

UNIVERZA V LJUBLJANI

FAKULTETA ZA MATEMATIKO IN FIZIKO

TEORIJA IZ PREDAVANJ PREDMETA

ALGEBRA 1

Maja Levak
Nace Kovačič

Predavatelj
Doc. dr. KLEMEN ŠIVIC

Študijsko leto 2018/2019

Kazalo

1	VEKTORSKI PROSTOR \mathbb{R}^3	3
1.1	Koordinatni sistem	3
1.2	Vektorji	4
1.2.1	Lastnosti računanja z vektorji	5
1.3	Vektorski produkt	9
1.3.1	Lastnosti vektorskega produkta	9
1.4	Mešani produkt	10
1.4.1	Lastnosti mešanega produkta	10
1.5	Dvojni vektorski produkt	11
2	Enačbe premic in ravnin v \mathbb{R}^3	12
2.1	Razdalja do ravnine	14
2.2	Enačba premice	15
2.3	Razdalja do premice	16
2.4	Razdalja med mimobežnima premicama	17
3	OSNOVNE ALGEBRSKE STRUKTURE	19
3.1	Ponovitev preslikav	19
3.2	Operacije	20
3.3	Grupe	23
3.3.1	Grupe permutacij	28
3.4	Podgrupe	35
3.5	Homomorfizem grup	37
3.6	Kolobarji	43
4	KONČNORAZSEŽNI VEKTORSKI PROSTORI	49
4.1	Baza in razsežnost	49
4.2	Vektorski podprostor	60
4.3	Linearne preslikave	61
5	KVOCIENTNE STRUKTURE	68
5.1	Ponovitev relacij	68
5.2	Nekaj lastnosti relacij	68
5.3	Ponovitev ekvivalenčne relacije	69
5.4	Usklajenost operacije z ekvivalenčno operacijo	71
5.5	Kvocienčne grupe Abelovih grup	72
5.6	Kvocienčni vektorski prostori	76
6	LINEARNE PRESLIKAVE IN MATRIKE	80
6.1	Množenje matrik	86
6.2	Dualni prostor in dualne preslikave	94
6.2.1	Dualna preslikava	98
6.3	Prehod na novi bazi	100
6.4	Sistem linearnih enačb	109
6.5	Podobnost matrik	114

7	DETERMINANTE	116
7.0.1	Lastnosti antisimetričnih n - linearnih preslikav	118
7.1	Definicija in lastnosti determinante	119
7.2	Razvoj determinante	123
7.2.1	Uporaba pri reševanju sistemov	125
8	STRUKTURA ENDOMORFIZMOV	127
8.1	Karakteristični in minimalni polinom	128
8.2	Korenski podprostor	137
8.3	Jordanova kanonična forma	142
8.4	Konstrukcija Jordanove baze	144
8.5	Funkcije matrik	148
9	PROSTORI S SKALARNIM PRODUKTOM	151
9.1	Osnovne lastnosti	151
10	ORTOGONALIZACIJA	158
10.1	Preslikave na prostorih s skalarnim produktom	163
10.1.1	Reprezentacija linearnih funkcionalov na vektorskih prostorih s skalarnim produktom	163
10.2	Hermitsko adjungirana preslikava	165
10.3	Normalni endomorfizmi	169
10.4	Sebi adjungirani endomorfizmi	172
10.5	Pozitivno (semi)definitni endomorfizmi	174
10.6	Unitarni endomorfizem	179
10.7	Kvadratni funkcionali	184

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.

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

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

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

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

Množica vseh urejenih trojic realnih števil:

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

Model za \mathbb{R}^3 je prostor z danim koordinatnim sistemom. Sestavljajo ga tri pravokotne številske premice, ki se sekajo v eni točki, ki je izhodišče vseh treh številskih premic. Temu presečišču pravimo **koordinatno izhodišče**, številske premice pa so **koordinatne osi**: x -os, y -os, z -os.¹

¹Dogovor: uporabljamo pozitivno orientiran koordinatni sistem. Če iz enote na z -osi pogledamo na xy -ravnino (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 .² 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 $T_2(x_2, y_2, z_2)$:

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

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 $\vec{a} = (x, y, z) \in \mathbb{R}^3$ poljubna točka. **Krajevni vektor** točke \vec{a} je usmerjena daljica od koordinatnega izhodišča do točke a . Oznaka: $\vec{a} = (x, y, z)$.³

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?

² z dobimo kot presečišče z -osi z ravnino skozi točko T , ki je vzporedna xy -ravnini.

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

- **Množenje s skalarjem:** Če je α pozitiven, je usmerjena daljica določena z vektorjem $\alpha\vec{a}$, vzporedno usmerjeni daljici, določeni z vektorjem a , α -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} , $(-\alpha)$ -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
- $\vec{O} + \vec{a} = \vec{a} + \vec{O} = \vec{a}$ ⁴
- $\vec{a} + (-\vec{a}) = -\vec{a} + \vec{a} = \vec{O}$ ⁵
- distributivnost $(\alpha + \beta)\vec{a} = \alpha\vec{a} + \beta\vec{a}$, $\alpha(\vec{a} + \vec{b}) = \alpha\vec{a} + \alpha\vec{b}$
- $(\alpha\beta)\vec{a} = \alpha(\beta\vec{a})$
- $1 \cdot \vec{a} = \vec{a}$ ⁶

⁴0 je enota za seštevanje.

⁵Obstoj nasprotnega elementa.

⁶1 je enota za množenje.

Definicija. Naj bodo $\vec{a}_1, \vec{a}_2, \vec{a}_3, \dots, \vec{a}_n$ poljubni vektorji. Vsak vektor oblike $\vec{x} = \alpha_1 \vec{a}_1 + \alpha_2 \vec{a}_2 + \dots + \alpha_n \vec{a}_n$ kjer so $\alpha_1, \dots, \alpha_n \in \mathbb{R}$, imenujemo **linearna kombinacija** vektorjev $\vec{a}_1, \dots, \vec{a}_n$.

Definicija. Vektorji $\vec{a}_1, \dots, \vec{a}_n$ so **linearno odvisni** kadar lahko vsaj enega od njih izrazimo kot linearno kombinacijo ostalih. Vektorji so **linearno neodvisni**, kadar niso linearno odvisni (vektorji so torej linearno neodvisni, kadar nobenega od njih ne moremo izraziti kot linearno kombinacijo ostalih). En vektor je linearno odvisen, kadar je ničelni vektor.⁷ 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} .

⁷ker je produkt česar koli z 0 še vedno 0

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 $\alpha\vec{a} + \beta\vec{b} + \gamma\vec{c} = \vec{0}$. Vektorji $\vec{a}, \vec{b}, \vec{c}$ so torej linearno neodvisni, kadar velja sklep $\alpha\vec{a} + \beta\vec{b} + \gamma\vec{c} = \vec{0} \Rightarrow \alpha = \beta = \gamma = 0$ (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 $\vec{x} = \vec{a} \cdot \vec{i}, y = \vec{a} \cdot \vec{j}, z = \vec{a} \cdot \vec{k}$.

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 ⁸: $\vec{a} \cdot \vec{a} \geq 0$ 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 $\vec{a} \cdot \vec{b} = 0$.

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

⁸Pozitivna definitnost deluje, ker je produkt dveh negativnih števil vedno pozitivno število, torej je ≤ 0 tudi če ima vektor \vec{a} kakšno negativno komponento.

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^{\perp} .

$$P = |\vec{a}_1| \cdot |\vec{a}_2| \cdot \sin\varphi$$

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^{\perp} . 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 $\cos\Theta = \cos(\frac{\pi}{2} - \varphi) = \sin\varphi$.

$$\begin{aligned} P &= |\vec{a}_1| \cdot |\vec{a}_2| \cdot \cos\Theta = |\vec{a}_1^{\perp}| \cdot |\vec{a}_2| \cdot \cos\Theta = \vec{a}_1^{\perp} \cdot \vec{a}_2 \\ \vec{a}_1^{\perp} &= |\vec{a}_1| \cdot (\cos\delta, \sin\delta) \\ \vec{a}_1^{\perp} &= |\vec{a}_1|(\cos(\delta + \frac{\pi}{2}), \sin(\delta + \frac{\pi}{2})) = |\vec{a}_1|(-\sin\delta, \cos\delta) = (-y_1, x_1) \\ \vec{a}_1^{\perp} &= (x_1, y_1) \\ P &= (-y_1, x_1)(x_2, y_2) = -x_2y_1 + x_1y_2 \end{aligned}$$

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 $\vec{a} \times \vec{b} \perp \vec{b}$ ⁹
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 vektorja \vec{b}).¹⁰

Vektorski produkt izračunamo

$$\begin{aligned}\vec{a} \times \vec{b} &= \\ &= (a_1, a_2, a_3) \times (b_1, b_2, b_3) \\ &= \begin{bmatrix} \vec{i} & \vec{j} & \vec{k} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{bmatrix} \\ &= \vec{i}(a_2b_3 - b_2a_3) - \vec{j}(a_1b_3 - a_3b_1) + \vec{k}(a_1b_2 - a_2b_1)\end{aligned}$$

Dogovor: Ničelni vektor je vzporeden vsakemu vektorju.

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

Definicija. Determinanta reda 3 je definirana s predpisom

$$\begin{aligned}\begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix} &= \\ &= a_1 \begin{bmatrix} b_2 & b_3 \\ c_2 & c_3 \end{bmatrix} - a_2 \begin{bmatrix} b_1 & b_3 \\ c_1 & c_3 \end{bmatrix} + a_3 \begin{bmatrix} b_1 & b_2 \\ c_1 & c_2 \end{bmatrix} \\ &= a_1(b_2c_3 - c_2b_3) - a_2(b_1c_3 - b_3c_1) + a_3(b_1c_2 - c_1b_2)\end{aligned}$$

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 $\alpha \in \mathbb{R}$

⁹Vektorski produkt je pravokoten na oba vektorja.

¹⁰Pravilo desne roke.

1.4 Mešani produkt

Mešani produkt vektorjev \vec{a} , \vec{b} in \vec{c} je število ¹¹ $[\vec{a}, \vec{b}, \vec{c}] = (\vec{a} \times \vec{b}) \cdot \vec{c}$.

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

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

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. $[\vec{a}, \vec{b}, \vec{c}] = [\vec{b}, \vec{c}, \vec{a}]^{12} = -[\vec{a}, \vec{c}, \vec{b}]^{13}$ 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

¹¹Vrne torej skalar.

¹²Faktorji se lahko spreminjajo ciklično in tudi predznak se ohrani.

¹³Če se faktorji spremenijo neciklično, se predznak zamenja.

1.5 Dvojni vektorski produkt

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

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

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

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

$$\text{Če } \vec{c} \perp \vec{a} \text{ in } \vec{c} \perp \vec{b} \Rightarrow \vec{c} \parallel \vec{a} \times \vec{b} \Rightarrow (\vec{a} \times \vec{b}) \times \vec{c} = \vec{0}$$

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

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

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

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

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

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

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

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

Temu pravimo tudi **Lagrangeva identiteta**.¹⁴

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

¹⁴ $|a \times b|^2 = |a|^2 |b|^2 \sin^2(\theta)$

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.

$(\vec{r} - \vec{r}_0)^{15} \cdot \vec{n} = 0$ 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

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

¹⁵Velja, ker je $\vec{r} - \vec{r}_0$ vektor na Σ , \vec{n} pa je \perp na vse vektorje v tej ravnini.

- 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}_0 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 $\frac{n}{|\vec{n}|}$ ¹⁶ kar je enotski vektor.

$$|\vec{n}| = \sqrt{a^2 + b^2 + c^2}$$

Dobimo enačbo

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

$$\frac{ax}{|\vec{n}|} + \frac{by}{|\vec{n}|} + \frac{cz}{|\vec{n}|} + \frac{d}{|\vec{n}|} = 0$$

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

¹⁶Nova "normirana" normala.

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 $\overrightarrow{T_0 T_1} = \vec{r}_1 - \vec{r}_0$ 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 ¹⁷ 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 .

¹⁷Enačba premice je sistem dveh linearnih enačb, ker je premica "element" obeh ravnin (je njun presek), torej mora zadoščati obema enačbama.

$$T \in p \Leftrightarrow \overrightarrow{T_0T} \parallel s \Leftrightarrow \overrightarrow{T_0T} = \vec{r} - \vec{r}_0 = \lambda s, \lambda \in \mathbb{R}$$

$\vec{r} = \vec{r}_0 + \lambda s$, $\lambda \in \mathbb{R}$ 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 že 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 točke 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 med 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 .

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

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 $f : A \rightarrow B$ je predpis, ki vsakemu¹⁸ elementu množice A priredi natanko en¹⁹ 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 **definijsko območje** preslikave, množico B pa **kodomena** ali **zaloga vrednosti**²⁰ preslikave.

Zaloga vrednosti preslikave $f : A \rightarrow B$ 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 $g : C \rightarrow D$ 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 $g = f|_C$.²¹ Preslikavi f pravimo **razširitev preslikave g** .

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

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

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

Če je preslikava $f : A \rightarrow B$ bijektivna, potem za vsak $y \in B$ obstaja enoličen $x \in A$, da je $f(x) = y$. Preslikava $G : B \rightarrow A$, definirana s predpisom $g(y) = \text{tisti } x \in A, \text{ za katerega je } f(x) = y$, 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** .

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

¹⁸Celovitost.

¹⁹Enoličnost.

²⁰Zaloga vrednosti je enaka kodomeni le, kadar je preslikava surjektivna.

²¹Namesto $f|_C$ bomo včasih pisali kar f in takrat bo moralo biti iz konteksta jasno, da gre za zožitev.

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 $f : A \rightarrow B$ in $g : B \rightarrow C$ je preslikava $g \circ f : A \rightarrow C$ definirana s predpisom $(g \circ f)(x) = g(f(x))$ za vsak $x \in A$. Ekvivalentno, to je tista preslikava $g \circ f : A \rightarrow C$, za katero komutira diagram preslikav.²²

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

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

Trditev. Naj bosta $f : A \rightarrow B$ in $g : B \rightarrow C$ 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. $f : A \rightarrow B$ je bijektivna preslikava z inverzom $g : B \rightarrow A \Leftrightarrow f \circ g = id_B$ in $g \circ f = id_A$. V tem primeru je $g = f^{-1}$.

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

3.2 Operacije

Operacija na množici A je preslikava $A \times A \rightarrow A$, 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.

²²Če gremo na katerikoli način v smeri puščic, dobimo isti rezultat.

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 $A \rightarrow A$. 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

$$\underbrace{A \times A \times A \times \dots \times A}_n \rightarrow A$$

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

PRIMERI:

- Naslednik je enočlena operacija na \mathbb{N} .
- Nasprotno število je enočlena operacija na $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
- $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$, $(a, b, c) \mapsto ab + c$ 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 $R \times A \rightarrow A$.

PRIMER:

- Množenje vektorja s skalarjem je preslikava

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

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

Če je na množici A definirana vsaj ena notranja ali 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 $a_1 \circ a_2 \circ \dots \circ a_n$, kjer so $a_1, \dots, a_n \in A$, neodvisen od tega, kako postavimo oklepaje.

Brez dokaza, lahko bi dokazali z indukcijo na n .

Posledica. Če je operacija \circ asociativna, je izraz $a_1 \circ a_2 \circ \dots \circ a_n$ 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
- $(\mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}, (z, w) \mapsto z|w|$ 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 (obojeustranska) 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 \circ .

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 operacijo \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 velja:

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 $a \circ e = e \circ a = a$, $\forall a \in G$
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
- $(\mathbb{C} \setminus \{0\}, \cdot), (\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot)$ so grupe, enota je 1, inverz od a je $\frac{1}{a}$
- $(\mathbb{Z} \setminus \{0\}, \cdot)$ ni grupa, ker npr. $\frac{1}{2} \notin \mathbb{Z}$

- Naj bo $A \neq \emptyset$ neprazna množica in $F(A)$ množica preslikav $A \rightarrow A$. Ali je $(F(A), \circ)$ grupa?

Če ima A vsaj 2 elementa, $F(A)$ ni grupa. Naj bo $a \in A$ poljuben element in $f : A \rightarrow A$ 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 $A \rightarrow A$.

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

V grupi običajno namesto $a \circ b$ pišemo kar $a \cdot b$ ali ab in operaciji rečemo *produkt*. Definiramo tudi $a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_n$, 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 je 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:

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

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, \dots, 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. PRIMERI: Poiščimo vse tabele množenja za grupe majhnih moči.

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

Zadnja tabela skriva v sebi seštevanje po modulu 2.

Tabela 1: Tabela množenja

\cdot	x_1	x_2	x_3	\dots	x_n
x_1	1	x_2	\dots	\dots	x_n
x_2	x_2	x_1^2	\dots	\dots	x_2x_n
\dots	\dots	\dots	\dots	\dots	\dots
x_n	x_n	x_nx_2	\dots	\dots	x_n^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

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

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

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

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: $\exists a \in G : a^2 \neq 1$

Obe tabeli sta \mathbb{Z}_4 .

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

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): $a^2 = b$.

\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 $A \rightarrow A$ grupa za kompozitum. Če je A končna množica, bijektivno preslikavo $A \rightarrow A$ imenujemo **permutacija** množice A . Ko gledamo permutacije, elemente množice A lahko preimenujemo in se lastnosti permutacij ne spremenijo. Zato običajno vzamemo $A = \{1, \dots, n\}$.

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

Permutacijo $\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ običajno zapišemo v obliki: $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$

PRIMER:

- S_3 vsebuje permutacije $id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,

\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

\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)

\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

$$d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

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

PRIMER:

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

Tabela 2: Tabela za množenje za S_3

o	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

$$(a \circ c)(1) = a(c(1)) = a(2) = 3$$

$$(a \circ c)(2) = a(c(2)) = a(3) = 2$$

$$(a \circ c)(3) = 1$$

$$(c \circ a)(1) = c(a(1)) = c(2) = 3$$

$$(c \circ c)(2) = c(c(2)) = c(3) = 1$$

$$(c \circ c)(3) = 2$$

$$(c \circ a)(1) = c(1) = 2$$

$$(c \circ a)(2) = c(3) = 1$$

$$(c \circ a)(3) = c(2) = 3$$

$$d^2 = (c^2)^2 = c^4 = c$$

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

Definicija. Naj bodo $a_1, \dots, a_k \in \{1, \dots, n\}$ paroma različni. Permutacija $\sigma \in S_n$, za katero velja $\sigma(a_i) = a_{i+1}$ za $i = 1, \dots, k-1$, $\sigma(a_k) = a_1$ in $\sigma(a) = a$ za vse $a \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\}$, se imenuje **cikel dolžine k**. Oznaka: $\sigma = (a_1, a_2, \dots, a_k)$. Cikla (a_1, \dots, a_k) in (b_1, \dots, b_k) sta **disjunktivna**, kadar sta množici $\{a_1, \dots, a_k\}$ in $\{b_1, \dots, b_k\}$ disjunktne. Disjunktne 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 disjunktih ciklov. Ti cikli med seboj komutirajo in so do vrstnega reda s permutacijo enolično določeni.

PRIMER:

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

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

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

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

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

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 $\{1, \pi(1), \pi^2(1), \pi^3(1), \dots\}$

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

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

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

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

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

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

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

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

Potem pa tudi $\pi = (a_1, \dots, a_k) \circ \rho$ lahko zapišemo kot produkt disjunktnih ciklov.

Enoličnost: Recimo, da je $\sigma_1 \sigma_2 \dots \sigma_k = \rho_1 \rho_2 \dots \rho_l = \pi$, 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 .

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

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

Trditev. Vsak cikel je produkt transpozicij.

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

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 $\pi = \sigma_1 \sigma_2 \dots \sigma_m$.

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

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

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

je dobro definirana preslikava.

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

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 disjunktne 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 $\tau = (a_1, b_1)$, $\sigma_1 = (a_1, \dots, a_k)$ 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. Naj bo $\pi = \tau_1 \dots \tau_k = \rho_1 \dots \rho_l$, kjer so τ_i in ρ_j transpozicije. Znak permutacije π je po definiciji neodvisen od teh dveh zapisov, odvisen je le od permutacije. Po predprejšnji posledici je $s(\pi) = (-1)^k = (-1)^l \Rightarrow k$ in l sta obe sodi ali obe lihi

□

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

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

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

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

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

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

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

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

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

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

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

3.4 Podgrupe

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

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

Trditev. Naj bo H podgrupa grupe G in e enota grupe 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 podgrupa $(\mathbb{R}, +)$, ta je podgrupa $(\mathbb{C}, +)$
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ je podgrupa $(\mathbb{R} \setminus \{0\}, \cdot)$, $(0, \infty)$ je podgrupa $(\mathbb{R} \setminus \{0\}, \cdot)$
- (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 .

Potem 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 podgrup je podgrupa.

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

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

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

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

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

□

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 $f : G \rightarrow H$ 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

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

$$f(x+y) = n(x+y)$$

$$f(x) + f(y) = nx + ny$$

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

•

$$f : (\mathbb{Z}, +) \rightarrow (\mathbb{Q} \setminus \{0\}, \cdot)$$

$$x \mapsto 2^x$$

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

•

$$f : (\mathbb{R} \setminus \{0\}, \cdot) \rightarrow ((0, \infty), \cdot)$$

$$x \mapsto f|x|$$

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

•

$$s : S_n \rightarrow \{-1, 1\}$$

$$\pi \mapsto s(\pi)$$

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

$$\bullet \text{ } id : G \rightarrow G \text{ je vedno homomorfizem}$$

•

$$f : G \rightarrow H$$

$$x \mapsto e, \forall x \in G$$

$$(\text{kjer je } e \text{ enota grupe } H) \text{ je tudi homomorfizem grup}$$

•

$$f : (\mathbb{R}^2, +) \rightarrow (\mathbb{R}, +)$$

$$(x, y) \mapsto ax + by$$

$$\text{kjer sta } a, b \text{ poljubni konstanti}$$

$$f((x, y) + (z, w)) = f(x + z, y + w)$$

$$= a(x + z) + b(y + w)$$

$$= ax + az + by + bw$$

$$= f((x, y)) + f((z, w))$$

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

Trditev. Naj bo $f : G \rightarrow H$ 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.

$$f(e) = f(e \cdot e) = f(e) \cdot f(e)$$

$$e' = f(e) \cdot f(e)^{-1} = f(e)$$

$$f(e) = e'$$

$$f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$$

$$Z\ leve\ smo\ pomno\tilde{z}ili\ z\ f(a)^{-1} \Rightarrow f(a)^{-1} = f(a^{-1})$$

□

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.

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

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

Če H ni Abelova, to ni res.

PRIMER:

$$f : S_3 \rightarrow S_3$$

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

Trditev.

(a) Kompozitum homomorfizmov grup je homomorfizem grup.

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

Dokaz.

