $j \in J$.

Po trditvi je zato $xy^{-1} \in H_j$ za vsak $j \in J$.

Torej je $xy^{-1} \in \bigcap_{j\in J} H_j = H$.

$\square$

Unija podgrup v splošnem ni podgrupa. Za primer lahko vzamemo:

- $G = S_3$
  $H_1 = \{id, (1, 2)\}$ in $H_2 = \{id, (1, 3)\}$ sta podgrupi v S_3.
  $H_1 \cup H_2$ ni podgrupa, saj $(1, 2)(1, 3) \notin H_1 \cup H_2$

3.5 Homomorfizem grup

Definicija. *Naj bosta $(G, \circ)$ in $(H, *)$ grupi. Preslikava $f : G \to H$ je* ***homomorfizem grup****, kadar velja $f(x \circ y) = f(x) * f(y)$ za vsaka $x, y \in G$.*

PRIMERI:

- Naj bo $n \in \mathbb{Z}$ in definiramo preslikavo

$$\begin{aligned} f : (\mathbb{Z}, +) &\to (\mathbb{Z}, +) \\ x &\mapsto nx \end{aligned}$$

$$\begin{aligned} f(x+y) &= n(x+y) \\ f(x) + f(y) &= nx + ny \end{aligned}$$

$$\Rightarrow f \text{ je homomorfizem grup}$$

- $$\begin{aligned} f : (\mathbb{Z}, +) &\to (\mathbb{Q}\backslash\{0\} \cdot) \\ x &\mapsto 2^x \end{aligned}$$

$$f(x+y) = x^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y) \Rightarrow f \text{ je homomorfizem grup}$$

- $$\begin{aligned} f : (\mathbb{R}\backslash\{0\}, \cdot) &\to ((0, \infty), \cdot) \\ x &\mapsto f|x| \end{aligned}$$

  To je tudi homomorfizem grup, saj je $f(xy) = |xy| = |x| \cdot |y| = f(x) \cdot f(y)$

- $$\begin{aligned} s : S_n &\to \{-1, 1\} \\ \pi &\mapsto s(\pi) \end{aligned}$$

  Je homomorfizem grup, saj vemo, da je $s(\pi_1 \circ \pi_2) = s(\pi_1)s(\pi_2)$

- $id : G \to G$ je vedno homomorfizem

- $$\begin{aligned} f : G &\to H \\ x &\mapsto e, \ \forall x \in G \end{aligned}$$

  (kjer je e enota grupe H) je tudi homomorfizem grup

- $$\begin{aligned} f : (\mathbb{R}^2, +) &\to (\mathbb{R}, +) \\ (x, y) &\mapsto ax + by \end{aligned}$$

  kjer sta a, b poljubni konstanti

  $$\begin{aligned} f((x,y) + (z,w)) &= f(x+z, y+w) \\ &= a(x+z) + b(y+w) \\ &= ax + az + by + bw \\ &= f((x,y)) + f((z,w)) \\ &\Rightarrow f \text{ je homomorfizem grup} \end{aligned}$$

Trditev. *Naj bo $f : G \to H$ homomorfizem grup, kjer je e enota v G in e' enota v H. Potem je $f(e) = e'$ in $f(a^{-1}) = f(a)^{-1}$ za vsak $a \in G$. Pri tem a^{-1} predstavlja inverz v G, a pa inverz v H.*

Dokaz.

$$\begin{gathered} f(e) = f(e \cdot e) = f(e) \cdot f(e) \\ e' = f(e) \cdot f(e)^{-1} = f(e) \\ f(e) = e' \\ f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1}) \\ \text{Z leve smo pomnožili z } f(a)^{-1} \Rightarrow f(a)^{-1} = f(a^{-1}) \end{gathered}$$

□

Izomorfizem je bijektiven homomorfizem grup.
Monomorfizem je injektiven homomorfizem grup.
Epimorfizem je surjektiven homomorfizem grup.
Endomorfizem je homomorfizem iz grupe vase.
Avtomorfizem je bijektiven endomorfizem.

$f : G \to H$ je monomorfizem $\Leftrightarrow$ za vsaka homomorfizma grupa $g, h : K \to G$ iz $f \circ g = f \circ h$ sledi $g = h$.

Če je H Abelova, je $f : G \to H$ epimorfizem $\Leftrightarrow$ za vsaka homomorfizma grup $g, h : H \to K$ iz $g \circ f = h \circ f$ sledi $g = h$.

Če H ni Abelova, to ni res.

PRIMER:

$$f : S_3 \to S_3$$

$$f(\pi) = \begin{cases} (1,2), & \pi \text{ liha} \\ id, & \pi \text{ soda} \end{cases}$$

Trditev.

(a) Kompozitum homomorfizmov grup je homomorfizem grup.

(b) Inverz izomorfizma grup je homomorfizem (in zato izomorfizem) grup.

Dokaz.

(a) $f : (G, \cdot) \to (H, \circ)$ in $g : (H, \circ) \to (K, *)$ naj bosta homomorfizma grup in naj bosta $x, y \in G$ poljubna.

Potem je

$$\begin{aligned} (g \circ f)(xy) &= g(f(xy)) \\ &= g(f(x) \circ f(y)) \\ &= g(f(x)) * g(f(y)) \\ &\Rightarrow g \circ f : (G, \cdot) \to (K, *) \\ &\text{je homomorfizem grup} \end{aligned}$$

(b) Naj bo $f : G \to H$ izomorfizem.

Hočemo dokazati, da je $f^{-1} : H \to G$ homomorfizem grup.

Naj bosta $x, y \in H$ poljubna.

Ker je f izomorfizem, obstajata enolična elementa $a, b \in G$, da je $x = f(a)$ in $y = f(b)$.

$$\begin{aligned} f \text{ je homomorfizem} \Rightarrow& \\ f(ab) &= f(a) \cdot f(b) \\ f(ab) &= xy \\ f^{-1} f^{-1}(y) &= ab = f^{-1}(xy) \\ &\Rightarrow f^{-1} \text{ je homomorfizem grup.} \end{aligned}$$

□

Definicija. *Grupi G in H sta **izomorfni**, če med njima obstaja izomorfizem. Oznaka: $G \cong H$.*

V algebri med izomorfiznimi grupami običajno ne ločujemo. Npr. $\mathbb{Z}_2$ označujemo vsako grupo z 2 elementoma. Npr., če je τ transpozicija, je $\{id_?\tau\} = \mathbb{Z}_2$.

Definicija. *Naj bo $f : G \to H$ homomorfizem grup. Zalogi vrednosti tega homomorfizma pravimo **slika** homomorfizma f in jo označimo $\operatorname{im} f$. Množico $\{x \in G, f(x) = e\}$ (kjer je e enota grupe H) pa imenujemo **jedro** preslikave f in ga označimo $\ker f$.*

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

Dokaz.

Ker je $f(e_G) = e_H$, je množica $\ker f$ neprazna.

Naj bosta $a, b \in \operatorname{Ker} f$.

Potem je $f(a) = f(b) = e_H$.

$$f(ab') = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_H e_H^{-1} = e_H \Rightarrow ab^{-1} \in \operatorname{Ker} f$$

Torej je $\ker f$ podgrupa grupe G.

Zaloga vrednosti je vedno neprazna.

Naj bosta $a, b \in \operatorname{Im} f$.

To pomeni, da obstajata $x, y \in G$, da je $a = f(x)$ in $b = f(y)$.

Potem je $ab^{-1} = f(x)f(y)^{-1} = f(xy^{-1})$.

Torej je $ab^{-1} \in \operatorname{Im} f$ in slika homomorfizma f je podgrupa grupe H.

$\square$

Očitno velja f je surjektiven homomorfizem $f : G \to H \Leftrightarrow \mathrm{Im} f = H$.

Izrek. *Homomorfizem grup $f : G \to H$ je injektiven $\Leftrightarrow$ $Kerf = \{1\}$. Pri tem je 1 enota grupe G.*

Dokaz.

($\Rightarrow$)

Vedno je $f(1_G) = 1_H$. $\ker f = \{x \in G, f(x) = 1_H\}$

Predpostavimo, da je f injektiven homomorfizem in naj bo $x \in \mathrm{Ker} f$ poljuben.

$$f(x) = 1_H = f(1_G)$$

Ker je f injektiven, od tod sledi $x = 1_G$. Torej je $\ker f = \{1_G\}$

($\Leftarrow$)

Predpostavimo, da je $\ker f = \{1_G\}$.

Hočemo dokazati, da je f injektivna.

Naj bosta $x, y \in G$ poljubna, za katera je $f(x) = f(y)$.

$$f(x) = f(y) \ / \cdot f(y)^{-1}$$
$$f(xy^{-1}) = f(x)f(y)^{-1} = 1_H$$

(pri znaku = vemo, da to velja, ker je f homomorfizem)

Ker je jedro preslikavde f po predpostavki trivialno, je $xy^{-1} = 1_G$ oziroma ko enačbo pomnožimo z y dobimo, da je $x = y$ in posledično dokažemo, da je f torej injektivna.

□

PRIMER:

- $$f(\mathbb{R},+) \to ((0,\infty),\cdot)$$
  $$x \mapsto 2^x$$

  Vemo, da je to homomorfizem grup. Ali je injektiven?

  Enota v grupi $((0,\infty),\cdot)$ je 1.

  Kdaj je $x \in \mathrm{Ker} f$?
  $$\Rightarrow f(x) = 1 \Leftrightarrow 2^x = 1$$

  To je res le v primeru, ko je $x = 0$ enota grupe $(\mathbb{R},+)$.

  Torej je $\ker f = \{0\}$ in zato je f injektiven homomorfizem.

  Kdaj je $z \in \mathrm{Ker} f$?

  $$\Leftrightarrow f(z) = 1 \Leftrightarrow |z| = 1 \Leftrightarrow z = \cos\varphi + i\sin\varphi \text{ za nek } \varphi \in [0, 2\pi].$$

  $$\mathrm{Ker} f = \{\cos\varphi + i\sin\varphi; \varphi \in [0, 2\pi]\}$$

  Jedro vsebuje poleg enote še druge elemente, zato f ni injektivna preslikava.

  Dokazali smo tudi, da je enotska krožnica podgrupa grupe $(\mathbb{C}\backslash\{0\},\cdot)$

3.6 Kolobarji

Definicija. *Neprazna množica K z operacijama seštevanja in množenja je **kolobar**, kadar velja:*

1) $(K, +)$ *je Abelova grupa (in tudi pišemo jo aditivno)*

2) $(K, \cdot)$ *je polgrupa (to pomeni: množenje je asociativno)*

3) velja distributivnost*:* $a(b + c) = ab + ac$ *in* $(b + a)a = ba + ca, \ \forall a, b, c \in K$

Kolobar K ima *enoto* (ali *enico*), če je $(K, \cdot)$ monoid. Enoto (kadar obstaja) običajno označujemo z 1.

Kolobar je *komutativen*, kadar je množenje v K komutativno.

Trditev. *V kolobarju velja:*

1) $a \cdot 0 = 0 \cdot a = 0, \ \forall a \in K$

2) $a(-b) = (-a)b = -(ab)$ *in* $(-a)(-b) = ab, \ \forall a, b \in K$

Dokaz.

1) $a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0.$

   Na obeh straneh odštejemo $a \cdot 0$ in dobimo $0 = a \cdot 0$.

   Na enak način dokažemo $0 \cdot a = 0, \ \forall a \in K$.

2) $a(-b) + ab = a(-b + b) = a \cdot 0 = 0 \Rightarrow a(-b)$ je nasproten element elementa $ab: \ a(-b) = -(ab)$

   Enako dokažemo $(-a) \cdot b = -(ab)$.

   Enakost $(-a)(-b) = ab$ dobimo tako, da enakost $a(-b)$ uporabimo za $-a$ in b.

□

Primeri kolobarjev:

- Številski kolobarji: $(\mathbb{Z},+,\cdot),(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot),(\mathbb{C},+,\cdot)$
- Na množici $F(\mathbb{R})$ vseh funkcija $\mathbb{R}\to\mathbb{R}$ definiramo seštevanje in množenje po točkah:

$$(f+g)(x)=f(x)+g(x),\ \forall x\in\mathbb{R}$$
$$(f\cdot g)(x)=f(x)\cdot g(x),\ \forall x\in\mathbb{R}$$

Hitro se da preveriti, da je $(F(\mathbb{R}),+,\cdot)$ kolobar. Ta kolobar ima enoto $e:\mathbb{R}\to\mathbb{R},\ e(x)=1$ za vsak $x\in\mathbb{R}$.

$$(e\cdot f)(x)=e(x)\cdot f(x)=1\cdot f(x)=f(x) \text{ za vsak } f\in f(\mathbb{R}) \text{ in za vsak } x\in\mathbb{R}$$

$\Rightarrow e\cdot f=f$, enako vidimo, da je $f\cdot e=f,\ \forall f\in F(\mathbb{R})$.

Kolobar je komutativen: $(f\cdot g)(x)=f(x)\cdot g(x)=g(x)\cdot f(x)=(gf)(x)$, za vse f,g

- Polinom z realnimi koeficienti je izraz oblike

$$p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0, \text{ kjer so } a_i\in\mathbb{R}$$

Množico polinomov z realnimi koeficietni označujemo z $\mathbb{R}[X]$. Na $\mathbb{R}[X]$ definiramo običajno seštevanje in množenje polinomov. Za to seštevanje in množenje je $\mathbb{R}[X]$ kolobar (dokaži doma). Ta kolobar je komutativen in ima enoto $p(x)=1$.

- $\mathbb{Z}_n$.

Ostanek števila a pri deljenju z n bomo označili z ?. Potem je

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

Na $\mathbb{Z}_n$ definiramo operaciji $+$ in $\cdot$ s predpisoma $[a]+[b]=[a+b]$ in $[a]\cdot[b]=[a\cdot b]$.

Preveriti moramo, da je definicija dobra, torej, da sta $[a+b]$ in $[a\cdot b]$ odvisna le od ostankov števil a in b.

Naj bo $[a]=[a']$ in $[b]=[b']$. To pomeni, da $n|a-a'$ in $n|b-b'$.

$$\Rightarrow n|a-a'+b-b'=a+b-(a'+b')\Rightarrow[a+b]=[a'+b']$$

Seštevanje je dobro definirano, saj je ostanek $[a+b]$ odvisen le od ostankov $[a]$ in $[b]$, ne pa tudi od a in b.

$$n|a-a',\ n|b-b'\Rightarrow n|(a-a')b+a'(b-b')=ab-a'b'\Rightarrow[ab]=[a'b']$$

Tudi množenje je dobro definirano.

Za tako definirano seštevanje in množenje je $\mathbb{Z}_n$ kolobar (preveri doma). Je komutativen in ima enoto [1].

Kadar ni bojazni, da bi ostanke zamešali s celimi števili, namesto $[a]$ pišemo kar a. Druga oznaka: $a + n\mathbb{Z}$.

- $(\mathbb{R}^3, +, x)$ ni kolobar, saj x ni asociativen
- Na $\mathbb{R}^3$ definiramo množenje.

  $$(x_1, y_1, z_1) \cdot (x_2, y_2, z_2) = (x_1x_2, x_1y_2 + y_1z_2, z_1z_2)$$

  Za to množenje in običajno seštevanje je $\mathbb{R}^3$ kolobar (preveri doma).

  Kolobar ima enoto $(1, 0, 1)$.

  Kolobar ni komutativen:

  $$(1, 0, 0) \cdot (0, 1, 0) = (0, 1, 0) \neq (0, 0, 0) = (0, 1, 0) \cdot (1, 0, 0)$$

- A naj bo (aditivno pisana) Abelova grupa in $\mathrm{End}(A)$ množica vseh endomorfizmov grupe A.

  Dokazali smo, da je kompozitum homomorfizmov grup spet homomorfizem grup, torej je $\circ$ dobro definirana operacija na $\mathrm{End}(A)$. Ta operacija je asociativna in ima enoto $id_A \Rightarrow (\mathrm{End}(A), \circ)$ je monoid.

Dokažimo $f, g \in \mathrm{End}(A) \Rightarrow f + g \in \mathrm{End}(A)$

Dokaz.

$a, b \in A$

$$\begin{aligned}(f+g)(a+b) &= f(a+b) + g(a+b \\ &= f(a) + f(b) + g(a) + g(b) \\ &= (f+g)(a) + (f+g)(b) \\ &\Rightarrow f + g \in \mathrm{End}(A)\end{aligned}$$

$\Rightarrow$ seštevanje je dobro definirana operacija na End(A).

Hitro se vidi, da je ta operacija asociativna in komutativna. Ta operacija ima enoto, ki je preslikava, ki vse elemente slika v 0.

$$\begin{aligned} 0\colon\ A &\to A \\ a &\mapsto 0\ \forall a \end{aligned}$$

$$(f+0)(a) = f(a) + 0(a) = f(a) + 0 = f(a),\ \text{za vsak } a \in A \Rightarrow f + 0 = f$$

Pri tem sta ničla pri $(f+0)(a)$ in $0(a)$ ničelni preslikavi. 0 pri $f(a)+0$ pa je nič v A.

Inverz preslikave $f \in \text{End}(A)$ za seštevanje je preslikava - f, definirana s predpisom $(-f)(a) = -f(a),\ \forall a \in A$.

Torej je $(\text{End}(A), +)$ Abelova grupa.

Vemo že, da je $(\text{End}(A), \circ)$ monoid.

Dokažimo še distributivnost.

Naj bodo $f, g, h \in \text{End}(A)$ poljubni endomorfizmi.

Radi bi dokazali, da je $f \circ (g+h) = f \circ g + f \circ h$ in $(g+h) \circ f = g \circ f + h \circ f$

Naj bo $a \in A$ poljuben.

Potem je

$$\begin{aligned} (f \circ (g+h))(a) &= f((g+h)(a)) \\ &= f(g(a) + h(a)) \\ &= f(g(a)) + f(h(a)) \\ &= (f \circ g)(a) + (f \circ h)(a) \\ &= (f \circ g + f \circ h)(a) \\ &\Rightarrow f \circ (g+h) = f \circ g + f \circ h \end{aligned}$$

$$\begin{aligned} ((g+h) \circ f)(a) &= (g+h)(f(a)) \\ &= g(g(a)) + h(f(a)) \\ &= (g \circ f)(a) + (h \circ f)(a) \\ &= (g \circ f + h \circ f)(a) \\ &\Rightarrow (g+h) \circ f = g \circ f + h \circ f \end{aligned}$$

$\Rightarrow (\text{End}(A), +, \circ)$ je kolobar z enoto id_A. V spolšnem komutativen.

$\square$

Definicija. *Naj bo K kolobar in $a, b \in K$ taka neničelna elementa, da je $ab = 0$. Elementoma a in b pravimo* ***delitelja niča****. Natančneje, a je* ***levi delitelj niča****, b pa* ***desni delitelj niča****.*

PRIMER

- V $\mathbb{Z}_6$ velja $[2][3] = [0]$
- V primeru 6 je veljajo $(0, 1, 0)(1, 0, 0) = (0, 0, 0)$
- $(F(\mathbb{R}, +, \cdot))$ naj bo kolobar vseh realnih funkcij z operacijama po točkah. Naj bo $f(x) = \begin{cases} 1; & x = 0 \\ 0; & x \neq 0 \end{cases}$ in $g(x) = \begin{cases} 0, & x = 0 \\ 1, & x \neq 0 \end{cases}$. Potem je $f(x) \cdot g(x) = 0,\ \forall x \in \mathbb{R}$.

  Torej je $f \cdot g = 0$. f in g sta delitelja niča.

Definicija. *Kolobar K je* ***obseg****, kadar ima enoto $1 \neq 0$ in je vsak njegov neničelni element obrnljiv: $\forall a \in K \backslash \{0\}\ \exists a^{-1} \in K$, da je $a \cdot a^{-1} = 1 = a^{-1} \cdot a$.*

Ekvivalentno: kolobar K je obseg $\Leftrightarrow K \backslash \{0\}$ grupa za množenje.

<u>Opomba 1:</u> Če ima K vsaj dva elementa, pogoj $1 \neq 0$ ni potreben. Če je $1 = 0$, namreč za vsak $x \in K$ velja $x = 1 \cdot x = 0 \cdot x = 0 \Rightarrow |K| = 1$.

<u>Opomba 2:</u> Če je K nekomutativen obseg, je lahko $xy^{-1} \neq y^{-1}x$, zato izraz $\frac{x}{y}$ ni dobro definiran.

Definicija. ***Polje*** *je komutativen obseg. Letos bodo vsi obsegi komutativni. Ne bomo posebej omenjali, da so komutativni.*

Trditev. *V obsegu ni deliteljev niča.*

Dokaz. Recimo, da obstajata $a, b \in K$ (K je obseg), da je $a \neq 0$, $b \neq 0$ in $ab = 0$.

Ker $a \neq 0$, obstaja $a^{-1} \in K$

$$a^{-1}\ /\ ab = 0$$
$$b = a^{-1}ab = 0$$
$$\text{Protislovje}$$

$\square$

PRIMERI OBSEGOV: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

Trditev. *$\mathbb{Z}_n$ je obseg $\Leftrightarrow$ n je praštevilo.*

Dokaz.

($\Rightarrow$): Predpostavimo, da je število n sestavjeno: $n = p \cdot q,\ 1 < p, q < n$.

Iz tega sledi: $[p][q] = [0]$.

$\mathbb{Z}_n$ ima torej delitelje niča, torej ni obseg.

($\Leftarrow$): Predpostavimo, da je n praštevilo.

Naj bo $[a] \neq [0], [a] \in \mathbb{Z}_n$ poljuben.

n ne deli števila a

$a, 2a, \ldots, (n-1)a$

Nobeno od števil $a, 2a, \ldots, (n-1)a$ ni deljiv z n, ker je n praštevilo.

Velja tudi, da dajo ta števila paroma različne ostanke pri deljenju z n.

Če bi namreč veljajo $[ka] = [la]$ za neka $1 \leq k < l \leq n-1$, potem bi n delil $(l-k)a$, kjer je $l - k \in \{1, \ldots, n-1\}$.

To nas dovede do protislovja.

Torej so ostanki $[a], [2a], \ldots, [(n-1)a]$ paroma različni in nobeden ni $[0]$.

Torej je $[ka] = [1]$ za vsak $1 \leq k \leq n-1$.

$\Rightarrow [k] = [a]^{-1}$ v $\mathbb{Z}_n \Rightarrow \mathbb{Z}_n$ je obseg.

$\square$

4 KONČNORAZSEŽNI VEKTORSKI PROSTORI

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

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

ki ustreza naslednjim pogojem:

- $(\alpha+\beta)v = \alpha v + \beta v,\ \forall \alpha, \beta \in \mathcal{O},\ \forall v \in V$
- $\alpha(u+v) = \alpha u + \alpha v,\ \forall \alpha \in \mathcal{O},\ \forall u, v \in V$
- $\alpha(\beta v) = (\alpha\beta)v,\ \forall \alpha, \beta \in \mathcal{O},\ \forall v \in V$
- $1v = v,\ \forall v \in V$

Elemente iz $\mathcal{O}$ imenujemo ***skalarji****, elemente iz V pa imenujemo* ***vektorji****. Zunanjo operacijo imenujemo* ***množenje s skalarji****.*

4.1 Baza in razsežnost

Definicija. *Naj bo V vektorski prostor nad obsegom $\mathcal{O}$ in $M \subseteq V$ poljubna množica. Pravimo, da je M **ogrodje** prostora V, kadar je Lin(M) $= V$. Pravimo tudi, da M **generira** V in elementom M pravimo **generatorji**.*

Ogrodje prostora V je torej taka množica M, da vsak vektor iz V lahko izrazimo kot (končno!) linearno kombinacijo elementov iz M.

Definicija. *Naj bo $M \in V$ neka neprazna množica. Pravimo, da je Lin(M) $= \{\alpha_1 x_1 + \ldots + \alpha_k x_k | x_1, \ldots, x_k \in M,\ \alpha_1, \ldots, \alpha_k \in \mathcal{O},\ k \in \mathbb{N}\}$ **linearna ogrinjača množice** M. Velja tudi, da je Lin(M) vektorski podprostor vektorskega prostora V (Lin(M) $\leq V$). Lin(M) je najmanjši vektorski podprostor, ki vsebuje M.*

PRIMERI:

- V $\mathcal{O}^n$ za vsak $j = 1, \ldots, n$ označimo $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$.

  Potem je $\{e_1, \ldots, e_n\}$ ogrodje prostora $\mathcal{O}^n$. Zakaj?

  Naj bo $x \in \mathcal{O}^n$ poljuben (pri čemer velja $x = x_1, x_2, \ldots, x_n$).

  Potem je $x = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n$.
- $\mathbb{R}[X]$.

  Ogrodje je $\{1, x, x^2, \ldots\}$.

  Ogrodje je neskončno, a vsak polinom $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ je končna linearna kombinacija polinomov $1, x, x^2, \ldots, x^n$.

Definicija. *Vektorski prostor je **končnorazsežen**, kadar ima kakšno končno ogrodje.*

PRIMERI:

- $\mathcal{O}^n$ je končnorazsežen
- $\mathbb{R}[X]$ ni končnorazsežen: Če je $M = \{p_1(x), \ldots, p_n(x)\}$ poljubna končna množica polinomov, potem noben polinom v Lin(M) nima stopnje večje od stopenj polinomov $p_1(x), \ldots, p_n(x)$.
- Prostor polinomov stopnje največ n je končnorazsežen.
- Prostor vseh funkcij $\mathbb{R} \to \mathbb{R}$ ni končnorazsežen.

Letos bodo vsi vektorski prostori končnorazsežni. Vsak vektorski prostor ima ogrodje, saj je Lin(V)=V. Radi bi našli čim manjše ogrodje.

Trditev. *Naj bo M ogrodje vektorskega prostora V in $v \in M$ tak vektor, ki* pripada Lin($M \backslash \{v\}$) [1]. *Potem je $M \backslash \{v\}$ tudi ogrodje prostora V.*

Dokaz. Naj bo $x \in V$ poljuben.

Potem, ker je M ogrodje za V, obstajajo $\alpha_1, \ldots, \alpha_n \in O$ in $u_1, \ldots, u_n \in M$, da je $x = \alpha_1 u_1 + \cdots + \alpha_n u_n$.

Če je $u_i \neq v$ za vsak $i = 1, \ldots, n$, je $x \in \text{Lin}(M \backslash \{v\})$.

Predpostavimo še, da je $v = u_i$, za nek i.

Predpostavimo lahko, da je $v = u_1$ in $v \neq u_j$ za $j \geq 2$.

Ker je $v \in \text{Lin}(M \backslash \{v\})$, obstajajo $v_1, \ldots, v_m \in M \backslash \{v\}$ in $\beta_1, \ldots, b_m \in O$, da je $v = \beta_1 v_1 + \ldots + \beta_m v_m$

Potem je $x =$ [2] $\alpha_1 \beta_1 v_1 + \ldots + \alpha_1 \beta_m v_m +$ [3] $\alpha_2 u_2 + \ldots + \alpha_n u_n \in \text{Lin}(M \backslash \{v\})$.

Vsak vektor iz V se da izraziti kot linearno kombinacijo elementov iz $M \backslash \{v\}$, torej je $M \backslash \{v\}$ ogrodje prostora V.

□

Definicija. *Vektorji $v_1, \ldots, v_n \in V$ so **linearno neodvisni**, kadar velja naslednji sklep: Če so $\alpha_1, \ldots, \alpha_n \in \mathcal{O}$ in je $\alpha_1 v_1 + \ldots + \alpha_n v_n = 0$, potem je $\alpha_1 = \ldots = \alpha_n = 0$.*

Vektorji so **linearno odvisni**, kadar niso linearno neodvisni.

Končna množica $M \subseteq V$ je **linearno neodvisna**, kadar je vsaka njena končna podmnožica sestavljena iz linearno neodvisnih vektorjev.

Vedno iz $\alpha_1 = \ldots = \alpha_n = 0$ sledi $\alpha_1 v_1 + \ldots + \alpha_n v_n = 0$.

Definicija linearne neodvisnosti je obrat te implikacije. $v_1, \ldots, v_n$ so linearno neodvisni, kadar se ne more zgoditi, da je $\alpha_1 v_1 + \ldots + \alpha_n v_n = 0$, vendar $\alpha_1, \ldots, \alpha_n$ niso vsi 0.

[1] v lahko izrazimo kot linearno kombinacijo ostalih vektorjev iz M

[2] $\in \text{Lin}(M \backslash \{v\})$

[3] $\in \text{Lin}(M \backslash \{v\})$

PRIMER:

- $\{0\}$ je linearno odvisna množica: $1 \cdot 0 = 0$ $(1 = \alpha \neq 0)$.
- $\{e_1, \ldots, e_n\}$ je linearno neodvisna množica v $\mathcal{O}^n$. Zakaj?

  Recimo, da je $\alpha_1 e_1 + \ldots + \alpha_n e_n = (0, \ldots, 0) \Rightarrow \alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$.

