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 šišemo $T(x, y)$.

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 sistmom. 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* $\vec{a} = (x, y, z) \in \mathbb{R}$ *poljubna točka.* ***Krajevni vektor*** *točke* $\vec{a}$ *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 $a_1, a_2, a_3, \ldots, a_n$ poljubni vektorji. Vsak vektor oblike $\alpha_1\vec{a_1} + \alpha_2\vec{a_2} + \ldots + \alpha_n\vec{a_n}$ kjer so $\alpha_1, \ldots \alpha \in \mathbb{R}$, imenujemo **linearna kombinacija** vektorjev $a_1, \ldots, a_n$.*

Definicija. *Vektorji $a_1, \ldots, a_n$ 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 $\vec{c}$. Rečemo, 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 norma 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 $cos\Theta = cos(\frac{\pi}{2} - \varphi) = sin\varphi$.

  $$P = |\vec{a_1}| \cdot |\vec{a_2}| \cdot cos\Theta = |\vec{a_1'}| \cdot |\vec{a_2}| \cdot cos\Theta = \vec{a_1'} \cdot \vec{a_2}$$
  $$\vec{a_1} = |\vec{a_1}| \cdot (cos\delta, sin\delta)$$
  $$\vec{a_1'} = |\vec{a_1}|(cos(\delta + \frac{\pi}{2}), sin(\delta + \frac{\pi}{2}) = |\vec{a_1}|(-sin\delta, cos\delta) = (-y_1, x_1)$$
  $$\vec{a_1} = (x_1, y_1)$$
  $$P = (-y_1, x_1)(x_2, y_2) = -x_2y_1 + x_1y_2$$

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 $OB'C'A'$.

  ... na to-do listi ...

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

. . . na to-do listi also . . .

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.

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

  $\vec{r} = \vec{r_0} + \lambda s,\ \lambda \in \mathbb{R}$ 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 $\vec{r} = \vec{r_0} + \lambda s,\ \lambda \in \mathbb{R}$, 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 $\vec{r} = \vec{r_1} + \lambda s,\ \lambda \in \mathbb{R}$ in $\vec{r} = \vec{r_2} + \lambda s,\ \lambda \in \mathbb{R}$.

  Predpostavimo, da s_1 ni vzporedna z 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.

  $$|\overrightarrow{Q_1Q_2}| \geq \Delta,\ \textit{po konstrukciji pa je}\ |\overrightarrow{Q_1Q_2}| = d(\Sigma_1, \Sigma_2)$$
  $$\Delta \leq |\overrightarrow{Q_1Q_2}| = d(\Sigma_1, \Sigma_2) \leq d(\Sigma_1, \Sigma_2) \leq \Delta \Rightarrow$$
  $$\Delta = |\overrightarrow{Q_1Q_2}| = d(\Sigma_1, \Sigma_2) = d(T_2, \Sigma_1)$$

  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

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

  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 operciji 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: $ac = cb \neq a = b$.

□

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 $a_1, \ldots, a_k \in \{1, \ldots, n\}$ paroma različni. Permutacija $\sigma \in S_n$, za katero velja $\sigma(a_i) = a_{i+1}$ za $i = 1, \ldots, k-1$, $\sigma(a_n) = a_1$ in $\sigma(a) = a$ za vse $a \in \{1, \ldots, n\} \backslash \{a_1, \ldots, a_n\}$, se imenuje **cikel dolžine** k. Oznaka: $\sigma = (a_1, a_2, \ldots, a_k)$. Cikla $(a_1, \ldots, a_k)$ in $(b_1, \ldots, b_k)$ sta **disjunktivna**, kadar sta množici $\{a_1, \ldots, a_k\}$ in $\{b_1, \ldots, b_k\}$ 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:

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

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).

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

1. možnost: 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

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

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

2. možnost: Števili iz transpozicije τ sta v istem ciklu.

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

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 $\pi = \tau_1\dots\tau_n$, 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 liheha 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 $x, y \in H$,

(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.

□

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

□

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

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

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

$\Rightarrow f$ je homomorfizem grup

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

$f(x + y) = x^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y) \Rightarrow f$ 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 grupi, 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* $\mathrm{im}\ f$. *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* $\mathrm{im} f$ *podgrupa grupe H.*

Dokaz.

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

Naj bosta $a, b \in \ker f$.

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

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

Torej je $\ker f$ podgrupa grupe G.

Zaloga vrednosti je vedno neprazna.