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

Potem je

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

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

Hočemo dokazati, da je $f^{-1} : H \rightarrow G$ 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 $f : G \rightarrow H$ homomorfizem grup. Zalogi vrednosti tega homomorfizma pravimo **slika** homomorfizma f in jo označimo $\text{im } f$. 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 $f : G \rightarrow H$ homomorfizem grup. Potem je $\ker f$ podgrupa grupe G in $\text{im } f$ 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 $f(a) = f(b) = e_H$.

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

Torej je $\ker f$ podgrupa grupe G .

Zaloga vrednosti je vedno neprazna.

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

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

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

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

□

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

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

Dokaz.

(\Rightarrow)

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

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 $f(x) = f(y)$.

$$\begin{aligned} f(x) &= f(y) \quad / \cdot f(y)^{-1} \\ f(xy^{-1}) &= f(x)f(y)^{-1} = 1_H \end{aligned}$$

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

Ker je jedro preslikave 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:

•

$$\begin{aligned} f(\mathbb{R}, +) &\rightarrow ((0, \infty), \cdot) \\ x &\mapsto 2^x \end{aligned}$$

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 $(\mathbb{C} \setminus \{0\}, \cdot)$

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 funkcij $\mathbb{R} \rightarrow \mathbb{R}$ definiramo seštevanje in množenje po točkah:

$$\begin{aligned}(f + g)(x) &= f(x) + g(x), \quad \forall x \in \mathbb{R} \\ (f \cdot g)(x) &= f(x) \cdot g(x), \quad \forall x \in \mathbb{R}\end{aligned}$$

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

$$\begin{aligned}(e \cdot f)(x) &= e(x) \cdot f(x) = 1 \cdot f(x) = f(x) \text{ za vsak } f \in F(\mathbb{R}) \text{ in za vsak } x \in \mathbb{R} \\ \Rightarrow e \cdot f &= f, \text{ enako vidimo, da je } f \cdot e = f, \quad \forall f \in F(\mathbb{R}).\end{aligned}$$

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

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

Množico polinomov z realnimi koeficienti 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 $[a]$. Potem je

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

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 .

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

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 $\text{End}(A)$ množica vseh endomorfizmov grupe A .

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

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

Dokaz.

$a, b \in A$

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

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

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

$$\begin{aligned} 0: A &\rightarrow A \\ a &\mapsto 0 \quad \forall a \end{aligned}$$

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

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

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

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

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

Dokažimo še distributivnost.

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

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

Naj bo $a \in A$ poljuben.

Potem je

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

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

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

□

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

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 ničā.

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

Ekvivalentno: kolobar K je obseg $\Leftrightarrow K \setminus \{0\}$ 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 ničā.

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 $a^{-1} \in K$

$$\begin{aligned} a^{-1} / ab &= 0 \\ b &= a^{-1}ab = 0 \\ &\text{Protislovje} \end{aligned}$$

□

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 sestavljeno: $n = p \cdot q$, $1 < p, q < n$.

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

\mathbb{Z}_n ima torej delitelje nič, 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

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

Nobeno od števil $a, 2a, \dots, (n-1)a$ 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 $l-k \in \{1, \dots, n-1\}$.

To nas dovede do protislovja.

Torej so ostanki $[a], [2a], \dots, [(n-1)a]$ 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

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

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

, ki ustreza naslednjim pogojem:

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

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

4.1 Baza in razsežnost

Definicija. Naj bo V vektorski prostor nad obsegom \mathcal{O} in $M \subseteq V$ poljubna množica. Pravimo, da je M **ogrodje** prostora V , kadar je $\text{Lin}(M) = V$. Pravimo tudi, da M **generira** V in elementom M pravimo **generatorji**.²³

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

Če je $M = \emptyset$ je $\text{Lin}M = \{0\}$.

PRIMERI:

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

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

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

Potem je $x = x_1 e_1 + x_2 e_2 + \dots + x_n e_n$.

²³Ogrodje prostora V je torej taka množica M , da vsak vektor iz V lahko izrazimo kot končno linearno kombinacijo elementov iz M .

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

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

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

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

PRIMERI:

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

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

Trditev. Naj bo M ogrodje vektorskega prostora V in $v \in M$ tak vektor, ki **pripada** $\text{Lin}(M \setminus \{v\})$.²⁴ Potem je $M \setminus \{v\}$ tudi ogrodje prostora V .

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

Potem, ker je M ogrodje za V , obstajajo $\alpha_1, \dots, \alpha_n \in \mathcal{O}$ in $u_1, \dots, u_n \in M$, da je $x = \alpha_1 u_1 + \dots + \alpha_n u_n$.

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

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

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

Ker je $v \in \text{Lin}(M \setminus \{v\})$, obstajajo $v_1, \dots, v_m \in M \setminus \{v\}$ in $\beta_1, \dots, \beta_m \in \mathcal{O}$, da je $v = \beta_1 v_1 + \dots + \beta_m v_m$

²⁴ v lahko izrazimo kot linearno kombinacijo ostalih vektorjev iz M

Potem je $x = {}^{25} \alpha_1 \beta_1 v_1 + \dots + \alpha_1 \beta_m v_m + {}^{26} \alpha_2 u_2 + \dots + \alpha_n u_n \in \text{Lin}(M \setminus \{v\})$.

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

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

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 $\alpha_1 = \dots = \alpha_n = 0$ sledi $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$.

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

PRIMER:

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

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

$$(\alpha_1 e_1 + \dots + \alpha_n e_n = \alpha_1, \alpha_2, \dots, \alpha_n)$$

- 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 $v_1, \dots, v_n \in V$ so linearno odvisni natanko takrat, ko enega od njih lahko izrazimo kot linearno kombinacijo prejšnjih.

Dokaz.

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

Potem obstajajo $\alpha_1, \dots, \alpha_n \in \mathcal{O}$, ne vsi 0, da je $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$.

²⁵ $\in \text{Lin}(M \setminus \{v\})$

²⁶ $\in \text{Lin}(M \setminus \{v\})$

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

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

$$\begin{aligned}\alpha_1 v_1 + \dots + \alpha_{k-1} v_{k-1} &= -\alpha_k v_k / : (-\alpha_k)^{-1} \\ v_k &= -\alpha_1 \alpha_k^{-1} v_1 - \dots - \alpha_{k-1} \alpha_k^{-1} v_{k-1}\end{aligned}$$

(\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 $\alpha_k \in \mathcal{O}$.

Potem je $\alpha_1 v_1 + \dots + \alpha_{j-1} v_{j-1} + (-1)v_j + \alpha_{j+1} v_{j+1} + \dots + \alpha_n v_n = 0 \Rightarrow$ Vektorji v_1, \dots, 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 $\{e_1, \dots, e_n\}$ ($e_j = (0, \dots, 0, 1, 0, \dots, 0)$) je baza prostora \mathcal{O}^n . Pravimo ji **standardna baza** prostora \mathcal{O}^n
- $\{1, x, x^2, \dots\}$ je (neskončna) baza prostora $\mathbb{R}[X]$.

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

Dokaz.

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

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

Dokazati je treba še enoličnost tega zapisa.

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

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

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

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

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

Potem takoj sledi, da je B ogrodje.

Dokažimo še linearno neodvisnost.

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

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

Torej so v_1, \dots, v_n linearno neodvisni.

□

Izrek. Vsak netrivialen končnorazsežen vektorski prostor ima bazo. Izberemo jo lahko iz poljubnega končnega ogrodja.²⁷

Dokaz. Naj bo $\{v_1, \dots, v_n\}$ 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 $\{u_1, \dots, u_m\}$. Ker se je postopek končal, noben vektor u_j ni linearna kombinacija prejšnjih. To pa pomeni, da so vektorji u_1, \dots, u_m linearno neodvisni in torej tvorijo bazo.

□

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

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

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

²⁷Tudi neskončnorazsežni vektorski prostori imajo bazo, kar lahko dokažemo z Zornovo lemo.

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 $\{u_1, v_1, \dots, v'_{m-1}\}$. To je ogrodje, zato je $u_2 \in \text{Lin}\{u_1, v_1, \dots, v_{m-1}\}$ in zato je množica $\{u_1, u_2, v'_1, \dots, v_{m-1}\}$ 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 $\{u_1, u_2, u''_1, \dots, u_{m-?}^{28''}\}$. To ponavljamo.

Recimo, da je $n > m$.

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

Ker je $n > m$ obstaja $u_{?}^{29}$ in ker je $\{u_1, \dots, u_m\}$ ogrodje, je $u_{?}$ linearna kombinacija vektorjev u_1, \dots, u_m .

To je v protislovju z linearno neodvisnostjo vektorjev u_1, \dots, 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: $\dim V$.

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

Dokaz. Naj bodo v_1, \dots, v_n linearno neodvisni vektorji in $B = \{u_1, \dots, u_m\}$ 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 $B' = \{v_1, \dots, v_n, u'_1, \dots, u'_{m-n}\}$.

²⁸dopiši

²⁹dopiši

Iz tega ogrodja lahko izberemo bazo.

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

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

Dokaz.

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

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

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

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

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

$$\dim W = m$$

$$\dim V = m + n$$

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

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

□

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

Dokaz. Na vajah.³⁰

□

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

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

□

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

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

Če je $W = V$, vzamemo $U = \{0\}$.

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

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

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

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

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

³⁰dopiši

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

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

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

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

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

- Če je \mathcal{A} injektivna, je slika vsake linearno neodvisne množice linearno neodvisna.
- Če je \mathcal{A} surjektivna, je slika vsakega ogrodka za U ogrodka za V .
- Če je \mathcal{A} bijektivna, je slika vsake baze prostora U baza prostora V .

1)

Dokaz. Naj bodo $u_1, \dots, u_n \in U$ linearno neodvisni in $\mathcal{A} : U \rightarrow V$ injektivna.

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

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

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

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

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

2)

Dokaz. Predpostavimo, da je $\{u_1, \dots, u_n\}$ ogrodka prostora U .

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

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

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

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

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

□

□

3)

Dokaz. Sledi iz 1) in 2)

Izrek.

- (1) Naj bo V n -razsežen vektorski prostor nad obsegom \mathcal{O} ($n > 0$). Potem je V izomorfizem \mathcal{O}^n
- (2) Končnorazsežna vektorska prostora nad istim obsegom sta izomorfna natanko takrat, ko imata isto razsežnost.

Dokaz.

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

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

Dokazati moramo, da je ϕ linearna in bijektivna.

Linearnost:

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

Potem je

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

Injektivnost:

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

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

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

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

Surjektivnost:

- Naj bo $x \in V$.

Potem je $x = \alpha_1 v_1 + \dots + \alpha_n v_n$ za neke $\alpha_1, \dots, \alpha_n \in \mathcal{O} \Rightarrow x = \phi(\alpha_1, \dots, \alpha_n) \in \text{im}\phi$.

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

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

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

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

(\Rightarrow) Naj bosta U in V izomorfna in $A : U \rightarrow V$ 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 \mathcal{O} in $\mathcal{A} : U \rightarrow V$ linearna preslikava. Potem je $\dim(\ker \mathcal{A}) + \dim(\text{im} \mathcal{A}) = \dim U$.

Dokaz. Naj bo $\{v_1, \dots, v_n\}$ baza prostora $\text{im} \mathcal{A}$.

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

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

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

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

B je linearno neodvisna

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

Potem je

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

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

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

B je ogrodje

Naj bo $x \in U$ poljuben.

Potem je $Ax \in \operatorname{im} \mathcal{A}$, zato je $\mathcal{A}x = \alpha_1 v_1 + \dots + \alpha_n v_n$.

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

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

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

□

4.2 Vektorski podprostor

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

- $x, y \in U \Rightarrow x + y \in U$ ³¹
- $x \in U \Rightarrow \alpha x \in U, \forall \alpha \in \mathcal{O}$
- $(U, +)$ je podgrupa grupe $(V, +)$.

³¹Zaprto za operacijo.

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

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

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

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

4.3 Linearne preslikave

Definicija. Naj bosta U in V vektorska prostora nad istim obsegom \mathcal{O} . Preslikava $\mathcal{A} : U \rightarrow V$ je linearna preslikava ali homomorfizem vektorskih prostorov, kadar velja:

- aditivnost

$$\mathcal{A}(x + y) = \mathcal{A}(x) + \mathcal{A}(y) \text{ za vsaka } x, y \in U$$

- homogenost

$$\mathcal{A}(\alpha x) = \alpha \mathcal{A}(x) \text{ za vsak } x \in U, \alpha \in \mathcal{O}$$

Kadar je $\mathcal{A} : U \rightarrow V$ linearna preslikava, običajno namesto $\mathcal{A}(x)$ pišemo Ax .

Z $\mathcal{L}(U, V)$ označujemo množico vseh linearnih preslikav iz $U \rightarrow V$. Z $\mathcal{L}(V)$ pa označujemo množico vseh endomorfizmov prostora V .

Linearni preslikavi $\mathcal{A} : V \rightarrow \mathcal{O}$, kjer je V vektorski prostor nad \mathcal{O} , pravimo **linearen funkcional**.

Množico vseh linearnih funkcionalov na vektorskem prostoru V ponavadi označujemo z V^* .³²

PRIMERI:

1. $id_V : V \rightarrow V$ je vedno linearna preslikava.
2. Ničelna preslikava je preslikava, ki vse preslika v 0. Tudi ta je linearna. Običajno jo označimo z $0 : U \rightarrow V$.

$$0x = 0^{33} \text{ za vsak } x \in U$$

3. Odvajanje je linearna preslikava.

$$D : \mathbb{R}[x] \rightarrow \mathbb{R}[x]$$

$$D(f) = f'$$

³²Ali tudi z V' .

³³Ničla v vektorskem prostoru V .

4. Preslikava

$$C : [0, 1] \rightarrow \mathbb{R}$$

$$C : f \rightarrow \int_0^1 f(x)dx$$

je linearna preslikava.

5. Naj bo $M \neq 0$ poljubna množica in \mathcal{F} vektorski prostor vseh funkcij $M \rightarrow \mathbb{R}$, z operacijama definiranimi po točkah.

Naj bo $a \in M$ poljuben element. Definiramo

$$F : \mathcal{F} \rightarrow \mathbb{R}$$

$$F(f) = f(a)$$

$$F(f + g) = (f + g)(a) = f(a) + g(a) = F(f) + F(g)$$

$$F(\alpha f) = (\alpha f)(a) = \alpha(f(a)) = \alpha F(f)$$

je linearna preslikava.

6. Naj bo V vektorski prostor nad \mathcal{O} in v_1, \dots, v_n poljubni vektorji.

$$F : \mathcal{O} \rightarrow V$$

$$F(\alpha_1, \dots, \alpha_n) = \alpha v_1 + \dots + \alpha_n v_n$$

Trditev. Preslikava $\mathcal{A} : V \rightarrow U$ je linearna natanko takrat, ko za vsak $n \geq 1$, vsak $x_1, \dots, x_n \in V$ in vsake $\alpha_1, \dots, \alpha_n \in \mathcal{O}$ velja $\mathcal{A}(\sum_{k=1}^n \alpha_k x_k) = \sum_{k=1}^n \alpha_k \mathcal{A}(x_k)$.

Dokaz.

\Leftarrow aditivnost $n = 2, \alpha_1 = \alpha_2 = 1, \mathcal{A}(x_1 + x_2) = \mathcal{A}(x_1) + \mathcal{A}(x_2)$

homogenost $n = 1 : \mathcal{A}(\alpha_1 x_1) = \alpha_1 \mathcal{A}(x_1)$

\Rightarrow Dokažemo z indukcijo na n P_n $n = 1$ je to definicija homogenosti.

$$n \rightarrow n + 1 :$$

$$\mathcal{A}\left(\sum_{k=1}^{n+1} \alpha_k x_k\right) =$$

$$= \mathcal{A}\left(\sum_{k=1}^n \alpha_k x_k\right) + \mathcal{A}(\alpha_{n+1} x_{n+1})$$

$$= \sum_{k=1}^n \alpha_k \mathcal{A}(x_k) + \alpha_{n+1} \mathcal{A}(x_{n+1})$$

□

Posledica. Preslikava $\mathcal{A} : V \rightarrow U$ je linearna natanko takrat, ko za vse $x, y \in V$ in vse $\alpha, \beta \in \mathcal{O}$ velja $\mathcal{A}(\alpha x + \beta y) = \alpha \mathcal{A}(x) + \beta \mathcal{A}(y)$.

Dokaz.

\Rightarrow Smo že dokazali v trditvi zgoraj.

$\Leftarrow \alpha = \beta = 1 \Rightarrow$ aditivnost

α poljuben, $\beta = 0 \Rightarrow$ homogenost. □

Definicija. Naj bo $\mathcal{A} : V \rightarrow U$ linearna preslikava. Zalogo vrednosti imenujemo **slika preslikave** \mathcal{A} in jo označimo z $\text{im}\mathcal{A}$, množico $\{x \in V; \mathcal{A}x = 0\}$ pa imenujemo **jedro preslikave** \mathcal{A} in ga označimo s $\ker\mathcal{A}$.

Trditev. Naj bo $\mathcal{A} : V \rightarrow U$ linearna preslikava. Potem je $\ker\mathcal{A}$ vektorski podprostor prostora V , $\text{im}\mathcal{A}$ pa vektorski podprostor prostora U .

Dokaz. Ker je linearna preslikava v posebnem primeru homomorfizem Abelovih grup, že vemo, da sta jedro in slika podgrupi. Dokazati moramo le zaprtost za množenje s skalarji.

Naj bo $x \in \ker\mathcal{A}$ in $\alpha \in \mathcal{O}$.

$$\Rightarrow \mathcal{A}x = 0 \Rightarrow \alpha \mathcal{A}x = 0$$

$$\alpha x \in \ker\mathcal{A}$$

Naj bo še $x \in \text{im}\mathcal{A}$ in $\alpha \in \mathcal{O}$. Potem obstaja $y \in V$, da je $x = \mathcal{A}y$.

$$\alpha x = \alpha \mathcal{A}y = \mathcal{A}(\alpha y) \in \text{im}\mathcal{A}$$

□

Ker je linearna preslikava homomorfizem Abelovih grup, velja

Trditev. Linearna preslikava $\mathcal{A} : V \rightarrow U$ je injektivna natanko takrat, ko je $\ker\mathcal{A} = \{0\}$.

Na množici $\mathcal{L}(V, U)$ vseh linearnih preslikav iz V v U definiramo seštevanje in množenje s skalarji po točkah.

$$(\mathcal{A} + \mathcal{B})(x) = \mathcal{A}x + \mathcal{B}x \text{ za } \forall x \in V$$

$$(\alpha \mathcal{A})(x) = \alpha \mathcal{A}x \text{ za vsak } x \in V$$

Trditev. Če sta $\mathcal{A}, \mathcal{B} : V \rightarrow U$ linearni preslikavi in $\alpha \in \mathcal{O}$ sta $\mathcal{A} + \mathcal{B}$, $\alpha \mathcal{A} : V \rightarrow U$ tudi linearni preslikavi.

Dokaz. Jasno je, da $\mathcal{A} + \mathcal{B}$ in $\alpha \mathcal{A}$ slikata iz V v U . Dokažimo, da sta linearni. Naj bosta $x, y \in V$ poljubna in $\beta, \gamma \in \mathcal{O}$ poljubna. Potem je

$$\begin{aligned} (\mathcal{A} + \mathcal{B})(\beta x + \gamma y) &= \\ &= \mathcal{A}(\beta x + \gamma y) + \mathcal{B}(\beta x + \gamma y) \\ &= \beta \mathcal{A}x + \gamma \mathcal{A}y + \beta \mathcal{B}x + \gamma \mathcal{B}y \\ &= \beta(\mathcal{A} + \mathcal{B})(x) + \gamma(\mathcal{A} + \mathcal{B})(y) \\ &\Rightarrow \mathcal{A} + \mathcal{B} \text{ je linearna.} \end{aligned}$$

$$\begin{aligned}
(\alpha\mathcal{A})(\beta x + \gamma y) &= \\
&= \alpha\mathcal{A}(\beta x + \gamma y) \\
&= \alpha(\beta\mathcal{A}x + \gamma\mathcal{A}y) \\
&= \alpha\beta\mathcal{A}x + \alpha\gamma\mathcal{A}y \\
&= \beta\alpha\mathcal{A}x + \gamma\alpha\mathcal{A}y \\
&= \beta(\alpha\mathcal{A})(x) + \gamma(\alpha\mathcal{A})(y) \\
&\Rightarrow \alpha\mathcal{A} \text{ je linearna.}
\end{aligned}$$

□

Trditev. Množica linearnih preslikav $\mathcal{L}(V, U)$ je vektorski prostor.

Dokaz. Po prejšnji trditvi je seštevanje notranja binarna operacija na $\mathcal{L}(V, U)$, množenje s skalarjem pa zunanja operacija $\mathcal{O} \times \mathcal{L}(V, U) \rightarrow \mathcal{L}(V, U)$.

Vemo že, da je seštevanje homomorfizem Abelovih grup. Je komutativno in asociativno.

Enota za seštevanje je ničelna preslikava, ki je res linearna.

Inverz preslikave \mathcal{A} za seštevanje pa je preslikava $\mathcal{A} : V \rightarrow U$, definirana s predpisom $(-\mathcal{A})(x) = -(\mathcal{A}(x))$ za vsak $x \in V$. Tudi ta preslikava je linearna.

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

Preverimo še ostale lastnosti:

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

$$\begin{aligned}
(\alpha(\mathcal{A} + \mathcal{B}))(x) &= \\
&= \alpha((\mathcal{A} + \mathcal{B})x) \\
&= \alpha(\mathcal{A}x + \mathcal{B}x) \\
&= \alpha\mathcal{A}x + \alpha\mathcal{B}x \\
&= (\alpha\mathcal{A})x + (\alpha\mathcal{B})x \\
&= (\alpha\mathcal{A} + \alpha\mathcal{B})(x) \text{ za } \forall x \in V
\end{aligned}$$

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

$$\begin{aligned} ((\alpha + \beta)\mathcal{A})x &= \\ &= (\alpha + \beta)\mathcal{A}x \\ &= \alpha\mathcal{A}x + \beta\mathcal{A}x \\ &= (\alpha\mathcal{A})x + (\beta\mathcal{A})x \\ &= (\alpha\mathcal{A} + \beta\mathcal{A})x \text{ za } \forall x \in V \end{aligned}$$

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

$$\begin{aligned} (\alpha(\beta\mathcal{A}))(x) &= \\ &= \alpha((\beta\mathcal{A})x) \\ &= \alpha(\beta\mathcal{A}x) \\ &= (\alpha\beta)\mathcal{A}x \\ &= ((\alpha\beta)\mathcal{A})x \text{ za } \forall x \in V \end{aligned}$$

$$\underline{1 \cdot \mathcal{A} = \mathcal{A}}$$

$$\begin{aligned} (1 \cdot \mathcal{A})(x) &= \\ &= 1 \cdot \mathcal{A}x \\ &= \mathcal{A}x \text{ za } \forall x \in V \end{aligned}$$

□

Trditev.