  $(\alpha_1 e_1 + \ldots + \alpha_n e_n = \alpha_1, \alpha_2, \ldots, \alpha_n)$
- Vektorji $(1, 1, -1), (1, 1, 2)$ in $(-2, 2, 2)$ so linearno odvisni, saj je $2 \cdot (1, 1, -1) + 0 \cdot (1, 1, 2) + 1 \cdot (-2, -2, 2) = (0, 0, 0)$.

Trditev. *Vektorji $v_1, \ldots, v_n \in V$ so linearno odvisni natanko takrat, ko enega od njih lahko izrazimo kot linearno kombinacijo prejšnjih.*

Dokaz.

$(\Rightarrow)$: Naj bodo $v_1, \ldots, v_n \in V$ linearno odvisni.

Potem obstajajo $\alpha_1, \ldots, \alpha_n \in O$, ne vsi 0, da je $\alpha_1 v_1 + \ldots + \alpha_n v_n = 0$.

Naj bo k največji indeks, za katerega je $\alpha_k \neq 0$.

Torej je $\alpha_1 v_1 + \ldots + \alpha_k v_k + 0 \cdot v_{k+1} + \ldots = 0$. Zato:

$$\alpha_1 v_1 + \ldots + \alpha_{k-1} v_{k-1} = -\alpha_k v_m / : \ (-\alpha_k)^{-1}$$
$$v_k = -\alpha_1 \alpha_k^{-1} v_1 - \ldots - \alpha_{k-1} \alpha_k^{-1} v_{k-1}$$

$(\Leftarrow)$: Dokazali bomo, da so vektorji linearno odvisni, če je kakšen linearna kombinacija ostalih (ne nujno prejšnjih).

Recimo, da je $v_j = \sum_{k \neq j} \alpha_k v_k$ za nek $\alpha_k \in O$.

Potem je $\alpha_1 v_1 + \ldots + \alpha_{j-1} v_{j-1} + (-1) v_j + \alpha_{j+1} v_{j+1} + \ldots + \alpha_n v_n = 0 \Rightarrow$ Vektorji $v_1, \ldots, v_n$ so linearno odvisni.

$\square$

Definicija. ***Baza*** *vektorskega prostora V je množica B, ki je hkrati linearno neodvisna in ogrodje.*

PRIMERI:

- Vsaki trije linearno neodvisni vektorji v $\mathbb{R}^3$ tvorijo bazo
- Množica $\{e_1, \ldots, e_n\}$ ($e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$) je baza prostora $\mathcal{O}^n$. Pravimo ji **standardna baza** prostora $\mathcal{O}^n$
- $\{1, x, x^2, \ldots\}$ je (neskončna) baza prostora $\mathbb{R}[X]$.

Izrek. *Množica $B = \{v_1, \ldots, v_n\}$ je baza vektorskega prostora V natanko takrat, ko vsak $x \in V$ lahko enolično zapišemo v obliki $x = \alpha_1 v_1 + \ldots + \alpha_n v_n$, kjer so $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$.*

Dokaz.

($\Rightarrow$) Naj bo B baza in $x \in V$ poljuben.

Ker je B ogrodje, je $x = \alpha_1 v_1 + \ldots + \alpha_n v_n$ za neki $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$.

Dokazati je treba še enoličnost tega zapisa.

Recimo, da je $x = \alpha_1 v_1 + \ldots + \alpha_n v_n = \beta_1 v_1 + \ldots + \beta_n v_n \Rightarrow$

$\Rightarrow (\alpha_1 - \beta_1)v_1 + \ldots + (\alpha_n - \beta_n)v_n = 0.$

Ker so $v_1, \ldots, v_n$ linearno neodvisni, je $\alpha_1 - \beta_1 = 0, \ldots, \alpha_n - \beta_n = 0 \Rightarrow$

$\Rightarrow \alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n$

($\Leftarrow$) Predpostavimo, da se da vsak vektor $x \in V$ na enoličen način zapisati kot $x = \alpha_1 v_1 + \ldots + \alpha_n v_n,\ \alpha \in O$.

Potem takoj sledi, da je B ogrodje.

Dokažimo še linearno neodvisnost.

Naj bo $\alpha_1 v_1 + \ldots + \alpha_n v_n = 0 = 0 \cdot v_1 + \ldots + 0 \cdot v_n$.

Ker je zapis $\alpha_1 v_1 + \ldots + \alpha_n v_n$ enoličen, je $\alpha_1 = 0, \alpha_2 = 0, \ldots, \alpha_n = 0$.

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

$\square$

Izrek. *Vsak netrivialen končnorazsežen vektorski prostor ima bazo. Izberemo jo lahko iz poljubnega končnega ogrodja.*

Opomba: Tudi neskončnorazsežni vektorski prostori imajo bazo, kar lahko dokažemo z Zornovo lemo.

Dokaz. Naj bo $\{v_1, \ldots, v_n\}$ poljubno končno ogrodje prostora V.

Predpostavimo lahko, da je $v_j \neq 0$ za vsak j.

Zaporedoma od leve proti desni iz ogrodja odstranjujemo vektorje, ki so linearna kombinacija prejšnjih. Na vsakem koraku odstranimo vektor, ki je linearna kombinacija ostalih, zato po odstranitvi še vedno imamo ogrodje. Postopek se po končno korakih konča in dobimo ogrodje $\{u_1, \ldots, u_m\}$. Ker se je postopek končal, noben vektor u_j ni linearna kombinacija prejšnjih. To pa pomeni, da so vektorji $u_1, \ldots, u_m$ linearno neodvisni in torej tvorijo bazo. □

Trditev. *Naj bo $\{v_1, \ldots, v_m\}$ poljubno ogrodje vektorskega prostora V. Potem nobena linearno neodvisna podmnožica prostora V nima več kot m elementov.*

Dokaz. Naj bo $\{u_1, \ldots, u_m\}$ linearno neodvisna množica vektorjev v V. Dokazu, ki bo sledil, rečemo nadomeščanje vektorjev.

Ker je $\{v_1, \ldots, v_m\}$ ogrodje, je $u_1 \in Lin\{v_1, \ldots, v_m\}$. Zato je $\{u_1, v_1, \ldots, v_m\}$ linearno odvisna množica.

Torej je en od vektorjev iz te množice linearna kombinacija prejšnjih. To ni u_1, torej je to eden od vektorjev v_j. Tega lahko odstranimo in še vedno dobimo ogrodje $\{u_1, v_1+, \ldots, v'_{m-1}\}$. To je ogrodje, zato je $u_2 \in Lin\{u_1, v_1+, \ldots, v_{m-1}\}$ in zato je množica $\{u_1, u_2, v'_1, \ldots, v_{m-1}\}$ linearno odvisna.

Eden od vektorjev iz te množice je linearna kombinacija prejšnjih. To je vektor v'_j za nek j, saj sta u_1 in u_2 linearno neodvisna. Ta v'_j odstranimo in spet dobimo ogrodje $\{u_1, u_2, u''_1, \ldots, u''_{m-?}\}$. To ponavljamo.

Recimo, da je $n > m$.

Na m-tem koraku dobimo ogrodje $\{u_1, \ldots, u_m\}$.

Ker je $n > m$ obstaja $u_{??}$ in ker je $\{u_1, \ldots, u_?\}$ ogrodje, je $u_{??}$ linearna kombinacija vektorjev $u_1, \ldots, u_m$.

To je v protislovju z linearno neodvisnostjo vektorjev $u_1, \ldots, u_n$. Torej je $n \leq m$. □

Posledica. *Vse baze končnorazsežnega vektorskega prostora imajo isto moč.*

Dokaz. Naj bosta B_1 in B_2 bazi prostora V in naj bo $|B_1| = n$ in $|B_2| = m$.

B_1 je ogrodje, B_2 pa linearno neodvisna $\Rightarrow n \geq m$.

B_2 je tudi ogrodje, B_1 pa linearno neodvisna $\Rightarrow m \geq n \Rightarrow m = n$.

□

Definicija. *Moč baze (končnorazsežnega) vektorskega prostora V se imenuje* ***razsežnost*** *ali* ***dimenzija*** *prostora V. Oznaka: $dimV$.*

Trditev. *Vsako linearno neodvisno podmnožico končnorazsežnega vektorskega prostora lahko dopolnimo do baze.*

Dokaz. Naj bodo $v_1, \ldots, v_n$ linearno neodvisni vektorji in $B = \{u_1, \ldots, u_m\}$ poljubna baza prostora V.

Vemo že, da je $m \geq n$.

Kot v dokazu prejšnje trditve vektorje u_i zaznamujemo z vektorji v_j.

Dobimo ogrodje $B' = \{v_1, \ldots, v_n, u'_1, \ldots, u'_{m-n}\}$.

Iz tega ogrodja lahko izberemo bazo.

Ker imajo vse baze m elementov, je B' že baza.

Množico $\{v_1, \ldots, v_n\}$ smo torej dopolnili do baze B'.

□

PRIMER:

- Vektorja $(1, 1, 1)$ in $(0, 1, 1)$ sta očitno linearno neodvisna. Dopolnimo ju do baze $\mathbb{R}^3$.

  Izberemo si standardno bazo $B = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ prostora $\mathbb{R}^3$. Potem je $\{(1, 1, 1), (0, 1, 1), (1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ ogrodje prostora $\mathbb{R}^3$. Od leve proti desni odstranjujemo vektorje, ki so linearna kombinacija prejšnjih. Ker sta $(1, 1, 1)$ in $(0, 1, 1)$ linearno neodvisna, ju ne odstranimo.

  $(1, 0, 0) = (1, 1, 1) - (0, 1, 1) \Rightarrow (1, 0, 0)$ odstranimo.

Ali je $(0,1,0) = \alpha(1,1,1) + \beta(0,1,1)$?

$$\begin{aligned} 0 &= \alpha \\ 1 &= \alpha + \beta \\ 0 &= \alpha + \beta \end{aligned}$$

To je protislovje $\Rightarrow (1,1,1), (0,1,1)$ in $(0,1,0)$ so linearno neodvisni.

$(0,0,1)$ bo zagotovo linearna kombinacija teh <u>treh linearno neodvisnih</u> vektorjev v $\underline{\mathbb{R}^3}$
$\Rightarrow \{(1,1,1),(0,1,1),(0,1,0)\}$ je baza $\mathbb{R}^3$.

Posledica.

1. *Če je dim$V = n$ in so vektorji $v_1, \ldots, v_n$ linearno neodvisni, potem tvorijo bazo*
2. *Naj bo W vektorski podprostor prostora V. Potem je dim$W \leq$ dim$V$ in enakost velja le v primeru, ko je $W = V$.*

Dokaz.

1. Ker so $v_1, \ldots, v_n$ linearno neodvisni, jih lahko dopolnimo do baze.

   Vse baze imajo n elementov, zato ne smemo ničesar dodati.

   Torej je $\{v_1, \ldots, v_n\}$ že baza.

2. V W izberemo bazo $\{w_1, \ldots, w_m\}$.

   Ta množica je linearno neodvisna, zato jo lahko dopolnimo do baze $\{w_1, \ldots, w_m, v_1, \ldots, v_n\}$ prostora V.

$$\begin{aligned} dimW &= m \\ dimV &= m + n \end{aligned}$$

   Kdaj je dim$W =$dim$V$? $\Leftrightarrow \{w_1, \ldots, w_m\}$ je baza za V.

   $W = \text{Lin}\{w_1, \ldots, w_m\} = V$.

$\square$

Trditev. *Naj bosta W in U vektorska podprostora prostora V. Potem je dim$(W + U) =$dim$W+$dim$U-$dim$(W \cap U)$.*

Dokaz. Na vajah.

□

Posledica. *dim*$(W \oplus U) =$*dim*$W+$*dim*U

Dokaz. Če je vsota direktna, je $W \cap U = \{0\}$.

□

Trditev. *Naj bo W vektorski podprostor končnorazsežnega vektorskega prostora V. Potem obstaja vektorski podprostor U prostora V, da je $W \oplus U = V$. Podprostoru U rečemo **direktni komplement** podprostora W.*

Dokaz. Če je $W = \{0\}$, vzamemo $U = V$.

Če je $W = V$, vzamemo $U = \{0\}$.

Predpostavimo, da je $W \neq \{0\}$ in $W \neq V$.

Izberemo bazo $\{w_1, \ldots, w_n\}$ prostora W in jo dopolnimo do baze $\{w_1, \ldots, w_n, u_1, \ldots, u_m\}$ prostora V.

$m > 0$, ker je $W \neq V$.

Definiramo $U =$Lin$\{u_1, \ldots, u_m\}$.

Dokažimo, da je $W \cap U = \{0\}$ in $W + U = V$.

Recimo, da je $x \in W \cap U$. Torej je $x = \alpha_1 w_1 + \ldots + \alpha_n w_n = \beta_1 u_1 + \ldots + \beta_m u_m$ za neke $\alpha_i, \beta_j \in O \Rightarrow \alpha_1 w_1 + \ldots + \alpha_n w_n - \beta_1 u_1 - \ldots \beta_m u_m = 0$.

Ker je $\{w_1, \ldots, w_n, u_1, \ldots, u_m\}$ baza prostora V, je $\alpha_1 = \ldots = \alpha_n = \beta_1 = \ldots = \beta_n = 0 \Rightarrow x = 0 \Rightarrow W \cap U = \{0\}$.

Naj bo $x \in V$ poljuben. Ker je $\{w_1, \ldots, w_n, u_1, \ldots, u_m\}$ baza za V, je $x = \alpha_1 w_1 + \ldots + \alpha_n w_n + \beta_1 u_1 + \ldots + \beta_m u_m$ za neke $\alpha_i, \beta_j \in O$.

Ker je $(\alpha_1 w_1 + \ldots + \alpha_n w_n) \in W$ in $(\beta_1 u_1 + \ldots + \beta_m u_m) \in U$, je $(\alpha_1 w_1 + \ldots + \alpha_n w_n + \beta_1 u_1 + \ldots + \beta_m u_m) \in W + U$.

□

Trditev. *Naj bosta U in V vektorska prostora nad obsegom $\mathcal{O}$ in $\mathcal{A} : U \to V$ linearna preslikava. Potem velja:*

- *Če je $\mathcal{A}$ injektivna, je slika vsake linearno neodvisne množice linearno neodvisna.*
- *Če je $\mathcal{A}$ surjektivna, je slika vskega ogrodja za U ogrodje za V.*
- *Če je $\mathcal{A}$ bijektivna, je slika vsake baze prostora U baza prostora V.*

1) *Dokaz.* Naj bodo $u_1, \ldots, u_n \in U$ linearno neodvisni in $\mathcal{A} : U \to V$ injektivna.

Naj bo $\alpha \mathcal{A} u_1 + \ldots + \alpha_n \mathcal{A} u_n = 0$ za neke $\alpha_j \in O$.

Radi bi dokazali, da je $\alpha_1 = \ldots = \alpha_n = 0$.

Upoštevamo linearnost: $\mathcal{A}(\alpha_1 u_1 + \ldots + \alpha_n u_n) = 0$.

Ker je $\mathcal{A}$ injektivna, je $\alpha_1 u_1 + \ldots + \alpha_n u_n = 0$.

Ker so $u_1, \ldots, u_n$ linearno neodvisni, sledi $\alpha_1 = \ldots = \alpha_n = 0 \Rightarrow \mathcal{A}u_1, \ldots, \mathcal{A}u_n$ so linearno neodvisni.

$\square$

2) *Dokaz.* Predpostavimo, da je $\{u_1, \ldots, u_n\}$ ogrodje prostora U.

Radi bi dokazali, da je $\{\mathcal{A}u_1, \ldots, \mathcal{A}u_n\}$ ogrodje prostora V, če je $\mathcal{A}$ surjektivna.

Naj bo $x \in V$ poljuben. Ker je $\mathcal{A}$ surjektivna, obstaja $y \in U$, da je $x = \mathcal{A}y$.

Ker je $\{u_1, \ldots, u_n\}$ ogrodje za U, je $y = \alpha_1 u_1 + \ldots + \alpha_n u_n$ za neke $\alpha_1, \ldots, \alpha_n \in O$

$\Rightarrow x = \mathcal{A}y = \mathcal{A}(\alpha_1 u_1 + \ldots + \alpha_n u_n) = \alpha_1 \mathcal{A} u_1 + \ldots + \alpha_n \mathcal{A} u_n$

$\Rightarrow \{\mathcal{A}u_1, \ldots, \mathcal{A}u_n\}$ je ogrodje za V.

$\square$

3) *Dokaz.* Sledi iz 1) in 2) $\square$

Izrek.

(1) Naj bo V n-razsežen vektorski prostor nad obsegom $\mathcal{O}$ ($n > 0$). Potem je V izomorfizem $\mathcal{O}^n$

(2) Končnorazsežna vektorska prostora nad istim obsegom sta izomorfna natanko takrat, ko imata isto razsežnost.

Dokaz.

(1) Naj bo $B = \{v_1, \ldots, v_n\}$ baza prostora V.

Definiramo preslikavo $\phi : \mathcal{O}^n \to V$ s predpisom $\phi(\alpha_1, \ldots, \alpha_n) = \alpha_1 v_1 + \ldots + \alpha_n v_n$.

Dokazati moramo, da je ϕ linearna in bijektivna.

<u>Linearnost</u>:

- Naj bosta $(\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n) \in \mathcal{O}^n$ poljubni n-terici in naj bosta $\lambda, \mu \in O$.

  Potem je

$$\begin{aligned}
\phi(\lambda(\alpha_1, \ldots, \alpha_n) + \mu(\beta_1, \ldots, \beta_n)) &= \phi(\lambda\alpha_1 + \mu\beta_1, \ldots, \lambda\alpha_n + \mu\beta_n) \\
&= (\lambda\alpha_1 + \mu\beta_1)v_1 + \ldots + (\lambda\alpha_n + \mu\beta_n)v_n \\
&= \lambda\alpha_1 v_1 + \mu\beta_1 v_1 + \ldots + \lambda\alpha_n v_n + \mu\beta_n v_n \\
&= \lambda(\alpha_1 v_1 + \ldots + \alpha_n v_n) + \mu(\beta_1 v_1 + \ldots + \beta_n v_n) \\
&= \lambda\phi(\alpha_1, \ldots, \alpha_n) + \mu\phi(\beta_1, \ldots, \beta_n)
\end{aligned}$$

<u>Injektivnost</u>:

- Dovolj je dokazati, da je $\ker\phi = \{(0, \ldots, 0)\}$.

  Naj bo $(\alpha_1, \ldots, \alpha_n) \in \mathrm{Ker}\phi$.

  Potem je $\alpha_1 v_1 + \ldots + \alpha_n v_n = 0$.

  Vektorji $v_1, \ldots, v_n$ so linearno neodvisni, zato je $\alpha_1 = \ldots = \alpha_n = 0$.

<u>Surjektivnost</u>:

- Naj bo $x \in V$.

  Potem je $x = \alpha_1 v_1 + \ldots + \alpha_n v_n$ za neke $\alpha_1, \ldots, \alpha_n \in O \Rightarrow x = \phi(\alpha_1, \ldots, \alpha_n) \in \mathrm{Im}\phi$.

(2) ($\Leftarrow$) Recimo, da je $n = \mathrm{dim}U = \mathrm{dim}V$.

Če je $n = 0$, sta U in V triviralna prostora in sta izomorfna.

Če je $n > 0$, pa je V izomorfen $\mathcal{O}^n$, prav tako U (po točki (1)).

Izomorfnost je ekvivalenčna relacija, zato sta U in V izomorfna.

($\Rightarrow$) Naj bosta U in V izomorfna in $A : U \to V$ izomorfizem.

Če je $U = \{0\}$, potem je očitno tudi $V = \{0\} \Rightarrow \mathrm{dim}U = \mathrm{dim}V = 0$.

Če je U netrivialen, pa ima bazo B.

Po prejšnji trditvi je $A(B) =$ baza za V.

Ker je A bijektivna, je $|B| = |A(B)| \Rightarrow \mathrm{dim}U = \mathrm{dim}V$.

$\square$

Izrek. *Naj bosta U in V končnorazsežna vektorska prostora nad $\mathcal{O}$ in $\mathcal{A} : U \to V$ linearna preslikava. Potem je dim(Ker$\mathcal{A}$) + dim(Im$\mathcal{A}$) = dim$U$.*

Dokaz. Naj bo $\{v_1, \ldots, v_n\}$ baza prostora Im$\mathcal{A}$.

(Predpostavimo, da je slika netrivialna, saj je sicer Ker$\mathcal{A} = U$ in formula očitno velja).

Izberemo poljubne vektorje $u_1, \ldots, u_n \in U$, da je $v_j = \mathcal{A}u_j$ za $j = 1, \ldots, n$.

Izberemo še bazo prostora Ker$\mathcal{A}$: $\{w_1, \ldots, w_k\}$.

Če dokažemo, da je $B = \{u_1, \ldots, u_n, w_1, \ldots, w_k\}$ baza prostora U, bo formula veljala, saj bo dim(Ker$\mathcal{A}$) $= k$, dim(Im$\mathcal{A}$) $= n$ in dim$U = n + k$.

B je linearno neodvisna

Recimo, da je $\alpha_1 u_1 + \ldots + \alpha_n u_n + \beta_1 w_1 + \ldots + \beta_n w_n = 0$.

Potem je

$$\begin{aligned} 0 = \mathcal{A}0 &= \mathcal{A}(\alpha_1 u_1 + \ldots + \alpha_n u_n + \beta_1 w_1 + \ldots + \beta_k w_k) \\ &= \alpha_1 \mathcal{A}u_1 + \ldots + \alpha_n \mathcal{A}u_n + \beta_1 \mathcal{A}w_1 + \ldots + \beta_k \mathcal{A}w_k \\ &= \alpha_1 v_1 + \ldots + \alpha_n v_n \end{aligned}$$

Vektorji $v_1, \ldots, v_n$ so linearno neodvisni, zato je $\alpha_1 = \ldots = \alpha_n = 0 \Rightarrow \beta_1 w_1 + \ldots + \beta_k w_k = 0$.

Vektorji $w_1, \ldots, w_k$ so linearno neodvisni, zato je $\beta_1 = \ldots = \beta_n = 0$.

B je ogrodje

Naj bo $x \in U$ poljuben.

Potem je $Ax \in \mathrm{Im}\mathcal{A}$, zato je $\mathcal{A}x = \alpha_1 v_1 + \ldots + \alpha_n v_n$.

Definirajmo $y = \alpha_1 u_1 + \ldots + \alpha_n u_n$.

Potem je $\mathcal{A}y = \alpha_1 v_1 + \ldots + \alpha_n v_n = \mathcal{A}x \Rightarrow \mathcal{A}(x-y) = 0 \Rightarrow x - y \in \mathrm{Ker}\mathcal{A}$.

Ker je $\{w_1, \ldots, w_k\}$ baza za $\mathrm{Ker}\mathcal{A}$, obstajajo $\beta_1, \ldots, \beta_k \in O$, da je $x - y = \beta_1 w_1 + \ldots + \beta_k w_k \Rightarrow x = \alpha_1 u_1 + \ldots + \alpha_n u_n + \beta_1 w_1 + \ldots + \beta_k w_k$.

$\square$

4.2 Vektorski podprostor

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

- $x, y \in U \Rightarrow x + y \in U$
- $x \in U \Rightarrow \alpha x \in U, \ \forall \alpha \in \mathcal{O}$
- $(U, +)$ *je podgrupa grupe* $(V, +)$.

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

Vsak podprostor vsebuje ničlo oz. ničelni vektor $\vec{O}$: $x \in U \Rightarrow 0 \cdot x = 0 \in U$.

Nasprotni element je element podprostora: $x, y \in U \Rightarrow x - y = x + (-1) \in U$

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

4.3 Kvocientne strukture

4.3.1 Ponovitev relacij

Binarna (dvočlena) relacija med elementi množice A in B je neprazna podmnožica kartezičnega produkta $A \times B$.

Relacijo si lahko mislimo kot posplošitev grafa preslikave $A \to B$. Običajno relacijo razumemo kot zvezo med elementi množice A in B. Če je relacija namesto $(x, y) \in R$ pišemo xRy. Pravimo, da je x **v relaciji** R **z** y.

Najbolj pogosto primer je, ko je $B = A$. V tem primeru rečemo, da je R **relacija na** A. Pišemo tudi $R \subseteq A \times A$.

4.3.2 Nekaj lastnosti relacij

Relacija R na A je **refleksivna**, kadar velja xRx za vsak $x \in A$.

Relacija R na A je **simetrična**, kadar velja sklep: $xRy \Rightarrow yRx$.

Relacija R na A je **antisimetrična**, kadar velja sklep: $(xRy, yRx) \Rightarrow x = y$.

Relacija R na A je **tranzitivna**, kadar velja sklep: $(xRy, yRz) \Rightarrow xRz$.

Relacija R na A je **relacija delne urejenosti**, kadar je refleksivna, antisimetrična in tranzitivna.

Naj R relacija delne urejenosti na A. Elementa $x, y \in A$ sta **primerljiva**, kadar je xRy ali yRx. Relacija delne urejenosti, kjer sta vsaka dva elementa primerljiva, se imenuje **relacija linearna urejenosti**.

Naj bo R relacija delne urejenosti na A. Element $x \in A$ je **maksimalen element** glede na relacijo R, kadar velja sklep $xRy \Rightarrow x = y$. Element $x \in A$ je **minimalen element** glede na relacijo R, kadar velja sklep $yRx \Rightarrow x = y$.

Minimalni in maksimalni elementi ne obstajajo nujno. Če obstajajo, niso nujno enolični.

Naj bo R relacija delne urejenosti na A. Element $x \in A$ je **največji element** glede na R, kadar velja yRx za vsak $y \in A$. Element $x \in A$ je **najmanjši element** glede na R, kadar velja xRy za vsak $y \in A$.

Največji in najmanjši elementi ne obstajajo nujno. Če obstajajo, so enolični. Največji element je vedno maksimalen, najmanjši pa minimalen. Obrat ne velja nujno.

PRIMER:

- $M \neq \emptyset$ naj bo poljubna množica, $|M| \geq 2$. A naj bo množica vseh nepraznih podmnožic množice M. A delno uredimo z inkluzijo.

  Edini maksimalni element je M. Je tudi največji, ker so vse podmnožice M (elementi A) vsebovani v M.

  Minimalni elementi so množice z 1 elementom. Ni najmanjšega elementa. Če bi bila množica X najmanjši element, bi bila tudi minimalen element, torej množica z 1 elementom: $X = \{a\}$. Ker je $|M| \geq 2, \exists b \in M \backslash \{a\}$. $X = \{a\} \not\subseteq \{b\}$. Torej X ni najmanjši element.

4.3.3 Ponovitev ekvivalenčne relacije

Relacija R na A je **ekvivalnečna relacija**, kadar je refleksivna, simetrična in tranzitivna. Če je $\sim$ ekvivalenčna relacija in je $x \sim y$, je tudi $y \sim x$. V tem primeru pravimo, da sta elementa x in y **ekvivalentna**.

Naj bo $\sim$ ekvivalnečna relacija na množici A in $a \in A$. **Ekvivalenčni razred** elementa a je množica $[a]_\sim = \{x \in A; x \sim a\}$. Kadar je jasno, za katero relacijo gre, pišemo $[a]$ namesto $[a]_\sim$. Elementu a rečemo **predstavnik** ekvivalenčnega razreda $[a]$. Vsak element ekvivalenčnega razreda $[a]$ je njegov predstavnik, in vsi predstavniki so med seboj ekvivalentni.

Izrek. *Ekvivalenčni razredi razdelijo množico A na unijo paroma disjunktnih ekvivalenčnih razredov, ki so neprazni. Pri tem sta dva elementa množice A ekvivalentna natanko takrat, ko ležita v istem ekvivalenčnem razredu.*

Dokaz. LMN

□

Definicija. ***Razdelitev (particija)*** *množice A je množica nepraznih podmnožic množice A, ki so paroma disjunktne in je njihova unija enaka A.*

Izrek. *Množica A je disjunktna unija nepraznih množic A_i natanko takrat, ko na A obstaja ekvivalenčna relacija za katero so A_i ekvivalenčni razredi.*

Dokaz. LMN

□

Definicija. *Naj bo $\sim$ ekvivalenčna relacija na množici A. Množico vseh ekvivalenčnih razredov glede na to relacijo imenujemo* ***kvocientna*** *ali* ***faktorska množica*** *množice A po relaciji $\sim$ in jo označimo $A/_\sim$. Preslikava $q : A \to A/_\sim$, definirana s predpisom $q(a) = [a]$, pa se imenuje* ***kanonična kvocientna preslikava****.*

PRIMERI:

- Na $\mathbb{Z} \times \mathbb{N}$ definiramo relacijo $\sim$ s predpisom $(m, n) \sim (p, q) \Leftrightarrow mq = np$.

  Refleksivnost: $mn = mn \Rightarrow (m, n) \sim (m, n)$

  Simetričnost je tudi očitna.

  Tranzitivnost: $(m, n) \sim (p, q), (p, q) \sim (r, s) \Rightarrow mq = np, ps = qr$.