Naj bosta $a, b \in \mathrm{im} f$.

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 $ab^{-1} \in \mathrm{im} f$ in slika homomorfizma f je podgrupa grupe H.

□

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

Izrek. *Homomorfizem grup $f : G \to H$ je injektiven $\Leftrightarrow ker f = \{1\}$. 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 $x \in \ker f$ 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 $x \in \ker f$?

  $$\Rightarrow f(x) = 1 \Leftrightarrow 2^x = 1$$

  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 $z \in \ker f$?

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

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

  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

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

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.

$$0\colon A \to A$$
$$a \mapsto 0 \ \forall a$$

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

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

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

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

Dokažimo še distributivnost.

Naj bodo $f, g, h \in \mathrm{End}(A)$ 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

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

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

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

□

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 $a \cdot a^{-1} = 1 = a^{-1}a$.*

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

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

Opomba 2: 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 $a^{-1} \in K$

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

□

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.

□

4 Končnorazsežni vektorski prostori

4.1 Baza in razsežnost

Definicija. *Naj bo V vektorski prostor nad obsegom 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.

PRIMERI:

- V 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 O^n. Zakaj?

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

  Potem je $x = x_1e_1 + x_2e_2 + \cdots + x_ne_n$.

- $\mathbb{R}[X]$.

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

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

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

PRIMERI:

- 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 $\mathrm{Lin}(M\backslash\{v\})$ [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 $x \in \mathrm{Lin}(M\backslash\{v\})$.

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 $v \in \mathrm{Lin}(M\backslash\{v\})$, 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] $\alpha_2 u_2 + \ldots + \alpha_n u_n \in \mathrm{Lin}(M\backslash\{v\})$.

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 $\alpha_1, \ldots, \alpha_n \in O$ 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] $\in \mathrm{Lin}(M\backslash\{v\})$
[3] $\in \mathrm{Lin}(M\backslash\{v\})$

PRIMER:

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

□

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 O^n. Pravimo ji **standardna baza** prostora 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.

□

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

$$0 = \alpha$$
$$1 = \alpha + \beta$$
$$0 = \alpha + \beta$$

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 treh linearno neodvisnih vektorjev v $\mathbb{R}^3$ $\Rightarrow \{(1,1,1),(0,1,1),(0,1,0)\}$ je baza $\mathbb{R}^3$.

Posledica.

1. *Če je $dimV = n$ in so vektorji $v_1, \ldots, v_n$ linearno neodvisni, potem tvorijo bazo*
2. *Naj bo W vektorski podprostor prostora V. Potem je $dimW \leq dimV$ 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.

   $$dimW = m$$
   $$dimV = m + n$$

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

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

□

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

Dokaz. Na vajah.

□

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

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

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 O in $A : U \to V$ linearna preslikava. Potem velja:*

- *Če je A injektivna, je slika vsake linearno neodvisne množice linearno neodvisna.*
- *Če je A surjektivna, je slika vskega ogrodja za U ogrodje za V.*
- *Če je 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 $A : U \to V$ injektivna.

   Naj bo $\alpha Au_1 + \ldots + \alpha_n Au_n = 0$ za neke $\alpha_j \in O$.

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

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

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

   Ker so $u_1, \ldots, u_n$ linearno neodvisni, sledi $\alpha_1 = \ldots = \alpha_n = 0 \Rightarrow Au_1, \ldots, Au_n$ so linearno neodvisni.

   □

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

   Radi bi dokazali, da je $\{Au_1, \ldots, Au_n\}$ ogrodje prostora V, če je A surjektivna.

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

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

   $\Rightarrow x = Ay = A(\alpha_1 u_1 + \ldots + \alpha_n u_n) = \alpha_1 Au_1 + \ldots + \alpha_n Au_n$

   $\Rightarrow \{Au_1, \ldots, Au_n\}$ je ogrodje za V.

   □

3) *Dokaz.* Sledi iz 1) in 2) □

Izrek.

(1) Naj bo V n-razsežen vektorski prostor nad obsegom O ($n > 0$). Potem je V izomorfizem 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 $\phi : O^n \to V$ 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.

Linearnost:

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

  Potem je

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

Injektivnost:

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

  Naj bo $(\alpha_1, \ldots, \alpha_n) \in \ker\phi$.

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

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

Surjektivnost:

- 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 $n = \dim U = \dim V$.

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

Če je $n > 0$, pa je V izomorfen 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 $V = \{0\} \Rightarrow \dim U = \dim V = 0$.