1. Kompozitum linearnih preslikav je linearna preslikava.
2. Inverz bijektivne linearne preslikave je linearna³⁴ preslikava.

Dokaz. Vemo že, da sta kompozitum in inverz homomorfizma grup. Dokazati moramo še homogenost.

Naj bo $\mathcal{A} : V \rightarrow U, \mathcal{B} : U \rightarrow W$.

$\mathcal{B} \circ \mathcal{A} : V \rightarrow W$ je homogena

$x \in V, \alpha \in \mathcal{O}$

$$\begin{aligned} (\mathcal{B} \circ \mathcal{A})(\alpha x) &= \\ &= \mathcal{B}(\mathcal{A}(\alpha x)) \\ &= \mathcal{B}(\alpha\mathcal{A}x) \\ &= \alpha\mathcal{B}(\mathcal{A}x) \\ &= \alpha(\mathcal{B} \circ \mathcal{A})x \end{aligned}$$

³⁴Preslikava je tudi bijektivna.

Recimo, da je \mathcal{A} bijektivna preslikava. Dokažimo, da je $\mathcal{A}^{-1} : U \rightarrow V$ homogena za $x \in U, \alpha \in \mathcal{O}$. Ker je \mathcal{A} bijektivna, obstaja enoličen $y \in V$, da je $x = \Delta y$.

$$y = \Delta^{-1}x$$

$$\begin{aligned} \Delta(\alpha x) &= \alpha \Delta x = \alpha x & / \mathcal{A}^{-1} \\ \alpha \mathcal{A}^{-1}x &= \alpha y = \mathcal{A}^{-1}(\mathcal{A}(\alpha y)) = \mathcal{A}^{-1}(\alpha x) \end{aligned}$$

□

Definicija. Bijektivna linearna preslikava se imenuje **izomorfizem vektorskih prostorov**.

Vektorska prostora sta izomorfna, če med njima obstaja izomorfizem.

Iz trditve sledi, da je inverz izomorfizma tudi izomorfizem.

Tudi kompozitum izomorfizmov je izomorfizem, zato je izomorfnost vektorskih prostorov ekvivalenčna relacija.

Posledica. Množica $\mathcal{L}(V)$ vseh endomorfizmov prostora V je kolobar za operaciji $+$ in \circ .

Dokaz. Po trditvi je kompozitum endomorfizmov spet endomorfizem. Vemo, da asociativnost in distributivnost veljata, saj veljata že v kolobarjih endomorfizmov poljubne Abelove grupe. Ta kolobar $(\mathcal{L}(V), +, \circ)$ ima enoto id_V , ki je res linearna preslikava. □

PRIMER:

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

$F : V \rightarrow V$ odvajanje

$$p(x) \mapsto p'(x)$$

$G : V \rightarrow V$ množenje z X

$$p(x) \mapsto X \cdot p(x)$$

To sta linearni preslikavi.

$$\begin{aligned} (F \circ G)(p(x)) &= F(G(p(x))) = F(X \cdot p(x)) = (X \cdot p(x))' = p(x) + X \cdot p'(x) \\ (G \circ F)(p(x)) &= G(F(p(x))) = G(p'(x)) = X \cdot p'(x) \end{aligned}$$

$\Rightarrow \mathcal{L}(V)$ je v splošnem nekomutativen kolobar.

Definicija. Množica \mathcal{A} skupaj s seštevanjem, množenjem in množenjem s skalarji iz obsega \mathcal{O} je **algebra nad \mathcal{O}** , kadar velja:

- \mathcal{A} je vektorski prostor nad \mathcal{O}

- $(\mathcal{A}, +, \cdot)$ je kolobar
- $(\alpha a)b = a(\alpha b) = \alpha(ab)$ za vsak $\alpha \in \mathcal{O}$ in vsaka $a, b \in \mathcal{A}$

Algebra \mathcal{A} je **komutativna**, kadar je množenje komutativno:

$$ab = ba \quad \forall a, b \in \mathcal{A}$$

Algebra \mathcal{A} ima **enoto**, kadar ima kolobar $(\mathcal{A}, +, \cdot)$ enoto:

$$\exists 1 \in \mathcal{A}. \quad a \cdot 1 = 1 \cdot a = a \quad \forall a \in \mathcal{A}$$

PRIMERI:

1. \mathcal{O} je vedno komutativna algebra nad \mathcal{O} .
2. \mathcal{O}^n je komutativna algebra nad \mathcal{O} , če množenje definiramo po komponentah:

$$(x_1, x_2, \dots, x_n)(y_1, y_2, \dots, y_n) = (x_1 y_1, x_2 y_2, \dots, x_n y_n)$$

Ta algebra ima enoto $(1, \dots, 1)$.

3. Naj bo $M \neq \emptyset$ poljubna množica in \mathcal{F} množica vseh funkcij $M \rightarrow \mathcal{O}$. Na \mathcal{F} vse operacije definiramo po točkah.

$$\begin{aligned} (f + g)(a) &:= f(a) + g(a) \\ (fg)(a) &:= f(a)g(a) \\ (\alpha f)(a) &:= \alpha f(a) \quad \forall a \in M \end{aligned}$$

Potem je \mathcal{F} komutativna algebra nad \mathcal{O} .

Preslikava, ki vse slika v 1, je enota te algebre.

4. $\mathcal{L}(V)$ je algebra nad \mathcal{O}
Vemo že, da je $\mathcal{L}(V)$ vektorski prostor nad \mathcal{O} in kolobar

$$(\alpha \mathcal{A}) \circ \mathcal{B} = \mathcal{A} \circ (\alpha \mathcal{B}) = \alpha(\mathcal{A} \circ \mathcal{B}) \quad \forall \alpha \in \mathcal{O}, \forall \mathcal{A}, \mathcal{B} \in \mathcal{L}(V)$$

Naj bo $x \in V$ poljuben. Potem je

$$\begin{aligned} ((\alpha \mathcal{A}) \circ \mathcal{B})(x) &= (\alpha \mathcal{A}) \circ (\mathcal{B}x) = \alpha \mathcal{A}(\mathcal{B}(x)) \\ (\mathcal{A} \circ \alpha \mathcal{B})(x) &= \mathcal{A} \circ ((\alpha \mathcal{B})x) = \mathcal{A}(\alpha \mathcal{B}x) = \alpha \mathcal{A}(\mathcal{B}(x)) \\ (\alpha(\mathcal{A} \circ \mathcal{B}))(x) &= \alpha(\mathcal{A} \circ \mathcal{B})x = \alpha(\mathcal{A}(\mathcal{B}(x))) \end{aligned}$$

V splošnem je nekomutativna algebra z enoto id .

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 $A \rightarrow B$. 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: $(xRy \wedge yRx) \Rightarrow x = y$.

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

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 $|M| \geq 2, \exists b \in M \setminus \{a\}$. $X = \{a\} \not\subseteq \{b\}$. Torej X ni najmanjši element.

5.3 Ponovitev ekvivalenčne relacije

Relacija R na A je **ekvivalenčna relacija**, kadar je **refleksivna**, **simetrična** in **transitivna**. 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 ekvivalenčna 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 disjunktne ekvivalenčnih razreda, ki so neprazni. Pri tem sta dva elementa množice A ekvivalentna natanko takrat, ko ležita v istem ekvivalenčnem razredu.*

Dokaz. *LMN*

□

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

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

Dokaz. (\Rightarrow) *LMN*

$(\Leftarrow) x \sim y \Leftrightarrow \exists i : x, y \in A_i$

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 $q : A \rightarrow A/\sim$, definirana s predpisom $q(a) = [a]$, pa se imenuje **kanonična kvocientna preslikava**.*

PRIMERI:

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

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

Simetričnost je tudi očitna.

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

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

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

$$(\mathbb{Z} \times \mathbb{N}) / \sim = \mathbb{Q}$$

$$[(m, n)] \mapsto \frac{m}{n}$$

- Dve usmerjeni daljici v prostoru sta v relaciji \sim , kadar sta vzporedni, enako dolgi in kažeta v isto smer. To je ekvivalenčna relacija na množici vseh usmerjenih daljic v prostoru. Kvocientna množica je množica vektorjev.³⁵
- Naj bo $n \in \mathbb{N}$. Na \mathbb{Z} definiramo relacijo \equiv s predpisom $a \equiv b$ (a je kongruentno b po modulu n) $\Rightarrow n | a - b$.

To je ekvivalenčna relacija.

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

To je množica ostankov pri deljenju z n .

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

Izrek. Naj bo $f : A \rightarrow B$ 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

³⁵Spomnimo se natančne definicije vektorja.

(2) Obstaja natanko ena (dobro definirana) preslikava $p : A/\sim \rightarrow B$, da diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow g & \nearrow p & \\ A/\sim & & \end{array}$$

komutira. Definirana je s predpisom $p([a]) = f(a)$.

(3) p je injektivna in velja $Z_p = Z_f$.³⁶

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

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

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

$$\begin{aligned} (mn' = m'n) / \cdot qq' &\rightarrow mn'qq' = m'nqq', \\ (pq' = p'q) / \cdot nn' &\rightarrow pq'nn' = p'qnn' \end{aligned}$$

³⁶Dokaz: LMN - kanonični razcep preslikave

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

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

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

$$\Leftrightarrow mqn'q' + npn'q' = nqm'q' + nqn'p' \rightarrow \text{Drži}$$

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

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

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

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 ekvivalenčno relacijo \sim s predpisom $a \sim b \Leftrightarrow a - b \in H$. Potem velja:

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

$$\begin{aligned} g : G &\rightarrow G/H \\ a &\mapsto [a] = a + H \end{aligned}$$

je homomorfizem grup.

Dokaz.

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

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

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

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 . $a \sim b \Leftrightarrow ab^{-1} \in H$.

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

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

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

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

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 $G/G = \{0\}$.
- $G = \mathbb{Z}$, $n \in \mathbb{N}$, $H = n \cdot \mathbb{Z} = \{nm; m \in \mathbb{Z}\}$.

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

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

$$\text{Seštevanje: } [a] + [b] = [a + b]$$

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

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

To **ne** sledi iz dejstva, da je G kolobar (čeprav je to res) in da je H njegov 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 $b \in \mathbb{Q}$.

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

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

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

Spomnimo se: Če je $f : A \rightarrow B$ preslikava, je na A s predpisom $a \sim b \Leftrightarrow f(a) = f(b)$ definirana ekvivalenčna relacija in obstaja natanko ena preslikava $p : A/\sim \rightarrow B$, da diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow g & \nearrow p & \\ A/\sim & & \end{array}$$

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 $f : A \rightarrow B$ 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 $f : G \rightarrow H$ homomorfizem grup. Potem velja:

1. Obstaja **natanko en** homomorfizem grup $p : G/\ker f \rightarrow H$, da diagram

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \downarrow q & \nearrow p & \\ G/\ker f & & \end{array}$$

komutira. Definirana je s predpisom $p([a]) = f(a)$.

2. p je injektiven in velja $\text{im } p = \text{im } f$. V posebnem primeru je $G/\ker f \cong \text{im } f$.

Opomba: Izrek velja tudi, če G in H nista Abelovi (algebra 2).

Dokaz. Dokazati je treba le, da je p homomorfizem grup (ostalo že vemo).

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

□

5.6 Kvocientni vektorski prostori

Naj bo V vektorski prostor nad obsegom \mathcal{O} in W njegov podprostor. Vemo že, da je V/W Abelova grupa za seštevanje $[x] + [y] = [x + y]$. Na V/W bi radi definirali še množenje s skalarjem.³⁷

Trditev. *Množenje s skalarjem na V je usklajeno z ekvivalenčno relacijo \sim . Če je $x \sim y$ in $y \in \mathcal{O}$, potem je $\alpha x \sim \alpha y$.*

Dokaz. $x \sim y \Rightarrow x - y \in W \Rightarrow \alpha(x - y) = \alpha x - \alpha y \in W \Rightarrow \alpha x \sim \alpha y$

□

Definicija. Na V/W definiramo množenje s skalarjem s predpisom $\alpha \cdot [x] = [\alpha x]$. Zaradi usklajenosti je operacija dobro definirana.³⁸

Posledica. V/W je vektorski prostor nad \mathcal{O} . Pravimo mu **kvocientni** ali **faktorski vektorski prostor** prostora V po podprostoru W .

Dokaz. Vemo že, da je $(V/W, +)$ Abelova grupa in da je množenje s skalarjem dobro definirano.

Ostale lastnosti se prenesejo z V :

- $\alpha([x] + [y]) = \alpha[x + y] = [\alpha x + \alpha y] = [\alpha x] + [\alpha y] = \alpha[x] + \alpha[y]$
- $(\alpha + \beta)[x] = [(\alpha + \beta)x] = [\alpha x + \beta x] = [\alpha x] + [\beta x] = \alpha[x] + \beta[x]$
- $\alpha(\beta[x]) = \alpha[\beta x] = [\alpha(\beta x)] = (\alpha\beta)[x]$
- $1 \cdot [x] = [1 \cdot x] = [x]$

□

Kaj je ekvivalenčni razred $[x]$?

$$\begin{aligned} [x] &= \{y \in V; y \sim x\} = \{y \in V; y - x \in W\} = \{z + w; z \in W\} \\ &\quad z = y - x \\ &\quad y = z + x \end{aligned}$$

Ekvivalenčni razred $[x]$ je vektorski prostor W , ki ga premaknemo za vektor x . Tako množico imenujemo **afin podprostor** prostora V in jo označimo $X + W$.

³⁷Spomnimo se: $x \sim y \Leftrightarrow x - y \in W$.

³⁸Če je $[x] = [y]$ in $\alpha \in \mathcal{O}$, je $x \sim y$ in zaradi usklajenosti $\alpha x \sim \alpha y \Rightarrow [\alpha x] = [\alpha y]$.

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 $q : V \rightarrow V/W$ 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 definicije seštevanja.

Tretja enakost velja zaradi definicije množenja s skalarjem.

□

Izrek. Naj bo $\mathcal{A} : V \rightarrow W$ linearna preslikava.

Potem velja:

1. Obstaja natanko ena linearna preslikava $\hat{\mathcal{A}} : V/\ker \mathcal{A} \rightarrow W$, da diagram

$$\begin{array}{ccc} V & \xrightarrow{\mathcal{A}} & W \\ \downarrow q & \nearrow \hat{\mathcal{A}} & \\ V/\ker \mathcal{A} & & \end{array}$$

komutira.

Definirana je s predpisom $\hat{\mathcal{A}}([x]) = \mathcal{A}x$.

2. $\hat{\mathcal{A}}$ je injektivna in velja $\operatorname{im} \hat{\mathcal{A}} = \operatorname{im} \mathcal{A}$.

3. $V/\ker \mathcal{A} \equiv \operatorname{im} \mathcal{A}$

Dokaz. Dokazati moramo le homogenost preslikave $\hat{\mathcal{A}}$, vse ostalo že vemo.

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

Tretja enakost velja zaradi tega, ker je \mathcal{A} linearna.

□

Posledica. Če je V končnorazsežen vektorski prostor in $\mathcal{A} : V \rightarrow W$ linearna preslikava, je $\dim(V/\ker \mathcal{A}) = \dim V - \dim(\ker \mathcal{A})$.

Dokaz. $\dim(V/\ker \mathcal{A}) = \dim(\operatorname{im} \mathcal{A}) = \dim V - \dim(\ker \mathcal{A})$

□

Trditev. Če je $V = W \oplus U$, potem je $V/W \equiv U$ in $V/U \equiv W$.

Dokaz. Zaradi simetrije je dovolj dokazati $V/W \equiv U$.

Konstruirali bomo surjektivno linearno preslikavo $V \rightarrow U$, katero jedro bo W .

Potem bo po izreku V/W izomorfen U .

$$\begin{array}{ccc} V & \xrightarrow{\mathcal{A}} & W \\ \downarrow & \nearrow \hat{\mathcal{A}} & \\ V/\ker \mathcal{A} & & \end{array}$$

Projektor $\mathcal{P} : V \rightarrow U$ definiran s predpisom $\mathcal{P}(w + u) = u$ ($w \in W$ in $u \in U$).

Po predpostavki je $V = W \oplus U$, zato se vsak element prostora V na enoličen način zapiše kot $w + u$, kjer je $w \in W$ in $u \in U$.

Torej je preslikava \mathcal{P} dobro definirana.

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

Dokažemo linearnost:

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

Izračunajmo še jedro:

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

\mathcal{P} je torej preslikava, ki jo iščemo.

□

Posledica. Če je V končnorazsežen vektorski prostor nad obsegom \mathcal{O} in W njegov podprostor, potem je tudi V/W končnorazsežen in velja $\dim V/W = \dim V - \dim W$.

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

Zato je $V/W \cong U \Rightarrow \dim(V/W) = \dim U$

Vemo pa, da je

$$\begin{aligned}\dim V &= \dim W + \dim U \\ &= \dim W + \dim(V/W) \\ &\Rightarrow \dim(V/W) \\ &= \dim V - \dim W.\end{aligned}$$

□

6 LINEARNE PRESLIKAVE IN MATRIKE

Trditev. Naj bo $\{v_1, \dots, v_n\}$ baza prostora V in $\mathcal{A} : V \rightarrow W$ linearna preslikava. Če poznamo $\mathcal{A}v_1, \dots, \mathcal{A}v_n$, potem lahko enolično izračunamo $\mathcal{A}x$ za poljuben $x \in V$.

39

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

$$\mathcal{A}x = \mathcal{A}(\alpha_1 v_1 + \dots + \alpha_n v_n) = \alpha_1 \mathcal{A}v_1 + \dots + \alpha_n \mathcal{A}v_n$$

Druga enakost velja zaradi linearnosti.

□

Naj bosta V in W vektorska prostora nad \mathcal{O} z bazama $B_V = \{v_1, \dots, v_n\}$ in $B_W = \{w_1, \dots, w_m\}$ in naj bo $\mathcal{A} : V \rightarrow W$ linearna preslikava.

$\mathcal{A}v_i \in W$ za $\forall i = 1, \dots, n$.

Ker je B_W baza za W , lahko vsak vektor $\mathcal{A}v_i$ razvijemo po tej bazi:

$$\begin{aligned} \mathcal{A}v_1 &= a_{11}w_1 + a_{21}w_2 + \dots + a_{m1}w_m \\ \mathcal{A}v_2 &= a_{12}w_1 + a_{22}w_2 + \dots + a_{m2}w_m \\ &\dots \\ \mathcal{A}v_n &= a_{1n}w_1 + a_{2n}w_2 + \dots + a_{mn}w_m, \text{ za neki } a_{ij} \in \mathcal{O} \end{aligned}$$

Kolobarje a_{ij} (kjer je $1 \leq i \leq m$ in $1 \leq j \leq n$) zapišemo v pravokotno tabelo, ki jo običajno postavimo med oglate (ali okrogle) oklepaje in ji rečemo **matrika reda** $m \times n$:

Koeficiente, ki jih dobimo pri razvoju vektorja $\mathcal{A}v_i$ napišemo v i -ti stolpec matrike A .

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

Elementi $a_{ij} \in \mathcal{O}$ se imenujejo **členi** matrike.

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

³⁹Ekvivalentno: Linearna preslikava je enolično določena s slikami baznih vektorjev.

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 $A_{(i)}$: $A_{(i)} = [a_{i1}, a_{i2}, \dots, a_{in}]$.

j -ti stolpec matrike A bomo označevali z $A^{(j)}$: $A^{(j)} = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}$.

Linearne preslikave bomo načeloma pisali z velikimi pisanimi črkami, pripadajoče matrike pa z ustreznimi velikimi tiskanimi črkami.

Matrika ni odvisna samo od preslikave, ampak tudi od baz B_V in B_W , ki smo jih izbrali. Kadar želimo to poudariti, pišemo $A = \mathcal{A}_{B_W}^{B_V}$. To pomeni: A je matrika, ki pripada preslikavi \mathcal{A} glede na bazi B_V in B_W .

Množico vseh matrik reda $m \times n$ s členi iz obsega \mathcal{O} bomo označevali z $\mathcal{O}^{m \times n}$.

PRIMER:

- Naj bo V prostor vseh realnih polinomov stopnje največ 3, W pa prostor polinomov stopnje največ 2.

$\mathcal{A} : V \rightarrow W$ 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 .

$$\mathcal{A}1 = 1' = 0 \cdot 1 + 0 \cdot x + 0 \cdot x^2$$

$$\mathcal{A}x = 1 = 1 \cdot 1 + 0 \cdot x + 0 \cdot x^2$$

$$\mathcal{A}x^2 = 2x = 0 \cdot 1 + 2 \cdot x + 0 \cdot x^2$$

$$\mathcal{A}x^3 = 3x^2 = 0 \cdot 1 + 0 \cdot x + 3 \cdot x^2$$

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

Dokaz.

Injektivnost:

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

Po konstrukciji je $\mathcal{A}v_i = a_{1i}w_1 + a_{2i}w_2 + \dots + a_{ni}w_n$ za vsak $i = 1, \dots, n$.

$$\mathcal{A}v_i = a_{1i}w_1 + \dots + a_{ni}w_n = \mathcal{A}'v_i \text{ za vsak } i = 1, \dots, n$$

Preslikavi \mathcal{A} in \mathcal{A}' se ujemata na bazi in po trditvi od včeraj sta enaki.

Surjektivnost:

Naj bo $A = [a_{ij}] \in \mathcal{O}^{m \times n}$ poljubna matrika.

Preslikavo $\mathcal{A} : V \rightarrow W$ definiramo s predpisom $\mathcal{A}(\sum_{i=1}^n \alpha_i v_i) = \sum_{i=1}^n \alpha_i \sum_{j=1}^m a_{ji} w_j$.

Ker je $\{v_1, \dots, v_n\}$ 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 $\mathcal{A}v_i = \sum_{j=1}^m a_{ji} w_j \Rightarrow A = \mathcal{A}_{B_W}^{B_V} = \Phi(\mathcal{A})$

□

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

Definicija. Naj bosta V, W in Φ kot v prejšnji trditvi. Na $\mathcal{O}^{m \times n}$ definiramo seštevanje in množenje s skalarji s predpisoma $A + B = \Phi(\Phi^{-1}(A) + \Phi^{-1}(B))$ in $\alpha A = \Phi(\alpha \Phi^{-1}(A))$.

Torej: $\mathcal{L}(V, W) \rightarrow \mathcal{O}^{m \times n}$ s preslikavo Φ , pri tem sta $A, B \in \mathcal{O}^{m \times n}$ in lahko zapišemo, da $\Phi^{-1}(B), \Phi^{-1}(A) \in \mathcal{L}(V, W)$. Posledično velja $\Phi^{-1}(B) + \Phi^{-1}(A) \in \mathcal{L}(V, W)$.