  $mq = np \Rightarrow mqps = npqr \Rightarrow ms = nr,$ če $p \neq 0, (m, n) \sim (r, s)$.

  $ms = nr$: Če $p = 0 \Rightarrow m = 0, r = 0 \Rightarrow ms = nr \Rightarrow \sim$ je ekvivalenčna relacija:

  $$(\mathbb{Z} \times \mathbb{N})/_\sim = \mathbb{Q}$$
  $$[(m, n)] \mapsto \frac{m}{n}$$

- Dve usmerjeni daljici v prostoru sta v relaciji $\sim$, kadar sta vzporedni, enako dolgi in kažeta v isto smer. To je ekvivalenčna relacija na množici vseh usmerjenih daljic v prostoru. Kvocientna množica je množica vektorjev. (Spomnimo se natančne definicije vektorja)

- Naj bo $n \in \mathbb{N}$. Na $\mathbb{Z}$ definiramo relacijo $\equiv$ s predpisom $a \equiv b$ (a je kongruentno b po modulu n) $\Rightarrow n|a - b$.

  To je ekvivalenčna relacija.

  Kvocientna množica je $\mathbb{Z}_n = \mathbb{Z}/_\equiv = \{[0], [1], \dots, [n - 1]\}$.

  To je množica ostankov pri deljenju z n.

  Namesto $[a]$ v tem primeru pogosto pišemo kar a (če je $0 \leq a \leq n - 1$), a se moramo zavedati, kaj to pomeni.

Izrek. *Naj bo $f : A \to B$ preslikava. Na A definiramo relacijo $\sim$ s predpisom $x \sim y \Rightarrow f(x) = f(y)$. Potem velja:*

(1) $\sim$ je ekvivalenčna relacija na A

(2) Obstaja natanko ena (dobro definirana) preslikava $p : A/_\sim \to B$, da diagram ☺ komutira. Definirana je s predpisom $p([a]) = f(a)$.

(3) p je injektivna in velja $Z_p = Z_f$. (Dokaz: LMN - kanonični razcep preslikave). Digram: ☺

4.3.4 Usklajenost operacije z ekvivalenčno relacijo

Definicija. *Na množici A imejmo definirano operacijo $\circ$ in ekvivalenčno relacijo $\sim$. Pravimo, da je operacija $\circ$* ***usklajena*** *z relacijo $\sim$, kadar velja sklep: $(a \sim a', b \sim b') \Rightarrow a \circ b \sim a' \circ b'$. Če je operacija $\circ$ usklajena z relacijo $\sim$, potem lahko na $A/_\sim$ definiramo operacijo $\bullet$ s predpisom $[a] \bullet [b] = [a \circ b]$.*

Ker je operacija na $A/_\sim$ definirana s pomočjo predstavnikov ekvivalenčnih razredov, moramo preveriti dobro definiranost.

$[a] = [a'], [b] = [b'] \Leftrightarrow [a \circ b] = [a' \circ b']$

$$\begin{cases} [a] = [a'] \Rightarrow a \sim a' \\ [b] = [b'] \Rightarrow b \sim b' \end{cases} \Rightarrow a \circ b \sim a' \circ b' \Rightarrow [a \circ b] = [a' \circ b']$$

Če operacija $\circ$ ne bi bila usklajena z $\sim$, potem $\bullet$ ne bi bila dobro definirana operacija.

PRIMER:

- Na $\mathbb{Z} \times \mathbb{N}$ imamo definirano relacijo $(m, n) \sim (p, q) \Leftrightarrow mq = np$, seštevanje $(m, n) + (p, g) = (mq + np, nq)$ in množenje $(m, n) \cdot (p, q) = (mp, nq)$.

  Ali sta $+$ in $\cdot$ usklajena z relacijo $\sim$?

  Dokažimo, da je to res za seštevanje (sicer glej predavanja iz analize).

  $(m, n) \sim (m', n'),\ (p, g) \sim (p', q')$

  $mn' = m'n,\ pq' = p'q$

  $(mn' = m'n)/ \cdot qq' \to mn'qq' = m'nqq'$,
  $(pq' = p'q)/ \cdot nn' \to pq'nn' = p'qnn'$

  $mn'qq' + pq'nn' = m'nqq' + p'qnn'$

  $(m, n) + (p, q) = (mq + np, nq),\ (m', n') + (p', q') = (m'q' + n'p', n'q')$

  Ali je $(mq + np, nq) \sim (m'q' + n'p', n'q')$?

  $\Leftrightarrow mqn'q' + npn'q' = nqm'q' + nqn'p' \to$ Drži

  Dokazali smo, da je seštevanje usklajeno z $\sim$. Zato lahko definiramo seštevanje na množici racionalnih števil s predpisom $\frac{m}{n} + \frac{p}{q} = \frac{mn+np}{nq}$, kot smo navajeni.

Enako bi dokazali, da je običajno množenje racionalnih števil dobro definirano.

- Na $\mathbb{Z}$ imamo definirani operaciji $+$ in $\cdot$. Naj bo $c \in \mathbb{Z}$ in $a \equiv b \Leftrightarrow n|a-b$.

  Dokazali smo, da iz $a \equiv a'$ in $b \equiv b'$ sledi $a+b \equiv a'+b'$ in $ab \equiv a'b'$. Zato je na $\mathbb{Z}_n$ dobro definirano seštevanje in množenje s predpisoma $[a]+[b]=[a+b]$ in $[a]\cdot[b]=[a\cdot b]$.

4.3.5 Kvocientne grupe Abelovih grup

G naj bo Abelova grupa in H njena podgrupa. Na G definiramo relacijo $a \sim b \Leftrightarrow a-b \in H$.

Trditev. *$\sim$ je ekvivalenčna relacija na G.*

Dokaz.

Refleksivnost: $a \cdot a = 0 \in H \Rightarrow a \sim a \; \forall a \in G$

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

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

Tudi če G ne bi bila komutativna grupa, bi bila s predpisom $a \sim b \Leftrightarrow ab^{-1} \in H$ definirana ekvivalenčna relacija na G. $ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H$ pri čemer je $b = ba^{-1}$.

□

Izrek. *G naj bo Abelova grupa in H njena podgrupa. Na G definiramo ekvivalečno relacijo $\sim$ s predpisom $a \sim b \Leftrightarrow a - b \in H$.* `Missing content`

`Missing content`

PRIMERI:

(1) Na kvocientni množici $G/_\sim$ lahko definiramo operacijo $+$ s predpisom $[a]+[b] = [a+b]$.

(2) Za to operacijo je $G/_\sim$ Abelova grupa. Pravimo ji **kvocientna** ali **faktorska grupa** grupe G po podgrupi H in jo označimo $G/_H$. Namesto $[a]$ pišemo $a + H$.

(3) Kvocientna preslikava

$$\begin{aligned} q : G &\Rightarrow G/_H \\ a &\mapsto [a] = a + H \end{aligned}$$

je homomorfizem grup.

Dokaz.

(1) Treba je dokazati, da je seštevanje v G usklajeno z relacijo $\sim$.

Naj bo $a \sim a'$ in $b \sim b'$.

$\Rightarrow a - a' \in H, b - b' \in H \Rightarrow a + b - (a' + b') = a - a' + b - b' \in H$ (ker je H podgrupa).

Upoštevali smo, da je G komutativna grupa.

$\Rightarrow a + b \sim a' + b'$.

Seštevanje v G je usklajeno z $\sim$, zato je seštevanje dobro definirano.

(2) Lastnosti operacije se prenesejo iz G na $G/_\sim$.

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

Inverz elementa $[a]$ je $[-a]$.

(3) $g(a + b) = [a + b] = [a] + [b] = q(a) + q(b)$

□

Če grupa G ni komutativna, operacija na $G/_\sim = G/_H$ lahko ni dobro definirana.

PRIMER:

- $G = S_3$, $H = \{id, (1\ 2)\}$. H je podgrupa v G. $a - b \Leftrightarrow ab^{-1} \in H$.

  $(1\ 3) \sim (1\ 2)(1\ 3)$

  $((1\ 3)((1\ 2)(1\ 3))^{-1}) = (1\ 3)(1\ 3)^{-1}(1\ 2)^{-1} = (1\ 2) \in H$

  $(2\ 3) \sim (1\ 2)(2\ 3) = (1\ 2\ 3)$

  $(1\ 3)(2\ 3) = (1\ 3\ 2) \not\sim (1\ 3\ 2)(1\ 2\ 3) = id$

  Operacija ni usklajena z relacijo $\sim$.

PRIMERI:

- $H = \{0\}$. $a \sim b \Leftrightarrow a - b \in H \Leftrightarrow a - b = 0 \Leftrightarrow a = b$.

  Ekvivalenčni razredi so enojci $[a] = \{a\}$.

  $G/_H \cong G$

- $H = G$. Potem so vsi elementi G ekvivalentni $\Rightarrow G/_H$ ima en sam element. Pogosto pišemo $G/_G = \{0\}$.

- $G = \mathbb{Z}$, $n \in \mathbb{N}$, $H = n \cdot \mathbb{Z} = \{nm; m \in \mathbb{Z}\}$.

  $a \sim b \Leftrightarrow a - b \in H \Leftrightarrow n | a - b \Leftrightarrow a \equiv b$

  $\Leftarrow G/_H = G/_\equiv = \mathbb{Z}_n = \{[0], \ldots, [n-1]\}$: grupa ostankov pri deljenju z n.

  Seštevanje: $[a] + [b] = [a + b]$

  V $\mathbb{Z}_5 : [3] + [4] = [2]$.

  Dokazali smo, da je $\mathbb{Z}_n$ celo kolobar za množenje $[a] \cdot [b] = [a \cdot b]$.

  To NE sledi iz dejstva, da je G kolobar (čeprav je to res) in da je H njegove podkolobar (čeprav je v tem primeru tudi to res).

Če je K kolobar in H njegove podkolobar, $K/_H$ ni nujno kolobar.

Primer:

- $K = \mathbb{Q},\ H = \mathbb{Z},\ a \sim b \Leftrightarrow a - b \in \mathbb{Z}$, pri čemer $a \in \mathbb{Q}$ in $b \in \mathbb{Q}$.

  $\frac{3}{2} - \frac{1}{2}, \frac{1}{3} \sim \frac{1}{3}$

  $\frac{1}{2} = \frac{3}{2} \cdot \frac{1}{3} \not\sim \frac{1}{2} \cdot \frac{1}{3} = \frac{1}{6}$, saj $\frac{1}{3} - \frac{1}{6} \notin \mathbb{Z}$

  $\Rightarrow$ Množenje na $\mathbb{Q}/_{\mathbb{Z}}$ ni dobro definirano.

Spomnimo se: Če je $f : A \to B$ preslikava, je na A s predpisom $a \sim b \Leftrightarrow f(a) = f(b)$ definirana ekvivalenčna relacija in obstaja natanko ena preslikava $p : A/_\sim \to B$, da diagram ☺ komutira. Določena je s predpisom $p([a]) = f(a)$. $Z_f = Z_p$, p je injektivna.

Oglejmo si primer, ko sta A in B Abelovi grupi in $f : A \to B$ homomorfizem grup.

$a \sim b \Leftrightarrow f(a) = f(b) \Leftrightarrow f(a) - f(b) = 0 \Leftrightarrow f(a - b) = 0 \Leftrightarrow a - b \in \mathrm{Ker} f$.

$A/_\sim = A/_{\mathrm{Ker} f}$.

Izrek. *Naj bosta G, H Abelovi grupi in $f : G \to H$ homomorfizem grup. Potem velja:*

1. *Obstaja natanko en homomorfizem grup $p : G/_{Ker f} \to H$, da diagram ☺ komutira. Definirana je s predpisom $p([a]) = f(a)$.*
2. *p je injektiven in velja $\mathrm{im} p = \mathrm{im} f$. V posebnem primeru je $G/_{Ker f} \cong Im f$.*

   Opomba: Izrek velja tudi, če G in H nista Abelovi (algebra 2).

Dokaz. Dokazati je treba le, da je p homomorfizem grup (ostalo že vemo).

$p([a] + [b]) = p([a + b]) = f(a + b) = f(a) + f(b) = p([a]) + p([b])$.

□

4.3.6 Kvocientni vektorski prostori

Naj bo V vektorski prostor nad obsegom $\mathcal{O}$ in W njegov podprostor. Vemo že, da je $V/_W$ Abelova grupa za seštevanje $[x]+[y]=[x+y]$. Na $V/_W$ bi radi definirali še množenje s skalarjem. Spomnimo se: $x \sim y \Leftrightarrow x-y \in W$.

Trditev. *Množenje s skalarjem na V je usklajeno z ekvivalenčno relacijo $\sim$. Če je $x \sim y$ in $\alpha \in \mathcal{O}$, potem je $\alpha x \sim \alpha y$.*

Dokaz. $x \sim y \Rightarrow x-y \in W \Rightarrow \alpha(x-y) = \alpha x - \alpha y \in W \Rightarrow \alpha x \sim \alpha y$

□

Definicija. *Na $V/_W$ definiramo množenje s skalarjem s predpisom $\alpha \cdot [x] = [\alpha x]$. Zaradi usklajenosti je operacija dobro definirana: Če je $[x]=[y]$ in $\alpha \in \mathcal{O}$, je $x \sim y$ in zaradi usklajenosti $\alpha x \sim \alpha y \Rightarrow [\alpha x] = [\alpha y]$.*

Posledica. *$V/_W$ je vektorski prostor nad $\mathcal{O}$. Pravimo mu **kvocientni** ali **faktorski vektorski prostor** prosotra V po podprostoru W.*

Dokaz. Vemo že, da je $(V/_W, +)$ Abelova grupa in da je množenje s skalarjem dobro definirano.

Ostale lastnosti se prenesejo z V:

- $\alpha([x]+[y]) = \alpha[x+y] = [\alpha x + \alpha y] = [\alpha x] + [\alpha y] = \alpha[x] + \alpha[y]$
- $(\alpha+\beta)[x] = [(\alpha+\beta)x] = [\alpha x + \beta x] = [\alpha x] + [\beta x] = \alpha[x] + \beta[x]$
- $\alpha(\beta[x]) = \alpha[\beta x] = [\alpha(\beta x)] = (\alpha\beta)[x]$
- $1 \cdot [x] = [1 \cdot x] = [x]$

□

Kaj je ekvivalenčni razred $[x]$?

$$
\begin{aligned}
[x] = \{y \in V; y \sim x\} = \{y \in V; y - x \in W\} = \{z + w; z \in W\} \\
z = y - x \\
y = z + w
\end{aligned}
$$

Ekvivalenčni razred $[x]$ je vektorski prostor W, ki ga premaknemo za vektor x. Tako množico imenujemo **afin podprostor** prostora V in jo označimo $X + W$.

Posebni primer: Kdaj je $[x]$ enota v $V/_W$?

$[x] = [0] \Rightarrow x \sim 0 \Leftrightarrow x - 0 \in W \Leftrightarrow x \in W$

Enota v $V/_W$ je podprostor W.

PRIMERI:

- Če je $W = \{0\}$, je $V/_W \equiv V$ $(V/_W = \{[x]; x \in V\} = \{\{x\}, x \in V\})$
  Če je $W = V$, potem so vsi elementi v V ekvivalentni in ima $V/_W$ en sam element. Pišemo $V/_V = \{0\}$.

- V $\mathbb{R}^3$ so pravi netrivialni podprostori premice skozi izhodišče ali ravnini skozi izhodišče. Poseben primer:

  - Naj bo W ravnina $z = 0$.
    Kdaj je $(x, y, z) \sim (x', y', z')$?
    $\Leftrightarrow (x, y, z) - (x', y', z') \in W$
    $\Leftrightarrow z = z'$
    $((x, y, z) = (x - x', y - y', z - z'))$

Dva elementa sta v istem ekvivalenčnem razredu, kadar imata enako tretjo komponento $\Leftrightarrow$ ležita na isti vodoravni ravnini. Ekvivalenčni razredi so vodoravne ravnine.

Ravnine seštevamo tako, da seštevamo njene tretje komponente, enako velja za množenje s skalarjem.

Trditev. *Kvocientna preslikava $q : V \to V/_W$ je linearna.*

Dokaz.

$$\begin{aligned} q(\alpha x + \beta y) &= [\alpha x + \beta y] \\ &= [\alpha x] + [\beta y] \\ &= \alpha[x] + \beta[y] \\ &= \alpha q(x) + \beta q(y) \end{aligned}$$

Druga enakost velja zaradi defincije seštevanja.
Tretja enakost velja zaradi definicije množenja s skalarjem.

$\square$

Izrek. *Naj bo $\mathcal{A} : V \to W$ linearna preslikava.*

Potem velja:

1. *Obstaja natanko ena linerna preslikava $\hat{\mathcal{A}} : V/_{ker\mathcal{A}} \to W$, da diagram komutira. Definirana je s predpisom $\hat{\mathcal{A}}([x]) = \mathcal{A}x$.*
2. *$\hat{\mathcal{A}}$ je injektivna in velja im$\hat{\mathcal{A}}$=Im$\mathcal{A}$.*
3. *$V/_{ker\mathcal{A}} \equiv Im\mathcal{A}$*

Dokaz. Dokazati moramo le homogenost preslikave $\hat{\mathcal{A}}$, vse ostalo že vemo.

$$\begin{aligned}\hat{\mathcal{A}}(\alpha[x]) &= \hat{\mathcal{A}}([\alpha x]) \\ &= \mathcal{A}(\alpha x) \\ &= \alpha\mathcal{A}x \\ &= \alpha\hat{\mathcal{A}}[x]\end{aligned}$$

Tretja enakost velja zaradi tega, ker je $\mathcal{A}$ linearna.

□

Posledica. *Če je V končnorazsežen vektorski prostor in $\mathcal{A} : V \to W$ linearna preslikava, je $dim(V/_{ker\mathcal{A}})$ =$dimV-dim(ker\mathcal{A})$.*

Dokaz. $\dim(V/_{ker\mathcal{A}}) = \dim(\mathrm{Im}\mathcal{A}) = \dim V - \dim(\mathrm{Ker}\mathcal{A})$

□

Trditev. *Če je $V = W \oplus U$, potem je $V/_W \equiv U$ in $V/_U \equiv W$.*

Dokaz. Zaradi simetrije je dovolj dokazati $V/_W \equiv U$.

Konstruirali bomo surjektivno linearno preslikavo $V \to U$, katero jedro bo W.

Potem bo po izreku $V/_W$ izomorfen U.

Projektor $\mathcal{P} : V \to U$ definiran s predpisom $\mathcal{P}(w + u) = u$ ($w \in W$ in $u \in U$).

Po predpostavki je $V = W \oplus U$, zato se vsak element prostora V na enoličen način zapiše kot $w + u$, kjer je $w \in W$ in $u \in U$.

Torej je preslikava $\mathcal{P}$ dobro definirana.

Očitno je surjektivna, saj je $\mathcal{P}(O + u) = u$ za $\forall u \in U$.

Dokažemo linearnost:

$$\begin{aligned}\mathcal{P}(\alpha(w+u)+\beta(w'+u')) &= \mathcal{P}((\alpha w+\beta w')+(\alpha u+\beta u')) \\ &= \alpha u+\beta u' \\ &= \alpha\mathcal{P}(w+u)+\beta\mathcal{P}(w'+u')\end{aligned}$$

Izračunajmo še jedro:

$$\mathcal{P}(w+u)=0 \Leftrightarrow u=0 \Rightarrow \mathrm{Ker}\mathcal{P}=\{w+0; w\in W\}=W$$

$\mathcal{P}$ je torej preslikava, ki jo iščemo.

□

Posledica. *Če je V končnorazsežen vektorski prostor nad obsegom $\mathcal{O}$ in W njegov podprostor, potem je tudi $V/_W$ končnorazsežen in velja dim($V/_W$) = dim$V-$ dim$W$.*

Dokaz. Ker je V končnorazsežen, obstaja v V direktni komplement U prostora W, torej tak podprostor, da je $V=W\oplus U$.

Zato je $V/_W \equiv U \Rightarrow \dim(V/_W)=\dim U$

Vemo pa, da je

$$\begin{aligned}\dim V &= \dim W+\dim U \\ &= \dim W+\dim(V/_W) \\ &\Rightarrow \dim(V/_W) \\ &= \dim V-\dim W.\end{aligned}$$

□

4.4 Linearne preslikave in matrike

Trditev. *Naj bo $\{v_1, \ldots, v_n\}$ baza prostora V in $\mathcal{A} : V \to W$ linearna preslikava. Če poznamo $\mathcal{A}v_1, \ldots, \mathcal{A}v_n$, potem lahko enolično izračunamo $\mathcal{A}x$ za poljuben $x \in V$. (Ekvivalentno: Linearna preslikava je enolično določena s slikami baznih vektorjev)*

Dokaz. $x \in V \Rightarrow x = \alpha_1 v_1 + \ldots + \alpha_n v_n$, ta zapis je enoličen.

$\mathcal{A}x = \mathcal{A}(\alpha_1 v_1 + \ldots + \alpha_n v_n) = \alpha_1 A v_1 + \ldots + \alpha_n \mathcal{A} v_n$

Druga enakost velja zaradi linearnosti.

□

Naj bosta V in W vektorska prostora nad $\mathcal{O}$ z bazama $B_V = \{v_1, \ldots, v_n\}$ in $B_W = \{w_1, \ldots, w_m\}$ in naj bo $\mathcal{A} : V \to W$ linearna preslikava.

$\mathcal{A}v_i \in W$ za $\forall i = 1, \ldots, n$.

Ker je B_W baza za W, lahko vsak vektor $\mathcal{A}v_i$ zadirjemo po tej bazi:

$$\begin{aligned}
\mathcal{A}v_1 &= a_{11}w_1 + a_{21}w_2 + \ldots + a_{m1}w_m \\
\mathcal{A}v_2 &= a_{12}w_1 + a_{22}w_2 + \ldots + a_{m2}w_m \\
&\ldots \\
\mathcal{A}v_n &= a_{1n}w_1 + a_{2n}w_2 + \ldots + a_{mn}w_m, \text{ za neki } a_{ij} \in O
\end{aligned}$$

Kolobarje a_{ij} (kjer je $1 \leq i \leq m$ in $1 \leq j \leq n$) zapišemo zapišemo v pravokotno tabelo, ki jo običajno postavimo med oglate (ali okrogle) oklepaje in ji rečemo **matrika reda** $m \times n$:

Koeficiente, ki jih dobimo pri razvoju vektorja $\mathcal{A}v_i$ napišemo v i-ti stolpec matrike A.

Matrika reda $m \times n$ ima m vrstic in n stolpcev.

Elementi $a_{ij} \in O$ se imenujejo **členi** matrike.

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}$$

Kadar imamo splošne člene, pišemo po kar $A = [a_{ij}]_{1\leq i\leq m,\ 1\leq j\leq n}$. Indeks i člena a_{ij} pove vrstico matrike, v kateri je člen, drugi indeks pa stolpec, v katerem je člen.

i-to vrstico matrike A bomo označevali z $A_{(i)}$: $A_{(i)} = [a_{i1}, a_{i2}, \ldots, a_{in}]$.

j-ti stolpec matrike A bomo označevali z $A^{(j)}$: $A^{(j)} = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}$.

Linearne preslikave bomo načeloma pisali z velikimi pisanimi črkami, pripadajoče matrike pa z ustreznimi velikimi tiskanimi črkami.

Matrika ni odvisna samo od preslikave, ampak tudi od baz B_V in B_W, ki smo jih izbrali. Kadar želimo to poudariti, pišemo $A = \mathcal{A}_{B_W}^{B_V}$. To pomeni: A je matrika, ki pripada preslikavi $\mathcal{A}$ glede na bazi B_V in B_W.

Množico vseh matrik reda $m \times n$ s členi iz obsega $\mathcal{O}$ bomo označevali z $\mathcal{O}^{m\times n}$.

PRIMER:

- Naj bo V prostor vseh realnih polinomov stopnje največ 3, W pa prostor polinomov stopnje največ 2.

  $\mathcal{A} : V \to W$ naj bo odvajanje.

  Vemo, da je to linearna preslikava. Poiščimo njeno matriko.

  Najprej izberimo bazi. $B_V = \{1, x, x^2, x^3\}$ in $B_W = \{1, x, x^2\}$ sta standardni bazi prostorov V in W.

$$\begin{aligned} \mathcal{A}1 &= 1' = 0\cdot 1 + 0 - x + 0\cdot x^2 \\ \mathcal{A}x &= 1 = 1\cdot 1 + 0\cdot x + 0\cdot x^2 \\ \mathcal{A}x^2 &= 2x = 0\cdot 1 + 2\cdot x + 0\cdot x^2 \\ \mathcal{A}x^3 &= 3x^2 = 0\cdot 1 + 0\cdot x + 3\cdot x^2 \end{aligned}$$

  Matrika odvajanja glede na bazi B_V in B_W je $A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$

Trditev. *Naj bosta V in W končnorazsežna vektorska prostora z bazama B_V in B_W, $|B_W| = n$, $|B_W| = m$. Potem je preslikava $\Phi : \mathcal{L}(V,W) \to \mathcal{O}^{m\times n}$, definirana s predpisom $\Phi(A) = \mathcal{A}_{B_W}^{B_V}$, bijekcija.*

Dokaz.

Injektivnost:

$\Phi(\mathcal{A}) = \Phi(\mathcal{A}') \Rightarrow \mathcal{A}_{B_W}^{B_V} = \mathcal{A}'^{B_V}_{B_W} = A = [a_{ij}]_{1\leq j\leq n,\ 1\leq j\leq m}$.

Po konstrukciji je $\mathcal{A}v_i = a_{1i}w_1 + a_{2i}w_2 + \ldots + a_{ni}w_n$ za vsak $i = 1, \ldots, n$.

$\mathcal{A}v_i = a_{1i}w_1 + \ldots + a_{ni}w_n = \mathcal{A}v_i$ za vsak $i = 1, \ldots, n$

Preslikavi $\mathcal{A}$ in $\mathcal{A}'$ se ujemata na bazi in po trditvi od včeraj sta enaki.

Surjektivnost:

Naj bo $A = [a_{ij}] \in \mathcal{O}^{m\times n}$ poljubna matrika.

Preslikavo $\mathcal{A} : V \to W$ definiramo s predpisom $\mathcal{A}(\sum_{i=1}^n \alpha_i v_i) = \sum_{i=1}^n \alpha_i \sum_{j=1}^n a_{ji}w_j$.

Ker je $\{v_1, \ldots, v_n\}$ baza za V, lahko vsak vektor $x \in V$ enolično zapišemo v obliki $x = \sum_{i=1}^n \alpha_i v_i \Rightarrow \mathcal{A}$ je dobro definirana preslikava.

Lahko je preveriti s preprostim računom, da je preslikava $\mathcal{A}$ linearna. Za vsak i velja $\mathcal{A}v_i = \sum_{j=1}^n a_{ji}w_j \Rightarrow A = \mathcal{A}_{B_W}^{B_V} = \Phi(\mathcal{A})$

$\square$

$\mathcal{L}(V,W)$ je vektorski prostor. Na $\mathcal{O}^{m\times n}$ bi radi definirali tako seštevanje in množenje s skalarjem, da bo $\mathcal{O}^{m\times n}$ vektorski prostor, $\Phi : \mathcal{L}(V,W) \to \mathcal{O}^{m\times n}$ pa izomorfizem vektorskih prostorov.

Definicija. *Naj bodo V, W in Φ kot v prejšnji trditvi. Na $\mathcal{O}^{m\times n}$ definiramo seštevanje in množenje s skalarji s predpisoma $A + B = \Phi(\Phi^{-1}(A) + \Phi^{-1}(B))$ in $\alpha A = \Phi(\alpha\Phi^{-1}(A))$.*

Torej: $\mathcal{L}(V,W) \to \mathcal{O}^{m\times n}$ s preslikavo Φ, pri tem sta $A, B \in \mathcal{O}^{m\times n}$ in lahko zapišemo, da $\Phi^{-1}(B), \Phi^{-1}(A) \in \mathcal{L}(V,W)$. Posledično velja $\Phi^{-1}(B) + \Phi^{-1}(A) \in \mathcal{L}(V,W)$.

To je edini način, kako lahko definiramo operaciji tako, da bo Φ izomorfizem.

Kaj te dve definiciji pomenita?

Naj bosta $A = [a_{ij}]$, $B = [b_{ij}] \in \mathcal{O}^{m\times n}$ in $\alpha \in \mathcal{O}$.

Označimo $\mathcal{A} = \Phi^{-1}(A)$ in $B = \Phi^{-1}(B)$.