Če je U netrivialen, pa ima bazo B.

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

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

□

Izrek. *Naj bosta U in V končnorazsežna vektorska prostora nad O in $A : U \to V$ linearna preslikava. Potem je $dim(kerA) + dim(imA) = dimU$.*

Dokaz. Naj bo $\{v_1, \ldots, v_n\}$ baza prostora $\mathrm{im}A$.

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

Izberemo poljubne vektorje $u_1, \ldots, u_n \in U$, da je $v_j = Au_j$ za $j = 1, \ldots, n$.

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

Če dokažemo, da je $B = \{u_1, \ldots, u_n, w_1, \ldots, w_k\}$ baza prostora U, bo formula veljala, saj bo $\dim(\ker A) = k$, $\dim(\mathrm{im}A) = n$ 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

$$\begin{aligned} 0 = A0 &= A(\alpha_1 u_1 + \ldots + \alpha_n u_n + \beta_1 w_1 + \ldots + \beta_k w_k) \\ &= \alpha_1 Au_1 + \ldots + \alpha_n Au_n + \beta_1 Aw_1 + \ldots + \beta_k Aw_k \\ &= \alpha_1 v_1 + \ldots + \alpha_n v_n \end{aligned}$$

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 $Ax \in \mathrm{im}A$, zato je $Ax = \alpha_1 v_1 + \ldots + \alpha_n v_n$.

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

Potem je $Ay = \alpha_1 v_1 + \ldots + \alpha_n v_n = Ax \Rightarrow A(x - y) = 0 \Rightarrow x - y \in \ker A$.

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

5 Kvocientne strukture

5.1 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 $R \subseteq A \times A$.

5.2 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.

5.3 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 razreda, ki so neprazni. Pri tem sta dva elementa množica A ekvivalentna natanko takrat, ko ležita v istem ekvivalenčnem razredu.*

Dokaz. LMN

□

!!!!!!!!!!!!!!!!!!!!Slikala sm shitty in se nč ne vidi!!!!!!!!!!!!!!!

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 $g(a) = [a]$, 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 $\mathbb{Z}_n = \mathbb{Z}/_\equiv = \{[0], [1], \ldots, [n-1]\}$.

  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: ☺

5.4 Usklajenost operacije z ekvivalenčno operacijo

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).

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

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

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

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

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

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

  $\Leftrightarrow mqn'q' + npn'q' = nqm'q' + nqn'p' \rightarrow$ 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 $[a]\cdot[b]=[a\cdot b]$.

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

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 $a \sim b \Leftrightarrow a - b \in H$. ???????*

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.

$a \sim b \Leftrightarrow f(a) = f(b) \Leftrightarrow f(a) - f(b) = 0 \Leftrightarrow f(a - b) = 0 \Leftrightarrow a - b \in \ker f$.

$A/_{\sim} = A/_{\ker f}$.

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 $imp = imf$. V posebnem primeru je $G/_{ker} f \cong imf$.*

   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).

$p([a] + [b]) = p([a + b]) = f(a + b) = f(a) + f(b) = p([a]) + p([b])$.

□

5.6 Kvocientni vektorski prostori

Naj bo V vektorski prostor nad obsegom 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 $y \in O$, 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 $\alpha \in O$, je $x \sim y$ in zaradi usklajenosti $\alpha x \sim \alpha y \Rightarrow [\alpha x] = [\alpha y]$.*

Posledica. *$V/_W$ je vektorski prostor nad 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 ekvivalenčno razred $[x]$?

$$[x] = \{y \in V; y \sim x\} = \{y \in V; y - x \in W\} = \{z + w; z \in W\}$$
$$z = y - x$$
$$y = z + w$$

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.

□

Izrek. *Naj bo $A : V \to W$ linearna preslikava.*

Potem velja:

1. *Obstaja natanko ena linerna preslikava $A : V/_{kerA} \to W$, da diagram komutira. Definirana je s predpisom $A([x]) = Ax$.*
2. *A! je injektivna in velja imA!=imA.*
3. *$V/_{kerA} \equiv imA$*

Dokaz. Dokazati moramo le homogenost preslikave $A!$, vse ostalo že vemo.

$$\begin{aligned} A!(\alpha[x]) &= A!([\alpha x]) \\ &= A(\alpha x) \\ &= \alpha Ax \\ &= \alpha A![x] \end{aligned}$$

Tretja enakost velja zaradi tega, ker je A linearna.