To je edini način, kako lahko definiramo operaciji tako, da bo Φ izomorfizem.

Kaj te dve definiciji pomenita?

Naj bosta $A = [a_{ij}], B = [b_{ij}] \in \mathcal{O}^{m \times n}$ in $\alpha \in \mathcal{O}$.

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

Po definiciji je

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

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

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

Ugotovili smo: Matrike seštevamo po členih.

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

Vidimo tudi, da je definicija seštevanja neodvisna od izbire prostorov V in W in baz B_V in B_W .

$$(\alpha\mathcal{A})v_i = \alpha\mathcal{A}v_i = \alpha \sum_{j=1}^n a_{ji}w_j = \sum_{j=1}^n \alpha a_{ji}w_j$$

\Rightarrow Matrike tudi množimo s skalarji po členih

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

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

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

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

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

Da je Φ bijektivna, že vemo.

Linearnost:

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

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

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

□

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

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

Posledica.

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

Dokaz. Zaradi trditve je dovolj dokazati le prvo točko.

$$\dim U^{m \times n} = m \cdot n$$

Za $i = 1, \dots, m$, $m_j = 1, \dots, n$, naj bo E_{ij} matrika, ki ima enico na križišču i -te vrstice in j -tega stolpca in ničle drugod.

$$E_{ij} = \begin{bmatrix} & & & \\ & & & \\ & & 1 & \\ & & & \end{bmatrix}$$

Enica je postavljena v i -ti vrstici in j -tem stolpcu.

Matrike E_{ij} se imenujejo **elementarne matrike** oziroma **matrične enote**.

Dokažimo, da je $\{E_{ij}; 1 \leq i \leq m, 1 \leq j \leq n\} = B$ baza prostora $\mathcal{O}^{m \times n}$.

Linearna neodvisnost: Naj bo $\sum_{i=1}^m \sum_{j=1}^n \alpha_{ij} E_{ij} = 0$.

$$\sum_{i=1}^m = \alpha_{11} \begin{bmatrix} 1 & & & \\ & & & \\ & & & \\ & & & \end{bmatrix} + \alpha_{12} \begin{bmatrix} 0 & 1 & & \\ & & & \\ & & & \\ & & & \end{bmatrix} + \dots = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{bmatrix} \Rightarrow \alpha_{ij} = 0 \quad \forall i, j$$

Ogrodje: Naj bo $A = [a_{ij}] \in \mathcal{O}^{m \times n}$ poljubna matrika.

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{bmatrix} = \sum_{i=1}^m \sum_{j=1}^n \alpha_{ij} E_{ij} = 0$$

.

□

Če je $\dim V = n$ in $\dim U = m$, potem je $\mathcal{L}(V, U) \equiv \mathcal{O}^{m \times n}$.

Oglejmo si dva primera:

- $m = 1 \Rightarrow U \equiv \mathcal{O}$

$$\mathcal{O}^{1 \times n} \equiv \mathcal{L}(V, \mathcal{O}) = V^*$$

Pri tem $\mathcal{O}^{1 \times n}$ predstavlja prostor $1 \times n$ matrik. $\mathcal{L}(V, \mathcal{O})$ pa je prostor linearnih funkcionalov na V .

Vsak linearen funkcional na V lahko predstavimo z vrstico velikosti $1 \times n$.

$\dim V^* = \dim \mathcal{O}^{1 \times n} = n = \dim V \Rightarrow V^*$ in V sta izomorfna.

- $n = 1$: $\mathcal{L}(\mathcal{O}, U) \equiv \mathcal{O}^{m \times 1}$.

$$\mathcal{L}(\mathcal{O}, U) \equiv U \equiv \mathcal{O}^m$$

$$\mathcal{A} : \mathcal{O} \rightarrow U$$

$\mathcal{A} \mapsto \mathcal{A}(1)$ je izomorfizem med $\mathcal{L}(\mathcal{O}, U)$ in U

Odslej bomo identificirali $\mathcal{O}^{m \times 1}$ in \mathcal{O}^m in na elemente \mathcal{O}^m bomo gledali kot na stolpce.

Standardno bazo \mathcal{O}^m sestavljajo vektorji

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \dots, e_m = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$$

6.1 Množenje matrik

Množenje matrik bi radi definirali na tak način, da bo ustrezalo kompozitumu linearnih preslikav.

Naj bosta $\mathcal{A} : V \rightarrow W$ in $\mathcal{B} : U \rightarrow V$ linearni preslikavi in naj bodo $B_U = \{u_1, \dots, u_n\}$, $B_V = \{v_1, \dots, v_m\}$ in $B_W = \{w_1, \dots, w_p\}$ baze prostorov U , V in W .

Množenje matrik bi radi definirali tako, da bo veljalo $(\mathcal{A} \circ \mathcal{B})_{B_W}^{B_U} = \mathcal{A}_{B_W}^{B_V} \cdot \mathcal{B}_{B_V}^{B_U}$.

Naj bodo

$$\Phi_{p,m} : \mathcal{L}(V, W) \rightarrow \mathcal{O}^{p \times m}$$

$$\mathcal{A} \mapsto \mathcal{A}_{B_W}^{B_V}$$

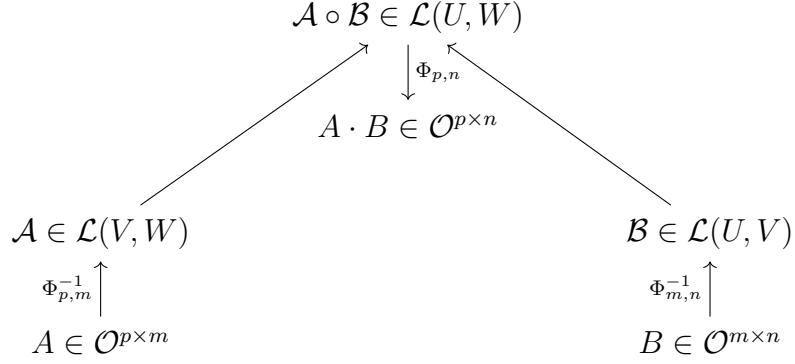
$$\Phi_{m,n} : \mathcal{L}(U, V) \rightarrow \mathcal{O}^{m \times n}$$

$$\mathcal{A} \mapsto \mathcal{A}_{B_V}^{B_U}$$

$$\Phi_{p,n} : \mathcal{L}(U, W) \rightarrow \mathcal{O}^{p \times n}$$

$$\mathcal{A} \mapsto \mathcal{A}_{B_W}^{B_V}$$

izomorfizmi.



Za poljubni matriki $A \in \mathcal{O}^{p \times n}$ in $B \in \mathcal{O}^{m \times n}$ definiramo $A \cdot B = \Phi_{p,n}(\Phi_{p,m}^{-1}(A) \cdot \Phi_{m,n}^{-1}(B)) \in \mathcal{O}^{p \times n}$.

Matriki lahko zmnožimo, če ima prva toliko stolpcev kot druga vrstic.

Prdukt ima toliko vrstic kot prva matrika in toliko stolpcev kot druga matrika.

Izpeljemo formulo za množenje matrik $A \in \mathcal{O}^{p \times n}$ in $B \in \mathcal{O}^{m \times n}$.

Obstajata linearni enolični preslikavi $\mathcal{A} : V \rightarrow W$ in $\mathcal{B} : U \rightarrow V$, da je $A = \mathcal{A}_{B_W}^{B_V}$ in $B = \mathcal{B}_{B_V}^{B_U}$.

Naj bo $A = [a_{ij}]_{1 \leq i \leq p, 1 \leq j \leq m}$ in $B = [b_{ij}]_{1 \leq i \leq m, 1 \leq j \leq n}$

To pomeni:

$$\begin{aligned}
\mathcal{A}v_1 &= a_{11}w_1 + a_{21}w_2 + \dots + a_{p1}w_p \\
\mathcal{A}v_2 &= a_{12}w_1 + a_{22}w_2 + \dots + a_{p2}w_p \\
&\vdots \\
\mathcal{A}v_m &= a_{nm}w_1 + \dots + a_{pm}w_p \\
\mathcal{B}u_1 &= b_{11}v_1 + b_{21}v_2 + \dots + b_{m1}v_m \\
\mathcal{B}u_2 &= b_{12}v_1 + b_{22}v_2 + \dots + b_{m2}v_m \\
&\vdots \\
\mathcal{B}u_n &= b_{1n}v_1 + b_{2n}v_2 + \dots + b_{mn}v_m
\end{aligned}$$

$$\begin{aligned}
(\mathcal{A} \circ \mathcal{B})u_i &= \mathcal{A}(\mathcal{B}u_i) \\
&= \mathcal{A}\left(\sum_{k=1}^m b_{ki}v_k\right) \\
&= \sum_{k=1}^m b_{ki}\mathcal{A}v_k \\
&= \sum_{k=1}^m b_{ki}\left(\sum_{j=1}^p a_{jk}w_j\right) \\
&= \sum_{j=1}^p \left(\sum_{k=1}^m a_{jk}b_{ki}\right)w_j
\end{aligned}$$

$(\sum_{k=1}^m a_{jk}b_{ki})$ so členi matrike $A \cdot B$, ki leži v i -tem stolpcu in j -ti vrstici.

Če je $C = A \cdot B = [c_{ij}]$, potem je $c_{ij} = \sum_{k=1}^m a_{ik}b_{kj}$ skalarni produkt i -te vrstice in j -tega stolpca.

Množenje matrik ni odvisno od prostorov U, V, W in baz B_U, B_V, B_W .

PRIMER:

$$\bullet A = \begin{bmatrix} 2 & 1 & 4 \\ 1 & -1 & 0 \end{bmatrix}, B = \begin{bmatrix} 1 & 3 \\ 1 & 2 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

AB ne obstaja, ker A ima 3 stolpce, B pa 4 stolpce. Toda BA obstaja.

$$B \cdot A = \begin{bmatrix} 5 & -2 & 4 \\ 0 & -3 & -4 \\ 1 & -1 & 0 \\ 3 & 0 & 4 \end{bmatrix}$$

$$\bullet A = \begin{bmatrix} 1 & 2 \\ -1 & 2 \end{bmatrix}, B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

$$A \cdot B = \begin{bmatrix} -2 & -1 \\ -2 & -3 \end{bmatrix}, B \cdot A = \begin{bmatrix} -1 & 2 \\ 0 & -4 \end{bmatrix}$$

$A \cdot B$ ni nujno enako $B \cdot A$, tudi če oba produkta obstajata in sta iste velikosti.

Poseben primer množenja matrik je množenje matrika z vektorjem: Če je $A = [a_{ij}] \in \mathcal{O}^{m \times n}$

in $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, je $y = Ax = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} \in \mathcal{O}^m$ vektor, za katerega velja $y_i = \sum_{k=1}^n a_{ik}x_k$ (y_i je

”skalarni produkt” i -te vrstice matrike A in stolpca x)

PRIMER:

$$\bullet \begin{bmatrix} 1 & 2 \\ -1 & 3 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 4 \\ -1 \end{bmatrix}$$

Trditev. Naj bosta U in V vektorska prostora, $B_U = \{u_1, \dots, u_n\}$ baza U in $\{v_1, \dots, v_m\} = B_V$ baza V . Naj bo $\mathcal{A} : U \rightarrow V$ linearna preslikava in $x \in U$. Naj bo $A = \mathcal{A}_{B_V}^{B_U}$ (matrika preslikave \mathcal{A} glede na bazi B_U in B_V). x razvijamo po bazi B_U : $x = \alpha_1 u_1 + \dots + \alpha_n u_n$. $\mathcal{A}x \in V$ razvijemo po bazi B_V : $\mathcal{A}x = \beta_1 v_1 + \dots + \beta_m v_m$.

Potem je $A \cdot \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix}$. Produkt matrike s stolpcem ustreza evalvaciji linearne preslikave na vektorju.

Dokaz.

$$\mathcal{A}x = \mathcal{A}\left(\sum_{i=1}^n \alpha_i u_i\right) = \sum_{i=1}^n \alpha_i \mathcal{A}u_i$$

$$\mathcal{A}u_1 = a_{11}v_1 + \dots + a_{m1}v_m$$

$$\vdots$$

$$\mathcal{A}u_n = a_{1n}v_1 + \dots + a_{mn}v_m$$

$$\mathcal{A}x = \sum_{i=1}^n \alpha_i \sum_{k=1}^m a_{ki} v_k = \sum_{k=1}^m \left(\sum_{i=1}^n a_{ki} \alpha_i\right) v_k$$

Izračunajmo k -to komponento produkta $A \cdot \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$. Ta komponenta je enaka $\sum_{i=1}^n a_{ki} \alpha_i = \beta_k$.

□

PRIMER

- Ravnino zavrtimo za kot $\frac{\pi}{3}$ v pozitivni smeri. Kam se preslika vektor $\begin{bmatrix} 1 \\ 2 \end{bmatrix}$?

Rotacija je linearna preslikava.

Napišemo matriko te preslikave.

Ugotoviti moramo, kam se slikajo bazni vektorji.

$$A = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix}$$

$$A = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -\frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix}$$

Matriko in preslikavo označimo kar enako

$$A = \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}$$

$$\text{Vektor } \begin{bmatrix} 1 \\ 2 \end{bmatrix} \text{ se slika v vektor } A \cdot \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & -\sqrt{3} \\ \frac{\sqrt{3}}{2} & 1 \end{bmatrix}$$

Naj bo $A \in \mathcal{O}^{m \times n}$ matrika. Potem je s predpisom $x \mapsto Ax$ definirana linearna preslikava $\mathcal{O}^n \rightarrow \mathcal{O}^m$ (linearnost preveri doma).

To linearno preslikavo označimo kar z A .

V \mathcal{O}^n in \mathcal{O}^m si izberemo standardni bazi S_n in S_m .

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix}, \text{ podobno velja za ostale stolpce.}$$

Preslikava A vektorje standardne baze slika v stolpce matrike A .

Preslikavi $\mathcal{O}^n \rightarrow \mathcal{O}^m$, ki je množenje z matriko A , glede na standardni bazi prostorov \mathcal{O}^n in \mathcal{O}^m pripada matriki A .

Posledica. Naj bosta $B_V = \{v_1, \dots, v_n\}$ in $B_W = \{w_1, \dots, w_m\}$ bazi prostorov V in W in naj bo $\mathcal{A} : V \rightarrow W$ linearna preslikava.

Naj bosta $\Phi_V : \mathcal{O}^n \rightarrow V$ in $\Phi_W : \mathcal{O}^m \rightarrow W$ izomorfizem, definirana s predpisoma

$$\Phi_V \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \sum_{i=1}^n \alpha_i v_i \text{ in } \Phi_W \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix} = \sum_{i=1}^m \beta_i w_i.$$

Naj bo $A = \mathcal{A}_{B_W}^{B_V}$ in $A : \mathcal{O}^n \rightarrow \mathcal{O}^m$ množenje z matriko A .

Potem diagram

$$\begin{array}{ccc} V & \xrightarrow{\mathcal{A}} & W \\ \Phi_V \uparrow & & \uparrow \Phi_W \\ \mathcal{O}^n & \xrightarrow{A} & \mathcal{O}^m \end{array}$$

komutira.

Dokaz. Dovolj je dokazati, da za vsak $x \in \mathcal{O}^n$ velja $\Phi_W(Ax) = \mathcal{A}(\Phi_V(x))$

$$\Phi_W\left(A \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}\right) = \Phi_W \begin{bmatrix} a_{11}\alpha_1 + a_{12}\alpha_2 + \dots + a_{1n}\alpha_n \\ \vdots \\ a_{m1}\alpha_1 + a_{m2}\alpha_2 + \dots + a_{mn}\alpha_n \end{bmatrix} = \sum_{i=1}^m \left(\sum_{k=1}^n a_{ik}\alpha_k\right)w_i$$

$$\mathcal{A}\left(\Phi_V\left(\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}\right)\right) = \mathcal{A}\left(\sum_{i=1}^n \alpha_i v_i\right) = \sum_{i=1}^n \alpha_i \mathcal{A}v_i = \sum_{i=1}^n \alpha_i \sum_{k=1}^m a_{ki}w_k$$

□

Trditev.

1. Naj bodo

$$\begin{aligned} \Phi_{m,n} &: \mathcal{L}(V, U) \rightarrow \mathcal{O}^{m \times n} \\ \Phi_{n,p} &: L(W, V) \rightarrow \mathcal{O}^{n \times p} \text{ in} \\ \Phi_{m,p} &: L(W, U) \rightarrow \mathcal{O}^{m \times p} \end{aligned}$$

izomorfni, določeni z izbirami baz prostorov U, V in W . Potem je $\Phi_{m,p}(A \circ B) = \Phi_{m,n}(A) \cdot \Phi_{n,p}(B)$ za vsak $B \in L(W, U)$ in vsak $A \in \mathcal{L}(V, U)$.

2. Če je $A \in \mathcal{O}^{m \times n}$, $B \in \mathcal{O}^{n \times p}$ in $C \in \mathcal{O}^{p \times q}$, potem je

$$(AB)C = A(BC)$$

(množenje matrik je asociativno)

Dokaz.

1. je definicija množenja matrik

2. Naj bo Z vektorski prostor dimenzije q in naj bodo

$$\begin{aligned} \Phi_{n,q} &: L(U, V) \rightarrow \mathcal{O}^{n \times q} \\ \Phi_{m,q} &: L(Z, U) \rightarrow \mathcal{O}^{m \times q} \text{ in} \\ \Phi_{p,q} &: L(Z, W) \rightarrow \mathcal{O}^{p \times q} \text{ izomorfizmi} \end{aligned}$$

po definiciji množenja matrik je $A(BC) = A \cdot \Phi_{n,q}$

□

Dokaz.

$$\begin{aligned}
& \Phi_{n,p}^{-1} : B \circ \Phi_{p,q}^{-1}(c) = \\
& \Phi_{m,q}(\Phi_{m,n}^{-1}(A) \circ \Phi_{n,q}^{-1}(\Phi_{n,q}^{-1}(B) \circ \Phi_{p,q}^{-1}(c))) = \\
& \Phi_{m,q}(\Phi_{m,n}^{-1}(A) \circ \Phi_{n,p}^{-1}(B) \circ \Phi_{p,q}^{-1}(C)) = \\
& \Phi_{m,q}(\Phi_{m,p}^{-1}(\Phi_{m,p}(\Phi_{m,n}^{-1}(A) \circ \Phi_{n,p}^{-1}(B)))) \circ \Phi_{p,q}^{-1}(C) = \\
& \Phi_{m,q}(\Phi_{m,p}^{-1}(AB) \circ \Phi_{p,q}^{-1}(C)) = \\
& (AB)C
\end{aligned}$$

□

Posledica. Množica kvadratnih matrik $\mathcal{O}^{m \times n}$ je **algebra** in preslikava $\mathcal{L}(V, V) \rightarrow \mathcal{O}^{n \times n}$ (kjer je $\dim V = n$), definirana s predpisom $\Phi(A) = A_{B_V}^{B_V}$, kjer je B_V baza V , je izomorfizem algebr.

Dokaz. Vemo že, da je $\mathcal{O}^{n \times n}$ vektorski prostor. Množenje $n \times n$ matrik je notranja operacija, ki je po prejšnji trditvi asociativna.

Distributivnost in enakost $(\alpha A)(\beta B) = (\alpha\beta)(AB)$, za $\alpha, \beta \in \mathcal{O}$ in $A, B \in \mathcal{O}^{n \times n}$ preverite sami. To je lahek račun.

Vemo že, da je Φ izomorfizem vektorskih prostorov, po prejšnji točki pa je tudi

$$\Phi(A) \cdot \Phi(B) = \Phi(A \circ B)$$

□

id_V je enota algebre $\mathcal{L}(U, V)$. Ker je Φ izomorfizem, je $\Phi(id_V)$ enota algebre $\mathcal{O}^{n \times n}$.

Matriko $\Phi(id_V)$ označimo z I_n , oz. kar z I , če je velikost znana.

I se imenuje identična matrika ali identiteta.

Izračunajmo I .

Naj bo $B_V = \{v_1, \dots, v_n\}$ baza V .

$$\begin{aligned}
id(v_1) &= v_1 = 1 \cdot v_1 + 0 \cdot v_2 + \dots + 0 \cdot v_n \\
id(v_2) &= v_2 = 0 \cdot v_1 + 1 \cdot v_2 + \dots + 0 \cdot v_n \\
&\vdots \\
id(v_n) &= v_n = 0 \cdot v_1 + 0 \cdot v_2 + \dots + 1 \cdot v_n
\end{aligned}$$

$$\Rightarrow \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}$$

$\mathcal{O}^{n \times n}$ je algebra z enoto I .

Velja še več:

če je $A \in \mathcal{O}^{m,n}$, je $A \cdot I_m = A$, in če je $B \in \mathcal{O}^{m,n}$, je $I_m \cdot B = B$

Dokaz.

$$\begin{aligned} A \cdot I_m &= \\ &= \Phi_{n,m}(\Phi_{n,m}^{-1}(A) \circ \Phi_{m,n}^{-1}(I)) \\ &= \Phi_{n,m}(\Phi_{n,m}^{-1}(A) \circ id) \\ &= \Phi_{n,m}(\Phi_{n,m}^{-1}(A)) \\ &= A \end{aligned}$$

□

Definicija. Matrika $A \in \mathcal{O}^{n \times n}$ je *diagonala*, če je $a_{ij} = 0$ za $i \neq j$. Pišemo

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

Torej je $I = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$ poseben primer diagonale matrike.

Definicija.

1. Endomorfizem $\mathcal{A} \in L(U, V)$ je *obrnljiv*, kadar obstaja $\mathcal{B} \in \mathcal{L}(V, U)$, da je $\mathcal{A} \circ \mathcal{B} = \mathcal{B} \circ \mathcal{A} = id_V$.
2. Matrika $A \in \mathcal{O}^{n \times n}$ je *obrnljiva*, kadar obstaja $B \in \mathcal{O}^{n \times n}$, da je $AB = BA = I$. Taki matriki B pravimo *inverz matrike A* in jo označimo z A^{-1} .

Naši prostori so končnorazsežni, zato je endomorfizem \mathcal{A} obrnljiv, ko obstaja \mathcal{B} , da je $\mathcal{A} \circ \mathcal{B} = id_V$ ali $\mathcal{B} \circ \mathcal{A} = id_V$.

Recimo, da velja $\mathcal{A} \circ \mathcal{B} = id_V$ (drugi primer se dokaže podobno). Potem je \mathcal{A} surjektiven.

$$\dim V = \dim(\ker \mathcal{A}) + \dim(\operatorname{Im} \mathcal{A}) \Rightarrow \dim V^{40}$$

$$\Rightarrow \dim(\ker \mathcal{A}) = 0 \Rightarrow \ker \mathcal{A} = \{0\} \Rightarrow A^{41}$$

\mathcal{A} ima torej inverz in zanj vemo, da je tudi linearna preslikava. Torej je \mathcal{A} obrnljiv.