Po definiciji je

$$\begin{aligned}\mathcal{A}v_i = \sum_{j=1}^{n} a_{ji}w_j \text{ in } \mathcal{B}v_i = \sum_{j=1}^{n} b_{ji}w_j \Rightarrow (\mathcal{A}+\mathcal{B})v_i \\ &= \mathcal{A}v_i + \mathcal{B}v_i \\ &= \sum_{j=1}^{n} a_{ji}w_j + \sum_{j=1}^{n} b_{ji}w_j \\ &= \sum_{j=1}^{n}(a_{ji}+b_{ji})w_j \\ &= *\end{aligned}$$

za vsak $i = 1, \dots, n$.

$$*(A+B)_{B_W}^{B_V} = \begin{bmatrix} a_{11}+b_{11} & \dots & a_{in}+b_{in} \\ a_{21}+b_{21} & \dots & a_{2n}+b_{2n} \\ \vdots & & \vdots \\ a_{m1}+b_{m1} & \dots & a_{mn}+b_{mn} \end{bmatrix} = \Phi(\Phi^{-1}(A)+\Phi^{-1}(B))$$

Ugotovili smo: Matrike seštevamo po členih.

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{bmatrix} = \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \dots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \dots & a_{2n}+b_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \dots & a_{mn}+b_{mn} \end{bmatrix}$$

Vidimo tudi, da je definicija seštevanja neodvisna od izbire prostorov V in W in baz B_V in B_W.

$$(\alpha\mathcal{A})v_i = \alpha\mathcal{A}v_i = \alpha\sum_{j=1}^{n} a_{ji}w_j = \sum_{j=1}^{n} \alpha a_{ji}w_j$$

$\Rightarrow$ Matrike množimo s skalarji tudi po členih

$$\alpha \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} = \begin{bmatrix} \alpha a_{11} & \alpha a_{12} & \dots & \alpha a_{1n} \\ \alpha a_{21} & \alpha a_{22} & \dots & \alpha a_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha a_{m1} & \alpha a_{m2} & \dots & \alpha a_{mn} \end{bmatrix}$$

Tudi množenje s skalarjem ni odvisno od izbire V, W, B_V in B_W.

S skalarjem lahko pomnožimo poljubno matriko, seštevamo pa matrike iste velikosti.

Trditev. *$\mathcal{O}^{m\times n}$ je vektorski prostor nad $\mathcal{O}$, preslikava $\Phi : \mathcal{L}(V,W) \to \mathcal{O}^{m\times n}$, definirana v prejšnji trditvi, pa izomorfizem vektorskih prostorov.*

Dokaz. Ker je $\mathcal{O}$ vektorski prostor nad $\mathcal{O}$ in so vse operacije, definirane po členih, bi moralo biti očitno, da je $\mathcal{O}^{m\times n}$ vektorski prostor nad $\mathcal{O}$. Preveri doma.

Da je Φ bijektivna, že vemo.

Linearnost:

$$\begin{aligned}\underbrace{\Phi(\mathcal{A})}_{\in\mathcal{O}^{m\times n}} + \underbrace{\Phi(\mathcal{B})}_{\in\mathcal{O}^{m\times n}} &= \Phi(\Phi^{-1}(\Phi(\mathcal{A})) + \Phi^{-1}(\Phi(B))) \\ &= \Phi(\mathcal{A}+\mathcal{B})\end{aligned}$$

Prva enakost velja zaradi definicije seštevanje v $\mathcal{O}^{m\times n}$.

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

□

Enota za seštevanje v $\mathcal{O}^{m\times n}$ je matrika, sestavljena iz raznih ničel. Pravimo ji **ničelna matrika** in jo običajno označimo kar z $\mathcal{O}$.

Kaj je $-A$, če je $A = [a_{ij}]$? $-A = [-a_{ij}]$

Posledica.

1. *$dim\mathcal{O}^{m\times n} = m \times n$*
2. *Če je $dimV = n$ in $dimW = m$, je $(dim\mathcal{L}(V,W)) = m \times n$*

Dokaz. Zaradi trditve je dovolj dokazati le prvo točko.

$\text{dim} U^{m\times n} = n \cdot n$

Za $i = 1, \ldots, m$, $m_j = 1, \ldots, n$, naj bo E_{ij} matrika, ki ima enico na križišču i-te vrstice in j-tega stolpca in ničle drugod.

$$E_{ij} = \begin{bmatrix} & & \\ & 1 & \\ & & \end{bmatrix}$$

Enica je postavljena v i-ti vrstici in j-tem stolpcu.

Matrike E_{ij} se imenujejo **elementarne matrike** oziroma **matrične enote**.

Dokažimo, da je $\{E_{ij}; 1 \leq i \leq m,\ 1 \leq j \leq n\} = B$ baza prostora $\mathcal{O}^{m\times n}$.

Linearna neodvisnost: Naj bo $\sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} E_{ij} = 0$.

$$\textstyle\sum_{i=1}^{m} = \alpha_{11} \begin{bmatrix} 1 & & \\ & & \\ & & \end{bmatrix} + \alpha_{12} \begin{bmatrix} 0 & 1 & \\ & & \\ & & \end{bmatrix} + \ldots = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{bmatrix} \Rightarrow \alpha_{ij} = 0\ \forall i, j$$

Ogrodje: Naj bo $A = [a_{ij}] \in \mathcal{O}^{m\times n}$ poljubna matrika.

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{bmatrix} = \sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} E_{ij} = 0$$

. □

Če je $\text{dim} V = n$ in $\text{dim} U = m$, potem je $\mathcal{L}(V, U) \equiv \mathcal{O}^{m\times n}$.

Oglejmo si dva primera:

- $m = 1 \Rightarrow U \equiv O$

  $O^{1\times n} \equiv \mathcal{L}(V, \mathcal{O}) = V*$

  Pri tem $O^{1\times n}$ predstavlja prostor $1 \times n$ matrik. $\mathcal{L}(V, \mathcal{O})$ pa je prostor linearnih funkcionalov na V.

Vsak linearen funkcional na V lahko predstavimo z vrstico velikosti $1 \times n$.

$\text{dim}V* = \text{dim}O^{1\times n} = n = \text{dim}V \Rightarrow V*$ in V sta izomorfna.

- $n = 1: \ \mathcal{L}(\mathcal{O}, U) \equiv \mathcal{O}^{m\times 1}$.

$\mathcal{L}(\mathcal{O}, U) \equiv U \equiv \mathcal{O}^m$

$$\mathcal{A} : O \to U$$
$$\mathcal{A} \mapsto \mathcal{A}(1) \text{ je izomorfizem med } \mathcal{L}(\mathcal{O}, U) \text{ in } U$$

Odslej bomo identificirali $\mathcal{O}^{m\times 1}$ in $\mathcal{O}^m$ in na elemente $\mathcal{O}^m$ bomo gledali kot na stolpce.

Standardno bazo $\mathcal{O}^m$ sestavljajo vektorji

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \ e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \ldots, \ e_m = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$$

4.4.1 Množenje matrik

Množenje matrik bi radi definirali na tak način, da bo ustrezalo kompozitumu linearnih preslikav.

Naj bosta $\mathcal{A} : V \to W$ in $\mathcal{B} : U \to V$ linearni preslikavi in naj bodo $B_U = \{u_1, \ldots, u_n\}$, $B_V = \{v_1, \ldots, v_m\}$ in $B_W = \{w_1, \ldots, w_p\}$ baze prostorov U, V in W.

Množenje matrik bi radi definirali tako, da bo veljalo $(\mathcal{A} \circ \mathcal{B})_{B_W}^{B_U} = \mathcal{A}_{B_W}^{B_V} \cdot \mathcal{B}_{B_V}^{B_U}$.

Naj bodo

$$\begin{aligned}
\Phi_{p,m} : \mathcal{L}(V, W) &\to \mathcal{O}^{p\times n} \\
\mathcal{A} &\mapsto \mathcal{A}_{B_W}^{B_V} \\
\Phi_{m,n} : \mathcal{L}(U, V) &\to \mathcal{O}^{m\times n} \\
\mathcal{A} &\mapsto \mathcal{A}_{B_V}^{B_U} \\
\Phi_{p,n} : \mathcal{L}(U, W) &\to O^{p\times n} \\
\mathcal{A} &\mapsto \mathcal{A}_{B_W}^{B_V}
\end{aligned}$$

izomorfizmi.

Missing image

Za poljubni matriki $A \in \mathcal{O}^{p\times n}$ in $B \in \mathcal{O}^{m\times n}$ definiramo $A \cdot B = \Phi_{p,n}(\Phi_{p,m}^{-1}(A) \cdot \Phi_{m,n}^{-1}(B))$ $\in O^{p\times n}$.

Matriki lahko zmnožimo, če ima prva toliko stolpcev kot druga vrstic.

produkt ima toliko vrstic kot prva matrika in toliko stolpcev kot druga matrika.

Izpeljemo formulo za množenje matrik $A \in \mathcal{O}^{p\times n}$ in $B \in \mathcal{O}^{m\times n}$.

Obstajata linearni enolični preslikavi $\mathcal{A} : V \to W$ in $\mathcal{B} : U \to V$, da je $A = \mathcal{A}_{B_W}^{B_V}$ in $B = \mathcal{B}_{B_V}^{B_U}$.

Naj bo $A = [a_{ij}]_{1\leq i\leq p,\ 1\leq j\leq m}$ in $B = [b_{ij}]_{1\leq i\leq m,\ 1\leq j\leq n}$

To pomeni:

$$
\begin{aligned}
\mathcal{A}v_1 &= a_{11}w_1 + a_{21}w_2 + \ldots + a_{p1}w_p \\
\mathcal{A}v_2 &= a_{12}w_1 + a_{22}w_2 + \ldots + a_{p2}w_p \\
&\vdots \\
\mathcal{A}v_m &= a_{nm}w_1 + \ldots + a_{pm}w_p \\
\mathcal{B}u_1 &= b_{11}v_1 + b_{21}v_2 + \ldots + b_{m1}v_m \\
\mathcal{B}u_2 &= b_{12}v_1 + b_{22}v_2 + \ldots + b_{m2}v_m \\
&\vdots \\
\mathcal{B}u_n &= b_{1n}v_1 + b_{2n}v_2 + \ldots + b_{mn}v_m
\end{aligned}
$$

$$
\begin{aligned}
(\mathcal{A} \circ \mathcal{B})u_i &= \mathcal{A}(\mathcal{B}u_i) \\
&= \mathcal{A}(\sum_{k=1}^{m} b_{ki}v_k) \\
&= \sum_{k=1}^{m} b_{ki}\mathcal{A}v_k \\
&= \sum_{k=1}^{m} b_{ki}(\sum_{j=1}^{p} a_{jk}w_j) \\
&= \sum_{j=1}^{p}(\sum_{k=1}^{m} a_{jk}b_{ki})w_j
\end{aligned}
$$

$(\sum_{k=1}^{m} a_{jk}b_{ki})$ so členi matrike $A \cdot B$, ki leži v i-tem stolpcu in j-ti vrstici.

Če je $C = A \cdot B = [c_{ij}]$, potem je $c_{ij} = \sum_{k=1}^{m} a_{ik}b_{kj}$ skalarni produkt i-te vrstice in j-tega stolpca.

Množenje matrik ni odvisno od prostorov U, V, W in baz B_U, B_V, B_W.

PRIMER:

- $A = \begin{bmatrix} 2 & 1 & 4 \\ 1 & -1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 3 \\ 1 & 2 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$.

  AB ne obstaja, ker A ima 3 stolpce, B pa 4 stolpce. Toda BA obstaja.

  $$B \cdot A = \begin{bmatrix} 5 & -2 & 4 \\ 0 & -3 & -4 \\ 1 & -1 & 0 \\ 3 & 0 & 4 \end{bmatrix}$$

- $A = \begin{bmatrix} 1 & 2 \\ -1 & 2 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$

  $A \cdot B = \begin{bmatrix} -2 & -1 \\ -2 & -3 \end{bmatrix}$, $B \cdot A = \begin{bmatrix} -1 & 2 \\ 0 & -4 \end{bmatrix}$

  $A \cdot B$ ni nujno enako $B \cdot A$, tudi če oba produkta obstajata in sta iste velikosti.

Poseben primer množenja matrik je množenje matrika z vektorjem: Če je $A = [a_{ij}] \in \mathcal{O}^{m \times n}$ in $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, je $y = Ax = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} \in \mathcal{O}^m$ vektor, za katerega velja $y_i = \sum_{k=1}^n a_{ik} x_k$ (y_i je "skalarni produkt" i-te vrstice matrike A in stolpca x)

PRIMER:

- $\begin{bmatrix} 1 & 2 \\ -1 & 3 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 4 \\ -1 \end{bmatrix}$

Trditev. *Naj bosta U in V vektorska prostora, $B_U = \{u_1, \ldots, u_n\}$ baza U in $\{v_1, \ldots, v_m\} = B_V$ baza V. Naj bo $\mathcal{A} : U \to V$ linearna preslikava in $x \in U$. Naj bo $A = \mathcal{A}_{B_V}^{B_U}$ (matrika preslikave $\mathcal{A}$ glede na bazi B_U in B_V). x razvijamo po bazi $B_V : x = \alpha_1 u_1 + \ldots + \alpha_n u_n$. $\mathcal{A}x \in V$ razvijemo po bazi $\mathcal{A}x = \beta_1 v_1 + \ldots + \beta_m v_n$*

Potem je $A \cdot \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix}$. Produkt matrike s stolpcem ustreza evalvaciji linearne preslikave na vektorju.

Dokaz.

$$\mathcal{A}x = \mathcal{A}(\sum_{i=1}^n \alpha_i u_i) = \sum_{i=1}^n \alpha_i \mathcal{A} u_i$$

$$\begin{aligned} \mathcal{A}u_1 &= a_{11} v_1 + \ldots + a_{m1} v_m \\ &\vdots \\ \mathcal{A}u_n &= a_{1n} v_1 + \ldots + a_{mn} v_m \end{aligned}$$

$$\mathcal{A}x = \sum_{i=1}^n \alpha_i \sum_{k=1}^m a_{ki} v_k = \sum_{k=1}^m (\sum_{i=1}^n a_{ki} \alpha_i) v_k$$

Izračunajmo k-to komponento produkta $A\cdot \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$. Ta komponenta je enaka $\sum_{i=1}^n a_{ki}\alpha_i = \beta_k$.

$\square$

PRIMER

- Ravnino zavrtimo za kot $\frac{\pi}{3}$ v pozitivni smeri. Kam se preslika vektor $\begin{bmatrix} 1 \\ 2 \end{bmatrix}$?

  Rotacija je linearna preslikava.

  Napišemo matriko te preslikave.

  Ugotoviti moramo, kam se slikajo bazni vektorji.

  $$A = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix}$$

  $$A = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -\frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix}$$

  Matriko in preslikavo označimo kar enako

  $$A = \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}$$

  Vektor $\begin{bmatrix} 1 \\ 2 \end{bmatrix}$ se slika v vektor $A \cdot \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & -\sqrt{3} \\ \frac{\sqrt{3}}{2} & 1 \end{bmatrix}$

Naj bo $A \in \mathcal{O}^{m\times n}$ matrika. Potem je s predpisom $x \mapsto Ax$ definirana linearna preslikava $\mathcal{O}^n \to \mathcal{O}^m$ (linearnost preveri doma).

To linearno preslikavo označimo kar z A.

V $\mathcal{O}^n$ in $\mathcal{O}^m$ si izberemo standardni bazi S_n in S_m.

$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix}$, podobno velja za ostale stolpce.

Preslikava A vektorje standardne baze slika v stolpce matrike A.

Preslikavi $\mathcal{O}^n \to \mathcal{O}^m$, ki je množenje z matriko A, glede na standardni bazi prostorov $\mathcal{O}^n$ in $\mathcal{O}^m$ pripada matriki A.

Posledica. *Naj bosta* $B_V = \{v_1, \ldots, v_n\}$ *in* $B_W = \{w_1, \ldots, w_m\}$ *bazi prostorov* V *in* W *in naj bo* $\mathcal{A} : V \to W$ *linearna preslikava.*

Naj bosta $\Phi_V : \mathcal{O}^n \to V$ *in* $\Phi_W : \mathcal{O}^m \to W$ *izomorfizem, definirana s predpisoma* $\Phi_V \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \sum_{i=1}^n \alpha_i v_i$ *in* $\Phi_W \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix} = \sum_{i=1}^m \beta_i w_i$.
Naj bo $A = \mathcal{A}_{B_W}^{B_V}$ *in* $A : \mathcal{O}^n \to \mathcal{O}^m$ *množenje z matriko* A.

Potem diagram ☺ *komutira.*

Dokaz. Dovolj je dokazati, da za vsak $x \in \mathcal{O}^n$ velja $\Phi_W(Ax) = \mathcal{A}(\Phi_V(x))$

$$\Phi_W(A \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}) = \Phi_W \begin{bmatrix} a_{11}\alpha_1 + a_{12}\alpha_2 + \ldots + a_{1n}\alpha_n \\ \vdots \\ a_{m1}\alpha_1 + a_{m2}\alpha_2 + \ldots + a_{mn}\alpha_n \end{bmatrix} = \sum_{i=1}^m (\sum_{k=1}^m a_{ik}\alpha_k) w_i$$

$$\mathcal{A}(\Phi_V(\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix})) = \mathcal{A}(\sum_{i=1}^n \alpha_i v_i) = \sum_{i=1}^n \alpha_i \mathcal{A} v_i = \sum_{i=1}^n \alpha_i \sum_{k=1}^m a_{ki} w_k$$

□

Trditev.

1. *Naj bodo* $\Phi_{m,n} : \mathcal{L}(V,U) \to \mathcal{O}^{m\times n}$, $\Phi_{n,p} : \mathcal{L}(W,V) \to \mathcal{O}^{n,p}$ *in* $\Phi_{m,p} : \mathcal{L}(W,U) \to \mathcal{O}^{m\times p}$ *izomorfizmi, določeni z izbirami baz prostorov* U, V *in* W. *Potem je* $\Phi_{m,p}(\mathcal{A} \circ B) = \Phi_{m,n}(\mathcal{A}) \cdot \Phi_{n,p}(B)$ *za vsak* $B \in \mathcal{L}(W,V)$ *in vsak* $\mathcal{A} \in \mathcal{L}(V,U)$.
2. *Če je* $A \in \mathcal{O}^{m\times n}$, $B \in \mathcal{O}^{n\times p}$ *in* $C \in \mathcal{O}^{p\times q}$, *potem je* $A(BC) = (AB)C$ *(množenje matrik je asocitativno).*

Dokaz.

1. Je definicija množenja matrik.
2. Naj bo Z vektorski prostor dimenzije q in naj bodo $\Phi_{n,q} : \mathcal{L}(Z,V) \to \mathcal{O}^{n\times q}$, $\Phi_{m,q} : \mathcal{L}(Z,U) \to \mathcal{O}^{m\times q}$ in $\Phi_{p,q} : \mathcal{L}(Z,W) \to \mathcal{O}^{p\times q}$ izomorfizmi.

Po definiciji množenja matrik je:

$$\begin{aligned}
A \cdot (B \cdot C) &= A \cdot \Phi_{n,q}(\Phi_{n,p}^{-1}(B) + \Phi_{p,q}^{-1}(C)) \\
&= \Phi_{m,q}(\Phi_{m,n}^{-1}(A) \circ \Phi_{n,q}^{-1} \circ (\Phi_{n,q}(\Phi_{n,p}^{-1}(B) + \Phi_{p,q}^{-1}(C)))) \\
&= \Phi_{m,q}(\Phi_{m,n}^{-1}(A) \circ \Phi_{n,p}^{-1}(B) \circ \Phi_{p,q}^{-1}(C)) \\
&= \Phi_{m,q}(\Phi_{m,p}^{-1}(\Phi_{m,p}(\Phi_{m,n}^{-1}(A) \circ \Phi_{n,p}^{-1}(B))) \circ \Phi_{p,g}^{-1}(C)) \\
&= \Phi_{m,q}(\Phi_{m,p}^{-1}(A \cdot B) \circ \Phi_{p,q}^{-1}(C)) \\
&= (A \cdot B) \cdot C
\end{aligned}$$

□

Posledica. *Množica kvadratnih matrik $\mathcal{O}^{n\times n}$ je algebra, in preslikava $\mathcal{L}(V,V) \to \mathcal{O}^{n\times n}$ (kjer je $dimV = n$), definirana s predpisom $\Phi(\mathcal{A}) = \mathcal{A}_{B_V}$ (kjer je B_V baza V), je izomorfizem iz algebre.*

Dokaz. Vemo že, da je $\mathcal{O}^{n\times n}$ vektorski prostor. Množenje $n \times n$ matrik je notranja operacija, ki je po prejšnji trditvi asociativna. Distributivnost in enakost $(\alpha A)(\beta B) = (\alpha\beta)(AB)$ za $\alpha, \beta \in \mathcal{O}$ in $A, B \in \mathcal{O}^{n\times n}$ preverite sami (lahek račun). Vemo že, da je Φ izomorfizem vektorskih prostorov, po prejšnji točki pa je $\Phi(\mathcal{A}) \cdot \Phi(B) = \Phi(A \cdot B)$.

□

id_V je enota algebre $\mathcal{L}(V,V)$. Ker je Φ izomorfizem, je $\Phi(id_V)$ enota algebre $\mathcal{O}^{n\times n}$. Matriko $\Phi(id_V)$ označimo z I_n, oziroma kar z I, če je velikost znana.

I se imenuje **identična matrika** ali **identiteta**.

- Izračunajmo I. Naj bo $B_V = \{v_1, \dots, v_n\}$ baza V.

$$\begin{aligned}
id(v_1) &= v_1 = 1 \cdot v_1 + 0 \cdot v_2 + \ldots + 0 \cdot v_n \\
id(v_2) &= v_2 = 0 \cdot v_1 + 1 \cdot v_2 + \ldots + 0 \cdot v_n \\
&\vdots \\
id(v_n) &= v_n = 0 \cdot v_1 + 0 \cdot v_2 + \ldots + 1 \cdot v_n
\end{aligned}$$

$$\Rightarrow I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

$\mathcal{O}^{n\times n}$ je algebra z enoto I.

Velja še več: če je $A \in \mathcal{O}^{n\times m}$, je $A \cdot I_m = A$ in, če je $B \in \mathcal{O}^{m\times n}$, je $B \cdot I_n = B$.

Dokaz.

$$\begin{aligned}A \cdot I_m &= \Phi_{n,m}(\Phi_{n,m}^{-1}(A) \circ \Phi_{m,m}^{-1}(I)) \\ &= \Phi_{n,m}(\Phi_{n,m}^{-1}(A) \circ id) \\ &= \Phi_{n,m}(\Phi_{n,m}^{-1}(A)) \\ &= A\end{aligned}$$

□

Definicija. *Matrika $A \in \mathcal{O}^{n\times m}$ je* ***diagonalna****, če je $a_{ij} = 0$ za $i \neq j$. Pišemo: $A = \begin{bmatrix} a_{11} & & & \\ & a_{22} & & \\ & & \ddots & \\ & & & a_{nn}\end{bmatrix}$. Torej je I: $I = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1\end{bmatrix}$ poseben primer diagonalne matrike.*

Definicija. *Endomorfizem $\mathcal{A} \in \mathcal{L}(V,V)$ je obrnljiv, kadar obstaja $\mathcal{B} \in \mathcal{L}(V,V)$, da je $\mathcal{A} \circ \mathcal{B} = \mathcal{B} \circ \mathcal{A} = id_V$. Matrika $A \in \mathcal{O}^{n\times n}$ je* ***obrnljiva****, kadar obstaja $B \in \mathcal{O}^{n\times m}$, da je $AB = BA = I$. V taki matriki B-ju rečemo* ***inverz matrike*** *A in jo označimo z A^{-1}. Naši prostori so končnorazsežni, zato je endomorfizem A obrnljiv, ko obstaja $B \in \mathcal{L}(V,V)$, da je $\mathcal{A} \circ B = id_V$ ali $B \circ \mathcal{A} = id_V$.*

Recimo, da je velja $\mathcal{A} \circ B = id_V$ (2. primer se podobno dokaže).

Potem je $\mathcal{A}$ surjektiven.

$$\begin{aligned}\dim V &= \dim(\mathrm{Ker} A) + \dim(\mathrm{Im} A) \\ &\Rightarrow \dim(\mathrm{Ker} A) = 0 \\ &\Rightarrow \mathrm{Ker} A = \{0\} \\ &\Rightarrow \mathcal{A} \text{ je injektivna} \\ &\Rightarrow \text{ je bijektivna}\end{aligned}$$

$\mathcal{A}$ ima torej inverz in za inverz že vemo, da je tudi linearna preslikava. Torej je A obrnljiv.

Kvadratna matrika A je obrnjljiva, kadar obstaja matrika B, da je $A \cdot B = I$ ali $B \cdot A = I$.

Posledica. *Izomorfizem $\Phi : \mathcal{L}(V,V) \to \mathcal{O}^{n\times n}$ slika obrnljive endomorfizme v obrnjljive matrike in za vsak obrnljiv endomorfizem A velja: $\Phi(\mathcal{A}^{-1}) = (\Phi(\mathcal{A}))^{-1}$.*

Dokaz.

$$\begin{aligned}\Phi(\mathcal{A}^{-1}) \cdot \Phi(\mathcal{A}) &= \Phi(\mathcal{A}^{-1}\mathcal{A}) \\ &= \Phi(id_A) = I \\ &\Rightarrow \Phi(\mathcal{A}^{-1}) \text{ je inverz za } \Phi(\mathcal{A})\end{aligned}$$

□

4.4.2 Dualni prostor in dualne preslikave

Naj bo V končnorazsežen vektorski prostor nad $\mathcal{O}$. Preslikava $\mathcal{L}(V\mathcal{O})$ vseh linearnih funkcionalov na V pravimo **dualni prostor prostora** V in ga običajno označimo z $V*$ (včasih tudi V').

Naj bo $n = \dim V$. Potem vemo, da je $V \cong \mathcal{O}^n \cong \mathcal{O}^{1\times m} \cong V*$ in $\dim V* = \dim V$.

Definicija. *Naj bo $B_V = \{v_1, \dots, v_n\}$ baza prostora V. Množica funkcionalov $\{\varphi_1, \dots, \varphi_n\} \subseteq V*$ je **dualna baza** baze B_V, če za vsaka $i_{id} = 1, \dots, n$ velja $\varphi_i(v_j) = \delta_{ij} = \begin{cases} 1, & \text{če je ?} \\ 0, & \text{če je ?} \end{cases}$. δ_{ij} se imenuje **Kroneckerjeva delta***

Trditev. *Dualna baza baze B_V vedno obstaja. Z B_V je enolično določena in je res baza prostora $V*$.*

Dokaz.

- <u>Enoličnost:</u> Recimo, da so $\varphi_1, \dots, \varphi_n : V \to \mathcal{O}$ taki funkcionali, da je $\varphi_i(v_j) = \delta_{ij}$ za vsaka i in j. Naj bo $x \in V$ poljuben vektor. Ker je $B_V = \{v_1, \dots, v_n\}$ baza za V, lahko x enolično razvijemo po tej bazi: $x = \alpha_1 v_1 + \ldots + \alpha_n v_n$.

$$\begin{aligned} \varphi_1(x) &= \varphi_i(\alpha_1 v_1 + \ldots + \alpha_n v_n) \\ &= \alpha_1 \varphi_1(v_1) + \ldots + \alpha_n \varphi_1(v_n) \\ &= \alpha_1 \delta_{i1} + \ldots + \alpha_n \delta_{in} \\ &= \alpha_i \text{ za vsak } i \end{aligned}$$

  Dokazali smo, da če je $\varphi_i(v_j) = \delta_{ij}$, potem je $\varphi_i(\sum_{j=1}^n \alpha_j v_j) = \alpha_{ji}$.

  φ_i v vsaki točki prostora V lahko zavzame le eno vrednost. Torej obstaja kvečjemu en linearen funkcional $\varphi_i : V \to \mathcal{O}$, da je $\varphi_i(v_j) = \delta_{ij}$ za vsak $j = 1, \dots, n$. To velja za vsak i.

- <u>Obstoj:</u> Za vsak $i = 1, \dots, n$ definiramo $\varphi_i(\sum_{j=1}^n \alpha_{ij} v_j) = \alpha_i$.

  Dokazati moramo, da je to linearen funkcional.

  Da je funkcional, je očitno.

- Linearnost: $x, y \in V$, $\alpha, \beta \in \mathcal{O}$. x in y lahko razvijemo po bazi $B_V : x = \sum_{j=1}^{n} \alpha_{ij} v_j$, $y = \sum_{j=1}^{n} \beta_j v_j$.

$$\begin{aligned}
\varphi_i(\alpha_x + \beta_y) &= \varphi_i(\alpha \sum_{j=1}^{n} \alpha_j v_j + \beta \sum_{j=1}^{n} \beta_j v_j) \\
&= \varphi_i(\sum_{j=1}^{n} (\alpha\alpha_j + \beta\beta_j) v_j) \\
&= \alpha\alpha_i + \beta\beta_i \\
&= \alpha \cdot \varphi_i(\sum_{j=1}^{n} \alpha_j v_j) + \beta \cdot \varphi_i(\sum_{j=1}^{n} \beta_j v_j) \\
&= \alpha\varphi_i(x) + \beta\varphi_i(y)
\end{aligned}$$

  Očitno je tudi $\varphi_i(v_j) = \sigma_{ij}$ za vsaka $i, j = 1, \ldots, n$.