□

Posledica. *Če je V končnorazsežen vektorski prostor in $A : V \to W$ linearna preslikava, je dim($V/_{kerA}$)=dim$V$-dim($kerA$).*

Dokaz. $\dim(V/_{kerA})=\dim(im\mathrm{A})=\dim V-\dim(ker\mathrm{A})$

□

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 $P : V \to U$ definiran s predpisom $P(w + u) = u$ ($w \in W$ 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 P dobro definirana.

Očitno je surjektivna, saj je $P(O + u) = u$ za $\forall u \in U$.

Dokažemo linearnost:

$$\begin{aligned} P(\alpha(w+u)+\beta(w'+u')) &= P((\alpha w+\beta w')+(\alpha u+\beta u')) \\ &= \alpha u+\beta u' \\ &= \alpha P(w+u)+\beta P(w'+u') \end{aligned}$$

Izračunajmo še jedro:

$$P(w+u)=0 \Leftrightarrow u=0 \Rightarrow \mathrm{ker}P=\{w+0; w\in W\}=W$$

P je torej preslikava, ki jo iščemo.

□

Posledica. *Če je V končnorazsežen vektorski prostor nad obsegom O in W njegov podprostor, potem je tudi $V/_W$ končno-razsežen in velja $dimV/W = dimV - dimW$.*

Dokaz. Ker je V končnorazsežen, obstaja v V direktni komplement U prostora W, torej tak podprostor, da je $V = W \oplus U$.

Zato je $V/W \equiv U \Rightarrow \mathrm{dim}(V/W) = \mathrm{dim}U$

Vemo pa, da je $\mathrm{dim}V = \mathrm{dim}W + \mathrm{dim}U = \mathrm{dim}W + \mathrm{dim}(V/W) \Rightarrow \mathrm{dim}(V/W) = \mathrm{dim}V - \mathrm{dim}W$.

□

6 Linearne preslikave in matrike

Trditev. *Naj bo $\{v_1, \ldots, v_n\}$ baza prostora V in $A : V \to W$ linearna preslikava. Če poznamo $Av_1, \ldots, Av_n$, potem lahko enoličnо izračunamo Ax za poljuben $x \in V$. (Ekvivalentno: Linearna preslikava je enoličnо določena s slikami baznih vektorjev)*

Dokaz. $x \in V \Rightarrow x = \alpha_1 v_1 + \ldots + \alpha_n v_n$, ta zapis je enoličen.

$Ax = A(\alpha_1 v_1 + \ldots + \alpha_n v_n) = \alpha_1 Av_1 + \ldots + \alpha_n Av_n$

Druga enakost velja zaradi linearnosti.

□

Naj bosta V in W vektorska prostora nad O z bazama $B_v = \{v_1, \ldots, v_n\}$ in $B_w = \{w_1, \ldots, w_m\}$ in naj bo $A : V \to W$ linearna preslikava.

$Av_i \in W$ za $\forall i = 1, \ldots, n$.

Ker je B_w baza za W, lahko vsak vektor Av_i zadirjemo po tej bazi:

$$\begin{aligned} Av_1 &= a_{11}w_1 + a_{21}w_2 + \ldots + a_{m1}w_m \\ Av_2 &= a_{12}w_1 + a_{22}w_2 + \ldots + a_{m2}w_m \\ &\ldots \\ Av_n &= a_{1n}w_1 + a_{2n}w_2 + \ldots + a_{mn}w_m, \text{ za neki } a_{ij} \in O \end{aligned}$$

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 Av_i napiešmo v i-ti stolpec matrike A.

Matrika reda $m \times n$ ima m vrstic in n stolpec.

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 $A = \mathcal{A}^{B_V}_{B_W}$. 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 O bomo označevali z $O^{m\times n}$.

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 $\Phi : \mathcal{L}(V, W) \to O^{m\times n}$, definirana s predpisom $\Phi(A) = \mathcal{A}^{B_V}_{B_W}$, bijekcija.*

Dokaz. Injektivnost:

$\Phi(\mathcal{A}) = \Phi(\mathcal{A}') \Rightarrow \mathcal{A}_{B_W}^{B_V} = \mathcal{A}_{B_W}^{\prime B_V} = A = [a_{ij}]_{1\leq j\leq n,\ 1\leq j\leq m}$.