Kvadratna matrika A je obrnljiva, kadar obstaja matrika B , da je $AB = I$ ali $BA = I$.

⁴⁰Zaradi surjektivnosti.

⁴¹Je injektivna, torej je bijektivna.

Posledica. Izomorfizem $\Phi : \mathcal{L}(V, U) \rightarrow \mathcal{O}^{n \times n}$ slika obrnljive endomorfizme v obrnljive matrike in za vsak obrnljiv enfomorfizem A velja

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

Dokaz.

$$\begin{aligned} \Phi(\mathcal{A}^{-1})\Phi(\mathcal{A}) &= \\ &= \Phi(\mathcal{A}^{-1}\mathcal{A}) \\ &= \Phi(id_V) \\ &= I^{42} \end{aligned}$$

□

6.2 Dualni prostor in dualne preslikave

Naj bo V končnorazsežen vektorski prostor nad \mathcal{O} . Preslikava $\mathbb{L}\mathcal{L}(V\mathcal{O})$ vseh linearnih funkcionalov na V pravimo **dualni prostor prostora** V in ga običajno označimo z V^* (včasih tudi V').

Naj bo $n = \dim V$. Potem vemo, da je $V \equiv \mathcal{O}^n \equiv \mathcal{O}^{1 \times n} \equiv V^*$ in $\dim V^* = \dim V$.

Definicija. Naj bo $B_V = \{v_1, \dots, v_n\}$ baza prostora V . Množica funkcionalov $\{\varphi_1, \dots, \varphi_n\} \subseteq V^*$ je **dualna baza** baze B_V , če za vsaka $i, j = 1, \dots, n$ velja $\varphi_i(v_j) = \delta_{ij} = \begin{cases} 1, & \text{če je } i = j \\ 0, & \text{če je } i \neq j \end{cases}$. δ_{ij} se imenuje **Kroneckerjeva delta**.

Trditev. Dualna baza baze B_V vedno obstaja. Z B_V je enolično določena in je res baza prostora V^* .

Dokaz.

- Enoličnost: Recimo, da so $\varphi_1, \dots, \varphi_n : V \rightarrow \mathcal{O}$ taki funkcionali, da je $\varphi_i(v_j) = \delta_{ij}$ za vsaka i in j . Naj bo $x \in V$ poljuben vektor. Ker je $B_V = \{v_1, \dots, v_n\}$ baza za V , lahko x enolično razvijemo po tej bazi: $x = \alpha_1 v_1 + \dots + \alpha_n v_n$.

$$\begin{aligned} \varphi_i(x) &= \varphi_i(\alpha_1 v_1 + \dots + \alpha_n v_n) \\ &= \alpha_1 \varphi_i(v_1) + \dots + \alpha_n \varphi_i(v_n) \\ &= \alpha_1 \delta_{i1} + \dots + \alpha_n \delta_{in} \\ &= \alpha_i \text{ za vsak } i \end{aligned}$$

⁴² $\Rightarrow \Phi(\mathcal{A}^{-1})$ je inverz od $\Phi(\mathcal{A})$.

Dokazali smo, da če je $\varphi_i(v_j) = \delta_{ij}$, potem je $\varphi_i(\sum_{j=1}^n \alpha_j v_j) = \alpha_{ji}$.

φ_i v vsaki točki prostora V lahko zavzame le eno vrednost. Torej obstaja kvečjemu en linearen funkcional $\varphi_i : V \rightarrow \mathcal{O}$, da je $\varphi_i(v_j) = \delta_{ij}$ za vsak $j = 1, \dots, n$. To velja za vsak i .

- Obstoj: Za vsak $i = 1, \dots, n$ definiramo $\varphi_i(\sum_{j=1}^n \alpha_{ij} v_j) = \alpha_i$.

Dokazati moramo, da je to linearen funkcional.

Da je funkcional, je očitno.

- Linearnost: $x, y \in V$, $\alpha, \beta \in \mathcal{O}$. x in y lahko razvijemo po bazi B_V : $x = \sum_{j=1}^n \alpha_{ij} v_j$, $y = \sum_{j=1}^n \beta_j v_j$.

$$\begin{aligned} \varphi_i(\alpha x + \beta y) &= \varphi_i(\alpha \sum_{j=1}^n \alpha_j v_j + \beta \sum_{j=1}^n \beta_j v_j) \\ &= \varphi_i(\sum_{j=1}^n (\alpha \alpha_j + \beta \beta_j) v_j) \\ &= \alpha \alpha_i + \beta \beta_i \\ &= \alpha \cdot \varphi_i(\sum_{j=1}^n \alpha_j v_j) + \beta \cdot \varphi_i(\sum_{j=1}^n \beta_j v_j) \\ &= \alpha \varphi_i(x) + \beta \varphi_i(y) \end{aligned}$$

Očitno je tudi $\varphi_i(v_j) = \delta_{ij}$ za vsaka $i, j = 1, \dots, n$.

- $\{\varphi_1, \dots, \varphi_n\}$ je baza V^*

Ker je $\dim V^* = n$ je dovolj dokazati, da so $\varphi_1, \dots, \varphi_n$ linearno neodvisni.

Potem je $(\alpha_1 \varphi_1 + \dots + \alpha_n \varphi_n)(x) = 0$ za vsak $x \in V$.

$$(\alpha_1 \varphi_1 + \dots + \alpha_n \varphi_n)(x) = \alpha_1 \varphi_1(x) + \dots + \alpha_n \varphi_n(x)$$

Za x vstavimo v_j :

$$\underbrace{\alpha_1 \underbrace{\varphi_1(v_j)}_{\delta_{1j}} + \dots + \alpha_n \underbrace{\varphi_n(v_j)}_{\delta_{nj}}}_{\alpha_j=0} = 0$$

j je bil poljuben, od koder sledi, da so $\varphi_1, \dots, \varphi_n$ linearno neodvisni.

□

Opomba: Tudi, da je $\{\varphi_1, \dots, \varphi_n\}$ ogrodje za V^* , je enostavno dokazati: če je $\psi \in V^*$ poljuben, potem je $\psi = \sum_{i=1}^n \underbrace{\psi(v_i)\varphi_i}_{\in \mathcal{O}}$ (preverite doma). To bi bil alternativen dokaz, da je

$V \equiv V^*$.

Trditev. Naj bo $B_V = \{v_1, \dots, v_n\}$ baza prostora V in $B_{V^*} = \{\varphi_1, \dots, \varphi_n\}$ njej dualna baza. Naj bosta $x \in V$ in $\psi \in V^*$ poljubna. Razvijemo ju po bazah $x = \sum_{i=1}^n \alpha_i v_i$, $\psi = \sum_{i=1}^n \beta_i \varphi_i$.

Označimo $a = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \in \mathcal{O}^n$ in $b = [\beta_1 \ \dots \ \beta_n] \in \mathcal{O}^{1 \times n}$. Potem je $\psi(x) = b \cdot a$. ("skalarni produkt" vrstice b in stolpca a).

Dokaz.

$$\begin{aligned} \psi(x) &= \left(\sum_{i=1}^n \beta_i \varphi_i\right) \left(\sum_{j=1}^n \alpha_j v_j\right) \\ &= \sum_{i,j=1}^n \beta_i \alpha_j \varphi_i(v_j) \\ &= \sum_{i=1}^n \beta_i \alpha_i \\ &= b \cdot a \end{aligned}$$

□

PRIMER:

- Naj bodo $a_0, \dots, a_n \in \mathbb{R}$ paroma različni? in $b_0, \dots, b_n \in \mathbb{R}$ poljubni. Potem vemo, da obstaja natanko en polinom $p(x)$ stopnje največ n , da je $p(a_i) = b_i$ za $i = 0, \dots, n$. Kako $p(x)$ poiščemo brez računanja?

V naj bo vektorski prostor realnih polinomov stopnje največ n .

Naj bo $a \in \mathbb{R}$.

Preslikava $V \rightarrow \mathbb{R}$, kjer se $p(x)$ slika v $p(a)$ je linearen funkcional.

Za $i = 0, \dots, n$ definiramo funkcional

$$\begin{aligned} \varphi_i : V &\rightarrow \mathcal{O} \\ \varphi_i(p(x)) &= p(a_i) \end{aligned}$$

V V bomo poiskali tako bazo $B_V = \{p_0, \dots, p_n\}$, da bo $B_{V^*} = \{\varphi_0, \dots, \varphi_n\}$ tej bazi dualna baza. (Ne vemo še, da je B_{V^*} res baza za V^*).

$$\underbrace{\varphi_i(p_j)}_{p_j(a_i)} = \delta_{ij} \quad \forall i, j = 0, \dots, n$$

$p_j(a_i) = 0$ za $i \neq j$: za $i \neq j$ je a : ničla polinoma $p_j(x) \Rightarrow$

$$p_j(x) = c \cdot \underbrace{(x - a_0) \dots (x - a_{j-1})(x - a_{j+1}) \dots (x - a_n)}_{\text{stopnje } n}$$

c je konstanta.

$$p_j(a_j) = 1$$

$$p_j(a_j) = c(a_j - a_0) \dots (a_j - a_{j-1})(a_j - a_{j+1}) \dots (a_j - a_n)$$

$$p_j(x) = \frac{(x - a_0) \dots (x - a_{j-1})(x - a_{j+1}) \dots (x - a_n)}{(a_j - a_0) \dots (a_j - a_{j-1})(a_j - a_{j+1}) \dots (a_j - a_n)}$$

Dokazati moramo, da je $\{p_0, \dots, p_n\}$ baza prostora V (in potem bo B_{V^*} tej bazi dualna baza).

Ker je $\dim V = n + 1$ je dovolj dokazati linearno neodvisnost.

$$\alpha_0 p_0(x) + \dots + \alpha_n p_n(x) = 0$$

$$\text{To izračunamo v } a_j: \underbrace{\alpha_0 \underbrace{p_0(a_j)}_{\delta_{0j}} + \dots + \alpha_n \underbrace{p_n(a_j)}_{\delta_{nj}}}_{\alpha_j = 0 \quad \forall j=0, \dots, n} = 0$$

Iz tega sledi: $B_V = \{p_0, \dots, p_n\}$ je res baza V in B_{V^*} je njej dualna baza. Iščemo $p(x)$, da bo $p(a_i) = b_i$ za vsak, ?. $p_j(a_i) = \delta_{ji}$.

$$p(x) = \sum_{i=1}^n b_i p_i(x)$$

To je **Lagrangeva interpolacija**.

6.2.1 Dualna preslikava

$\mathcal{A} \in \mathbb{L}\mathcal{L}(V, W)$, $\varphi \in W^*$, $\varphi : W \rightarrow \mathcal{O}$ je linearen funkcional.

$\varphi \circ \mathcal{A}$ je kompozitum linearnih preslikav, torej je linearna preslikava. Je celo linearni funkcional, saj slika v $\mathcal{O} : \varphi^{43} \mapsto \varphi \circ \mathcal{A} \in V^*$

Definicija. Naj bosta V in W končnorazsežna vektorska prostora nad \mathcal{O} in $\mathcal{A} : V \rightarrow W$ linearna preslikava. Preslikava $\mathcal{A}^d : W^* \rightarrow V^*$, definirana s predpisom $\mathcal{A}^d(\varphi) = \varphi \circ \mathcal{A}$, se imenuje **dualna preslikava** preslikave \mathcal{A} .

Trditev. $\mathcal{A}^d \in \mathcal{L}(W^*, V^*)$.

Dokaz.

$$\begin{aligned}\mathcal{A}^d(\alpha\varphi + \beta\psi) &= (\alpha\varphi + \beta\psi) \circ \mathcal{A} \\ &= \alpha\varphi \circ \mathcal{A} + \beta\psi \circ \mathcal{A} \\ &= \alpha\mathcal{A}^d(\varphi) + \beta\mathcal{A}^d(\psi)\end{aligned}$$

□

Trditev. Naj bodo U, V, W vektorski prostori, $\mathcal{A}, \mathcal{B} \in \mathcal{L}(U, V)$, $\varphi \in \mathbb{L}\mathcal{L}(V, W)$ in $\lambda \in \mathcal{O}$. Potem je $(\mathcal{A} + \mathcal{B})^d = \mathcal{A}^d + \mathcal{B}^d$, $(\lambda\mathcal{A})^d = \lambda \cdot \mathcal{A}^d$ in $(\varphi \circ \mathcal{A})^d = \mathcal{A}^d \circ \varphi^d$

Dokaz. Za $\varphi \in V^*$ je

$$\begin{aligned}(\mathcal{A} + \mathcal{B})^d(\varphi) &= \varphi \circ (\mathcal{A} + \mathcal{B}) \\ &= \varphi \circ \mathcal{A} + \varphi \circ \mathcal{B} \\ &= \mathcal{A}^d(\varphi) + \mathcal{B}^d(\varphi) \\ &= (\mathcal{A}^d + \mathcal{B}^d)(\varphi)\end{aligned}$$

$$\begin{aligned}(\lambda\mathcal{A})^d &= \varphi \circ (\lambda\mathcal{A}) \\ &= \lambda\varphi \circ \mathcal{A} \\ &= \lambda\mathcal{A}^d(\varphi) \\ &= (\lambda\mathcal{A}^d)(\varphi)\end{aligned}$$

⁴³ $\varphi \in W^*$

Za $\psi \in W^*$ je

$$\begin{aligned}
(\varphi \circ \mathcal{A})^d(\psi) &= \psi \circ \varphi \circ \mathcal{A} \\
&= (\psi \circ \varphi) \circ \mathcal{A} \\
&= \mathcal{A}^d(\psi \circ \varphi) \\
&= \mathcal{A}^d(\varphi^d(\psi)) \\
&= (\mathcal{A}^d \circ \varphi^d)(\psi)
\end{aligned}$$

□

Definicija. Naj bo $A \in \mathcal{O}^{m \times n}$. **Transponirana matrika** matrike $A = [a_{ij}]$ je matrika $A^T = [a_{ji}] \in \mathcal{O}^{n \times m}$. Transponiranje je zrcaljenje matrike čez diagonalo.

PRIMER:

- $\begin{bmatrix} 1 & 0 & 1 \\ -1 & 2 & -2 \end{bmatrix}^T = \begin{bmatrix} 1 & -1 \\ 0 & 2 \\ 1 & -2 \end{bmatrix}$
- $A^{TT} = A$ po definiciji.

Izrek. Če linearni preslikavi $\mathcal{A} : V \rightarrow W$ glede na bazi B_V in B_W pripada matrika A , potem dualni preslikavi $\mathcal{A}^d : W^* \rightarrow V^*$ glede na dualni bazi baz B_W in B_V pripada matrika A^T .

Dokaz. Naj bo $B_V = \{v_1, \dots, v_n\}$ baza V in $B_{V^*} = \{\varphi_1, \dots, \varphi_n\} \subseteq V^*$ njej dualna baza.

Naj bo $B_W = \{w_1, \dots, w_m\}$ baza W in $B_{W^*} = \{\psi_1, \dots, \psi_m\} \subseteq W^*$ njej dualna baza.

Naj bo $A = [a_{ij}]_{1 \leq i \leq m, 1 \leq j \leq n}$ in naj bo $C = [C_{ij}]_{1 \leq i \leq n, 1 \leq j \leq m}$ matrika preslikave \mathcal{A}^d glede na bazi B_{W^*} in B_{V^*} .

Dokazujemo, da je $C = A^T$, oziroma, da za vsaka i in j velja $c_{ij} = a_{ji}$.

$$\begin{aligned}
\mathcal{A}^{d_{\tau_i}}{}^{44} &= \sum_{j=1}^n c_{ji} \varphi_j \\
\Rightarrow (\psi_i \circ \mathcal{A})(x) &= \sum_{j=1}^n c_{ji} \varphi_j(x) \quad \forall x \in V \\
x = v_k : (\psi_i \circ \mathcal{A})(v_k) &= \sum_{j=1}^n c_{ji} \varphi_j(v_k) = \underline{c_{ki}}, \quad \forall i = 1, \dots, m, \quad \forall k = 1, \dots, n \\
(\psi_i \circ \mathcal{A})(v_k) &= \psi_i(\mathcal{A}(v_k)) \\
&= \psi_i\left(\sum_{j=1}^n a_{jk} w_j\right) \\
&= \sum_{j=1}^m a_{jk} \psi_i(w_j) \\
&= \underline{a_{ik}} \\
\Rightarrow C &= A^T
\end{aligned}$$

□

Posledica. Naj bodo $A, B \in \mathcal{O}^{m \times n}$, $C \in \mathcal{O}^{n \times p}$ in $\lambda \in \mathcal{O}$. Potem je $(A + B)^T = A^T + B^T$, $(\lambda A)^T = \lambda A^T$ in $(AC)^T = C^T A^T$.

6.3 Prehod na novi bazi

Naj bosta $B_V = \{v_1, \dots, v_n\}$ in $B'_V = \{v'_1, \dots, v'_n\}$ bazi prostora V . Potem elemente B'_V lahko razvijemo po bazi B_V :

$$\begin{aligned}
id(v'_1) &= v'_1 = p_{11}v_1 + p_{21}v_2 + \dots + p_{n1}v_n \\
id(v'_2) &= v'_2 = p_{12}v_1 + p_{22}v_2 + \dots + p_{n2}v_n \\
&\vdots \\
id(v'_n) &= v'_n = p_{1n}v_1 + p_{2n}v_2 + \dots + p_{nn}v_n
\end{aligned}$$

Matrika $P = [p_{ij}]_{i,j=1} \in \mathcal{O}^{n \times m}$ se imenuje **prehodna matrika** iz baze B_V v bazo B'_V .

$$P = id_{B'_V}$$

Prehodna matrika je matrika, ki pripada identiteti glede na dve različni bazi.

$$\Rightarrow P \text{ je obrnljiva in } P^{-1} = id_{B'_V}^{B_V}.$$

$$\textbf{Dokaz.} \quad id_{B'_V}^{B'_V} \cdot id_{B'_V}^{B_V} = id_{B'_V}^{B_V} = I$$

□

⁴⁴ = $\psi_i \circ \mathcal{A}$, $\forall i = 1, \dots, m$

Poseben primer: Če je $V = \mathcal{O}^n$ in je B_V standardna baza prostora \mathcal{O}^n , potem so stolpci matrike P ravno elementi baze B'_V .

Trditev. Naj bo $\mathcal{A} : V \rightarrow W$ linearna preslikava, naj bosta B_V in B'_V bazi prostora V , naj bosta B_W in B'_W bazi prostora W , naj preslikavi \mathcal{A} glede na bazi B_V in B_W pripada matrika A , glede na bazi B'_V in B'_W pa matrika A' . P naj bo prehodna matrika iz baze B_V v bazo B'_V , Q pa prehodna matrika iz baze B_W v bazo B'_W . Potem je $A' = Q^{-1}AP$.

Dokaz.

$$\begin{aligned}
A &= \mathcal{A}_{B_W}^{B_V}, \\
A' &= \mathcal{A}_{B'_W}^{B'_V}, \\
P &= id_{B_V}^{B'_V}, \\
Q &= id_{B_W}^{B'_W}, \\
Q^{-1} &= id_{B'_W}^{B_W}, \\
A' &= \mathcal{A}_{B_W}^{B'_V} \\
&= (id_W \circ \mathcal{A} \circ id_V)_{B'_W}^{B'_V} \\
&= id_{B'_W}^{B_W} \cdot \mathcal{A}_{B_W}^{B_V} \cdot id_{B_V}^{B'_V} \\
&= Q^{-1} \cdot A \cdot P
\end{aligned}$$

Pri predzadnji enakosti smo upoštevali definicijo množenja matrik. □

PRIMER:

- Določi matriko preslikave $\mathcal{A} : \mathcal{O}^3 \rightarrow \mathcal{O}^2$, definirane s predpisom $\mathcal{A}(x, y, z) = (x, y)$, glede na bazi $B = \left\{ \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\}$ in $B' = \left\{ \begin{bmatrix} 4 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \end{bmatrix} \right\}$.

Matriko preslikave \mathcal{A} je lahko napisati glede na standardni bazi $S = \{e_1, e_2, e_3\}$ in $S' = \{e_1, e_2\}$ prostorov \mathcal{O}^3 in \mathcal{O}^2 .

$$\begin{aligned}
* \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} &= \frac{1}{ad-bc} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \\
* \quad \mathcal{A}_{S'}^S &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = A \\
* \quad P = id_S^B &= \begin{bmatrix} 1 & 1 & 1 \\ -1 & 0 & 1 \\ 0 & -1 & 1 \end{bmatrix}
\end{aligned}$$

$$* id_{S'}^{B'} = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix} = Q$$

*

$$\begin{aligned} \mathcal{A}_{B'}^B &= id_{B'}^{S'} \cdot \mathcal{A}_{S'}^S \cdot id_S^B \\ &= Q^{-1}AP \\ &= \frac{1}{4 \cdot 2 \cdot 3 \cdot 3} \cdot \begin{bmatrix} 2 & -3 \\ -3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ -1 & 0 & 1 \\ 0 & -1 & -1 \end{bmatrix} \\ &= \begin{bmatrix} -2 & 3 \\ 3 & -4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ -1 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} -5 & -2 & 1 \\ 7 & 3 & -1 \end{bmatrix} \end{aligned}$$

Definicija. Matrika $B \in \mathcal{O}^{m \times n}$ je **ekvivalentna** matriki $A \in \mathcal{O}^{m \times n}$, kadar obstajata obrnljivi matriki $P \in \mathcal{O}^{m \times n}$ in $Q \in \mathcal{O}^{m \times n}$, da je $B = Q^{-1}AP$. Oznaka: $B \sim A$.

Trditev. Ekvivalentnost je ekvivalenčna relacija.

Dokaz.

- Refleksivnost: $A = I^{-1}AI \Rightarrow A \sim A$
- Simetričnost: $B \sim A \Rightarrow \exists P, Q$ obrnljivi, da je $B = Q^{-1}AP / P^{-1}$
 $(\underbrace{Q^{-1}}_{\text{obrnljiva}})^{-1}BP^{-1} = QB \underbrace{P^{-1}}_{\text{obrnljiva}} = A \Rightarrow A \sim B$
- Tranzitivnost: $B \sim A, C \sim B \Rightarrow \exists P, Q, R, S$ obrnljive, da je $B = Q^{-1}AP$,
 $C = S^{-1}BR \Rightarrow C = S^{-1}Q^{-1}APR = (\underbrace{QS}_{\text{obrnljivi}})^{-1}A(\underbrace{PR}_{\text{obrnljivi}}) \Rightarrow C \sim A$.