- $\{\varphi_1, \ldots, \varphi_n\}$ je baza $V*$

  Ker je dim$V* = n$ je dovolj dokazati, da so $\varphi_1, \ldots, \varphi_n$ linearno neodvisni.

  Potem je $(\alpha_1\varphi_1 + \ldots + \alpha_n\varphi_n)(x) = 0$ za vsak $x \in V$.

  $(\alpha_1\varphi_1 + \ldots + \alpha_n\varphi_n)(x) = \alpha_1\varphi_1(x) + \ldots + \alpha_n\varphi_n(x)$

  Za x vstavimo v_j:

  $\underbrace{\alpha_1 \underbrace{\varphi_1(v_j)}_{\delta_{1j}} + \ldots + \alpha_n \underbrace{\varphi_n(v_j)}_{\delta_{nj}}}_{\alpha_j = 0} = 0$

  j je bil poljuben, od koder sledi, da so $\varphi_1, \ldots, \varphi_n$ linearno neodvisni.

□

Opomba: Tudi, da je $\{\varphi_1, \ldots, \varphi_n\}$ ogrodje za $V*$, je enostavno dokazati: če je $\psi \in V*$ poljuben, potem je $\psi = \sum_{i=1}^{n} \underbrace{\psi(v_i)\varphi_i}_{\in \mathcal{O}}$ (preverite doma). To bi bil alternativen dokaz, da je $V \cong V*$.

Trditev. *Naj bo $B_V = \{v_1, \ldots, v_n\}$ baza prostora V in $B_{V*} = \{\varphi_1, \ldots, \varphi_n\}$ njej dualna baza. Naj bosta $x \in V$ in $\psi \in V*$ poljubna. Razvijemo ju po bazah $x = \sum_{i=1}^n \alpha_i v_i$, $\psi = \sum_{i=1}^n \beta_i \varphi_i$. Označimo $a = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \in \mathcal{O}^n$ in $b = \begin{bmatrix} \beta_1 & \ldots & \beta_n \end{bmatrix} \in \mathcal{O}^{1\times n}$. Potem je $\psi(x) = b \cdot a$. ("skalarni produkt" vrstice b in stolpca a).*

Dokaz.

$$\begin{aligned}
\psi(x) &= (\sum_{i=1}^n \beta_i \varphi_i)(\sum_{j=1}^n \alpha_j v_j) \\
&= \sum_{i,j=1}^n \beta_i \alpha_j \varphi_i(v_j) \\
&= \sum_{i=1}^n \beta_i \alpha_i \\
&= b \cdot a
\end{aligned}$$

□

PRIMER:

- Naj bodo $a_0, \ldots, a_n \in \mathbb{R}$ paroma različni ? in $b_0, \ldots, b_n \in \mathbb{R}$ poljubni. Potem vemo, da obstaja natanko en polinom $p(x)$ stopnje največ n, da je $p(a_i) = b_i$ za $i = 0, \ldots, n$. Kako $p(x)$ poiščemo brez računanja?

  V naj bo vektorski prostor realnih polinomov stopnje največ n.

  Naj bo $a \in \mathbb{R}$.

  Preslikava $V \to \mathbb{R}$, kjer se $p(x)$ slika v $p(a)$ je linearen funkcional.

  Za $i = 0, \ldots, n$ definiramo funkcional

$$\begin{gathered}
\varphi_i : V \to \mathcal{O} \\
\varphi_i(p(x)) = p(a_i)
\end{gathered}$$

  V V bomo poiskali tako bazo $B_V = \{p_0, \ldots, p_n\}$, da bo $B_{V*} = \{\varphi_0, \ldots, \varphi_n\}$ tej bazi dualna baza. (Ne vemo še, da je B_{V*} res baza za $V*$).

$$\underbrace{\varphi_i(p_j)}_{p_j(a_i)} = \delta_{ij} \ \forall i, j = 0, \ldots, n$$

$p_j(a_i) = 0$ za $i \neq j$: za $i \neq j$ je a : ničla polinoma $p_j(x) \Rightarrow$

$$p_j(x) = c \cdot \underbrace{(x - a_0)\dots(x - a_{j-1})(x - a_{j+1})\dots(x - a_n)}_{\text{stopnje } n}$$

c je konstanta.

$$p_j(a_j) = 1$$

$$p_j(a_j) = c(a_j - a_0)\dots(a_j - a_{j-1})(a_j - a_{j+1})\dots(a_j - a_n)$$

$$p_j(x) = \frac{(x - a_0)\dots(x - a_{j-1})(x - a_{j+1})\dots(x - a_n)}{(a_j - a_0)\dots(a_j - a_{j-1})(a_j - a_{j+1})\dots(a_j - a_n)}$$

Dokazati moramo, da je $\{p_0, \dots, p_n\}$ baza prostora V (in potem bo B_{V*} tej bazi dualna baza).

Ker je dim$V = n + 1$ je dovolj dokazati linearno neodvisnost.

$$\alpha_0 p_0(x) + \ldots + \alpha_n p_n(x) = 0$$

To izračunamo v a_j: $\underbrace{\alpha_0 \underbrace{p_0(a_j)}_{\delta_{0j}} + \ldots + \alpha_n \underbrace{p_n(a_j)}_{\delta_{nj}}}_{\alpha_j = 0 \;\; \forall j = 0,\dots,n} = 0$

Iz tega sledi: $B_V = \{p_0, \dots, p_n\}$ je res baza V in B_{V*} je njej dualna baza. Iščemo $p(x)$, da bo $p(a_i) = b_i$ za vsak, ?. $p_j(a_i) = \delta_{ji}$.

$$p(x) = \sum_{i=1}^{n} b_i p_i(x)$$

To je **Lagrangeva interpolacija**.

Dualna preslikava

$\mathcal{A} \in \mathcal{L}(V, W),\ \varphi \in W*,\ \varphi : W \to \mathcal{O}$ je linearen funkcional.

$\varphi \circ \mathcal{A}$ je kompozitum linearnih preslikav, torej je linearna preslikava. Je celo linearni funkcional, saj slika v $\mathcal{O}$: $\underbrace{\varphi}_{\in W*} \mapsto \varphi \circ \mathcal{A} \in V*$

Definicija. *Naj bosta V in W končnorazsežna vektorska prostora nad $\mathcal{O}$ in $\mathcal{A} : V \to W$ linearna preslikava. Preslikava $\mathcal{A}^d : W* \to V*$, definirana s predpisom $\mathcal{A}^d(\varphi) = \varphi \circ \mathcal{A}$, se imenuje **dualna preslikava** preslikave $\mathcal{A}$.*

Trditev. *$\mathcal{A}^d \in \mathcal{L}(W*, V*)$.*

Dokaz.

$$\begin{aligned}\mathcal{A}^d(\alpha\varphi + \beta\psi) &= (\alpha\varphi + \beta\psi) \circ \mathcal{A} \\ &= \alpha\varphi \circ \mathcal{A} + \beta\psi \circ \mathcal{A} \\ &= \alpha\mathcal{A}^d(\varphi) + \beta\mathcal{A}^d(\psi)\end{aligned}$$

□

Trditev. *Naj bodo U, V, W vektorski prostori, $\mathcal{A}, \mathcal{B} \in \mathcal{L}(U, V)$, $\varphi \in \mathcal{L}(V, W)$ in $\lambda \in \mathcal{O}$. Potem je $(\mathcal{A} + \mathcal{B})^d = \mathcal{A}^d + \mathcal{B}^d$, $(\lambda\mathcal{A})^d = \lambda \cdot \mathcal{A}^d$ in $(\varphi \circ \mathcal{A})^d = \mathcal{A}^d \circ \varphi^d$*

Dokaz. Za $\varphi \in V*$ je

$$\begin{aligned}(\mathcal{A} + \mathcal{B})^d(\varphi) &= \varphi \circ (\mathcal{A} + \mathcal{B}) \\ &= \varphi \circ \mathcal{A} + \varphi \circ \mathcal{B} \\ &= \mathcal{A}^d(\varphi) + \mathcal{B}^d(\varphi) \\ &= (\mathcal{A}^d + \mathcal{B}^d)(\varphi)\end{aligned}$$

$$\begin{aligned}(\lambda\mathcal{A})^d &= \varphi \circ (\lambda\mathcal{A}) \\ &= \lambda\varphi \circ \mathcal{A} \\ &= \lambda\mathcal{A}^d(\varphi) \\ &= (\lambda\mathcal{A}^d)(\varphi)\end{aligned}$$

Za $\psi \in W*$ je

$$\begin{aligned}(\varphi \circ \mathcal{A})^d(\psi) &= \psi \circ \varphi \circ \mathcal{A} \\ &= (\psi \circ \varphi) \circ \mathcal{A} \\ &= \mathcal{A}^d(\psi \circ \varphi) \\ &= \mathcal{A}^d(\varphi^d(\psi)) \\ &= (\mathcal{A}^d \circ \varphi^d)(\psi)\end{aligned}$$

$\square$

Definicija. *Naj bo $A \in \mathcal{O}^{m\times n}$.* ***Transponirana matrika*** *matrike $A = [a_{ij}]$ je matrika $A^T = [a_{ji}] \in \mathcal{O}^{n\times m}$. Transponiranje je zrcaljenje matrike čez diagonalo.*

PRIMER:

- $\begin{bmatrix} 1 & 0 & 1 \\ -1 & 2 & -2 \end{bmatrix}^T = \begin{bmatrix} 1 & -1 \\ 0 & 2 \\ 1 & -2 \end{bmatrix}$
- $A^{TT} = A$ po definiciji.

Izrek. *Če linearni preslikavi $\mathcal{A} : V \to W$ glede na bazi B_V in B_W pripada matrika A, potem dualni preslikavi $\mathcal{A}^d : W* \to V*$ glede na dualni bazi baz B_W in B_V pripada matrika A^T.*

Dokaz. Naj bo $B_V = \{v_1, \ldots, v_n\}$ baza V in $B_{V*} = \{\varphi_1, \ldots, \varphi_2\} \subseteq V*$ njej dualna baza.

Naj bo $B_W = \{w_1, \ldots, w_m\}$ baza W in $B_{W*} = \{\psi_1, \ldots, \psi_m\} \subseteq W*$ njej dualna baza.

Naj bo $A = [a_{ij}]_{1\leq i\leq m,\ 1\leq j\leq n}$ in naj bo $C = [C_{ij}]_{1\leq i\leq n,\ 1\leq j\leq m}$ matrika preslikave $\mathcal{A}^d$ glede na bazi B_{W*} in B_{V*}.

Dokazujemo, da je $C = A^T$, oziroma, da za vsaka i in j velja $c_{ij} = a_{ji}$

$$
\begin{aligned}
\underbrace{\mathcal{A}^d \tau_i}_{=\psi_i\circ\mathcal{A},\ \forall i=1,\dots,m} &= \sum_{j=1}^{n} c_{ji}\varphi_j \\
\Rightarrow (\psi_i \circ \mathcal{A})(x) &= \sum_{j=1}^{n} c_{ji}\varphi_j(x)\ \forall x \in V \\
x = v_k:\ \ (\psi_i \circ \mathcal{A})(v_k) &= \sum_{j=1}^{n} c_{ji}\varphi_j(v_k) = \underline{c_{ki}},\ \forall i = 1,\dots,m,\ \forall k = 1,\dots,n \\
(\psi_i \circ \mathcal{A})(v_k) &= \psi_i(\mathcal{A}(v_k)) \\
&= \psi_i(\sum_{j=1}^{n} a_{jk}w_j) \\
&= \sum_{j=1}^{m} a_{jk}\psi_i(w_j) \\
&= \underline{a_{ik}} \\
&\Rightarrow C = A^T
\end{aligned}
$$

$\square$

Posledica. *Naj bodo* $A, B \in \mathcal{O}^{m\times n}$, $C \in \mathcal{O}^{n\times p}$ *in* $\lambda \in \mathcal{O}$. *Potem je* $(A+B)^T = A^T + B^T,\ (\lambda A)^T = \lambda A^T$ *in* $(AC)^T = C^T A^T$.

4.4.3 Prehod na novi bazi

Naj bosta $B_V = \{v_1, \ldots, v_n\}$ in $B'_V = \{v'_1, \ldots, v'_n\}$ bazi prostora V. Potem elemente B'_V lahko razvijemo po bazi B_V:

$$\begin{aligned}
id(v'_1) &= v'_1 = p_{11}v_1 + p_{21}v_2 + \ldots + p_{n1}v_n \\
id(v'_2) &= v'_2 = p_{12}v_1 + p_{22}v_2 + \ldots + p_{n2}v_n \\
&\vdots \quad \vdots \\
id(v'_n) &= v'_n = p_{1n}v_1 + p_{2n}v_2 + \ldots + p_{nn}v_n
\end{aligned}$$

Matrika $P = [p_{ij}]_{i,j=1} \in \mathcal{O}^{n\times m}$ se imenuje **prehodna matrika** iz baze B_V v bazo B'_V.

$$P = id_{B_V}$$

Prehodna matrika je matrika, ki pripada identiteti glede na dve različni bazi.

$\Rightarrow P$ je obrnljiva in $P^{-1} = id_{B'_V}^{B_V}$.

Dokaz. $id_{B_V}^{B'_V} \cdot id_{B'_V}^{B_V} = id_{B_V}^{B_V} = I$

□

Poseben primer: Če je $V = \mathcal{O}^n$ in je B_V standardna baza prostora $\mathcal{O}^n$, potem so stolpci matrike P ravno elementi baze B'_V.

Trditev. *Naj bo $\mathcal{A}: V \to W$ linearna preslikava, naj bosta B_V in B'_V bazi prostora V, naj bosta B_W in B'_W bazi prostora W, naj preslikavi $\mathcal{A}$ glede na bazi B_V in B_W pripada matrika A, glede na bazi B'_V in B'_W pa matrika A'. P naj bo prehodna matrika iz baze B_V v bazo B'_V, Q pa prehodna matrika iz baze B_W v bazo B'_W. Potem je $A' = Q^{-1}AP$.*

Dokaz.

$$\begin{aligned}
A &= \mathcal{A}_{B_W}^{B_V}, \\
A' &= \mathcal{A}_{B'_W}^{B'_V}, \\
P &= id_{B_V}^{B'_V}, \\
Q &= id_{B_W}^{B'_W}, \\
Q^{-1} &= id_{B'_W}^{B_W} \\
A' &= \mathcal{A}_{B_W}^{B'_V} \\
&= (id_W \circ \mathcal{A} \circ id_V)_{B'_W}^{B'_V} \\
&= id_{B'_W}^{B_W} \cdot \mathcal{A}_{B_W}^{B_V} \cdot id_{B_V}^{B'_V} \\
&= Q^{-1} \cdot A \cdot P
\end{aligned}$$

Pri predzadnji enakosti smo upoštevali definicijo množenja matrik.

□

PRIMER:

- Določi matriko preslikave $\mathcal{A} : \mathcal{O}^3 \to \mathcal{O}^2$, definirane s predpisom $\mathcal{A}(x,y,z) = (x,y)$, glede na bazi $B = \{ \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \}$ in $B' = \{ \begin{bmatrix} 4 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \end{bmatrix} \}$.

  Matriko preslikave $\mathcal{A}$ je lahko napisati glede na standardni bazi $S = \{e_1, e_2, e_3\}$ in $S' = \{e_1, e_2\}$ prostorov $\mathcal{O}^3$ in $\mathcal{O}^2$.

  * $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$
  * $\mathcal{A}_{S'}^{S} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = A$
  * $P = id_S^B = \begin{bmatrix} 1 & 1 & 1 \\ -1 & 0 & 1 \\ 0 & -1 & 1 \end{bmatrix}$
  * $id_{S'}^{B'} = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix} = Q$
  *

$$\begin{aligned}
\mathcal{A}_{B'}^{B} &= id_{B'}^{S'} \cdot \mathcal{A}_{S'}^{S} \cdot id_S^B \\
&= Q^{-1}AP \\
&= \frac{1}{4 \cdot 2 \cdot 3 \cdot 3} \cdot \begin{bmatrix} 2 & -3 \\ -3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ -1 & 0 & 1 \\ 0 & -1 & -1 \end{bmatrix} \\
&= \begin{bmatrix} -2 & 3 \\ 3 & -4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ -1 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} -5 & -2 & 1 \\ 7 & 3 & -1 \end{bmatrix}
\end{aligned}$$

Definicija. *Matrika $B \in \mathcal{O}^{m\times n}$ je* ***ekvivalentna*** *matriki $A \in \mathcal{O}^{m\times n}$, kadar obstajata obrnljivi matriki $P \in \mathcal{O}^{m\times n}$ in $Q \in \mathcal{O}^{m\times n}$, da je $B = Q^{-1}AP$. Oznaka: $B \sim A$.*

Trditev. *Ekvivalentnost je ekvivalenčna relacija.*

Dokaz.

- Refleksivnost: $A = I^{-1}AI \Rightarrow A \sim A$
- Simetričnost: $B \sim A \Rightarrow \exists P, Q$ obrnljivi, da je $B = Q^{-1}AP \;/P^{-1}$
  $(\underbrace{Q^{-1}}_{obrnljiva})^{-1}BP^{-1} = QB\underbrace{P^{-1}}_{obrnljiva} = A \Rightarrow A \sim B$
- Tranzitivnost: $B \sim A$, $C \sim B \Rightarrow \exists P, Q, R, S$ obrnljive, da je $B = Q^{-1}AP$, $C = S^{-1}BR \Rightarrow C = S^{-1}Q^{-1}APR = (\underbrace{QS}_{obrnljivi})^{-1}A(\underbrace{PR}_{obrnljivi}) \Rightarrow C \sim A.$

□

Trditev. *Matriki $A, B \in \mathcal{O}^{m\times n}$ sta ekvivalentni natanko takrat, ko pripadata isti linearni preslikavi (morda glede na različne baze).*

Dokaz.

$\Leftarrow$ Že vemo

$\Rightarrow$ $A, B \in \mathcal{O}^{m\times n}$, $B = Q^{-1}AP$
Definirajmo linearno preslikavo:

$$\begin{aligned} \mathcal{A} : \mathcal{O}^n &\to \mathcal{O}^m \\ x &\mapsto Ax \end{aligned}$$

Glede na standardni bazi S_n in S_m preslikavi $\mathcal{A}$ pripada matrika A.

$B_n = P(S_n)$, $B_m = Q(S_m)$

P in Q sta obrnljivi, zato sta B_n in B_m bazi.

$$\begin{aligned} \mathcal{A}_{B_m}^{B_n} &= (id_m \circ \mathcal{A} \circ id_n)_{B_m}^{B_n} \\ &= id_{B_m}^{S_m} \cdot \mathcal{A}_{S_m}^{S_n} \cdot id_{S_n}^{B_n} \\ &= Q^{-1} \cdot A \cdot P \\ &= B \end{aligned}$$

□

Definicija. ***Rang*** *matrike $A \in \mathcal{O}^{m\times n}$ je rang linearne preslikave $\mathcal{O}^n \to \mathcal{O}^m$, definirana s predpisom $x \mapsto A \cdot x$.*

Trditev. *Naj bo $\mathcal{A} : V \to W$ linearna preslikava in $A \in \mathcal{O}^{m\times n}$ njena matrika, glede na poljubni bazi prostorov V in W. Potem je rang$A =$ rang$\mathcal{A}$.*

Dokaz. Vemo, da izbiri baz prostorov V in W določata izomorfizma $\Phi_V : \mathcal{O}^n \to V$ in $\Phi_W : \mathcal{O}^m \to W$ $((\alpha_1, \dots, \alpha_n) \mapsto \alpha_1 v_1 + \dots + \alpha_n v_n)$, in da diagram komutira.

$$\begin{aligned} A : \mathcal{O}^n &\to O^m \\ x &\mapsto Ax \end{aligned}$$

$$\begin{aligned} \text{rang}\mathcal{A} &= \text{rang}(\Phi_W \circ A \circ \Phi_v^{-1}) \\ &= \dim(\text{Im}(\Phi_W \circ A \circ \Phi_V^{-1})) \\ &= \dim((\Phi_W \circ A \circ \Phi_V^{-1})[V]) \\ &= \dim(\Phi_W(A(\Phi_V^{-1}(V)))) \\ &= \dim(\Phi_W(A(\mathcal{O}^n))) \\ &= \dim(\Phi_W(\text{Im}A)) \end{aligned}$$

Dokazali smo tudi, da je Im$\mathcal{A} = \Phi_W(\text{Im}A)$.

Φ_W je izomorfizem, zato je Im$\mathcal{A} \cong$ im$A$.

$\Rightarrow \underbrace{\dim(\text{Im}\mathcal{A})}_{\text{rang}\mathcal{A}} = \underbrace{\dim(\text{Im}A)}_{\text{rang}A}$

□

Posledica. *Ekvivalentni matriki imata enak rang. To je rang linearne preslikave, ki ji pripadata.*

Posledica. *Množenje matrik z obrnljivo matriko (z leve ali desne) ne spremeni ranga.*

Dokaz. Naj bo $B = A \cdot P$, kjer je P obrnljiva. Potem je $B = I^{-1} \cdot A \cdot P \sim A$ $\Rightarrow$ rang$B =$ rang$A$.

Podoben dokaz za množenje s P-jem z leve.

□

Izrek. *Vsaka matrika* $A \in \mathcal{O}^{m\times n}$ *je ekvivalentna matriki*

$$A_0 = \begin{bmatrix} 1 & & 0 & \cdots 0 \\ & \ddots & & \\ 0 & & 1 & \cdots 0 \\ \vdots & & \vdots & \vdots \\ 0 & & 0 & 0 \end{bmatrix} = \begin{bmatrix} I_r & O_{r\times n(-r)} \\ O_{(m-r)\times r} & O_{(m-r)\times(n-r)} \end{bmatrix}$$

za nek $r \in \{0, 1, \ldots, min\{m, n\}\}$. *Pri tem je* r *enolično določen in velja* $rangA = r$.

Dokaz. Matriko A identificiramo z linearno preslikavo

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

Če je $A = 0$, je A že zahtevane oblike in število $r(= 0)$ je očitno enolično.

Naj bo $A \neq 0$. Potem je im$A \neq \{0\}$.

Izberimo bazo $\{w_1, \ldots, w_r\}$ za im$A$ in jo dopolnimo do baze $\{w_1, \ldots, w_r, \ldots, w_m\}$ prostora $\mathcal{O}^m$.

V dokazu dimenzijske enačbe smo razmislili, da v $\mathcal{O}^n$ obstaja baza $\{v_1, \ldots, v_r, \ldots, v_n\}$, da je $Av_i = w_i$ za $i = 1, \ldots, r$ in $Av_i = 0$ za $i > r$.

Glede na ti dve bazi preslikavi A ustreza matrika $\begin{bmatrix} 1 & 0 & & 0 & 0 & \cdots & 0 \\ 0 & 1 & & 0 & \vdots & & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & 1 & \vdots & & \vdots \\ \vdots & \vdots & & 0 & \vdots & & \vdots \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & & 0 & 0 & \cdots & 0 \end{bmatrix} = A_0$. Matriki A in A_0 pripadata isti linearni preslikavi, zato sta ekvivalentni.

$r = \dim(\text{Im}A) = \text{rang}A$.

Dokazati moramo še, da je r enolično določen.

Recimo, da je $A \sim \begin{bmatrix} Is & 0_{s\times(n-s)} \\ 0_{(m-s)\times s} & 0_{(m-s)\times(n-s)} \end{bmatrix} = A'$:

Dokažimo, da je Im$B = \text{Lin}\{B^{(1),\ldots,B^n}\}$ za vsako matriko $B \in \mathcal{O}^{m\times n}$.

Če je $y \in \text{Im}B$, potem je $Bx = y$ za nek $x \in \mathcal{O}^n$.

x razvijemo po standardni bazi:

$$\begin{aligned} x &= \alpha_1 e_1 + \cdots \alpha_n e_n \\ &\Rightarrow y = Bx \\ &= \alpha_1 B e_1 + \alpha_2 B e_2 + \cdots + \alpha_n B e_n \\ &= \alpha_1 B^{(1)} + \alpha_2 B^{(2)} + \cdots + \alpha_n B^{(n)} \in \mathrm{Lin}\{B^{(1)}, \ldots, B^{(n)}\}. \end{aligned}$$

Obratno, naj bo $y \in \mathrm{Lin}\{B^{(1)}, \ldots, B^{(n)}\}$.

Potem je

$$\begin{aligned} y &= \alpha_1 B^{(1)} + \cdots + \alpha_n B^{(n)} \\ &= \alpha_1 B e_1 + \alpha_2 B e_2 + \cdots + \alpha_n B e_n \\ &= B(\alpha_1 e_1 + \cdots + \alpha_n e_n) \in \mathrm{Im} B \end{aligned}$$

V našem primeru je $\mathrm{Im} A' = \mathrm{Lin}\{e_1, \ldots, e_s\} \cong \mathcal{O}^s \Rightarrow \mathrm{rang} A' = s$.

$$A' \sim A \Rightarrow \underbrace{\mathrm{rang} A'}_{s} = \mathrm{rang} A = r$$

□

Hkrati smo dokazali še:

Trditev. *Slika vsake matrike je enaka linearni ogrinjači njenih stolpcev.*

Posledica. *Matriki $A, B \in \mathcal{O}^{m \times n}$ sta ekvivalentni natanko takrat, ko imata enak rang.*

Dokaz.

($\Rightarrow$) Že vemo.

($\Leftarrow$) Naj bo $r = \mathrm{rang} A = \mathrm{rang} B$. Potem je $A \sim \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}$ in $B \sim \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$. Po tranzitivnosti ekvivalentnosti (in simetričnosti) je $A \sim B$.

□

Lema. *Če je $A \in \mathcal{O}^{n \times n}$ obrnljiva matrika, je tudi A^T obrnljiva in velja $(A^T)^{-1} = (A^{-1})^T$.*

Dokaz.

$$\begin{aligned} AA^{-1} &= A^{-1} \cdot A = I \\ (A^{-1})^T \cdot A^T &= A^T (A^{-1})^T = I^T = I \\ &\Rightarrow A^T \text{ je obrnljiva in } (A^T)^{-1} = (A^{-1})^T. \end{aligned}$$

□

Posledica. *Za vsako matriko $A \in \mathcal{O}^{m\times n}$ je rangA^T = rang$A$ (in ($A^T \sim A$)).*

Dokaz. Obstajata obrnljivi matriki P in Q, da je $Q^{-1}AP = \begin{bmatrix} I_R & 0_{r\times(n-r)} \\ 0_{(m-r)\times r} & 0_{(m-r)\times(n-r)} \end{bmatrix}$.

$P^TA^T(Q^{-1})^T = \begin{bmatrix} I_r & 0_{r\times(m-r)} \\ 0_{(n-r)\times r} & 0_{(n-r)\times(m-r)} \end{bmatrix}$

$\Rightarrow A^T \sim \begin{bmatrix} I_r & 0_{r\times(m-r)} \\ 0_{(n-r)\times r} & 0_{(n-r)\times(m-r)} \end{bmatrix}$.

$\Rightarrow \mathrm{rang}A^T = r = \mathrm{rang}A$.

Če je $m = n$, dobimo tudi $A^T \sim \begin{bmatrix} I_r & 0_{r\times(n-r)} \\ 0_{(n-r)\times r} & 0_{(n-r)\times(n-r)} \end{bmatrix} \sim A$.

□

Posledica. *Naj bo $A \in \mathcal{O}^{m\times n}$ poljubna matrika. Naslednja števila so enaka:*

- *maksimalno število linearno neodvisnih vrstic matrike A*
- *maksimalno število linearno neodvisnih stolpcev matrike A*
- *rang$A$*

Dokaz. $r_r(A)$ naj bo število iz (a), $r_s(A)$ pa število iz (b).

Vemo, da je $\mathrm{Im}A = \mathrm{Lin}\{A^{(1)}, \ldots, A^{(n)}\}$

Vzemimo $r_s(A)$ stolpcev matrike A, ki so linearno neodvisni. $\{A^{(1)}, \ldots, A^{(n)}\}$ je ogrodje za im$A$. Če izbrani stolpci ne bi bili baza za im$A$, bi jih s preostalimi stolpci lahko dopolnili do baze za im$A$. To pa je v protislovju z maksimalnostjo števila $r_s(A)$. Torej izbrani stolpci tvorijo bazo za im$A$.

$\Rightarrow r_s(A) = \mathrm{rang}A$.

Na enak način je $r_v(A) = \mathrm{rang}A^T = \mathrm{rang}A$.