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 $A = [a_{ij}] \in O^{m\times n}$ 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 $\mathcal{A}v_i = \sum_{j=1}^n a_{ji}w_j \Rightarrow A = \mathcal{A}_{B_W}^{B_V} = \Phi(\mathcal{A})$

□

$\mathcal{L}(V, W)$ je vektorski prostor. Na $O^{m\times n}$ bi radi definirali tako seštevanje in množenje s skalarjem, da bo $O^{m\times n}$ vektorski prostor, $\Phi : \mathcal{L}(V, W) \to O^{m\times n}$ pa izomorfizem vektorskih prostorov.

Definicija. *Naj bodo V, W in Φ kot v prejšnji trditvi. Na $O^{m\times n}$ 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: $\mathcal{L}(V, W) \to O^{m\times n}$ s preslikavo Φ, pri tem sta $A, B \in O^{m\times n}$ 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 $A = [a_{ij}]$, $B = [b_{ij}] \in O^{m\times n}$ in $\alpha \in O$.

Označimo $\mathcal{A} = \Phi^{-1}(A)$ in $B = \Phi^{-1}(B)$.

Po definiciji je

$$\mathcal{A}v_i = \sum_{j=1}^{n} a_{ji}w_j \text{ in } \mathcal{B}v_i = \sum_{j=1}^{n} b_{ji}w_j \Rightarrow (\mathcal{A}+\mathcal{B})v_i$$
$$= \mathcal{A}v_i + \mathcal{B}v_i$$
$$= \sum_{j=1}^{n} a_{ji}w_j + \sum_{j=1}^{n} b_{ji}w_j$$
$$= \sum_{j=1}^{n} (a_{ji}+b_{ji})w_j$$
$$= *$$

za vsak $i = 1, \ldots, n$.

$$*(A+B)_{B_W}^{B_V} = \begin{bmatrix} a_{11}+b_{11} & \ldots & a_{in}+b_{in} \\ a_{21}+b_{21} & \ldots & a_{2n}+b_{2n} \\ \vdots & & \vdots \\ a_{m1}+b_{m1} & \ldots & a_{mn}+b_{mn} \end{bmatrix} = \Phi(\Phi^{-1}(A)+\Phi^{-1}(B))$$

Ugotovili smo: Matrike seštevamo po členih.

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{m1} & b_{m2} & \ldots & b_{mn} \end{bmatrix} = \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \ldots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \ldots & a_{2n}+b_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \ldots & a_{mn}+b_{mn} \end{bmatrix}$$

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

$$\alpha \cdot \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix} = \begin{bmatrix} \alpha a_{11} & \alpha a_{12} & \ldots & \alpha a_{1n} \\ \alpha a_{21} & \alpha a_{22} & \ldots & \alpha a_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha a_{m1} & \alpha a_{m2} & \ldots & \alpha a_{mn} \end{bmatrix}$$

Tudi množenje s skalarjem ni odvisno od izbire V, V, B_V in B_W.

S skalarjem lahko pomnožimo poljubno matriko, seštevamo pa matrike iste velikosti.

Trditev. *$O^{m\times n}$ je vektorski prostor nad O, preslikava $\Phi : \mathcal{L}(V,W) \to O^{m\times n}$, definirana v prejšnji trditvi, pa izomorfizem vektorskih prostorov.*

Dokaz. Ker je O vektorski prostor nad O in so vse operacije, definirane po členih, bi moralo biti očitno, da je $O^{m\times n}$ vektorski prostor nad O. Preveri doma.

Da je Φ bijektivna, že vemo.

Linearnost:

$$\begin{aligned}\underbrace{\Phi(\mathcal{A})}_{\in O^{m\times n}} + \underbrace{\Phi(\mathcal{B})}_{\in O^{m\times n}} &= \Phi(\Phi^{-1}(\Phi(\mathcal{A})) + \Phi^{-1}(\Phi(B))) \\ &= \Phi(\mathcal{A}+\mathcal{B})\end{aligned}$$

Prva enakost velja zaradi definicije seštevanje v $O^{m\times n}$.

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

□

Enota za seštevanje v $O^{m\times n}$ je matrika, sestavljena iz raznih ničel. Pravimo ji **ničelna matrika** in jo običajno označimo kar z O.

Kaj je $-A$, če je $A = [a_{ij}]$? $-A = [-a_{ij}]$

Posledica.

1. *$dim O^{m\times n} = m \times n$*
2. *Če je $dim V = n$ in $dim W = m$, je $(dim\mathcal{L}(V,W)) = m \times n$*

Dokaz. Zaradi trditve je dovolj dokazati le prvo točko. □