□

Trditev. Matriki $A, B \in \mathcal{O}^{m \times n}$ sta ekvivalentni natanko takrat, ko pripadata isti linearni preslikavi (morda glede na različni bazi).

Dokaz.

\Leftarrow Že vemo

$\Rightarrow A, B \in \mathcal{O}^{m \times n}$, $B = Q^{-1}AP$
 Definirajmo linearno preslikavo:

$$\begin{aligned} \mathcal{A} : \mathcal{O}^n &\rightarrow \mathcal{O}^m \\ x &\mapsto Ax \end{aligned}$$

Glede na standardni bazi S_n in S_m preslikavi \mathcal{A} pripada matrika A .

$$B_n = P(S_n), B_m = Q(S_m)$$

P in Q sta obrnljivi, zato sta B_n in B_m bazi.

$$\begin{aligned} \mathcal{A}_{B_m}^{B_n} &= (id_m \circ \mathcal{A} \circ id_n)_{B_m}^{B_n} \\ &= id_{B_m}^{S_m} \cdot \mathcal{A}_{S_m}^{S_n} \cdot id_{S_n}^{B_n} \\ &= Q^{-1} \cdot A \cdot P \\ &= B \end{aligned}$$

□

Definicija. *Rang* matrike $A \in \mathcal{O}^{m \times n}$ je rang linearne preslikave $\mathcal{O}^n \rightarrow \mathcal{O}^m$, definirane s predpisom $x \mapsto A \cdot x$.

$$\begin{aligned} \mathcal{O}^n &\rightarrow \mathcal{O}^m \\ x &\mapsto Ax \end{aligned}$$

Trditev. Naj bo $A : V \rightarrow W$ linearna preslikava in $A \in \mathcal{O}^{m \times n}$ njena matrika glede na poljubni bazi prostorov V in W . Potem je $\text{rang} A = \text{rang} A$.

Dokaz. Vemo, da izbiri baz prostorov V in W določata izomorfizma $\emptyset_v : \mathcal{O}^n \rightarrow V$ in $\emptyset_w : \mathcal{O}^m \rightarrow W$

$$((\alpha_1, \dots, \alpha_n) \mapsto \alpha_1 v_1 + \dots + \alpha_n v_n)$$

in da diagram

$$\begin{array}{ccc} V & \xrightarrow{A} & W \\ \Phi_V \uparrow & & \uparrow \Phi_W \\ \mathcal{O}^n & \xrightarrow{A} & \mathcal{O}^m \end{array}$$

komutira.

$$\begin{aligned} A : \mathcal{O}^n &\rightarrow \mathcal{O}^m \\ x &\mapsto Ax \end{aligned}$$

Dokaz.

$$\begin{aligned}
 \text{rang} A &= \\
 &= \dim(\text{im}(\Phi w \circ A \circ \Phi v^{-1})) \\
 &= \dim((\Phi w \circ \circ \Phi v^{-1})[v]) \\
 &= \dim(\Phi(A(\Phi v^{-1}(v)))) \\
 &= \dim(\Phi_w(A(\mathcal{O}^n))) \\
 &= \dim(\Phi_w(\text{im} A)) \\
 \Rightarrow \dim(\text{im} A) &= \dim(\text{im} A)
 \end{aligned}$$

Dokazali smo tudi, da je $\text{im} A = \Phi_w(\text{im} A)$. Φ_w je izomorfizem, zato je $\text{im} A \cong \text{im} A$ □

□

Posledica. Ekvivalentni matriki imata enak rang. To je rang linearne preslikave, ki ji pripadata.

Posledica. Množenje matrike z obrnljivo matriko (z leve ali z desne) ne spremeni ranga.

Dokaz. Naj bo $B = A \cdot P$, kjer je P obrnljiva. Potem je $B = I^{-1} A \cdot P \sim A$
 $\Rightarrow \text{rang} B = \text{rang} A$ Podoben dokaz za množenje s P -jem z leve. □

Izrek. Vsaka matrika $A \in \mathcal{O}^{m \times n}$ je ekvivalentna matriki

$$A_0 = \begin{bmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & 0 \\ & & 0 & 0 \end{bmatrix} = \begin{bmatrix} I_r^{45} & O_{r \times (n-r)} \\ O_{(m-r) \times r} & O_{(r-m) \times (n-r)} \end{bmatrix}$$

za nek $r \in \{0, 1, \dots, \min\{m, n\}\}$. Pri tem je r enolično določen in velja $\text{rang} A = r$.

Dokaz. Matriko A identificiramo z linearno preslikavo

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

$$x \mapsto Ax$$

Če je $A = 0$, je A že zahtevane oblike in število $r (= 0)$ je očitno enolično določeno.

Naj bo $A \neq 0$. Potem je $\text{im} A \neq \{0\}$. Izberimo bazo $\{w_1, \dots, w_r\}$ za $\text{im} A$ in jo dopolnimo do baze $\{w_1, \dots, w_r, \dots, w_m\}$ prostora \mathcal{O}^m . V dokazu dimenzijske enačbe smo razmislili, da v \mathcal{O}^n obstaja baza $\{v_1, \dots, v_n\}$, da je $A_i = w$ za $i = 1, \dots, r$ in $A_{vi} = 0$ za $i > r$.

⁴⁵Kjer je r število enic v matriki.

Glede na ti dve bazi, preslikavi A ustreza matrika

$$A_0 = \begin{bmatrix} 1 & 0 & & 0 & 0 & \cdots & 0 \\ 0 & 1 & & 0 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots & \vdots & & \\ \vdots & \vdots & & 1 & \vdots & & \\ \vdots & \vdots & & 0 & \vdots & & \\ \vdots & \vdots & & \vdots & \vdots & & \\ 0 & 0 & & 0 & 0 & \cdots & 0 \end{bmatrix}$$

Matriki A_0 pripadata isti linearni preslikavi, zato sta ekvivalentni.

$$r = \dim(\operatorname{im} A) = \operatorname{rang} A$$

Dokazati moramo še, da je r enolično določen. Recimo, da je

$$A \sim \begin{bmatrix} I_s & O_{s \times (n-s)} \\ O_{(m-s) \times s} & O_{(m-s) \times (n-s)} \end{bmatrix} = A'$$

Dokažimo, da je $\operatorname{im} B = \operatorname{Lin}\{B^{(1)}, \dots, B^{(n)}\}$ za vsako matriko $B \in \mathcal{O}^{m \times n}$.

Če je $y \in \operatorname{im} B$, potem je $Bx = y$ za nek $x \in \mathcal{O}^n$. x razvijemo po standardni bazi

$$\begin{aligned} x &= \\ &= \alpha_1 e_1 + \cdots + \alpha_n e_n \\ &\Rightarrow y = Bx \\ &= \alpha_1 B e_1 + \cdots + \alpha_n B e_n \\ &= \alpha_1 B^{(1)} + \cdots + \alpha_n B^{(n)} \\ &\in \operatorname{Lin}\{B^{(1)}, \dots, B^{(n)}\} \end{aligned}$$

Obratno, naj bo $y \in \operatorname{Lin}\{B^{(1)}, \dots, B^{(n)}\}$. Potem je

$$\begin{aligned} y &= \\ &= \alpha_1 B^{(1)} + \cdots + \alpha_n B^{(n)} \\ &= \alpha_1 B e_1 + \cdots + \alpha_n B e_n \\ &= B(\alpha_1 e_1 + \cdots + \alpha_n e_n) \\ &\in \operatorname{im} B \end{aligned}$$

V našem primeru je $\operatorname{im} A' = \operatorname{Lin}\{e_1, \dots, e_s\} \cong O^s$

$$\Rightarrow \operatorname{rang} A' = s$$

$$A' \sim A \Rightarrow \operatorname{rang} A' = \operatorname{rang} A = r$$

□

Hkrati smo dokazali še trditev.

Trditev. Slika vsake matrike je enaka linearni ogrinjači njenih stolpcev.

Posledica. Dve matriki $A, B \in \mathcal{O}^{m \times n}$ sta ekvivalentni natanko takrat, ko imata isti rang.

Dokaz.

\Rightarrow že vemo

\Leftarrow : Naj bo $r = \text{rang} A = \text{rang} B$. Potem je $A \sim \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ in $B \sim \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$. Po tranzitivnosti (in simetričnosti) ekvivalentnosti je $A \sim B$. \square

Lema:

Če je $A \in \mathcal{O}^{n \times n}$ obrnljiva matrika, je tudi A^T transponirana in velja $(A^T)^{-1} = (A^{-1})^T$.

Dokaz.

$$\begin{aligned} AA^{-1} &= A^{-1}A = I \\ (A^{-1})^T &= A^T(A^{-1})^T = I^T = I \end{aligned}$$

A^T je obrnljiva in $(A^T)^{-1} = (A^{-1})^T$ \square

Posledica. Za vsako matriko $A \in \mathcal{O}^{m \times n}$ je $\text{rang} A^T = \text{rang} A$ (in $A^T \sim A$)

Dokaz.

$$\begin{aligned} Q^{-1}AP &= \begin{bmatrix} I_r & O_{r \times (n-r)} \\ O_{(m-r) \times r} & O_{(m-r) \times (n-r)} \end{bmatrix} \\ ((PT)^{-1})^{-1} &= P^T A^T (Q^{-1})^T = \begin{bmatrix} I_r & O_{r \times (m-r)} \\ O_{(n-r) \times r} & O_{(n-r) \times (m-r)} \end{bmatrix} \Rightarrow \\ \Rightarrow A^T &\sim \begin{bmatrix} I_r & O_{r \times (m-r)} \\ O_{(n-r) \times r} & O_{(n-r) \times (m-r)} \end{bmatrix} \\ \Rightarrow \text{rang} A^T &= \text{rang} A \end{aligned}$$

Če je $m = n$, dobimo tudi

$$A^T \sim \begin{bmatrix} I_r & O_{r \times (n-r)} \\ O_{(n-r) \times r} & O_{(n-r) \times (n-r)} \end{bmatrix}$$

\square

Posledica. Naj bo $A \in \mathcal{O}^{m \times n}$ poljubna matrika. Naslednja števila so enaka:

- maksimalno število linearno neodvisnih vrstic matrike A
- maksimalno število linearno neodvisnih stolpcev
- $\text{rang} A$

Dokaz. $r_v(A)$ naj bo število iz (a), $r_S(A)$ pa število iz (b). Vemo, da je $\text{im}A = \text{Lin}\{A^{(1)}, \dots, A^{(n)}\}$

Vzemimo $r_S(A)$ stolpcev matrike A , ki so linearno neodvisni.

$\{A^{(1)}, \dots, A^{(n)}\}$ je ogródje za $\text{im}A$. Če izbrani stolpci ne bi bili baza za $\text{im}A$, bi jih s preostalimi stolpci lahko dopolnili do baze za $\text{im}A$, To pa je v protislovju z maksimalnostjo števila $r_S(A)$.

Torej izbrani stolpci tvorijo bazo za $\text{im}A$.

$$\Rightarrow r_S(A) = \text{rang}A$$

Na enak način je $r_S(A) = \text{rang}A^T = \text{rang}A = r_V(A)$ □

Definirajmo posebne vrste obrnljivih matrik:

1. $p, q \in \{1, \dots, n\}, p \neq q$ $P_{p,q}$ naj bo matrika, ki jo dobimo tako, da v I_n (identiteta $n \times n$) zamenjamo p -ti in q -ti stolpec.

Množenje s $P_{p,q}$ z desne zamenja p -ti in q -ti stolpec matrike A .

Množenje s $P_{p,q}$ z leve zamenja p -to in q -to vrstico.

$$\begin{bmatrix} 1 & & & & & & & & & & & & & & & & 0 \\ & \ddots & & & & & & & & & & & & & & & \\ & & 1 & & & & & & & & & & & & & & \\ & & & 0 & & & & & 1 & & & & & & & & \\ & & & & 1 & & & & & & & & & & & & \\ & & & & & \ddots & & & & & & & & & & & \\ & & & & & & 1 & & & & & & & & & & \\ & & & & 1 & & & 0 & & & & & & & & & \\ & & & & & & & & 1 & & & & & & & & \vdots \\ & & & & & & & & & \ddots & & & & & & & 0 \\ & & & & & & & & & & \ddots & & & & & & 1 \end{bmatrix}$$

2. za $\alpha \in \mathcal{O} \setminus \{0\}$ in $p \in \{1, \dots, n\}$ definiramo

$$P_{p,q} = \begin{bmatrix} 1 & & & & & & & & & & & & & & & & \\ & \ddots & & & & & & & & & & & & & & & \\ & & 1 & & & & & & & & & & & & & & \\ & & & \alpha & & & & & & & & & & & & & \\ & & & & \ddots & & & & & & & & & & & & \\ & & & & & & 1 & & & & & & & & & & \\ & & & & & & & & & & & & & & & & 1 \end{bmatrix}$$

$P_{p,q}$ je obrnljiva in $(P_{p,q})^{-1} = P_{p,\alpha^{-1}}$

$$\begin{aligned}
AP_{p,q} &= \\
&= A \begin{bmatrix} e_1, \dots, e_{p-1}, \alpha e_p, e_{p+1}, \dots, e_n \end{bmatrix} \\
&= \begin{bmatrix} Ae_1, \dots, Ae_{p-1}, \alpha Ae_p, Ae_{p+1}, \dots, Ae_n \end{bmatrix} \\
&= \begin{bmatrix} A^{(1)}, \dots, \alpha A^{(p)}, A^{(p+1)}, \dots, A^{(n)} \end{bmatrix}
\end{aligned}$$

Množenje s $P_{p,\alpha}$ z desne p - ti stolpec matrike A pomnoži z α .

Množenje s $P_{p,\alpha}$ z leve p - to vrstico matrike A pomnoži z α .

3.

$$E_{p,q} = \begin{bmatrix} & & \\ & 1 & \\ & & \end{bmatrix} \text{ je elementarna matrika}$$

Naj bo $p \neq q$ in $\alpha \in \mathcal{O}$. Definirajmo $P = I + \alpha E_{p,q}$.

Ker je $p \neq q$, je $E_{p,q} = 0$

$$\begin{aligned}
&\Rightarrow (I + \alpha E_{p,q})(I - \alpha E_{p,q}) = 1 \\
&\Rightarrow I + \alpha E_{p,q}
\end{aligned}$$

je obrnljiva in

$$(I + \alpha E_{p,q})^{-1}$$

$$\begin{aligned}
A(I + \alpha E_{p,q}) &= \\
&= A + \alpha A E_{p,q} \\
&= [A^{(1)}, \dots, A^{(n)}] + \alpha A [0, 0, \dots, e_p, \dots, 0] \\
&= [A^{(1)}, \dots, A^{(n)}] + [0, \dots, 0, \alpha A e_p, 0 \dots, 0] \\
&= [A^{(1)}, \dots, A^{(q-1)}, A^{(q)} + \alpha A^{(p)}, A^{(q+1)}, \dots, A^{(n)}]
\end{aligned}$$

Množenje z $I + \alpha E_{p,q}$ z desne q - temu stolpcu matrike A prišteje α - kratnik p - tega stolpca matrike A .

Množenje z $I + \alpha E_{p,q}$ z leve p - ti vrstici matrike A prišteje α - kratnik q - te vrstice matrike A .

$$(E_{p,q})^T = E_{q,p}$$

Izrek. Z uporabo množenj z matrikami 1), 2), 3) lahko iz matrike A postopoma prideltamo matriko $A_0 = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$, kjer je $r = \text{rang} A$


Dokaz. Denimo, da imamo na k -tem koraku ($0 \leq k \leq \min\{m, n\}$) matriko $\begin{bmatrix} I_k & 0 \\ 0 & A \end{bmatrix}$ za neko matriko $A' \in \mathcal{O}^{(m-k) \times (n-k)}$

Če je $A' = 0$, smo končali.

Sicer ima A' nek neničelni člen. Zamenjamo ustrezni vrstici in stolpca, da je ta člen v prvem stolpcu in prvi vrstici A' .

Nato prvo vrstico A' delimo s tem členom, da dobimo $a'_{11} = 1$

Od vrstic matrike odštejemo ustrezen večkratnik prve vrstice, da dobimo ničle v prvem stolpcu. Enako naredimo na stolpcih, da dobimo ničle v prvi vrstici matrike A' .

Dobimo $\begin{bmatrix} I_{k+1} & \\ & A'' \end{bmatrix}$ za nek $A \in \mathcal{O}^{(n-k-1) \times (n-k-1)}$ in ponovimo postopek. 

Postopek se po končno korakih konča in na vsakem koraku se rang ohranja, ker so matrike v primerih 1), 2), 3) obrnljive. \square

6.4 Sistem linearnih enačb

Radi bi rešili sistem enačb:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + a_{m3}x_3 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

kjer so b_i in a_{ij} dani elementi iz obsega \mathcal{O} , x_1, \dots, x_n pa neznanke.

Zanima nas, kdaj je sistem rešljiv, koliko je rešitev in kako jih dobimo.

Definirajmo matriko koeficientov sistema $A = [a_{ij}]_{1 \leq i \leq m, 1 \leq j \leq n}$, vektor desnih strani $b =$

$\begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$ in vektor neznank $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$. Potem je sistem ekvivalenten enačbi $Ax = b$.

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ \vdots \\ b_m \end{bmatrix}$$

Sistem $Ax = b$ je **homogen**, če je $b = 0$,⁴⁶ sicer je **nehomogen**.

⁴⁶ $b_i = 0$ za $\forall i$

Vsak $x \in \mathcal{O}^n$, za katerega je $Ax = b$, je rešitev sistema $Ax = b$.

Sistem $Ax = b$ je **neprotisloven**, kadar je množica njegovih rešitev neprazna. Sicer je **protisloven**.

Matriko A identificiramo s preslikavo

$$\begin{aligned} A : \mathcal{O}^n &\rightarrow \mathcal{O}^m \\ x &\mapsto Ax \end{aligned}$$

Homogen sistem $Ax = 0$ je vedno neprotisloven. Vse rešitve sistema $Ax = 0$ pa tvorijo natanko jedro matrike/ preslikave A .

Sistem $Ax = 0$ ima torej samo eno rešitev ($x = 0$), natanko takrat ko je $\ker A = \{0\}$

Spomnimo se dimenzijske enačbe:

$$\dim(\ker A) + \text{rang} A = n$$

Vedno je $\text{rang} A \leq n$. Sistem $Ax = 0$ ima samo trivialno rešitev.

$x = 0 \Leftrightarrow \text{rang} A = n$. V posebnem primeru mora biti $m \geq n$, kar pomeni, da je več enačb neznanck. Lahko pa se zgodi, da je $m \leq n$ ($\text{im}(\text{rang} A) < n$), da rešitev ni trivialna.

V splošnem je rešitev sistema $Ax = 0$ vektorski podprostor prostora \mathcal{O}^n razsežnosti $n - \text{rang} A$.

Kaj pa nehomogen sistem?

Definiramo razširjeno matriko sistema:

$$\hat{A} = \left[\begin{array}{c|c} A & b \end{array} \right] \text{ matrika z vektorjem desnih strani}$$

Sistem $Ax = b$ je neprotisloven $\Leftrightarrow \exists x \in \mathcal{O}^n : Ax = b \Leftrightarrow b \in \text{im} A$.

Izrek. Kronecker - Cappelijev izrek:

Sistem $Ax = b$ je neprotisloven $\Leftrightarrow \text{rang} \hat{A} = \text{rang} A$

Dokaz.

(\Rightarrow)

$$\begin{aligned} b \in \text{im} A &\Rightarrow \\ &\Rightarrow b \in \text{Lin}\{A^{(1)}, \dots, A^{(n)}\} \\ &\Leftrightarrow \text{rang} \hat{A} \\ &= \dim\{A^{(1)}, \dots, A^{(n)}, b\} \\ &= \dim\{A^{(1)}, \dots, A^{(n)}\} \\ &\Rightarrow \text{rang} A \end{aligned}$$

□

Trditev. Če je sistem $Ax = b$ neprotisloven in je x neka rešitev tega sistema, ki ji pravimo **partikularna rešitev**, potem je množica rešitev sistema enaka $x + \ker A = \{x + y; y \in \ker A\}$

$$\begin{aligned} x + \ker A &= \\ &= \{x + y; y \in \ker A\} \end{aligned}$$

To je **afin podprostor**.⁴⁷

Dokaz. Naj bo z rešitev sistema $Az = b$

$$\begin{aligned} \Rightarrow Az &= b \\ -Ax &= b \\ A(z - x) &= 0 \\ \Rightarrow z - x &\in \ker A \\ z &= x + (z - x) \in x + \ker A \end{aligned}$$

Obratno, če je $z \in x + \ker A$, potem obstaja $y \in \ker A$, da je

$$z = x + y$$

$$\begin{aligned} \Rightarrow Az &= \\ &= A(x + y) \\ &= Ax + Ay \\ &= b + 0 \\ &= b \end{aligned}$$

□

Sistem $Ax = b$ običajno rešujemo z Gaussovo eliminacijo:

$Ax = b, P \in \mathcal{O}^{m \times m}$ obrnljiva matrika

\Rightarrow sistem $Ax = b$ je ekvivalenten sistemu $PAx = Pb$

Rešitve sistema z razširjeno matriko $\hat{A} = \left[\begin{array}{c|c} A & b \end{array} \right]$ so torej enake rešitvam sistema, ki ustreza razširjeni matriki $P \cdot \hat{A} = \left[\begin{array}{c|c} PA & Pb \end{array} \right]$. Če torej z leve razširjeno matriko pomnožimo s poljubno obrnljivo matriko, se rešitev sistema ne spremeni.

Rešitve sistemov, ki ustrezajo razširjenima matrikama $\left[\begin{array}{c|c} A & b \end{array} \right]$ in $\left[\begin{array}{c|c} PA & Pb \end{array} \right]$, sta enaki, če je P obrnljiva matrika. Za P lahko vzamemo matrike, ki smo jih uporabljali pri računanju ranga. Če na vrsticah razširjene matrike $\hat{A} = \left[\begin{array}{c|c} A & b \end{array} \right]$ opravljamo enake operacije kot pri računanju ranga, se torej rešitev sistema ne spremeni. Lahko tudi zamenjamo dva

⁴⁷Jedro, premaknjeno za vektor x .

stolpca matrike A^{48} , vendar moramo v tem primeru zamenjati tudi ustrezne neznanke.