□

Definirajmo posebne vrste obrnljivih matrik:

- $p, q \in \{1, \ldots, n\},\ p \neq q$
  $P_{p,q}$ naj bo matrika, ki jo dobimo tako, da v I_n zamenjamo p-ti in q-ti stolpec:

  $$P_{p,q} = [e_1, \ldots, e_{p-1}, e_q, e_{p+1}, \ldots, e_{q-1}, e_p, e_{q+1}, \ldots, e_n] = \begin{bmatrix} I & & & & \\ & 0 & & 1 & \\ & & I & & \\ & 1 & & 0 & \\ & & & & I \end{bmatrix}.$$ To je poseben primer permutacijske matrike (ustreza transpoziciji $(p\ \ q)$).

$P_{p,q}^2 = I \Rightarrow P_{p,q}$ je obrnjljiva in $P_{p,q}^{-1} = P_{p,q}$.

$$\begin{aligned} A \cdot P_{p,q} &= A \cdot [e_1, \dots, \underbrace{e_q}_{p}, \dots, \underbrace{e_p}_{q}, \dots, e_n] \\ &= [Ae_1, \dots, \underbrace{Ae_q}_{p}, \dots, \underbrace{Ae_p}_{q}, \dots, Ae_n] \\ &= [A^{(1)}, \dots, \underbrace{A^{(q)}}_{p}, \dots, \underbrace{A^{(p)}}_{q}, \dots, A^{(n)}] \end{aligned}$$

Množenje s $P_{p,q}$ z leve zamenja p-to in q-to vrstico matrike A.

- Za $\alpha \in \mathcal{O} \backslash \{0\}$ in $p \in \{1, \dots, \}$ definiramo $P_{p,\alpha} = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \alpha & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix}$.

  $P_{p,\alpha}$ je obrnljiva in $(P_{p,\alpha})^{-1} = P_{p,\alpha^{-1}}$.

$$\begin{aligned} A \cdot P_{p,\alpha} &= A \cdot [e_1, \dots, e_{p-1}, \underbrace{\alpha e_p}_{p}, e_{p+1}, \dots, e_n] \\ &= [Ae_1, \dots, Ae_{p-1}, \underbrace{\alpha Ae_p}_{p}, Ae_{p+1}, \dots, Ae_n] \\ &= [A^{(1)}, \dots, A^{(p-1)}, \underbrace{\alpha A^{(p)}}_{p}, A^{(p+1)}, \dots, A^{(n)}] \end{aligned}$$

  Množenje s $P_{p,\alpha}$ z desne p-ti stolpec matrike A pomnoži z α.

  Množenje s $P_{p,\alpha}$ z leve p-to vrstico matrike A pomnoži z α.

- $E_{p,q} = \begin{bmatrix} & & \\ & 1 & \\ & & \end{bmatrix}$ je elementarna matrika.

  Naj bo $p \neq q$ in $\alpha \in \mathcal{O}$. Definirajmo $P = I + \alpha \cdot E_{p,q}$.

  Ker je $p \neq q$, je $E_{p,q}^2 = 0 \Rightarrow (I + \alpha E_{p,q})(I - \alpha E_{p,q}) = I$ $\Rightarrow I + \alpha E_{p,q}$ je obrnljiva in $(I + \alpha E_{p,q})^{-1} = I - \alpha E_{p,q}$.

$$
\begin{aligned}
A\cdot(I+\alpha E_{p,q}) &= A+\alpha\cdot A\cdot E_{p,q}\\
&= [A^{(1)},\dots,A^{(n)}]+\alpha\cdot A\cdot[0,\dots,0,\underbrace{e_p}_{q},0,\dots,0]\\
&= [A^{(1)},\dots,A^{(n)}]+[0,\dots,0,\alpha\cdot\underbrace{A_{ep}}_{q},0,\dots,0]\\
&= [A^{(1)},\dots,A^{(q-1)},A^{(q)}\underbrace{+}_{q}\alpha\cdot A^{(p)},A^{(q+1)},\dots,A^{(n)}]
\end{aligned}
$$

Množenje z $I+\alpha E_{p,q}$ z desne q-temu stolpcu matrike A prišteje α-kratnik p-tega stolpca matrike A.

Množenje z $I+\alpha E_{p,q}$ z leve p-ti vrstici matrike A prišteje α-kratnik q-te vrstice matrike A.

$(E_{p,q}^T = E_{p,q})$

Izrek. *Z uporabo množenj z matrikami* 1), 2), 3) *lahko iz matrike A postopoma pridelamo matriko* $A_0=\begin{bmatrix} I_r & 0\\ 0 & 0\end{bmatrix}$*, kjer je $r = rang A$.*

Dokaz. Denimo, da imamo na k-tem koraku ($0\le k\le \min\{m,n\}$) matriko $\begin{bmatrix} I_k & 0\\ 0 & A'\end{bmatrix}$ za neko matriko $A'\in\mathcal{O}^{(m-k)\times(n-k)}$.

Če je $A'=0$, smo končali. Sicer ima A' nek neničelni člen. Zamenjamo ustrezni vrstici in stolpca, da je ta člen v prvem stolpcu in prvi vrstici A'. Nato prvo vrstico A' delimo s tem členom, da dobimo $a'_{11}=1$. Od vrstic matrike A' odštejemo ustrezne večkratnike prve vrstice, da dobimo ničle v prvem stolpcu. Enako naredimo na stolpcih, da dobimo ničle v prvi vrstici matrike A'. Dobimo $\begin{bmatrix} I_{k+1} & \\ & A''\end{bmatrix}$ za nek $A''\in\mathcal{O}^{(m-k-1)\times(n-k-1)}$ in ponovimo postopek. Postopek se po končno korakih konča in na vsakem koraku se rang ohranja, ker so matrike iz primerov 1), 2), 3) obrnljive.

□

PRIMER:

- $\begin{bmatrix} 1 & 0 & 2\\ -1 & 1 & -3\\ 0 & 1 & -1\\ 1 & 2 & 0\end{bmatrix}\sim\begin{bmatrix} 1 & 0 & 2\\ 0 & 1 & -1\\ 0 & 1 & -1\\ 0 & 2 & -2\end{bmatrix}\sim\begin{bmatrix} 1 & 0 & 0\\ 0 & 1 & -1\\ 0 & 1 & -1\\ 0 & 2 & -2\end{bmatrix}\sim\begin{bmatrix} 1 & 0 & 0\\ 0 & 1 & -1\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}\sim\begin{bmatrix} 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}\Rightarrow$

  $\operatorname{rang} A = 2$

4.4.4 Sistemi linearnih enačb

Radi bi rešili sistem enačb

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

kjer so b_i in a_{ij} dani elementi iz obsega $\mathcal{O}$, $x_1, \ldots, x_n$ pa neznanke. Zanima nas, kdaj je sistem enačb rešljiv, koliko je rešitev in kako jih dobimo.

Definiramo matriko koeficientov sistema: $A = [a_{ij}]_{1 \leq i \leq m,\ 1 \leq j \leq n}$, vektor desnih strani $b = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$ in vektor neznank $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$. Potem je sistem enačb ekvivalenten enačbi $Ax = b$.

Sistem $Ax = b$ je homogen, če je $b = 0$ (t.j. $b_i = 0$ za vsak i), sicer je nehomogen. Vsak $x \in \mathcal{O}^n$ za katerega je $Ax = b$ je neprotisloven kadar je množica njegovih rešitev neprazna. Sicer je protisloven. Matriko A identificiramo s preslikavo

$$\begin{aligned} A : \mathcal{O}^n &\to \mathcal{O}^m \\ x &\mapsto Ax \end{aligned}$$

Homogen sistem $Ax = 0$ je vedno neprotisloven. Ena rešitev je $x = 0$. Vse rešitve sistema $Ax = 0$ pa tvorijo natanko jedro matrike (preslikave) A. Sistem $Ax = 0$ ima torej samo eno rešitev ($x = 0$) natanko ko je $\mathrm{Ker}A = \{0\}$.

Spomnimo se dimenzijske enačbe: $\dim(\mathrm{Ker}A) + \mathrm{rang}A = n$. Vedno je $\mathrm{rang}A \leq n$. Sistem $Ax = n$ ima samo trivialno rešitev: $x = 0 \Leftrightarrow \mathrm{rang}A = n$.

V posebnem primeru mora biti $m \geq n$, kar pomeni, da je več enačb kot neznank. Lahko pa se zgodi, da je $m \geq n$ (in $\mathrm{rang}A < n$), da rešitev ni trivialna.

V splošnem je rešitev sistema $Ax = 0$ vektorski $\underbrace{\text{podprostor}}_{\mathrm{Ker}A}$ prostora $\mathcal{O}^n$ razsežnosti $n = \underbrace{\mathrm{rang}A}_{\dim(\mathrm{Ker}A)}$.

Kaj pa homogen sistem?

Definirajmo razširjeno matriko sistema: $\hat{A} = [A \vdots b]$ sistem $Ax = b$ je neprotisloven $\Leftrightarrow \exists x \in \mathcal{O}^n : Ax = b \Leftrightarrow b \in \mathrm{Im}A$

Kronecker-Capelljev izrek: *Sistem $Ax = b$ je neprotisloven $\Leftrightarrow$ rang$\hat{A}$ = rang$A$.*

Dokaz.

$$\begin{aligned} b \in \mathrm{Im}A \Leftrightarrow b \in \mathrm{Lin}\{A^{(1)}, \dots, A^{(n)}\} \Leftrightarrow \mathrm{rang}\hat{A} \\ = \dim\{A^{(1)}, \dots, A^{(n)},\ b\} \\ = \dim\{A^{(1)}, \dots, A^{(n)}\} \\ = \mathrm{rang}A \end{aligned}$$

□

Trditev. *Če je sistem $Ax = b$ neprotisloven in je x neka rešitev tega sistema (rečemo ji* ***partikularna rešitev****), potem je množica rešitev sistema enaka $x + KerA = \{x + y, y \in KerA\}$. To je* ***afin podprostor*** *{jedro, premaknjeno za vektor x }.*

Dokaz. Naj bo z rešitev sistema $Aw = b$.

$Az = b$ in $Ax = b$

$A(z - x) = 0 \Rightarrow z - x \in \mathrm{Ker}A$
$z = x + (z - x) \in x + \mathrm{Ker}A$

Obratno, če je $z \in x + \mathrm{Ker}A$, potem obstaja $y \in \mathrm{Ker}A$, da je

$$\begin{aligned} z &= x + y \\ &\Rightarrow Az = A(x + y) \\ &= Ax + Ay \\ &= b + 0 \\ &= b \end{aligned}$$

□

Sistem $Ax = b$ običajno rešujemo z Gaussovo eliminacijo.

$Ax = b,\ P \in \mathcal{O}^{m \times n}$ je obrnljiva matrika.

$\Rightarrow$ Sistem $Ax = b$ je ekvivalenten sistemu $Pax = Pb$. Rešitev sistema z razširjeno matriko $\hat{A} = [A \vdots b]$ so enake rešitvam sistema, ki ustreza razširjeni matriki $[PA \vdots Pb] = P \cdot \hat{A}$. Če torej z leve razširjeno matriko pomnožimo s poljubno obrnljivo matriko se množica rešitev ne spremeni.

Rešitvi sistemov, ki ustrezata razširjenima matrikama $[A \vdots B]$ in $[PA \vdots Pb]$, sta enaki, če je P obrnljiva matrika.

Za P lahko vzamemo matriki, ki smo jih uporabljali pri računanju ranga. Če na vrsticah razširjene matrike $\hat{A} = [A \vdots b]$ uporabljamo enake operacije kot pri računanju ranga, se torej ? sistema ne spremeni.

Lahko tudi zamenjamo dva stolpca matrike A (ne $\hat{A}$!) vendar moramo v tem primeru zamenjati tudi ustrezne neznanke.

S temi operacijami matriko $\hat{A}$ lahko presekamo(?) do matrike: $\begin{bmatrix} 1 & & * & \vdots & * \\ & \ddots & & \vdots & \vdots \\ & & 1 & \vdots & * \\ & 0 & 0 & \vdots & * \\ & & & \vdots & \vdots \\ & & & \vdots & * \end{bmatrix}$

Enic je toliko, kot je $\text{rang} A' = \text{rang} A$.

Naj bo $(x'_1, \ldots, x'_n)$ permutacija spremenljivk $(x_1, \ldots, x_n)$, ki jo dobimo s pomočjo operacij, ki smo jih naredili na stolpcih matrike A.

Dobimo nov sistem $A'x' = b'$, ki je ekvivalenten prvotnemu: ob upoštevanju permutacije spremenljivk sta rešitvi sistemov $Ax = b$ in $A'x' = b'$ enaki.

$$
\begin{aligned}
x'_1 + a'_{1,r+1}x'_{r+1} + \ldots + a'_{1n}x'_n &= b'_1 \\
x'_2 + a'_{2,r+1}x'_{r+1} + \ldots + a'_{2n}x'_n &= b'_2 \\
\vdots \\
x'_n + a'_{r,r+1}x'_{r+1} + \ldots + a'_{rn}x'_n &= b'_r
\end{aligned}
$$

$$
\begin{aligned}
0 &= b_{r+1} \\
\vdots \\
0 &= b'_m
\end{aligned}
$$

Ta sistem je rešljiv natanko takrat, ko je $b'_{r+1} = \ldots = b'_m = 0$.

To se vidi tudi iz Kronecker-Capelljevega izreka, saj je natanko v tem primeru $\text{rang}\hat{A} = \text{rang}A'$, oziroma $\text{rang}\hat{A} = \text{rang}A$.

Rešitve:

$$\begin{aligned}
&\alpha_1 = x'_{r+1}, \ldots, \alpha_{n-r} = x'_n \in \mathcal{O} \text{ so poljubni parametri}\\
&x'_1 = b'_1 - a'_{1,r+1}\alpha_1 - \ldots - a'_{1n}\alpha_{n-r}\\
&x'_2 = b'_2 - a'_{2,r+1}\alpha_1 - \ldots - a'_{2n}\alpha_{n-r}\\
&\quad\vdots\\
&x'_r = b'_r - a'_{r,r+1}\alpha_1 - \ldots - a'_{rn}\alpha_{n-r}
\end{aligned}$$

V vektorski obliki dobimo: $x' = b' = \alpha_1 v_1 - \ldots - \alpha_{??} v_{??}$ za neke vektorje $v_1, \ldots, v_{??}$.

Vektorji $v_1, \ldots, v_{??}$ so natanko baza jedra matrike A'. Če med postopkom reševanja sistema nismo menjavali stolpcev, je $\{v_1, \ldots, v_{??}\}$ tudi baza jedra matrike A.

Pogosto sistema ne prenesemo v obliko $\begin{bmatrix} 1 & & & & \vdots & * \\ & \ddots & 0 & * & \vdots & \vdots \\ & & 1 & & \vdots & \vdots \\ 0 & & & 0 & \vdots & * \end{bmatrix}$ ampak v obliko $\begin{bmatrix} \underline{0*} & & & * & \vdots & * \\ & \underline{0*} & & & \vdots & \vdots \\ & & \underline{0*} & & \vdots & \vdots \\ & & & \underline{0*} & \vdots & \vdots \\ & & & & \vdots & \vdots \\ 0 & & & & \vdots & * \end{bmatrix}$

Sistem potem rešujemo od spodaj gor.

PRIMER:

- $$\begin{aligned}
x_1 + 2x_2 + 3x_3 + 4x_4 &= -1\\
8x_1 + 7x_2 + 6x_3 + 5x_4 &= 10\\
9x_1 + 10x_2 + 11x_3 + 12x_4 &= 7
\end{aligned}$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & \vdots & -1 \\ 8 & 7 & 6 & 5 & \vdots & 10 \\ 9 & 10 & 11 & 12 & \vdots & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 3 & 4 & \vdots & -1 \\ 0 & -9 & -19 & -27 & \vdots & 18 \\ 0 & -8 & -16 & -24 & \vdots & 16 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 3 & 4 & \vdots & -1 \\ 0 & 1 & 2 & 3 & \vdots & -2 \\ 0 & 1 & 2 & 3 & \vdots & -2 \end{bmatrix} \sim$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & \vdots & -1 \\ 0 & 1 & 2 & 3 & \vdots & -2 \\ 0 & 0 & 0 & 0 & \vdots & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & -1 & -2 & \vdots & 3 \\ 0 & 1 & 2 & 3 & \vdots & -2 \\ 0 & 0 & 0 & 0 & \vdots & 0 \end{bmatrix}$$

Ker je na zadnjem mestu (spodaj desno) 0, je sistem rešljiv.

Naj bosta $\alpha_1, \alpha_2 \in \mathcal{O}$ poljubna parametra. Rešitev sistema je $x_3 = \alpha_1,\ x_4 = \alpha_2,$ $x_2 = -2 - 2\alpha_1 - 3\alpha_2,\ x_1 = 3 + \alpha_1 + 2\alpha_2$. V vektorski obliki je ta rešitev videti takole:

$$x = \begin{bmatrix} 3+\alpha_1+2\alpha_2 \\ -2-2\alpha_1-3\alpha_2 \\ \alpha_1 \\ \alpha_2 \end{bmatrix} = \begin{bmatrix} 3 \\ -2 \\ 0 \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} 1 \\ -2 \\ 1 \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 2 \\ -3 \\ 0 \\ 1 \end{bmatrix}$$

Vektorja $\alpha_1 \begin{bmatrix} 1 \\ -2 \\ 1 \\ 0 \end{bmatrix}$ in $\alpha_2 \begin{bmatrix} 2 \\ -3 \\ 0 \\ 1 \end{bmatrix}$ ustavljata bazi za Ker$A$.

Včasih je treba seštevati več sistemov z isto matriko koeficientov:

$$\begin{gathered} Ax_1 = b_1 \\ Ax_2 = b_2 \\ \vdots \\ Ax_n = b_n \end{gathered}$$

V tem primeru lahko A množimo z vsemi stolpci: $\hat{A} = [A \vdots b_1 b_2 \dots b_n]$ in delamo Gaussovo eliminacijo na vrsticah. Dobimo $\hat{A}' = [A' \vdots b_1' \dots b_n']$, kjer je A' lepa matrika, in sočasno vsak sistem

$$\begin{gathered} A' {\cdot} x_1' = b_1' \\ \vdots \\ A' x_n' = b_n' \end{gathered}$$

posebej.

Poseben primer je iskanje inverza: $A \cdot B = I$ natanko takrat, ko velja $A \cdot B = b_i$ za vsak $i = 1, \dots, n$. Če na matriki $[A \vdots I]$ izmenjamo Gaussovo eliminacijo po vrsticah in je A obrnljiva, dobimo $[I,\ B]$, kjer je $B = A^{-1}$. Če A ni obrnljiva, pa sistem ni rešljiv (inverz ne obstaja).

PRIMER: Poišči inverz:

- $A^{-1} = \begin{bmatrix} 1 & 2 & -1 \\ 2 & 1 & 0 \\ 2 & -1 & 1 \end{bmatrix}^{-1}$

$$\begin{bmatrix} 1 & 2 & -1 & \vdots & 1 & 0 & 0 \\ 2 & 1 & 0 & \vdots & 0 & 1 & 0 \\ 2 & -1 & 1 & \vdots & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -3 & \vdots & 1 & 0 & 0 \\ 0 & -3 & 2 & \vdots & -2 & 1 & 0 \\ 0 & -5 & 3 & \vdots & -2 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -1 & \vdots & 1 & 0 & 0 \\ 0 & -3 & 2 & \vdots & -2 & 1 & 0 \\ 0 & 0 & -\frac{1}{3} & \vdots & \frac{4}{3} & -\frac{5}{3} & 1 \end{bmatrix} \sim$$

$$\begin{bmatrix} 1 & 2 & -1 & \vdots & 1 & 0 & 0 \\ 0 & 1 & -\frac{2}{3} & \vdots & \frac{2}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & 1 & \vdots & -4 & 5 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 0 & \vdots & -3 & 5 & -3 \\ 0 & 1 & 0 & \vdots & -2 & 3 & -2 \\ & & & \vdots & -4 & 5 & -3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & \vdots & 1 & -1 & 1 \\ 0 & 1 & 0 & \vdots & -2 & 3 & -2 \\ 0 & 0 & 1 & \vdots & -4 & 5 & -3 \end{bmatrix}$$

$$\Rightarrow A^{-1} = \begin{bmatrix} 1 & -1 & 1 \\ -2 & 3 & -21 \\ -4 & 5 & -3 \end{bmatrix}$$

4.4.5 Podobnost matrik

Naj bo $\mathcal{A} \in \mathcal{L}(V)$ endomorfizem prostora V. Običajno se splača matriko za A zapisati v eni bazi prostora V: A_B^B, ne pa $\mathcal{A}_{\mathcal{B}_2}^{\mathcal{B}_1}$, kjer sta $\mathcal{B}_1$ in $\mathcal{B}_2$ dve različni bazi.

Naj bo $\mathcal{B}'$ še ena baza prostora V in naj bo $A' = \mathcal{A}_{\mathcal{B}'}^{\mathcal{B}'}$ in $A = \mathcal{A}_{\mathcal{B}}^{\mathcal{B}}$.

Naj bo $P = id_{\mathcal{B}}^{\mathcal{B}'}$ prehodna matrika iz baze $\mathcal{B}$ v bazo $\mathcal{B}'$. Potem vemo, da je: $A' = \mathcal{A}_{\mathcal{B}'}^{\mathcal{B}'} = id_{\mathcal{B}'}^{\mathcal{B}} \circ \mathcal{A}_{\mathcal{B}}^{\mathcal{B}} \circ id_{\mathcal{B}}^{\mathcal{B}'} = P^{-1} \cdot A \cdot P$. Torej $A' = P^{-1}AP$.

Definicija. *Kvadratni matriki $A, B \in \mathcal{O}^{n\times m}$ sta* ***podobni****, kadar obstaja obrnljiva matrika $P \in ‰^{n\times m}$, da je $B = P^{-1} \cdot A \cdot P$.*

Na enak način kot v primeru ekvivalentnosti matrik dokažemo:

Trditev. *Podobnost je ekvivalenčna relacija na $\mathcal{O}^{n\times m}$.*

Trditev. *Matriki $A, B \in \mathcal{O}^{n\times m}$ sta podobni natanko takrat, ko pripadata istemu endomorfizmu nekega n-razsežnega vektorskega prostora, morda glede na različni bazi.*

Vemo, da je obrnljiva $n \times n$ matrika ekvivalentna identiteti. Ali je tudi podobna identiteti?

Recimo: $A = \underbrace{P^{-1} \cdot I \cdot P}_{P^{-1}\cdot P = I}$.

Edina matrika, ki je podobna identiteti je identiteta.

Največ, kar lahko upamo, je, da je matrika podobna diagonalni matriki. Videli bomo, da je to pogosto, ne pa vedno.

$A = [a_{ij}]_{i,j=1}^n$ je **diagonalna matrika**, če je $a_{ij} = 0$, za $i \neq j$.

Definicija. *Endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ se da diagonalizirati, kadar obstaja taka baza prostora V, da glede na to bazo endomorfizmu $\mathcal{A}$ pripada diagonalna matrika.*

Naj se $\mathcal{A}$ da diagonalizirati v bazi $B = \{v_1, \ldots, v_n\}$ in naj bo A ustrezna diagonalna matrika. Potem velja $\mathcal{A}v_1 = a_{11}v_1$

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

$$\begin{aligned} \mathcal{A}v_2 &= a_{22}v_2 \\ &\vdots \\ \mathcal{A}v_n &= a_{nn}v_n \end{aligned}$$

$\mathcal{A}$ slika vsak v_i v večkratnik tega vektorja. Takemu vektorju rečemo **lastni vektor**.

Definicija. *Vektor $v \in V$ je* ***lastni vektor*** *endomorfizma $\mathcal{A}$, kadar je $v \neq 0$ in obstaja $\lambda \in \mathcal{O}$, da je $Av = \lambda v$. Skalar λ je* ***lastna vrednost*** *endomorfizma $\mathcal{A}$, ki pripada lastnemu vektorju v.*

Lastna vrednost je z lastnim vektorjem enolično določena:

$$\begin{aligned} \mathcal{A}v = \lambda v,\ \mathcal{A}v = \mu \cdot v &\Rightarrow \lambda v = \mu v \\ &\Rightarrow (\lambda - \mu) \cdot \underbrace{v}_{\neq 0} = 0 \\ &\Rightarrow \lambda = \mu \end{aligned}$$

Če se v lastni vektor za lastno vrednost λ, ni enolično določen, saj so npr. vsi njegovi neničelni večkratniki tudi lastni vektorji za lastno vrednost λ.

Kako dobimo lastne vrednosti in lastne vektorje?

- λ je lastna vrednost

$$\begin{aligned} &\Leftrightarrow \exists \underbrace{v}_{\neq 0} : \mathcal{A}v = \lambda v \\ &\Leftrightarrow \mathcal{A}v - \lambda v = 0 \text{ za nek} v \neq 0 \\ &\Leftrightarrow (\mathcal{A} - \lambda I)v = 0 \text{ za nek} v \neq 0 \\ &\Leftrightarrow \operatorname{Ker}(\mathcal{A} - \lambda I) \neq \{0\} \\ &\Leftrightarrow \mathcal{A} - \lambda I \text{ ni obrnljiv.} \end{aligned}$$

4.5 Determinante

4.5.1 n-linearne preslikave

Definicija. *Naj bodo $V_1, \ldots, V_n$ in U vektorski prostori nad $\mathcal{O}$. Preslikavo $F : V_1 \times V_2 \times \ldots \times V_n \to U$ je n-**linearna**, kadar velja:*

- *Če je $i \in \{1, \ldots, n\}$ poljuben in so $v_1 \in V_1, \ldots, v_{i-1} \in V_{i-1}, v_{i+1} \in V_{i+1}, \ldots, v_n \in V_n$ poljubni vektorji, potem je preslikava $F_i : V_i \to U$ definirana s predpisom $F_i(x) = F(v_1, \ldots, v_{i-1}, x, v_{i+1}, \ldots, v_n)$ linearna.*
- *Če je $U = \mathcal{O}$, n-linearni preslikavi $F : V_1 \times \ldots \times V_n \to \mathcal{O}$ pravimo n-**linearen funkcional**.*

Množica vseh n-linearnih preslikav $V_1 \times \ldots \times V_n \to U$ je vektorski prostor za običajno seštevanje in množenje s skalarjem po točkah. Ta vektorski prostor običajno označimo z $V_1^* \otimes V_2^* \otimes \ldots \otimes V_n^* \otimes U$ in mu rečemo **tenzorski produkt prostorov** $V_1^* \ldots, V_n^*, U$. Elemente tega prostora imenujemo **tenzorji**. V zapisu $V_1^* \otimes \ldots \otimes V_n^* \otimes \mathcal{O}$ $\mathcal{O}$ kar izpuščamo.

Definicija. *Preslikava $F : V^n \to U$ je simetrična, kadar velja:*

- *$F(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = F(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n)$ za vsaka i in j in za vse $v_1, \ldots, v_n \in V$.*

Preslikava $F : V^n \to U$ je antisimetrična, kadar velja:

- *$F(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = -F(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n)$ za vsaka i in j in za vse $v_1, \ldots, v_n \in V$.*

PRIMERI:

- *Skalarni produkt v* $\mathbb{R}^3$*:*

$$F(\vec{a},\vec{b}) = \vec{a}\cdot\vec{b},\ \ (n=2)$$
$$F : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$$

  Ali je F linearna (bilinearna)?

  $\vec{a} \in \mathbb{R}^3$ fiksiramo.

$$\begin{aligned} F_2(\alpha\vec{x}+\beta\vec{y}) &= F(\vec{a},\alpha\vec{x}+\beta\vec{y}) \\ &= \vec{a}(\alpha\vec{x}+\beta\vec{y}) \\ &= \alpha\vec{a}\vec{x}+\beta\vec{a}\vec{y} \\ &= \alpha F(\vec{a},\vec{x})+\beta F(\vec{a},\vec{y}) \\ &= \alpha F_2(\vec{x})+\beta F_2(\vec{y}) \\ &\Rightarrow F \text{ je linearna} \end{aligned}$$

  Podobno preverimo, da je F linearna v prvem faktorju.

  $\Rightarrow F$ je **bilinearna**. Slika v $\mathbb{R} \Rightarrow$ je bilinearen funkcional.

  Je simetrična, saj je $F(\vec{a},\vec{b}) = \vec{a}\cdot\vec{b} = \vec{b}\cdot\vec{a} = F(\vec{b},\vec{a})$ za vsak $\vec{a},\vec{b} \in \mathbb{R}^3$.

- *Vektorski produkt:*

$$F : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3\ (n=2)$$
$$F(\vec{a},\vec{b}) = \vec{a}\times\vec{b}$$

  Podobno kot prej ugotovimo, da je F linearna preslikava. Ni funkcional (ker slika v $\mathbb{R}^3$ in ne v $\mathbb{R}$). Je antisimetrična, saj za poljubna $\vec{a},\vec{b} \in \mathbb{R}^3$ velja $F(\vec{a},\vec{b}) = \vec{a}\times\vec{b} = -\vec{b}\times\vec{a} = -F(\vec{b},\vec{a})$.

- *Mešani produkt:*

$$F : \mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R},\ (n = 3)$$
$$F(\vec{a}, \vec{b}, \vec{c}) = [\vec{a}, \vec{b}, \vec{c}] = (\vec{a} \times \vec{b}) \cdot \vec{c}$$

Če $\vec{a}$ in $\vec{b}$ fiksiramo, je

$$\begin{aligned} F_3 &= (\alpha\vec{x} + \beta\vec{y}) \\ &= F(\vec{a}, \vec{b}, \alpha\vec{x} + \beta\vec{y}) \\ &= [\vec{a}, \vec{b}, \alpha\vec{x} + \beta\vec{y}] \\ &= \alpha[\vec{a}, \vec{b}, \vec{x}] + \beta[\vec{a}, \vec{b}, \vec{y}] \\ &= \alpha F(\vec{a}, \vec{b}, \vec{x}) + \beta F(\vec{a}, \vec{b}, \vec{y}) \\ &= \alpha F_3(\vec{x}) + \beta F_3(\vec{y}) \\ &\Rightarrow F_3 \text{ je linearna} \end{aligned}$$

Podobno je F linearna tudi v prvem in drugem faktorju $\Rightarrow$ je trilinearna. Je trilinearen funkcional, saj je $[\vec{a}, \vec{b}, \vec{c}] = -[\vec{b}, \vec{a}, \vec{c}]$ za poljuben $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$.

- *Množenje matrik:*

$$F : \mathcal{O}^{n\times n} \times \mathcal{O}^{n\times n} \to \mathcal{O}^{n\times n}$$
$$F(A, B) = A \cdot B$$

To je bilinearna preslikava in ni funkcional. Ni niti simetrična niti antisimetrična, saj je v splošnem $A \cdot B \neq B \cdot A$ in $A \cdot B \neq -B \cdot A$.

Lastnosti antisimetričnih n-linearnih preslikav

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

- Če je $v_i = v_j$ za neka $i \neq j$ in je $2 \neq 0$ v $\mathcal{O}$ (obseg ni karakteristike 2), potem je: $F(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = 0$.

  Dokaz:

$$\begin{aligned} F(v_1, \dots, v_i, \dots, v_j, \dots, v_n) &= -F(v_1, \dots, v_j, \dots, v_i, \dots, v_n) \\ &\Rightarrow 2 \cdot F(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = 0 \end{aligned}$$

- $F(v_1, \dots, v_i + \alpha v_j, \dots, v_j, \dots, v_n) = F(v_1, \dots, v_i, \dots, v_j, \dots, v_n)$, če $2 \neq 0$.

  Dokaz:

$$F(v_1, \dots, v_i{+}\alpha v_j, \dots, v_j, \dots, v_n) = F(v_1, \dots, v_i, \dots, v_j, \dots, v_n){+}\underbrace{\alpha(v_1, \dots, v_j, \dots, v_j, \dots, v_n)}_{=0 \text{ po } (1)}.$$

- Če je $\pi = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ i & i_2 & \cdots & i_n \end{smallmatrix}\right) \in S_n$, je $F(v_i, \dots, v_{i_n}) = S(\pi) F(v_1, \dots, v_n)$ za poljubne $v_1, \dots, v_n \in V$.

Če je F antisimetrična n-linearna preslikava in $\pi = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{smallmatrix}\right) \in S_n$, potem je $F(V_{i1}, \dots, v_{in}) = s(\pi) F(v_1, \dots, v_n)$.

Dokaz. Z indukcijo na število transpozicij v razcepu permutacij π. Če je π transpozicija, enakost sledi po definiciji antisimetričnosti. Naj bo $\pi = \tau_1, \cdots, \tau_m$ razcep π na transpozicije in predpostavimo, da enakost velja za vse permutacije, ki jih je mogoče zapisati kot produkt $m - 1$ transpozicij.

$\rho := \tau_2 \cdots \tau_m$. Potem je $\pi = \tau_1 \cdot \rho$.

Naj bo $\rho = \left(\begin{smallmatrix} 1 & \cdots & n \\ i'_1 & \cdots & i'_n \end{smallmatrix}\right)$. Potem je

$$\begin{aligned} F(v_{i1} \cdots v_{in}) &= F(v_{\pi(1)}, \dots, v_{\pi(n)}) \\ &= F(v_{\tau_1(\rho(1))}, \dots, v_{\tau_1(\rho(n))}) \\ &= -F(v_{\rho(1)}, \dots, v_{\rho(n)}) \\ &= -F(v_{i1'}, \dots, v_{in'}) \\ &= -s(\rho) F(v_1, \dots, v_n) \\ &= s(\pi) F(v_1, \dots, v_m). \end{aligned}$$

$\square$

4.5.2 Definicija in lastnosti determinante

Zaenkrat predpostavimo, da obseg $\mathcal{O}$ nima karakteristike 2 ($2 \neq 0$). Naj bo $A \in \mathcal{O}^{n\times n}$ poljubna matrika. Mislimo si jo kot n-terico tolpcev (oz. identificiramo $\mathcal{O}^{n\times n} = (\mathcal{O}^n)^n$). Naj bo $F : \mathcal{O}^{n\times n} = (\mathcal{O}^n)^n \to \mathcal{O}$ antisimetričnen n-linearen funkcional.

$$A = [a_{ij}]_{i,j=1}^n = [A^{(1)}, \dots, A^{(n)}]$$

.

$$\begin{aligned}
F(A) &= F(A^{(1)}, \dots, A^{(n)}) \\
&= F(a_{11}e_1 + a_{21}e_2 + \dots + a_{n1}e_n, \dots, a_{1n}e_1 + a_{2n}e_2 + \dots + a_{nn}e_n) \\
&= \sum_{i_1,\dots,i_n=1}^{n} a_{i_1,1} \cdots a_{i_n,n}\ F(E_{i1}, \dots, e_{in})
\end{aligned}$$

Po lastnosti (1) je $F(e_{i1}, \dots, e_{in}) = 0$, če je $e_{ij} := e_{ik}$ za neka $j \neq k$.

Neničelne člene dobimo torej le v primeru, ko je $(i_1, \dots, i_n)$ permutacija števil $\{1, \dots, n\}$. Označimo $\pi = \left(\begin{smallmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{smallmatrix}\right)$

Torej je

$$\begin{aligned}
F(A) &= \sum_{\pi \in S_n} a_{\pi(1),1} \cdots a_{\pi(n),n}\ F(e_{\pi(1)}, \dots, e_{\pi(n)}) \\
&= \sum_{\pi \in S_n} a_{\pi(1),1} \cdots a_{\pi(n),n} \cdot s(\pi)\ F(\underbrace{e_1, \dots, e_n}_{I})
\end{aligned}$$

Definicija. *Naj bo $\mathcal{O}$ poljuben obseg. Preslikavo $det : \mathcal{O}^{n\times n} \to \mathcal{O}$, definiramo s predpisom $detA = \sum_{\pi \in S_n} s(\pi) a_{\pi(1),1} \cdots a_{\pi(n),n}$ (kjer je $A = [a_{ij}]$), imenujemo **determinanta**. Oznaka:* $det \begin{Bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{Bmatrix} = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & A_{nn} \end{vmatrix}$. *Če je $2 \neq 0$ in je $F : \mathcal{O}^{n\times n} \to \mathcal{O}$ antisimetričen n-linearen funkcional, je torej $F(A) = (detA) \cdot F(I)$ za vsak $A \in \mathcal{O}^{n\times n}$.*

PRIMERI:

- 2×2: $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = s(\mathrm{id}) a_{11}a_{22} + s(1\ 2) a_{21}a_{12} = a_{11}a_{22} - a_{21}a_{12}$
- 3×3: $\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$

$$\begin{aligned}
&= s(\mathrm{id}) a_{11}a_{22}a_{33} + s(1\ 2) a_{21}a_{12}a_{33} + s(1\ 3) a_{31}a_{22}a_{13} + s(2\ 3) a_{11}a_{32}a_{23} + \\
&+ s(1\ 2\ 3) a_{21}a_{32}a_{13} + s(1\ 3\ 2) a_{31}a_{23}a_{12}.
\end{aligned}$$

Trditev. *Če je $A = [a_{ij}]$, je $detA = \sum_{\rho \in S_n} s(\rho) a_{1,\rho(1)} \cdots a_{n,\rho(n)}$.*

Dokaz.

$$\sum_{\rho \in S_n} s(\rho) a_{1,\rho(1)} \cdots a_{n,\rho(n)} = \sum_{\pi \in S_n} s(\pi^{-1}) a_{\pi(1),1} \cdots a_{\pi(n),n}$$
$$= \det A$$

□

Posledica. *$det(A^T) = detA$.*

Lema. *Determinanta je antisimetričen n-linearen funkcional.*

Dokaz. Zaradi simetrije zadošča dokazati linearnost prvega stolpca in razmisliti, kaj se zgodi, če zamenjamo prva dva stolpca.

$$\begin{aligned}
\det(\alpha u + \beta v, A^{(2)}, \ldots, A^{(n)}) &= \sum_{\pi \in S_n} s(\pi)(\alpha u_{\pi(1)} + \beta v_{\pi(1)}) a_{\pi(2),2} \cdots a_{\pi(n),n} \\
&= \alpha \sum_{\pi \in S_n} s(\pi) u_{\pi(1)} a_{\pi(2),2} \cdots a_{\pi(n),n} + \beta \sum_{\pi \in S_n} s(\pi) v_{\pi(1)} a_{\pi(2),2} \cdots a_{\pi(n),n} \\
&= \alpha \cdot \det(u, A^{(2)}, \ldots, A^{(n)}) + \beta \cdot \det(v, A^{(2)}, \ldots, A^{(n)})
\end{aligned}$$

Podobno velja linearnost v ostalih stolpcih $\Rightarrow F$ je n-linearna.

Naj bo $B = [b_{ij}]$ matrika, ki jo dobimo tako, da v A zamenjamo prva dva stolpca. Potem je

$$\begin{aligned}
\det B &= \sum_{\pi \in S_n} s(\pi) b_{\pi(1),1} b_{\pi(2),2} b_{\pi(3),3} \cdots b_{\pi(n),n} \\
&= \sum_{\pi \in S_n} s(\pi) a_{\pi(1),2} a_{\pi(2),1} a_{\pi(3),3} \cdots a_{\pi(n),n} \\
&= \sum_{\rho \in S_n} s(\rho\tau) a_{\rho(2),2} a_{\rho(1),1} a_{\rho(3),3} \cdots a_{\rho(n),n} \\
&= -\det A \\
&\Rightarrow \text{antisimetričnost}
\end{aligned}$$

Pri predzadnji enakosti smo upoštevali, da $\pi = \rho\tau,\ \tau = (1\ 2)$.

□

Posledica. *Determinanta matrike se ne spremeni, če kakšnemu stolpcu prištejemo večkratnik kakšnega drugega stolpca. Če dva stolpca zamenjamo, se determinanti spremeni predznak. Če stolpec pomnožimo z α, se determinanta pomnoži z α. Enako velja za vrstice.*

Dokaz. Če je $2 \neq 0$, vse to sledi iz lastnosti n-linearnih antisimetričnih preslikav. Za $2 = 0$ študent lahko preveri z računom.

□

V posebnem primeru: Če ima matrika dve vrstici ali dva stolpca enaka, je njena determinanta enaka 0.

Determinante lahko računamo podobno kot rang:

- Če dve vrstici (ali stolpca) zamenjamo, se determinanti spremeni predznak.
- Če vrstico ali stolpec pomnožimo z $\alpha \in \mathcal{O}$, se determinanta pomnoži z α.
- Če vrstici (oz. stolpcu) prištejemo večkratnik kakšne druge vrstice (oz. stolpca), se determinanta ne spremeni.

Vemo, da s pomočjo operacij (1), (2), (3) (pri čemer je $\alpha \neq 0$ v (2)) matriko A lahko prevedemo na zgornje trikotno matriko $B = \begin{bmatrix} b_{11} & & & * \\ & b_{22} & & \\ & & \ddots & \\ 0 & & & b_{nn} \end{bmatrix}$ $\det A = c \cdot B$ za $c \neq 0$ (c dobimo z izpostavljanjem skalarja iz vrstice/stolpca in z zamenjavo vrstic/stolpcev).

$\det B = \sum_{\pi \in S_n} s(\pi) b_{\pi(1),1} \cdots b_{\pi(n),n}$

Če je $\pi(i) > i$, potem je $B_{\pi(i),i} := 0$ in je zato tudi cel produkt enak 0. V zgornji vsoti torej ostanejo le tiste permutacije, kjer je $\pi(i) \leq i$ za vsak i. Taka permutacija je samo identiteta $\Rightarrow \det B = b_{11} b_{22} \dots b_{nn}$.

Determinanta zgornje trikotne matrike je enaka produktu diagonalnih členov. Enako velja za spodnje trikotne matrike.

PRIMER:

- $$\begin{vmatrix} 1 & 0 & -1 & 2 \\ 2 & 1 & -1 & 3 \\ -1 & 2 & 0 & -1 \\ 3 & -1 & 1 & 0 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -1 & 2 \\ 0 & 1 & 1 & -1 \\ 0 & 2 & -1 & 1 \\ 0 & -1 & 4 & -6 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -1 & 2 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & -3 & 3 \\ 0 & 0 & 5 & -7 \end{vmatrix} = 3 \cdot \begin{vmatrix} 1 & 0 & -1 & 2 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 5 & -7 \end{vmatrix}$$

$$= 3 \cdot \begin{vmatrix} 1 & 0 & -1 & 2 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -2 \end{vmatrix} = 3 \cdot 1 \cdot 1 \cdot (-1) \cdot (-2) = 6$$

.

Posledica. *$n \times n$ matrika A je obrnljiva $\Leftrightarrow$ $detA \neq 0$.*

Dokaz. A je obrnljiva $\Leftrightarrow$ preslikava

$$\begin{aligned} x &\mapsto Ax \\ \mathcal{O}^n &\to \mathcal{O}^n \end{aligned}$$

je izomorfizem.

$$\begin{aligned} \dim \mathcal{O}^n &= \dim(\mathrm{Ker} A) + \mathrm{rang} A \\ &\Rightarrow \dim(\mathrm{Ker} A) = 0 \\ &\Leftrightarrow \mathrm{rang} A = n \\ &\Rightarrow \text{ preslikava } x \mapsto Ax \text{ je bijektivna} \\ &\Leftrightarrow \text{ injektivna } \Leftrightarrow \text{ surjektivna} \\ &\Rightarrow A \text{ je obrnljiva} \Leftrightarrow \mathrm{rang} A = n \end{aligned}$$

Vemo, da lahko s pomočjo operacij (1), (2) (kjer je $\alpha \neq 0$) in (3) matriko A prevedmo v matriko $A_0 = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ kjer je $r = \mathrm{rang} A$.

$$\det A = \underbrace{c}_{\neq 0} \cdot \det A_0 = \begin{cases} c \neq 0 & ; r = n \\ 0 & ; r < n \end{cases}$$

$\square$

Definicija. *Naj bo $A \in \mathcal{O}^{m \times n}$ in $q \leq k \leq min\{m, n\}$.* ***Minor reda*** *$k$ matrika A je determinanta podmatrike, ki jo dobimo tako, da v A izberemo k vrstic in k stolpcev, v podmatriki pa so členi na križiščih teh vrstic in stolpcev. Členi matrike so minorji reda 1. Determinante $n \times n$ matrike je njen minor reda n.*

Izrek. *Rang neničelne matrike $A \in \mathcal{O}^{m \times n}$ je enak najvišjemu redu neničelnega minorja te matrike.*

Dokaz. Naj bo $r = \text{rang}A$. Potem v A obstaja r linearno neodvisnih stolpcev. Naj ti stolpci tvorijo podmatriko B matrike A. $\text{rang}B = r$, zato v B obstaja r linearno neodvisnih vrstic. Te matrike naj tvorijo matriko C. $C \in \mathcal{O}^{r \times r}$, je ranga r, je podmatrika v A. Potem je $\det C \neq 0$ in to je neničelni minor matrike A.

Dokazati je treba še, da so vsi minorji višjih redov neničelni. Naj bo $k > r$ in predpostavimo, da v A obstaja $k \times k$ podmatrika D z determinanto $\neq 0$. D je obrnljiva, torej jo sestavjajo linearno neodvisni stolpci. Ustrezni stolpci so linearno neodvisni stolpci matrike A. Protislovje, saj je $k > \text{rang}A$. $\Rightarrow$ Vsi minorji reda k v A so enaki 0.

$\square$

Izrek. *Determinanta je **multiplikativen funkcional**: $det(AB) = (detA)(detB)$ za vsaki matriki $A, B \in \mathcal{O}^{n \times n}$.*

Dokaz. Samo v primeru, ko je $2 \neq 0$ (primer, ko je $2 = 0$, študenti enakost lahko sami preverijo z računom). Fiksirajmo $A \in \mathcal{O}^{n \times n}$ in definirirajmo preslikavo $F : (\mathcal{O}^n)^n \to \mathcal{O}$ s predpisom $F(v_1, \ldots, v_n) = \det[Av_1, Av_2, \ldots, Av_n]$. To je n-linearen antisimetričen funkcional. Ker je $2 \neq 0$, vemo, da je $F(v_1, \ldots, v_n) = \det[v_1, \ldots, v_n] \cdot F(e_1, \ldots, e_n)$. Za vektorje v_i vzamemo stolpce matrike B. Dobimo

$$F(B^{(1)}, \ldots, B^{(n)}) = \det[B^{(1)}, \ldots, B^n] \cdot F(e_1, \ldots, e_n)$$

$$\det[\underbrace{A \cdot B^{(1)}, \ldots, A \cdot B^{(n)}]}_{\det(AB)} = \det B \cdot \underbrace{\det[Ae_1, \ldots, Ae_n]}_{\det[A^{(1)}, \ldots, A^{(n)}] = \det A}$$

$\square$

Posledica. *Če je A obrnljiva matrika, je $detA \neq 0$ (kar že vemo) in velja $det(A^{-1}) = (detA)^{-1}$.*

Dokaz.

$$A \cdot A^{-1} = I$$

$$\underbrace{\det(A \cdot A^{-1})}_{(\underbrace{\det A}_{\neq 0}) \cdot (\det A^{-1}) \Rightarrow \det A^{-1} = (\det A)^{-1}} = \det I = 1$$

$\square$

Posledica. *Podobni matriki imata enako determinanto.*

Dokaz.

$$\begin{aligned} B = P^{-1}AP \Rightarrow \det B &= \det(P^{-1}AP) \\ &= (\det P^{-1})(\det A)(\det P) \\ &= (\det P)^{-1}(\det A)(\det P) \\ &= \det A \end{aligned}$$

□

Definicija. *Determinanta endomorfizma $\mathcal{A} \in \mathcal{L}(V)$ je determinanta poljubne matrike, ki pripada temu endomorfizmu. Oznaka: det$\mathcal{A}$. Zaradi zadnje posledice je definicija dobra.*

4.5.3 Razvoj determinante

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

Naj bo $A \in \mathcal{O}^{n\times n}$, $A = [a_{ij}] = [A^{(1)}, \dots, A^{(n)}]$. Naj bosta $i, j \in \{1, \dots, \}$ poljubna. Z A_{ij} označimo podmatriko matrike A, ki jo dobimo tako, da iz A odstranimo i-to vrstico in j-ti stolpec.

$\widetilde{a_{ij}} = (-1)^{i+j} \cdot \det A_{ij}$: **poddeterminanta** matrike A.

$\widetilde{A} = [A_{ij}]_{i,j=1}$: **prirejenka** matrike A: to je matrika poddeterminant.

PRIMER:

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

$$A_{11} = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix},\ A_{12} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},\ A_{13} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix},\ A_{21} = \begin{bmatrix} 0 & -1 \\ -1 & 1 \end{bmatrix},\ A_{22} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix},$$

$$A_{23} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ A_{31} = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix},\ A_{32} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix},\ A_{33} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$\widetilde{a_{11}} = 2,\ \widetilde{a_{12}} = -1,\ \widetilde{a_{13}} = -1,\ \widetilde{a_{21}} = 1,\ \widetilde{a_{22}} = 1,\ \widetilde{a_{23}} = 1,\ \widetilde{a_{31}} = 1,$$
$$\widetilde{a_{32}} = -2,\ \widetilde{a_{33}} = 1$$

$$\widetilde{A} = \begin{bmatrix} 2 & -1 & -1 \\ 1 & 1 & 1 \\ 1 & -2 & 1 \end{bmatrix}$$

Izrek. *Naj bo $A \in \mathcal{O}^{n\times n}$ poljubna matrika. Potem velja:*

- *Razvoj po i-ti vrstici: $a_{i1}\widetilde{a_{i1}} + a_{i2}\widetilde{a_{i2}} + \ldots + a_{in}\widetilde{a_{in}} = \det A$ za vsak i*
- *Razvoj po j-tem stolpcu: $a_{1j}\widetilde{a_{1j}} + a_{2j}\widetilde{a_{2j}} + \ldots + a_{nj}\widetilde{a_{nj}} = \det A$ za vsak j*

Dokaz. Zaradi enakosti $\det A = \det A^T$ zadošča dokazati formulo za razvoj po stolpcih.

Najprej formulo dokažemo v posebnem primeru, ko je $A^{(j)} = e_j$:

$$
\begin{aligned}
\det A &= \det[A^{(1)}, \dots, A^{(j-1)}, e_j, A^{(j+1)}, \dots, A^{(n)}] \\
&= \sum_{\pi \in S_n} s(\pi) a_{\pi(1),1} \dots a_{\pi(n),n} \\
&= \sum_{\pi \in S_n,\ \pi(j)=j} s(\pi) a_{\pi(1),1} \dots a_{\pi(j-1),j-1} \cdot \underbrace{1}_{a_{jj}} \cdot a_{\pi(j+1),j+1} \dots a_{\pi(n),n} \\
&= \sum_{\pi \text{ permutacija množice } \{1,\dots,j-1,j+1,\dots,n\}} s(\pi) a_{\pi(1),1} \dots a_{\pi(j-1),j-1} a_{\pi(j+1),j+1} \dots a_{\pi(n),n} \\
&= \det A_{jj} \\
&= S_{n-1}
\end{aligned}
$$

Formulo zdaj dokažemo v primeru, ko je $A^{(j)} = e_i$. Potem je

$$
\begin{aligned}
\det[A^{(1)}, \dots, A^{(j-1)}, e_i, A^{(j+1)}, \dots, A^{(n)}] &= -\det[A^{(1)}, \dots, A^{(j-1)}, A^{(j+1)}, e_i, \dots, A^{(n)}] \\
&= \cdots \\
&= (-1)^{i-j} \cdot \det[A^{(1)}, \dots, A^{(j-1)}, A^{(j+1)}, \dots, A^{(i)}, e_i, A^{(i+1)}, \\
&\dots, A^{(n)}] \\
&= (-1)^{i+j} \det A_{ij} = \widetilde{a_{ij}}
\end{aligned}
$$

SPLOŠNI PRIMER:

$$
\begin{aligned}
\det A &= \det[A^{(1)}, \dots, A^{(n)}] \\
&= \det[A^{(1)}, \dots, A^{(j-1)}, \sum_{i=1}^{n} a_{ij} e_i, A^{(j+1)}, \dots, A^{(n)}] \\
&= \sum_{i=1}^{n} a_{ij} \cdot \det[A^{(1)}, \dots, A^{(j-1)}, e_i, A^{(j+1)}, \dots, A^{(n)}] \\
&= \sum_{i=1}^{n} a_{ij} \widetilde{a_{ij}}
\end{aligned}
$$

□

PRIMER:

$$
\begin{vmatrix} 1 & 0 & -1 \\ 1 & 1 & 1 \\ 0 & -1 & 1 \end{vmatrix} = 1 \cdot \begin{vmatrix} 1 & 1 \\ -1 & 1 \end{vmatrix} - 0 \cdot \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} + (-1) \cdot \begin{vmatrix} 1 & 1 \\ 0 & -1 \end{vmatrix} = 1 \cdot 2 + 1 = 3
$$

Pri prvi enakosti smo upoštevali razvoj po prvi vrstici.

Izrek. *Za vsako matriko* $A \in \mathcal{O}^{n\times n}$ *velja* $A \cdot \widetilde{A}^T = \widetilde{A}^T A = (detA) \cdot I$.

Dokaz. Za vsak i velja $a_{i1}\widetilde{a_{i1}} + a_{i2}\widetilde{a_{12}} + \ldots + a_{in}\widetilde{a_{in}} = \det A$ in $a_{1i}\widetilde{a_{1i}} + a_{2i}\widetilde{a_{2i}} + \ldots + a_{ni}\widetilde{a_{ni}} = \det A$. To pomeni: Diagonalni elementi matrik $A\widetilde{A}^T$ in $\widetilde{A}^T A$ so enaki $\det A$. Dokazati moramo še, da so vsi izvendiagonalni členi matrik $A\widetilde{A}^T$ in $\widetilde{A}^T A$ enaki 0.

Naj bosta i in j različna. Potem je $0 = \det[A^{(1)}, \ldots, A^{(i)}, \ldots, A^{(i)}, \ldots, A^{(n)}] = \sum_{k=1}^{n} a_{ki}\widetilde{a_{kj}}$: (j,i)-ti člen v matriki $\widetilde{A}^T A$. Pri tej enakosti smo upoštevali razvoj po j-tem stolpcu. To velja za vsaka različna i in j, torej je $\widetilde{A}^T A = \begin{bmatrix} \det & & 0 \\ & \ddots & \\ 0 & & \det \end{bmatrix} = (\det A) \cdot I$. Podobno dobimo $A\widetilde{A}^T = (\det A) \cdot I$.

$\square$

Posledica. *Če je* $detA \neq 0$, *potem je* A *obrnljiva (kar že vemo) in velja* $A^{-1} = \frac{1}{detA} \cdot \widetilde{A}^T$.

PRIMERI:

- $\begin{bmatrix} 1 & 0 & -1 \\ 1 & 1 & 1 \\ 0 & -1 & 1 \end{bmatrix}^{-1} = \frac{1}{3} \begin{bmatrix} 2 & 1 & 1 \\ -1 & 1 & -2 \\ -1 & 1 & 1 \end{bmatrix}$
- $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

4.5.4 Uporaba pri reševanju sistemov

Imejmo sistem $Ax = b$, kjer je $A \in \mathcal{O}^{n\times n}$ kvadratna matrika in $b \in \mathcal{O}^n$. Ta sistem je enolično rešljiv natanko takrat, ko je A obrnljljiva. Takrat je rešitev $x = A^{-1}b = \frac{1}{\det A} \cdot \widetilde{A}^T \cdot b$.

Naj bo $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ in j-ti člen vektorja $\frac{1}{\det A} \cdot \widetilde{A}^T \cdot b$ označimo z $\frac{1}{\det A}(\widetilde{A}^T b)_j$. Potem je

$$\begin{aligned} x_j &= \frac{1}{\det A}(\widetilde{A}^T \cdot b)_j \\ &= \frac{1}{\det A} \cdot \sum_{k=1}^{n} \widetilde{a_{kj}} \cdot b_k \\ &= \frac{1}{\det A} \cdot \det[A^{(1)}, \ldots, A^{(j-1)}, b, A^{(j+1)}, \ldots, A^{(n)}] \end{aligned}$$

Pri zadnji enakosti smo upoštevali razvoj po j-tem stolpcu.

Izrek. ***(Cramerjeve formule)***: *Če je $A \in \mathcal{O}^{n\times n}$ in $b \in \mathcal{O}^n$, potem je sistem $Ax = b$ enolično rešljiv natanko takrat, ko je $detA \neq 0$. Takrat je rešitev podana s predpisi $x_j = \frac{det[A^{(n)},\ldots,A^{(j-1)},b,A^{(j+1)},\ldots,A^{(n)}]}{detA}$ za $j = 1, \ldots, n$, kjer je $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$.*

PRIMER:

- $ax + by = c$ in $dx + ey = f$. Potem $x = \frac{\begin{vmatrix} c & b \\ f & e \end{vmatrix}}{\begin{vmatrix} a & b \\ d & e \end{vmatrix}}$ in $y = \frac{\begin{vmatrix} a & c \\ d & f \end{vmatrix}}{\begin{vmatrix} a & b \\ d & e \end{vmatrix}}$, če $\begin{vmatrix} a & b \\ d & e \end{vmatrix} \neq 0$.