S temi operacijami lahko matriko \hat{A} prevedemo do matrike

$$\left[\begin{array}{ccc|ccc} 1 & & & * & & \\ & \ddots & & * & & \\ & & 1 & * & & \\ & & & * & & \\ & & 0 & * & & \\ & & & 0 & & \end{array} \right]$$

Enic je toliko kolikor je $\text{rang} A' = \text{rang} A$. Naj bo (x'_1, \dots, x'_n) permutacija spremenljivke (x_1, \dots, x_n) , ki jo dobimo s pomočjo operacij, ki smo jih naredili na stolpcih matrike A . Dobimo nov sistem $A'x' = b'$, ki je ekvivalenten prvotnemu. Ob upoštevanju permutacije spremenljivke sta rešitvi sistemov $Ax = b$ in $A'x' = b'$ enaki.

$$\begin{aligned} x'_1 + a'_{1,r+1}x'_{r+1} + \dots + a'_{1n}x'_n &= b'_1 \\ x'_2 + a'_{2,r+1}x'_{r+1} + \dots + a'_{2n}x'_n &= b'_2 \\ &\vdots \\ x'_r + a'_{r,r+1}x'_{r+1} + \dots + a'_{rn}x'_n &= b'_r \\ &0 = b'_{r+1} \\ &\vdots \\ &0 = b'_m \end{aligned}$$

Ta sistem je rešljiv natanko takrat, ko je $b'_{r+1} + \dots + b'_m = 0$. To se vidi tudi iz *Kronecker - Capellijevega izreka*, saj je natanko v tem primeru $\text{rang} \hat{A}' = \text{rang} A'$, oz. $\text{rang} \hat{A} = \text{rang} A$.

Rešitve $\alpha_1 = x'_{r+1}, \dots, \alpha_{n-r} = x'_n \in C$ so poljubni parametri.

$$\begin{aligned} x'_1 &= b'_1 - a'_{1,r+1}\alpha_1 - \dots - a'_{1n}\alpha_{n-r} \\ x'_2 &= b'_2 - a'_{2,r+1}\alpha_1 - \dots - a'_{2n}\alpha_{n-r} \\ &\vdots \\ x'_r &= b'_r - a'_{r,r+1}\alpha_1 - \dots - a'_{rn}\alpha_{n-r} \end{aligned}$$

V vektorski obliki dobimo $x' = b' - \alpha_1 v_1 - \dots - \alpha_{n-r} v_{n-r}$ za neke vektorje v_1, \dots, v_{n-r} . Vektorji v_1, \dots, v_{n-r} so natanko baza jedra matrike A' . Če med postopkom reševanja sistema nismo menjali stolpcev je $\{v_1, \dots, v_{n-r}\}$ tudi baza jedra matrike A .

Pogosto sistema ne prevedemo v obliko $\left[\begin{array}{cc|c} 1 & 0 & * \\ & & \vdots \\ 0 & & \vdots \\ & & \vdots \\ & 0 & * \end{array} \right]$, ampak v obliko

⁴⁸Stolpcev matrike \hat{A} ne smemo menjati.

$$\left[\begin{array}{ccc|c} \neq 0 & & & * \\ & \neq 0 & & \vdots \\ & & & \vdots \\ 0 & & \neq 0 & \vdots \\ & & & \vdots \\ & & & * \end{array} \right].$$

Sistem rešujemo od spodaj gor.

Naj bosta $\alpha_1, \alpha_2 \in \mathcal{O}$ poljubna parametra. Rešitev sistema je $x_3 = \alpha_1$, $x_4 = \alpha_2$, $x_2 = -2 - 2\alpha_1 + 3\alpha_2$, $x_1 = 3 + \alpha_1 + 2\alpha_2$

Včasih je treba reševati več sistemov z lastno matriko koeficientov:

$$\begin{aligned} Ax_1 &= b_1 \\ Ax_2 &= b_2 \\ &\vdots \\ Ax_n &= b_n \end{aligned}$$

V tem primeru lahko A razširimo z vsemi stolpci $\hat{A} = [A \mid b_1, b_2, \dots, b_n]$ in delamo Gaussovo eliminacijo na vrsticah. Dobimo $\hat{A} = [A' \mid b'_1, b'_2, \dots, b'_n]$, kjer je A' lepa matrika in rešimo vsak sistem

$$\begin{aligned} A'x'_1 &= b'_1 \\ &\vdots \\ A'x'_n &= b'_n \end{aligned}$$

posebej.

Poseben primer je iskanje inverza $A \cdot B = I$ natanko takrat, ko velja $A \cdot B^{(i)} = e_i$ za nek $i = 1, \dots, n$

$$e_i = \begin{bmatrix} & & 1 & & \\ & & & & \\ & & & & \\ & & & & \\ & & & & \end{bmatrix}, B = [B^{(1)}, \dots, B^{(n)}]$$

Če na matriki $[A \mid I]$ izvajamo Gaussovo eliminacijo po vrsticah in je A obrnljiva, dobimo $[I \mid B]$ kjer je $B = A^{-1}$. Če A ni obrnljiva, sistem ni rešljiv. ⁴⁹

⁴⁹Inverz ne obstaja.

6.5 Podobnost matrik

Naj bo \mathcal{A} endomorfizem prostora V . Običajno se spleča matriko z A zapisati v eni bazi prostora V : A_B^B , ne pa $A_{B_2}^{B_1}$, kjer sta B_1 in B_2 dve različni bazi. Naj bo B' še ena baza prostora V in naj bo $A' = A_{B'}^{B'}$ in $A = A_B^B$.

Naj bo $P = id_B^{B'}$ prehodna matrika iz baze B v bazo B' . Potem vemo, da je

$$\begin{aligned} A' &= \\ &= A_{B'}^{B'} \\ &= id_{B'}^B \circ A_B^B \circ id_B^{B'} \\ &= P^{-1}AP \\ &\Rightarrow A' = P^{-1}AP \end{aligned}$$

Definicija. Kvadratni matriki $A, B \in \mathcal{O}^{n \times n}$ sta podobni, kadar obstaja obrnljiva matrika $P \in \mathcal{O}^{n \times n}$, da je $B = P^{-1}AP$.

Na enak način kot v primeru ekvivalentnosti matrik dokažemo:

Trditev. Podobnost je ekvivalenčna relacija na $\mathcal{O}^{n \times n}$.

Trditev. A in B sta podobni natanko takrat, ko pripadata istemu endomorfizmu nekega n - razsežnega vektorskega prostora, morda glede na različni bazi.

Vemo, da je obrnljiva $n \times n$ matrika ekvivalentna identiteti.

Ali ji je tudi podobna?

Recimo

$$\begin{aligned} A &= P^{-1}I \cdot P \\ P^{-1}P &= I \end{aligned}$$

Edina matrika, ki je podobna identiteti, je identiteta.

Največ, kar lahko upamo je, da je matrika podobna diagonalni matriki. Videli bomo, da je to pogosto res, ne pa vedno.

A je diagonalna matrika, če je $a_{ij} = 0$ za $i \neq j$.

Definicija. Endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ se da diagonalizirati, kadar obstaja taka baza prostora V , da glede na to bazo endomorfizmu \mathcal{A} pripada diagonalna matrika.

Naj se A da diagonalizirati v bazi $B_V = \{v_1, \dots, v_n\}$ in naj bo A ustrezna diagonalna matrika. Potem velja

$$\begin{aligned} \mathcal{A}v_1 &= a_{11}v_1 \\ \mathcal{A}v_2 &= a_{22}v_2 \\ &\vdots \\ \mathcal{A}v_n &= a_{nn}v_n \end{aligned}$$

A slika vsak v_i v večkratnik tega vektorja. Takemu vektorju rečemo **lastni vektor**.

Definicija. Vektor $v \in V$ je lastni vektor endomorfizma $\mathcal{A} \in \mathcal{L}(V)$, kadar je $v \neq 0$ in obstaja $\lambda \in \mathcal{O}$, da je $\mathcal{A}v = \lambda v$.

Skalar $\lambda \in \mathcal{O}$ je lastna vrednost endomorfizma \mathcal{A} , ki pripada lastnemu vektorju v .

Lastna vrednost je z lastnim vektorjem enolično določena.

$$\begin{aligned}\mathcal{A}v &= \\ &= \lambda v_1 \mathcal{A}v = \mu v \Rightarrow \\ &\Rightarrow \lambda v = \mu v \Rightarrow \\ &\Rightarrow (\lambda - \mu)v = 0 \\ &\lambda = \mu\end{aligned}$$

Če je v lastni vektor za lastno vrednost λ , ni enolično določen, saj so npr. vsi njegovi neničelni večkratniki tudi lastni vektorji za lastno vrednost λ .

Kako dobimo lastne vrednosti in lastne vektorje?

λ je lastna vrednost $\Leftrightarrow \exists v : \mathcal{A}v \Leftrightarrow \mathcal{A}v - \lambda v = 0$ za nek $v \neq 0 \Leftrightarrow (\mathcal{A} - \lambda I)v = 0$ za nek $v \neq 0 \Leftrightarrow \ker(\mathcal{A} - \lambda I) \neq \{0\} \Leftrightarrow \mathcal{A} - \lambda I$ ni obrnljiv.

7 DETERMINANTE

1. n - linearne preslikave

Definicija. Naj bodo V_1, V_2, \dots, V_n in U vektorski prostori nad \mathcal{O} . Preslikava $\mathcal{F} : V_1 \times V_2 \times \dots \times V_n \rightarrow U$ je **n - linearna**, kadar velja: Če je $i \in \{1, \dots, n\}$ poljuben in so $v_1 \in V_1, \dots, v_n \in V_n$ poljubni vektorji, potem je preslikava $\mathcal{F}_i : V_i \rightarrow U$, definirana s predpisom $\mathcal{F}_i(x) = \mathcal{F}(v_1, \dots, v_{i-1}, x, v_{i+1}, \dots, v_n)$ linearna.

Če je $U = \mathcal{O}$ n - linearni preslikavi $\mathcal{F} : \prod_{i=1}^n V_i \rightarrow \mathcal{O}$ pravimo **n - linearni funkcional**.

Množica vseh n - linearnih preslikav $V_1 \times \dots \times V_n$ vektorski prostor za običajno seštevanje in množenje s skalarjem po točkah. Ta vektorski prostor običajno označimo z $V_1^* \otimes V_2^* \otimes \dots \otimes V_n^*$ mu rečemo **tenzorski produkt** prostorov $V_1^*, V_2^*, \dots, V_n^*$.

Elemente tega prostora imenujemo **tenzorji**. V zapisu $V_1^* \otimes \dots \otimes V_n^* \otimes \mathcal{O}, \mathcal{O}$ navadno kar spuščamo.

Definicija. Preslikava $\mathcal{F} : V^n \rightarrow U$ je **simetrična**, kadar velja $\mathcal{F}(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = \mathcal{F}(v_1, \dots, v_j, \dots, v_i, \dots, v_n)$ za vsaka i in j in za vse $v_1, v_2, \dots, v_n \in V$.

Definicija. Preslikava $\mathcal{F} : V^n \rightarrow U$ je **antisimetrična**, kadar velja $\mathcal{F}(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = -\mathcal{F}(v_1, \dots, v_j, \dots, v_i, \dots, v_n)$ za vsaka i in j in za vse $v_1, \dots, v_n \in V$.

PRIMER:

(a) Skalarni produkt v \mathbb{R}^3

$$\mathcal{F}(\vec{a}, \vec{b}) = \vec{a}\vec{b}, n = 2, \mathcal{F} : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$$

Ali je \mathcal{F} 2 - linearna (bilinearna)?

$a \in \mathbb{R}^3$ fiksiramo

$$\begin{aligned} \mathcal{F}_2(\alpha \vec{x} + \beta \vec{y}) &= \\ &= \mathcal{F}_2(\vec{a}_1, \alpha \vec{x} + \beta \vec{y}) \\ &= \alpha \vec{a}_1 x + \beta \vec{a}_1 y \\ &= \alpha \mathcal{F}(\vec{a}, \vec{x}) + \beta \mathcal{F}(\vec{a}, \vec{y}) \\ &= \alpha \mathcal{F}_2(x) + \beta \mathcal{F}_2(y) \\ &\Rightarrow \mathcal{F}_2 \text{ je linearna} \end{aligned}$$

Podobno preverimo, da je \mathcal{F} linearna v prvem faktorju.

$\Rightarrow \mathcal{F}$ je linearna, slika v $\mathbb{R} \Rightarrow$ je linearen funkcional.

Je simetrična, saj je $\mathcal{F}(\vec{a}, \vec{b}) = \vec{a}\vec{b} = \vec{b}\vec{a} = \mathcal{F}(\vec{b}, \vec{a})$

(b) Vektorski produkt

$$\mathcal{F} : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}^3 (n = 2)$$

$$\mathcal{F}(\vec{a}, \vec{b}) = \vec{a} \times \vec{b}$$

Podobno kot prej ugotovimo, da je \mathcal{F} linearna preslikava. Ni funkcional. Je antisimetrična, saj za poljubna $\vec{a}, \vec{b} \in \mathbb{R}^3$ velja $\mathcal{F}(\vec{a}, \vec{b}) = \vec{a} \times \vec{b} = -\vec{b} \times \vec{a} = -\mathcal{F}(\vec{b}, \vec{a})$

(c) Mešani produkt

$$\mathcal{F} : \mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R} (n = 3)$$

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

Če \vec{a} in \vec{b} fiksiramo je

$$\begin{aligned} \mathcal{F}_3(\alpha\vec{x} + \beta\vec{y}) &= \\ &= \mathcal{F}(\vec{a}, \vec{b}, \alpha\vec{x} + \beta\vec{y}) \\ &= [a, b, \alpha\vec{x} + \beta\vec{y}] \\ &= \alpha[\vec{a}, \vec{b}, \vec{x}] + \beta[\vec{a}, \vec{b}, \vec{y}] \\ &= \alpha\mathcal{F}(\vec{a}, \vec{b}, \vec{x}) + \beta\mathcal{F}(\vec{a}, \vec{b}, \vec{y}) \\ &= \alpha\vec{\mathcal{F}}_3(\vec{x}) + \beta\vec{\mathcal{F}}_3(\vec{y}) \end{aligned}$$

$\Rightarrow \mathcal{F}_3$ je linearna

Podobno je \mathcal{F}_3 linearna tudi v prvem in drugem faktorju \Rightarrow je 3 - linearna (trilinearna). Je trilinearen funkcional, saj slika v \mathbb{R} . Je antisimetrična, saj je $[\vec{a}, \vec{b}, \vec{c}] = -[\vec{b}, \vec{a}, \vec{c}]$ za poljubna $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$

(d) Množenje matrik

$$\mathcal{F} : \mathcal{O}^{n \times n} \times \mathcal{O}^{n \times n} \rightarrow \mathcal{O}^{n \times n}$$

$$\mathcal{F}(A, B) = A \cdot B$$

To je bilinearna preslikava in ni funkcional. Ni niti simetrična, niti antisimetrična, saj v splošnem velja $AB \neq BA$ in $AB \neq -BA$

7.0.1 Lastnosti antisimetričnih n - linearnih preslikav

Naj bo $\mathcal{F} : V^n \rightarrow V$ antisimetrična n - linearna preslikava. Potem velja:

- (a) Če je $v_i = v_j$ za neka $i \neq j$ in je $2 \neq 0$ v \mathcal{O} ⁵⁰, potem je $\mathcal{F}(v_1, \dots, v_j, \dots, v_i, \dots, v_n) = 0$

Dokaz.

$$\begin{aligned}\mathcal{F}(v_1, \dots, v_j, \dots, v_j, \dots, v_n) &= \\ &= -\mathcal{F}(v_1, \dots, v_j, \dots, v_i, \dots, v_n) \\ &\Rightarrow 2\mathcal{F}(v_1, \dots, v_i, \dots, v_i, \dots, v_n) = 0\end{aligned}$$

□

- (b) $\mathcal{F}(v_1, \dots, v_i + \alpha v_j, \dots, v_j, \dots, v_n) = \mathcal{F}(v_1, \dots, v_i, \dots, v_i, \dots, v_n)$, če $2 \neq 0$

Dokaz.

$$\begin{aligned}\mathcal{F}(v_1, \dots, v_i + \alpha v_j, \dots, v_j, \dots, v_n) &= \\ &= \mathcal{F}(v_1, \dots, v_i, \dots, v_j, \dots, v_n) + \\ &\quad \alpha \mathcal{F}(v_1, \dots, v_j, \dots, v_j, \dots, v_n) \\ &= \mathcal{F}(v_1, \dots, v_i, \dots, v_j, \dots, v_n)\end{aligned}$$

□

- (c) Če je $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \in S_n$ je $\mathcal{F}(v_{i_1}, \dots, v_{i_n}) = S(\pi)\mathcal{F}(v_1, \dots, v_n)$ za poljubne $v_1, \dots, v_n \in V$.⁵¹

Dokaz. Z indukcijo na število transpozicij v razcepu permutacije π . Če je π transpozicija, enakost sledi po definiciji antisimetričnosti.

Naj bo $\pi = \tau_1, \dots, \tau_m$ razcepna transpozicija za π . Predpostavimo, da enakost velja za vse permutacije, ki jih je mogoče zapisati kot produkt $m - 1$ transpozicij.

$\rho := \tau_2, \dots, \tau_m$, potem je $\pi = \tau \cdot \rho$. Naj bo $\rho = \begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}$. Potem je

$$\begin{aligned}\mathcal{F}(v_{i_1} \cdots v_{i_n}) &= \\ &= \mathcal{F}(v_{\pi(1)} \cdots v_{\pi(n)}) \\ &= s(\pi) \cdot \mathcal{F}(v_1 \cdots v_n)\end{aligned}$$

□

⁵⁰Obseg ni karakteristika 2.

⁵¹Če je \mathcal{F} antisimetrična n - linearna preslikava.

7.1 Definicija in lastnosti determinante

Zaenkrat predpostavimo, da obseg \mathcal{O} nima karakteristike 2.⁵² Naj bo $A \in \mathcal{O}^{n \times n}$ poljubna matrika. Mislimo si jo kot n - terico stolpcev.⁵³ Naj bo $\mathcal{F} : \mathcal{O}^{n \times n} = (\mathcal{O}^n)^n \rightarrow \mathcal{O}$ **antisimetričen n - linearen funkcional**.

$$A = [a_{ij}]_{ij=1}^n = [A^{(1)}, \dots, A^{(n)}]$$

$$\begin{aligned} \mathcal{F}(A) &= \\ &= \mathcal{F}(A^{(1)}, \dots, A^{(n)}) \\ &= \mathcal{F}(a_{11}e_1 + a_{21}e_2 + \dots + a_{n1}e_n + \dots + a_{1n}e_1 + a_{2n}e_2 + \dots + a_{nn}e_n) \\ &= \sum_{i1, \dots, 1n=1}^n a_{11}, \dots, a_{1n} \mathcal{F}(e_{i1}, \dots, e_{in}) \end{aligned}$$

Po lastnosti 1 je $\mathcal{F}(e_{i1}, \dots, e_{in}) = 0$, če je $e_{ij} = e_{ik}$ za neka $j \neq k$. Neničelne člene dobimo torej le v primeru, ko je $(i1, \dots, in)$ permutacija števil $\{1, \dots, n\}$. Označimo

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

Torej je

$$\begin{aligned} \mathcal{F}(A) &= \\ &= \sum_{\pi \in S_n} a_{\pi(1),1}, \dots, a_{\pi(n),n} \mathcal{F}(e_{\pi(1)}, \dots, e_{\pi(n)}) \\ &= \sum_{\pi \in S_n} a_{\pi(1),1}, \dots, a_{\pi(n),n} s(\pi) \mathcal{F}(e_1, \dots, e_n) \end{aligned}$$

Definicija. Naj bo \mathcal{O} poljuben obseg. Preslikavo $\det : \mathcal{O}^{n \times n} \rightarrow \mathcal{O}$, definirano s predpisom tako

$$\det A = \sum_{\pi \in S_n} s(\pi) a_{\pi(1),1}, \dots, a_{\pi(n),n} \quad ^{54}$$

imenujemo **determinanta**.

Oznaka:

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

Če je $2 \neq 0$ in je $\mathcal{F} : \mathcal{O}^{m \times n} \rightarrow \mathcal{O}$ antisimetričen n - linearni funkcional, je torej $\mathcal{F}(A) = (\det A) \cdot \mathcal{F}(I)$ za vsak $A \in \mathcal{O}^{m \times n}$.

⁵² $2 \neq 0$

⁵³Identificiramo $\mathcal{O}^{n \times n} = (\mathcal{O}^n)^n$

⁵⁴Kjer je $A = [a_{ij}]$.

Trditev. Če je $A = [a_{ij}]$ je $\det A = \sum_{\rho \in S_n} s(\rho) a_{1,\rho(1)}, \dots, a_{n,\rho(n)}$

Dokaz.

$$\begin{aligned} \sum_{\rho \in S_n} s(\rho) a_{1,\rho(1)}, \dots, a_{n,\rho(n)} &= \\ &= \sum_{\pi \in S_n} s(\pi^{-1}) a_{\pi(1),1}, \dots, a_{\pi(n),n} \\ &= \det A \end{aligned}$$

□

Posledica.

$$\det(A^T) = \det A$$

Lema. Determinanta je antisimetričen, n - linearen funkcional.

Dokaz. Zaradi simetrije zadošča dokazati linearnost prvega stolpca in razmisliti, kaj se zgodi, če zamenjamo prva dva stolpca:

$$\begin{aligned} \det(\alpha u + \beta v, A^{(1)} \dots A^{(n)}) &= \\ &= \sum_{\pi \in S_n} s(\pi) (\alpha u \pi(1) + \beta v \pi(1)) a_{\pi(2)}, \dots, a_{\pi(n)} \\ &= \alpha \det(u, A^{(2)}, \dots, A^{(n)}) + \beta \det(v, A^{(2)}, \dots, A^{(n)}) \end{aligned}$$

\Rightarrow Podobno velja linearnost v ostalih stolpcih $\Rightarrow \mathcal{F}$ je n - linearen.

Naj bo $B = [b_{ij}]$ matrika, ki jo dobimo tako, da v A zamenjamo prva dva stolpca. Potem je

$$\det B = \sum s(\pi) b_{\pi(1)}, \dots, b_{\pi(n)} = -\det A$$

\Rightarrow antisimetričnost

□

Posledica. Determinanta matrike se ne spremeni, če kakšnemu stolpcu prištejemo večkratnik kakšnega drugega stolpca. Če dva stolpca zamenjamo, se determinanti spremeni predznak. Če stolpec pomnožimo z α , se determinanta pomnoži z α . Enako velja za vrstice.

Dokaz. Če je $2 \neq 0$, vse to sledi iz lastnosti antisimetričnih preslikav. Za $2 = 0$ lahko študent preveri z računom. □

V posebnem primeru, ko ima matrika dve vrstici ali dva stolpca enaka, je njena determinanta enaka 0.

Determinanto lahko računamo podobno kot rang.

1. Če dve vrstici ali stolpca zamenjamo, se determinanti spremeni predznak.
2. Če vrstico ali stolpec pomnožimo z α , se determinanta pomnoži z α .
3. Če vrstici ali stolpcu prištejemo večkratnik kakšnega drugega stolpca oz. kakšne druge vrstice, se determinanta ne spremeni.