5 STRUKTURA ENDOMORFIZMOV

5.1 Lastne vrednosti in lastni vektorji

Definicija. *Neničelni vektor $v \in V$ je **lastni vektor** endomorfizma $\mathcal{A} \in \mathcal{L}V$, kadar obstaja $\lambda \in \mathcal{O}$, da je $\mathcal{A}v = \lambda v$. λ se imenuje **lastna vrednost** endomorfizma $\mathcal{A}$, ki pripada lastnemu vektorju v.*

Trditev. *Naj bo $\lambda \in \mathcal{O}$ lastna vrednost endomorfizma $\mathcal{A} \in \mathcal{L}(v)$. Potem je množica $\{v \in V; \mathcal{A}v = \lambda v\} = \{$lastni vektorji, ki pripadajo lastni vrednosti λ $\} \cup \{0\}\}$ vektorski podprostor prostora V. Pravimo mu **lastni podprostor** endomorfizma $\mathcal{A}$ za lastno vrednost λ. Razsežnost tega lastnega podprostora pa se imenuje **geometrična večkratnost** lastne vrednosti λ.*

Dokaz.

$$\begin{aligned}\{v \in V; \mathcal{A}v = \lambda v\} &= \{v \in V; (\mathcal{A} - \lambda id_v)v = 0\} \\ &= \operatorname{Ker}(\mathcal{A} - \lambda id_v)\end{aligned}$$

□

Trditev. *Naj bo $V \neq \{0\}$. Endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ se da diagonalizirati natanko takrat, ko v V obstaja baza, sestavljena iz lastnih vektorjev endomorfizma $\mathcal{A}$.*

Dokaz.

($\Rightarrow$) Če diagonalna matrika $A = [a_{ij}]$ pripada endomorfizmu $\mathcal{A}$ glede na bazo $B = \{v_1, \ldots, v_n\}$, potem za vsak i velja $\mathcal{A}v_i = a_{ii}v_i$.

($\Leftarrow$) Če je $\{u_1, \ldots, u_n\}$ baza iz lastnih vektorjev, potem obstajajo $\lambda_1, \ldots, \lambda_n \in \mathcal{O}$, da je $\mathcal{A}u_i = \lambda_i u_i$ za vsak i. Potem endomorfizmu $\mathcal{A}$ glede na bazo B pripada matrika

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

□

Posledica. *Endomorfizem $\mathcal{A} \in \mathcal{L}(v)$, kjer je $dimV = n$, se da diagonalizirati natanko takrat, ko ima $\mathcal{A}$ n linearno neodvisnih lastnih vektorjev.*

PRIMER:

- Naj bo $A \in \mathcal{O}^{n\times n}$ in $\mathcal{A} : \mathcal{O}^n \to \mathcal{O}^n$ preslikava, definirana s predpisom $\mathcal{A}x = Ax$. (Včasih to preslikavo tudi označimo kar z A). Predpostavimo, da se $\mathcal{A}$ da diagonalizirati. To pomeni, da je matrika A podobna neki diagonalni matriki: $A = PDP^{-1}$, kjer je D diagonalna. Kaj je D in kaj je P?

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

$$\begin{aligned} De_i &= \lambda_i e_i \\ PDP^{-1}Pe_i &= \lambda_i Pe_i \\ APe_i &= \lambda_i Pe_i \\ \mathcal{A}(Pe_i) &= \lambda_i(Pe_i) \text{ za vsak } i. \end{aligned}$$

Diagonalni elementi matrik D so lastne vrednosti endomorfizma $\mathcal{A}$. Pe_i je i-ti stolpec matrike P. Stolpci matrike P so torej lastni vektorji endomorfizma $\mathcal{A}$.

Trditev. *Naj bo $\mathcal{A} \in \mathcal{L}(v)$ in naj bodo $\lambda_1, \ldots, \lambda_m$ paroma različne lastne vrednosti endomorfizma $\mathcal{A}$, $v_1, \ldots, v_m$ pa pripadajoči lastni vektorji. Potem so $v_1, \ldots, v_m$ linearno neodvisni.*

Dokaz. Predpostavimo, da so $v_1, \ldots, v_m$ linearno odvisni. $v_1 \neq 0$, zato je $m > 1$. Obstaja najmanjši k, da je v_k linearna kombinacija vektorjev z manjšimi indeksi. $v_k = \sum_{i=1}^{k-1} \alpha_i v_i$ *. Na tej enakosti uporabimo $\mathcal{A}$:

$$\mathcal{A}v_k = \mathcal{A}(\sum_{i=1}^{k-1} \alpha_i v_i) = \sum_{i=1}^{k-1} \alpha_i \mathcal{A}v_i$$

Upoštevamo, da so v_i lastni vektorji za lastne vrednosti λ_i:

$$\lambda_k v_k = \sum_{i=1}^{k-1} \alpha_i \lambda_i v_i$$

* pomnožimo z λ_k:

$$\lambda_k v_k = \sum_{i=1}^{k-1} \alpha_i \lambda_k v_i$$

Enačbi odštejemo:

$$\sum_{i=1}^{k-1} \alpha_i(\lambda_i - \lambda_k)v_i = 0$$

Ker je $v_k \neq 0$, je $\lambda_i \neq 0$ za vsak en $i = 1, \ldots, k{-}1$. $\lambda_i{-}\lambda_k \neq 0$. V vsoti $\sum_{i=1}^{k-1} \alpha_i(\lambda_i{-}\lambda_k)v_i = 0$ je zato vsaj en od koeficientov pred vektorji v_i neničeln. Zato so $v_1, \ldots, v_{k-1}$ linearno odvisni. To je v protislovju z minimalnostjo k-ja $\Rightarrow$ $v_1, \ldots, v_m$ so linearno neodvisni.

$\square$

Posledica. *Naj bo* $\dim V = n$ *in* $\mathcal{A} \in \mathcal{L}(V)$. *Če ima* $\mathcal{A}$ n *paroma različnih lastnih vrednosti, se da diagonalizirati.*

5.2 Karakteristični in minimalni polinom

$\mathcal{A} \in \mathcal{L}(V)$. Kako poiščemo lastne vrednosti (in lastne vektorje)?

A naj bo matrika endomorfizma $\mathcal{A}$ glede na neko bazo. λ je lastna vrednost endomorfizma $\mathcal{A} \Leftrightarrow \exists \underbrace{v}_{\neq 0} \in V$:

$$\begin{aligned}\mathcal{A}v = \lambda v \Leftrightarrow &\Leftrightarrow \exists x \neq 0, x \in \mathcal{O}^n : Ax = \lambda x \\ &\Leftrightarrow \exists x \neq 0, x \in \mathcal{O}^n : Ax - \lambda I x = 0 \\ &\Leftrightarrow \exists x \neq 0, x \in \mathcal{O}^n : (A - \lambda I)x = 0 \\ &\Leftrightarrow \exists x \in \mathrm{Ker}(A - \lambda I) \backslash \{0\} \\ &\Leftrightarrow A - \lambda I \text{ ni obrnljiva} \\ &\Leftrightarrow \det(A - \lambda I) = 0\end{aligned}$$

$$\begin{aligned}\det(A - \lambda I) &= \det \begin{bmatrix} a_{11} - \lambda & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - \lambda & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - \lambda \end{bmatrix} \\ &= \sum_{\pi \in S_n} s(\pi)(a_{\pi(1),1} - \lambda\delta_{\pi(1),1}) \cdots (a_{\pi(n),} - \lambda\delta_{\pi(n),n})\end{aligned}$$

To je polinom stopnje največ n v spremenljivki λ. n-krat dobimo λ v produktu $(a_{\pi(1),1} - \lambda\delta_{\pi(1),1}) \cdots (a_{\pi(n),n} - \lambda\delta_{\pi(n),n})$. $\Leftrightarrow \pi(i) = i$ za vsak $i \Leftrightarrow \pi = id$. Zato je $\det(A - \lambda I)$ polinom stopnje n in njegov vodilni koedfinicent je enak $(-1)^n$.

Definicija. *Naj bo $A \in \mathcal{O}^{n \times n}$. Polinom det$(A - \lambda I)$ se imenuje* ***karakteristični polinom*** *matrike A. Oznaka: $\Delta_A(\lambda)$.*

Trditev. *Podobni matriki imata enak karakteristični polinom.*

Dokaz. $B = P^{-1}AP$, P obrnljiva.

$$\begin{aligned}\Rightarrow \delta_B(\lambda) &= \det(B - \lambda I) \\ &= \det(P^{-1}AP - \lambda I) \\ &= \det(P^{-1}AP - \lambda P^{-1}P) \\ &= \det(P^{-1}(A - \lambda I)P) \\ &= (\det P)^{-1}\det(A - \lambda I)\det P \\ &= \Delta_A(\lambda)\end{aligned}$$

□

Definicija. ***Karakteristični polinom endomorfizma*** *$\mathcal{A} \in \mathcal{L}(V)$ (oznaka: $\Delta_{\mathcal{A}}(\lambda)$) je $\Delta_A(\lambda)$, kjer je A poljubna matrika, ki pripada endomorfizmu $\mathcal{A}$.*

Prejšnja trditev nam pove, da je definicija dobra.

Če je obseg $\mathcal{O}$ neskončen, lahko vsak polinom $p(x) \in \mathcal{O}[x]$ identificiramo s polinomsko funkcijo

$$\begin{aligned} \mathcal{O} &\to \mathcal{O} \\ a &\mapsto p(a) \end{aligned}$$

Elementu $p(a)$ rečemo **vrednost polinoma** p v točki a. Če je $p(a) = 0$, a imenujemo **ničla polinoma** p.

Zadnjič smo dokazali:

Izrek. *Lastne vrednosti endomorfizma $\mathcal{A} \in \mathcal{L}(V)$ so natanko tiste ničle karakterističnega polinoma $\Delta_{\mathcal{A}}(\lambda)$, ki ležijo v $\mathcal{O}$ $\mathcal{A}v = \lambda v$, $\lambda \in OO$.*

PRIMER:

- $V = \mathbb{R}^3$, $\vec{a} = (1, 0, 0)$, $\mathcal{A} : V \to V$, $\mathcal{A}x = \vec{a} \times \vec{x}$ je linearna preslikava.

  Za V vzamemo standardno bazo $B = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$.

  Glede na to bazo preslikavi $\mathcal{A}$ pripada matrika $A = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}$

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

  $\Delta_{\mathcal{A}}(\lambda) = \det(A - \lambda I) = \begin{vmatrix} -\lambda & 0 & 0 \\ 0 & -\lambda & -1 \\ 0 & 1 & -\lambda \end{vmatrix} = -\lambda^3 - \lambda$

  $\lambda^3 + \lambda = 0$, $\lambda(\lambda^2 + 1) = 0$, $\lambda_1 = 0$, $\lambda_2 = i$, $\lambda_3 = -i$.

  i in $-i$ nista lastni vrednosti preslikave $\mathcal{A}$, saj v $\mathbb{R}^3$ ne obstaja neničelni vektor $\vec{x}$, za katerega je $\vec{a} \times \vec{x} = + - i\vec{x}$, 0 pa je lastna vrednost z lastnim vektorjem $\vec{a}$.

  Endomorfizem $\mathcal{A}$ se ne da diagonalizirati, saj $\mathbb{R}^3$ ne vsebuje baze iz lastnih vektorjev preslikave $\mathcal{A}$.

$\Delta_{\mathcal{A}}(\lambda)$ sicer ima 3 različne ničle, toda ne ležijo vse v $\mathbb{R}$ in torej niso vse ničle lastne vrednosti endomorfizma $\mathcal{A}$.

Odslej naprej bomo (če ne bomo rekli drugače) predpostavili, da je $\mathcal{O} = \mathbb{C}$ (in matrike z realnimi členi bomo razumeli kot kompleksne matrike). Razlog za to je **osnovni izrek algebre**, ki pravi, da *ima vsak nekonstanen polinom s kompleksnimi koeficienti vsaj eno ničlo v množici kompleksnih števil.*

Izrek. *Vsak nekonstanen polinom s kompleksnimi koeficienti ima vsaj eno ničlo v množici kompleksnih števil.*

Posledica. *Vsak nekonstanen polinom s kompleksnimi koeficienti lahko zapišemo v obliki $p(x) = a_n(x - x_1)^k_1(x - x_2)^k_2 \cdots (x - x_m)^k_m$, kjer so $x_1, \ldots, x_m$ vse različne ničle polinoma p. Pri tem je $k_1 + k_2 + \ldots + k_m$ enako stopnji polinoma p, ki se imenuje* ***red ničle*** *x_i.*

Karakteristični polinom endomorfizma $\mathcal{A} \in \mathcal{L}(V)$ (oziroma pripadajoče matrike $A \in \mathbb{C}^{n\times n}$) je torej oblike $\Delta_A(\lambda) = a_n(\lambda - \lambda_1)^k_1(\lambda - \lambda_2)^k_2 \cdots (\lambda - \lambda_m)^k_m$, kjer so $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$ vse različne lastne vrednosti ($\lambda_i \neq \lambda_j$ za $i \neq j$) endomorfizma $\mathcal{A}$, $a_n = (-1)^n$, $k_1 + k_2 + \ldots + k_m = n$.

Lastne vrednosti matrike $A \in \mathbb{C}^{n\times n}$ so ničle $\lambda_1, \ldots, \lambda_m$ karakterističnega polinoma $\Delta_A(\lambda)$.

Množica $\{\lambda_1, \ldots, \lambda_m\}$ vseh lastnih vrednosti matrike A (oziroma endomorfizma $\mathcal{A}$) se imenuje **spekter** matrike A (oziroma endomorfizma $\mathcal{A}$). OZnaka: $\delta(A)$ ali $\delta(\mathcal{A})$. Število k_i, ki je red ničle λ_i v $\Delta_A(\lambda)$, se imenuje **algebraična večkratnost** lastne vrednosti λ_i.

$n \times n$ matrike ima lahko največ n lastnih vrednosti, vsota njihovih algebraičnih večkratnosti pa je enaka n.

Spomnimo se: Geometrična večkratnost lastne vrednosti λ_i je $\dim(\mathrm{Ker}(A - \lambda_i I))$.

PRIMER:

– $A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & 2 & 3 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ Poiščimo lastne vrednosti in lastne vektorje.

$$\begin{aligned} 0 = \Delta_A(\lambda) &= \det(A - \lambda I) \\ &\begin{vmatrix} 1-\lambda & 1 & 1 & 1 \\ -1 & -1-\lambda & 2 & 3 \\ 0 & 0 & 2-\lambda & 2 \\ 0 & 0 & 0 & 1-\lambda \end{vmatrix} \\ &= (1-\lambda)(2-\lambda)((1-\lambda)(-1-\lambda)+1) \\ &= (1-\lambda)(2-\lambda)(\lambda^2-1+1) \\ &= \lambda^2(\lambda-1)(\lambda-2) \end{aligned}$$

Lastne vrednosti: 0 (alg. večkratnost 2), 1 (alg. večkratnost 1), 2 (alg. večkratnost 1).

Lastni vektorjo so elementi $\mathrm{Ker}(A - \lambda I)$.

– $\lambda = 0: \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & 2 & 3 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 3 & 4 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = 0$$

.

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 = 0 &\Rightarrow x_1 = -x_2 \\ x_3 + x_4 = 0 &\Rightarrow x_4 = 0 \\ x_3 &= 0 \end{aligned}$$

Lastni podprostor: $\{ \begin{bmatrix} -x_2 \\ x_2 \\ 0 \\ 0 \end{bmatrix} ; x_2 \in \mathbb{C} \}$

Baza za $\mathrm{Ker} A$ je $\{ \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \}$

Geometrična večkratnost lastne vrednosti 0 je 1.

- $\lambda = 1$:

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ -1 & -2 & 2 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -2 & -3 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = 0.$$

$$\begin{aligned} x_1 + 2x_2 - 2x_3 - 3x_4 = 0 &\Rightarrow x_1 = -3x_4 \\ x_2 + x_3 + x_4 = 0 &\Rightarrow x_2 = x_4 \\ x_3 + 2x_4 = 0 &\Rightarrow x_3 = -2x_4 \end{aligned}$$

Lastni podprostor: $\mathrm{Ker}(A - I) = \{\begin{bmatrix} -3x_4 \\ x_4 \\ -2x_4 \\ x_4 \end{bmatrix}, x_4 \in \mathbb{C}\}$

Baza: $\{\begin{bmatrix} -3 \\ 1 \\ -2 \\ 1 \end{bmatrix}\}$

Geometrična večkratnost lastne vrednosti 1 je 1.

- Podobno izračunamo lastne vektorje za $\lambda = 2$, geometrična večkratnost 2 je 1.

Izrek. *Matrika A se da diagonalizirati natanko tedaj, ko sta algebraična in geometrična večkratnost vsake njene lastne vrednosti enaki.*

Dokaz.

($\Rightarrow$) Naj bo A podobna diagonalni matriki $D = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}$ kjer so $\lambda_1, \ldots, \lambda_n$ (ne nujno različne) lastne vrednosti matrike A.

$\Delta_A(\lambda) = (\lambda_1 - \lambda)(\lambda_2 - \lambda) \cdots (\lambda_n - \lambda)$.

Algebraična večkratnost lastne vrednosti λ_i je število pojavitev $\lambda_i - \lambda$ v zgornjem produktu.

$\mathrm{Ker}(D - \lambda_i I) = \mathrm{Lin}\{e_j; \lambda_j = \lambda_i\}$

$\dim(\mathrm{Ker}(A-\lambda_i I)) = \dim(\mathrm{Ker}(D-\lambda_i I))$, saj je $A = P^{-1}DP$ in $A-\lambda_i I = P^{-1}(D-\lambda_i I)P$, množenje z obrnljivo matriko ohranja rang.

$\Rightarrow \mathrm{rang}(A-\lambda_i I) = \mathrm{rang}(D-\lambda_i I) \Rightarrow \dim(\mathrm{Ker}(A-\lambda_i I)) = \dim(\mathrm{Ker}(D-\lambda_i I))$

$\Rightarrow \dim(\mathrm{Ker}(A-\lambda_i I)) =$ število indeksov j, za katere je $\lambda_j = \lambda_i$

$\Rightarrow$ algebraična in geometrična večkratnost lastne vrednosti λ_i sta enaka za vsak i

($\Leftarrow$) Naj bo $\Delta_A(\lambda) = (-1)^n(\lambda-\lambda_1)_1^k(\lambda-\lambda_2)_2^k \cdots (\lambda-\lambda_m)_m^k$, kjer so $\lambda_i \neq \lambda_j$ za $i \neq j$.

Dokazati moramo, da v $\mathbb{C}^n$ obstaja naza iz lastnih vektorjev matrike A.

Po predpostavki je $k_i = \dim(\mathrm{Ker}(A-\lambda_i I))$ za vsak i.

Naj bo $\{x_1, \ldots, x_{k_1}\}$ baza za $\mathrm{Ker}(A-\lambda_1 I)$, $\{x_{k_1+1}, \ldots, x_{k_1+k_2}\}$ baza $\mathrm{Ker}(A-\lambda_2 I)$, $\ldots \{x_{k_1+\ldots+k_{m-1}+1}, \ldots, x_{k_1+\ldots+k_m}\}$ baza $\mathrm{Ker}(A-\lambda_m I)$.

Zadošča dokazati, da je $\{x_1, \ldots, x_{k_1+\ldots+k_m}\}$ baza.

Ker je $k_1 + \ldots k_m = n$, zadošča dokazati, da so $x_1, \ldots, x_n$ linearno neodvisni.

Predpostavimo, da je $\sum_{j=1}^n \alpha_j x_j = 0$ za neke $\alpha_j \in \mathbb{C}$.

Za nek i definirajmo $v_i = \sum_{j=1}^{k_i} \alpha_{k_1+\ldots k_{i-1}+j} x_{k_1+\ldots+k_{i-1}+j}$. x predstavlja lastni vektor za λ_i.

Ker je $Ax_{k_1} + \ldots + k_{i-1} + j = \lambda_i x_{k_1+\ldots+k_{i-1}+j}$ za vsak j, je tudi $Av_i = \lambda_i v_i$; to velja za vsak i.

Za vsak $i = 1, \ldots, m$ je $Av_i = \lambda_i v_i$, $la_i \neq la_j$ za $i \neq j$ in $\sum_{i=1}^m v_i = 0$.

Ker so λ_i paroma različni, so lastni vektorji za te lastne vrednosti linearno neodvisni.

Torej $v_1, \ldots, v_m$ niso lastni vektorji.

Torej je $v_i = 0$ za vsak i.

Za vsak i torej velja $\sum_{j=1}^{k_1} \alpha_{k_1+\ldots+k_{i-1}+j} x_{k_1+\ldots+k_{i-1}+j} = 0$.

Vektorji $x_{k_1+\ldots+k_{i-1},\ldots}, x_{k_1+\ldots+k_i}$ so baza prostora $\mathrm{Ker}(A-\lambda_i I)$, torej so linearno neodvisni.

$\Rightarrow \alpha_k + \ldots k_{i-1} + j = 0 \; \forall j = 1, \ldots, k_i, \; \forall i = 1, \ldots, m.$

$\Rightarrow x_1, \ldots, x_n$ so linearno neodvisni.

$\square$

Izrek. ***Cayley-Hamiltonov izrek***. *Naj bo $p(x) = a_m x^m + \ldots + a_1 x + a_0 \in \mathcal{O}[x]$ nek polinom in $A \in \mathcal{O}^{n \times n}$. Potem lahko izračunamo $a_m A^m + a_{m-1} A^{m-1} + \ldots + a_1 A + a_0 I \in \mathcal{O}^{n\times n}$. To matriko označimo s $p(A)$ in imenujemo vrednost polinoma p v matriki A. Če je $p(A) = 0$ (ničelna $n \times n$ matrika), pravimo, da je A ničla polinoma p.*

Izrek. ***Cayley, Hamilton***. *Vsaka kvadratna matrika je ničla svojega karakterističnega polinoma $\Delta_A(A) = 0$.*

Dokaz. Prirejenka $\widetilde{A - \lambda I}$ ima za člene polinome v λ stopnje največ $n-1$. Označimo $B(\lambda) = (\widetilde{A - \lambda I})^T$.

$B(\lambda)$ lahko napišemo kot vsoto matrik, kjer so vsi neničelni členi monomi iste stopnje.

Najvišjo potenco λ lahko iz vsake od teh matrik v vsoti izpostavimo in dobimo $B(\lambda) = B_0 + B_1\lambda + B_2\lambda^2 + \ldots + B_{n-1}\lambda^{n-1}$ za neke matrike $B_0, \ldots, B_{n-1} \in \mathcal{O}^{n\times n}$.

Za vsak $\lambda \in \mathbb{C}$ je $B(\lambda) = (\widetilde{A - \lambda I})^T = B_0 + B_1\lambda + \ldots + B_{n-1}\lambda^{n-1}$.

Spomnimo se:

$$
\begin{aligned}
(\widetilde{A - \lambda I})^T(A - \lambda I) = \det(A - \lambda I) \cdot I& \\
&\Rightarrow (B_0 + B_1\lambda + \ldots + B_{n-1}\lambda^{n-1})(A - \lambda I) = \Delta_A(\lambda) \cdot I \text{ za vsak } \lambda \in \mathbb{C} \\
&\text{Naj bo } \Delta_A(\lambda) = a_n\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0 \\
&\Rightarrow B_0A + (B_1A - B_0)\lambda + (B_2A - B_1)\lambda^2 + \ldots + (B_{n-1}A - B_{n-2})\lambda^{n-1} - B_{n-1}\lambda^n \\
&= (a_0I) + (a_1I)\lambda + \ldots + (a_nI)\lambda^n \text{ za vsak } \lambda \in \mathbb{C}
\end{aligned}
$$

$\square$

Dokazujemo Cayley-Hamiltonov izrek.

Dokaz. $(a_oI) + (a_1I)\lambda + \ldots + (a_nI)\lambda^n = B_0A + (BA - B_0)\lambda + \ldots + (B_{n-1}A - B_{n-2})\lambda^{n-1} - B_{n-1}\lambda^n$ za vsak $\lambda \in \mathbb{C}$

Členi matrike na levi se v vseh številih ujemajo z ustreznimi členi matrike na desni.

Ker je $\mathbb{C}$ neskončen obseg, to pomeni, da sta za vsaka i in j polinoma na (i, j)-tem mestu v levi in desni matriki enaka, kar pomeni, da imata enake koeficiente. Zato so matrični koeficienti v enakosti zgoraj na levi in na desni enaki.

$$
\begin{aligned}
a_0 I &= B_0 A \\
a_0 I &= B_1 A - B_0 \quad / \cdot A \\
a_2 I &= B_2 A - B_1 \quad / \cdot A^2 \\
&\vdots \\
a_{n-1} I &= B_{n-1} A - B_{n-2} \quad /A^{n-1} \\
a_n I &= -B_{n-1} \quad /A^n
\end{aligned}
$$

$$
\begin{aligned}
a_0 I &= B_0 A \\
a_1 A &= B_1 A^2 - B_0 A \\
a_2 A^2 &= B_2 A^3 - B_1 A^2 \\
&\vdots \\
a_{m-1} A^{n-1} &= B_{n-1} A^n - B_{n-2} A^{n-1} \\
a_n A^n &= -B_{n-1} A^n
\end{aligned}
$$

$$\Delta_A(A) = a_n A^n + a_{n-1} A^{n-1} + \ldots + a_0 I = 0$$

□

Posledica. *Če je $A \in \mathcal{O}^{n\times n}$ obrnljiva matrika, obstaja polinom $q(x) \in \mathcal{O}[x]$, da je $A^{-1} = q(A)$. Inverz torej vedno leži v algebri, generira z A.*

Dokaz. A je obrnljiva $\Rightarrow \det A \neq 0$.

$$
\begin{aligned}
\Delta_A(\lambda) &= a_n \lambda^n + \ldots + a_1 \lambda + a_0 = \det(A - \lambda I) \text{ za vsak } \lambda \\
&\Rightarrow \Delta_A(0) = \det A = a_0 \\
&\Rightarrow a_0 \neq 0 \\
&\Rightarrow a_0 \text{ je obrnljiv.}
\end{aligned}
$$

Cayley-Hamiltonov izrek:

$$
\begin{aligned}
a_n A^n + a_{n-1} A^{n-1} + \ldots + a_1 A + a_0 I &= 0 \\
-\frac{a_n}{a_0} A^n - \frac{a_{n-1}}{a_0} A^{n-1} - \ldots - \frac{a_1}{a_0} A &= I \\
A(-\frac{a_n}{a_o} A^{n-1} - \ldots - \frac{a_1}{a_0} I) = \underbrace{(-\frac{a_n}{a_0} A^{n-1} - \ldots - \frac{a_1}{a_0} I)}_{A^{-1}\text{: inverz je polinom v } A} A &= I
\end{aligned}
$$

□

Opomba: Cayley-Hamiltonov izrek smo formulirali za matrike na $\mathbb{C}$ in dokazali za matrike nad neskončnim obsegom. Velja pa za matrike nad poljubnim obsegom.

Cayley-Hamiltonov izrek nam med drugim pove, da za vsako matriko $A \in \mathcal{O}^{n\times n}$ obstaja vsaj en polinom iz $\mathcal{O}[x]$, ki ima A za ničlo. Zato je naslednja definicija smiselna.

Definicija. ***Minimalni polinom*** *matrike* $A \in \mathcal{O}^{n\times n}$ *je polinom (v* $\mathcal{O}[x]$*), ki ima ničlo* A *in vodilni koeficient 1 in je najmanjše možne stopnje med vsemi neničelnimi polinomi, ki imajo* A *za ničlo.*

Trditev. *Minimalni polinom matrike je z matriko enolično določen.*

Dokaz. Recimo, da sta $p(x) = x^k + a_{k-1}x^{k-1} + \ldots + a_0$ in $q(x) = x^k + b_{k-1}x^{k-1} + \ldots + b_0$ minimalna polinoma za A. Iz tega sledi:

$$A^k + a_{k-1}A^{k-1} + \ldots + a_0 I = A^k + (b_{k-1})A^{k-1} + \ldots + b_0 I$$
$$(a_{k-1} - b_{k-1})A^{k-1} + (a_{k-2} - b_{k-2})A^{k-2} + \ldots + (a_0 - b_0)I = 0$$

Če v zgornji vsoti niso vsi koeficienti 0, dobimo polinom stopnje $\leq k-1$, ki ima A za ničlo, kar je v protislovju z minimalnostjo k-ja. Torej je $b_{k-1} = a_{k-1}$, $b_{k-2} = a_{k-2}$, …, $b_0 = a_0$.

□

Trditev. *Naj bo* $A \in \mathcal{O}^{n\times n}$ *in* $p \in \mathcal{O}[x]$. *Če je* $p(A) = 0$, *potem minimalni polinom matrike* A *(oznaka:* m_A*) deli* p.

Dokaz. Po izreku o deljenju obstajata polinoma $q, r \in \mathcal{O}[x]$, da je $p(x) = m_A(x) \cdot q(x) + r(x)$ in je stopnja polinoma r strogo manjša od stopnje m_A.

Preslikava

$$\mathcal{O}[x] \to \mathcal{O}^{n\times n}$$
$$f(x) \mapsto f(A)$$

je homomorfizem kolobarjev. $\Rightarrow$ v prejšnjo enačbo lahko vstavimo A namesto x:

$$\underbrace{p(A)}_{=0} = \underbrace{m_A}_{=0}(A) \cdot q(A) + r(A) \Rightarrow r(A) = 0$$

Ker je stopnja r manjša od stopnje m_A in je $r(A) = 0$, mora biti r ničelni polinom

$$\Rightarrow m_A(x) \mid p(x)$$

□

Posledica. *Minimalni polinom matrike vedno deli njen karakteristični polinom.*