Vemo, da s pomočjo operacij 1., 2., 3., ⁵⁵ matriko A lahko prevedemo na zgornjo trikotno matriko.

$$B = \begin{bmatrix} b_{11} & & & \\ & b_{22} & & \\ & & \ddots & \\ & & & b_{nn} \end{bmatrix}$$

$\det A = c \cdot \det B$ za $c \neq 0$ ⁵⁶

$$\det B = \sum_{\pi \in S_n} b_{\pi(1),1}, \dots, b_{\pi(n),n}$$

Če je $\pi(i) > i$, potem je $b_{\pi(i),i} = 0$ in je zato tudi cel produkt 0 v zgornji vsoti, torej ostanejo le tiste permutacije, kjer je $\pi(i) \leq i$ za $\forall i$. Taka permutacija je samo identiteta $\Rightarrow \det B = b_{11}, b_{22}, \dots, b_{nn}$

Determinanta zgornje trikotne oblike je enaka produktu diagonalnih členov. Enako velja za spodnje trikotne matrike.

Posledica. $n \times n$ matrika A je obrnljiva $\Leftrightarrow \det A \neq 0$.

Dokaz. A je obrnljiva \Leftrightarrow preslikava $x \mapsto Ax, \mathcal{O}^n \rightarrow \mathcal{O}^n$ je izomorfizem.

$$\dim \mathcal{O}^n = \dim(\ker A) + \text{rang} A$$

$\Rightarrow \dim(\ker A) = 0 \Leftrightarrow \text{rang} A = n \Rightarrow$ preslikava $x \mapsto Ax$ je bijektivna \Leftrightarrow injektivna \Leftrightarrow surjektivna

$\Rightarrow A$ je obrnljiva $\Leftrightarrow \text{rang} A = n$

Vemo, da lahko s pomočjo operacij 1, 2 (kjer je $\alpha \neq 0$) in 3 matriko A prevedemo v matriko

$$A_0 = \begin{bmatrix} Ir & 0 \\ 0 & 0 \end{bmatrix}$$

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

$$\det A = c \cdot \det A_0 = \begin{cases} c \neq 0; & r = n \\ 0; & r < n \end{cases}$$

□

⁵⁵Pri čemer je $\alpha \neq 0$ v 2.

⁵⁶ c dobimo z izpostavljanjem skalarja iz vrstice.

Definicija. Naj bo $A \in \mathcal{O}^{n \times m}$ in $1 \leq k \leq \min\{m, n\}$. **Minor** reda k matrike A je determinanta podmatrike, ki jo dobimo tako, da v A izberemo k vrstic in k stolpcev, v podmatriki pa so členi na križiščih teh vrstic in stolpcev.

Členi matrike so minorji reda 1.

Determinanta $n \times n$ matrike je njen minor reda n .

Izrek. Rang neničelne matrike $A \in \mathcal{O}$ je enak najvišjemu redu neničelnega minorja te matrike.

Dokaz. Naj bo $r = \text{rang} A$. Potem v A obstaja r - linearno neodvisnih stolpcev. Naj ti stolpci tvorijo podmatriko B matrike A . $\text{Rang} B = r$, zato v B obstaja r linearno neodvisnih vrstic.

Te matrike naj tvorijo matriko C . $C \in \mathcal{O}^{n \times r}$ je ranga r , je podmatrika v A . Potem je $\det C \neq 0$ in to je neničelni minor matrike A .

Dokazati je treba še, da so vsi minorji višjih redov neničelni. Naj bo $k = r$ in predpostavimo, da v A obstaja $k \times k$ podmatrika D z determinanto $\neq 0$. D je obrnljiva, torej jo sestavljajo linearno neodvisni stolpci. Ustrezni stolpci so linearno neodvisni stolpci matrike A . Proti-slovje, saj je $k > \text{rang} A$.

\Rightarrow vsi minorji reda k v A so enaki 0. □

Izrek. Determinanta je multiplikativen funkcional.

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

za vsaki matriki $A, B \in \mathcal{O}^{n \times n}$.

Dokaz. Samo v primeru, ko je $2 \neq 0$ (primer, ko je $2 = 0$ lahko študenti preverijo z računom.)

Fiksirajmo $A \in \mathcal{O}^{n \times n}$ in definirajmo preslikavo $F : (\mathcal{O}^n)^n \rightarrow \mathcal{O}$ s predpisom $F(v_1, \dots, v_n) = \det A[Av_1, \dots, Av_n]$. To je n - linearen antisimetričen funkcional.

Ker je $2 \neq 0$ vemo, da je $F(v_1, \dots, v_n) = \det[v_1, \dots, v_n] \cdot F(e_1, \dots, e_n)$

$$e_i = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} e_i$$

Za vektorje v_i vzamemo stolpce matrike B . Dobimo $F(B^{(1)}, \dots, B^{(n)}) = \det[B^{(1)}, \dots, B^{(n)}] \cdot F(e_1, \dots, e_n)$

$$\det[AB^{(1)}, \dots, AB^{(n)}] = \det B \cdot \det[Ae_1, \dots, Ae_n]$$

□

Posledica. Če je A obrnljiva, je $\det A \neq 0$ (kar že vemo) in velja $\det(A^{-1}) = (\det A)^{-1}$

Dokaz.

$$\begin{aligned} A \cdot A^{-1} &= I \\ \det(A \cdot A^{-1}) &= \det I = 1 \\ &\parallel \\ (\det A) \cdot (\det A^{-1}) &\Rightarrow \det A^{-1} = (\det A)^{-1} \end{aligned}$$

□

Posledica. Podobni matriki imata enako determinanto.

Dokaz.

$$\begin{aligned} B &= \\ &= P^{-1}AP \\ &\Rightarrow \det B \\ &= \det(P^{-1}AP) \\ &= \det(P^{-1})(\det A) \end{aligned}$$

$$\begin{aligned} (\det P) &= \\ &= (\det P)^{-1}(\det A)(\det P) \\ &= \det A \end{aligned}$$

□

Definicija. Determinanta endomorfizma $\mathcal{A} \in \mathcal{L}(V)$ je determinanta poljubne matrike, ki pripada temu endomorfizmu. Oznaka: $\det A$. Zaradi zadnje posledice je definicija dobra.

7.2 Razvoj determinante

$$\begin{bmatrix} \vec{i} & \vec{j} & \vec{k} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{bmatrix} = \begin{bmatrix} a_2 & a_3 \\ b_2 & b_3 \end{bmatrix} \vec{i} - \begin{bmatrix} a_1 & a_3 \\ b_1 & b_3 \end{bmatrix} \vec{j} + \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix} \vec{k}$$

Naj bo $A \in \mathcal{O}^{n \times n}$, $A = [a_{ij}] = [A^{(1)}, \dots, A^{(n)}]$. Naj bosta $i, j \in \{1, \dots, n\}$ poljubna. Z A_{ij} označimo podmatriko matrike A , ki jo dobimo tako, da iz A odstranimo i -to vrstico in j -ti stolpec.

$\tilde{a}_{ij} = (-1)^{i+j} \cdot \det A_{ij}$: poddeterminanta matrike A



$\tilde{A}_{ij} = [a_{ij}]_{i,j=2}^n$: prirejenka matrike A : to je matrika poddeterminant

Izrek. Naj bo $A \in \mathcal{O}^{n \times n}$ poljubna matrika. Potem velja:

- razvoj po i -ti vrstici:

$$a_{i1}\tilde{a}_{i1} + a_{i2}\tilde{a}_{i2} + \cdots + a_{in}\tilde{a}_{in} = \det A \quad \forall i$$

- razvoj po j -tem stolpcu

$$a_{1j}\tilde{a}_{1j} + a_{2j}\tilde{a}_{2j} + \cdots + a_{nj}\tilde{a}_{nj} = \det A \quad \forall j$$

Dokaz. Zaradi enakosti $\det A = \det A^T$ zadošča dokazati formulo za razvoj po stolpcih.

Najprej dokažemo v posebnem primeru, ko je $A^{(j)} = e_j$:

$$\begin{aligned} \det A &= \\ &= \det[A^{(1)}, \dots, A^{(j-1)}, e_j, A^{(j+1)}, \dots, A^{(n)}] \\ &= \sum_{\pi \in S_n} s(\pi) a_{\pi(1),1} \cdots a_{\pi(n),n} \\ &= \sum_{\pi \in S_n} s(\pi) a_{\pi(1),1} \cdots a_{\pi(j-1),j-1} \cdot 1 \cdot a_{\pi(j+1),j+1} \cdots a_{\pi(n),n} \\ &= \sum s(\pi) a_{\pi(1),1} \cdots a_{\pi(j-1),j-1} \cdot a_{\pi(j+1),j+1} \cdots a_{\pi(n),n} \\ &= \det A_{jj} \end{aligned}$$

Formulo sedaj dokažemo v primeru, ko je $A^{(j)} = e_i$. Potem je

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

Splošen primer:

$$\begin{aligned} \det A &= \\ &= \det[A^{(1)}, \dots, A^{(n)}] \\ &= \det[A^{(1)}, \dots, A^{(j-1)}, \sum_{i=1}^n a_{ij} e_i, A^{(j+1)}, \dots, A^{(n)}] \\ &= \sum_{i=1}^n a_{ij} \det[A^{(1)}, \dots, A^{(j-1)}, e_i, A^{(j+1)}, \dots, A^{(n)}] \\ &= \sum_{i=1}^n a_{ij} \tilde{a}_{ij} \end{aligned}$$

□

Izrek. Za vsako matriko $A \in \mathcal{O}^{n \times n}$ velja $A \cdot \tilde{A}^T = \tilde{A}^T \cdot A = \det(A) \cdot I$

Dokaz. Za vsak i velja:

$$a_{i1}\tilde{a}_{i1} + a_{i2}\tilde{a}_{i2} + \cdots + a_{in}\tilde{a}_{in} = \det A$$

in

$$a_{1i}\tilde{a}_{1i} + a_{2i}\tilde{a}_{2i} + \cdots + a_{ni}\tilde{a}_{ni} = \det A$$

To pomeni: Diagonalni elementi matrik $A\tilde{A}^T$ in $\tilde{A}^T A$ so enaki $\det A$.

Dokazati moramo še, da so vsi izvendiagonalni členi matrik $A\tilde{A}^T$ in $\tilde{A}^T A$ enaki 0.

Naj bosta i in j različna. Potem je

$$\begin{aligned} 0 &= \\ &= \det[A^{(1)}, \dots, A^{(i)}, \dots, A^{(i)}, \dots, A^{(n)}] \\ &= \sum_{k=1}^n a_{ki}\tilde{a}_{kj} \end{aligned}$$

(razvoj po j -tem stolpcu)

To velja za vsaka različna i in j , torej je $\tilde{A}^T A = \begin{bmatrix} \det & & 0 \\ & \ddots & \\ 0 & & \det \end{bmatrix} = (\det A) \cdot I$ Podobno

dobimo $A\tilde{A}^T = (\det A) \cdot I$ □

Posledica. Če je $\det A \neq 0$, potem je A obrnljiva (kar že vemo) in velja

$$A^{-1} = \frac{1}{\det A} \tilde{A}^T$$

7.2.1 Uporaba pri reševanju sistemov

Imejmo sistem $Ax = b$, kjer je $A \in \mathcal{O}^{n \times n}$ kvadratna matrika in $b \in \mathcal{O}^n$. Ta sistem je enolično rešljiv natanko takrat, ko je A obrnljiva. Takrat je rešitev $x = A^{-1}b = \frac{1}{\det A} \tilde{A}^T \cdot b$

Naj bo $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ in j -ti člen vektorja $\frac{1}{\det A} \tilde{A}^T b$ označimo z $\frac{1}{\det A} (\tilde{A}^T b)_j$. Potem je

$$\begin{aligned} x_j &= \\ &= \frac{1}{\det A} (\tilde{A}^T b)_j \\ &= \frac{1}{\det A} \sum_{k=1}^n \tilde{a}_{kj} b_k \\ &= \frac{1}{\det A} \cdot \det[A^{(1)}, \dots, A^{(j-1)}, b, A^{(j+1)}, \dots, A^{(n)}] \end{aligned}$$

Izrek. Cramejeva formula

Če je $A \in \mathcal{O}^{n \times n}$ in $b \in \mathcal{O}^n$, potem je sistem $Ax = b$ enolično rešljiv natanko takrat, ko je $\det A \neq 0$. Takrat je rešitev podana s predpisi $x_j = \frac{\det[A^{(1)}, \dots, A^{(j-1)}, b, A^{(j+1)}, \dots, A^{(n)}]}{\det A}$ za

$$j = 1, \dots, n, \text{ kjer je } x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

8 STRUKTURA ENDOMORFIZMOV

Definicija. Neničelni vektor $v \in V$ je lastni vektor endomorfizma $\mathcal{A} \in \mathcal{L}(V)$, kadar obstaja $\lambda \in \mathcal{O}$, da je $Av = \lambda v$. λ se imenuje lastna vrednost endomorfizma \mathcal{A} , ki pripada lastnemu vektorju v .

Trditev. Naj bo $\lambda \in \mathcal{O}$ lastna vrednost endomorfizma $\mathcal{A} \in \mathcal{L}(V)$. Potem je množica $\{v \in V : Av = \lambda v\} = \{\text{lastni vektorji, ki pripadajo lastni vrednosti } \lambda\} \cup \{0\}$

Razsežnost ali dimenzija tega lastnega podprostora se imenuje **geometrična večkratnost** lastne vrednosti λ .

Dokaz.

$$\begin{aligned} \{v \in V; Av = \lambda v\} &= \\ &= \{v \in V; (A - \lambda \text{id}_V)v = 0\} \\ &= \ker(A - \lambda \text{id}_V)^{57} \end{aligned}$$

□

Trditev. Naj bo V neničeln vektorski prostor.⁵⁸ Endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ se da diagonalizirati natanko takrat, ko v V obstaja baza, sestavljena iz lastnih vektorjev endomorfizma \mathcal{A} .

Dokaz.

(\Rightarrow) če diagonalna matrika $A = [a_{ij}]$ pripada endomorfizmu \mathcal{A} glede na bazo $B = \{v_1, \dots, v_n\}$, potem za vsak i velja $Av_i = a_{ii}v_i$

(\Leftarrow) če je $\{u_1, \dots, u_n\}$ baza iz lastnih vektorjev, potem obstajajo $\lambda_1, \dots, \lambda_n \in \mathcal{O}$, da je $Au_i = \lambda_i u_i$ za vsak i . Potem endomorfizmu \mathcal{A} glede na bazo B pripada matrika $A =$

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

□

Posledica. Endomorfizem $\mathcal{A} \in \mathcal{L}(V)$, kjer je $\dim V = n$, se da diagonalizirati natanko takrat, ko ima A n linearno neodvisnih vektorjev.

Trditev. Naj bo $\mathcal{A} \in \mathcal{L}(V)$ in naj bodo $\lambda_1, \dots, \lambda_n$ paroma različne vrednosti endomorfizma \mathcal{A} , v_1, \dots, v_m pa pripadajoči lastni vektorji. Potem so v_1, \dots, v_m linearno neodvisni.

Dokaz. Predpostavimo, da so v_1, \dots, v_m linearno odvisni. $v_1 \neq 0$, zato je $m > 1$.

Obstaja najmanjši k , da je v_k linearna kombinacija vektorjev z manjšimi indeksi.

$$v_k = \sum_{i=1}^{k-1} \alpha_i v_i \quad (*)$$

⁵⁷Jedro je vedno vektorski prostor

⁵⁸Ker ničelni vektorski prostori nimajo baze.

Na tej enakosti uporabimo A :

$$Av_k = A\left(\sum_{i=1}^{k-1} \alpha_i v_i\right) = \sum_{i=1}^{k-1} \alpha_i Av_i$$

Upoštevamo, da so v_i lastni vektorji za lastne vrednosti λ_i :

$$\lambda_k v_k : \sum_{i=1}^{k-1} \alpha_i \lambda_i v_i$$

Enačbi odštejemo

$$\sum_{i=1}^{k-1} \alpha_i (\lambda_i - \lambda_k) v_i = 0 \quad (**)$$

Ker je $v_k \neq 0$, je $\alpha_i \neq 0$ za vsaj en $i = 1, \dots, k-1$. $\lambda_i - \lambda_k \neq 0$. V vsoti $(**)$ je zato vsaj eden od koeficientov pred vektorji v_i neničeln. Zato so v_1, \dots, v_{k-1} linearno odvisni.

To je v protislovju z minimalnostjo k -ja $\Rightarrow v_1, \dots, v_m$ so linearno neodvisni. \square

Posledica. Naj bo $\dim V = n$ in $A \in \mathcal{L}(V)$. Če ima A n paroma različnih lastnih vrednosti, se da diagonalizirati.

8.1 Karakteristični in minimalni polinom

$A \in \mathcal{L}(V)$. Kako poiščemo lastne vrednosti (in lastne vektorje?) A naj bo matrika endomorfizma \mathcal{A} glede na neko bazo. λ je lastna vrednost endomorfizma

$$\begin{aligned} A &\Leftrightarrow \\ &\Leftrightarrow \exists v (\neq 0) \in V : Av = \lambda v \\ &\Leftrightarrow \exists x \in \mathcal{O}^n; x \neq 0 : Ax = \lambda x \\ &\Leftrightarrow \exists x \in \mathcal{O}^n; x \neq 0 : Ax - \lambda Ix = 0 \\ &\Leftrightarrow \exists x \in \ker(A - \lambda I) \setminus \{0\} \\ &\Leftrightarrow \ker(A - \lambda I) \neq \{0\} \\ &\Leftrightarrow A - \lambda I \text{ ni obrnljiva} \\ &\Leftrightarrow \det(A - \lambda I) = 0 \end{aligned}$$

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

$$\begin{aligned} &= \det \begin{bmatrix} a_{11} - \lambda & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - \lambda & \cdots & a_{2n} \\ \vdots & & \ddots & \\ a_{n1} & \cdots & \cdots & a_{nn} - \lambda \end{bmatrix} \\ &= \sum_{\pi \in S_n} s(\pi) (a_{\pi(1),1} - \lambda \delta_{\pi(1),1}) \cdots (a_{\pi(n),n} - \lambda \delta_{\pi(n),n}) \end{aligned}$$

To je polinom stopnje največ n v spremenljivki λ . n - krat dobimo λ v produkt $(a_{\pi(1),1} - \lambda \delta_{\pi(1),1}) \cdots (a_{\pi(n),n} - \lambda \delta_{\pi(n),n})$

$$\Leftrightarrow \pi(i) = i \text{ za vsak } i \Leftrightarrow \pi = id$$

Zato je $\det(A - \lambda I)$ polinom stopnje n in njegov vodilni koeficient je enak $(-1)^n$

Definicija. Naj bo $A \in \mathcal{O}^{n \times n}$. Polinom $\det(A - \lambda I)$ se imenuje *karakteristični polinom* matrike A . Oznaka: $\Delta_A(\lambda)$

Trditev. Podobni matriki imata enak karakteristični polinom.

Dokaz. $B = P^{-1}AP$, P obrnljiva.

$$\begin{aligned} \Leftarrow \Delta_B(\lambda) &= \\ &= \det(B - \lambda I) \\ &= \det(P^{-1}AP - \lambda I) \\ &= \det(P^{-1}AP - \lambda P^{-1}P) \\ &= \det(P^{-1}(A - \lambda I)P) \\ &= \det(A - \lambda I) \\ &= \Delta_A(\lambda) \end{aligned}$$

□

Definicija. Karakteristični polinom endomorfizma $\mathcal{A} \in \mathcal{L}(V)$ (oznaka: $\Delta_{\mathcal{A}}(\lambda)$ je $\Delta_A(\lambda)$, kjer je A poljubna matrika, ki pripadeta endomorfizmu \mathcal{A} . Prejšnja trditev nam pove, da je definicija dobra.

Če je obseg \mathcal{O} neskončen, lahko vsak polinom $p(x) \in \mathcal{O}[x]$ identificiramo s polinomsko funkcijo $\mathcal{O} \rightarrow \mathcal{O}, a \mapsto p(a)$. Elementu $p(a)$ rečemo **vrednost** polinoma p v točki a . Če je $P(a) = 0$, potem a imenujemo **ničla polinoma** p .

Zadnjič smo dokazali:

Izrek. Lastne vrednosti endomorfizma $\mathcal{A} \in \mathcal{L}(V)$ so natanko tiste ničle karakterističnega polinoma $\Delta_{\mathcal{A}}(\lambda)$, ki ležijo v \mathcal{O} .

PRIMER:

$V = \mathbb{R}^3, \vec{a} = (1, 0, 0), A : V \rightarrow V, Ax = \vec{a} \times \vec{x}$ linearna preslikava. Za V vzamemo standardno bazo $B = (1, 0, 0), (0, 1, 0), (0, 0, 1)$. Glede na to bazo preslikavi A pripada matrika

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}$$

i in $-i$ nista lastni vrednosti preslikave A , saj ne obstaja neničelni vektor \vec{x} , za katerega je $\vec{a} \times \vec{x} = \pm i\vec{x}$

O pa je lastna vrednost z lastnim vektorjem \vec{a} .

Endomorfizem \mathcal{A} se ne da diagonalizirati, saj \mathbb{R}^3 ne vsebuje baze iz lastnih vektorjev preslikave A . $\Delta_A(\lambda)$ sicer ima 3 različne ničle, toda ne ležijo vse v \mathbb{R} in torej niso vse ničle lastnih vrednosti endomorfizma \mathcal{A} .

Odslej naprej bomo (če ne bomo rekli drugače) predpostavili, da je $\mathcal{O} = \mathbb{C}$ (in matrike z realnimi členi bomo razumeli kot kompleksne matrike). Razlog za to je **osnovni izrek algebre**:

Izrek. Vsak nekonstanten polinom s kompleksnimi koeficienti ima vsaj eno ničlo v \mathbb{C} .

(Dokaz pri analizi 2)

Posledica. Vsak nekonstanten polinom s kompleksnimi koeficienti lahko zapišemo v obliki $p(x) = a_n(X - x_1)^{k_1}(X - x_2)^{k_2} \cdots (X - x_m)^{k_m}$, kjer so x_1, \dots, x_m vse različne ničle polinoma p .

Pri tem je $k_1 + k_2 + \cdots + k_m$ enako stopnji polinoma p , ki se imenuje **red ničle** x_i .

Karakteristični polinom endomorfizma $\mathcal{A} \in \mathcal{L}(V)$ ⁵⁹ je torej oblike $\Delta_A(\lambda) = a_1(\lambda - \lambda_1)^{k_1}(\lambda - \lambda_2)^{k_2} \cdots (\lambda - \lambda_m)^{k_m}$, kjer so $\lambda_1, \dots, \lambda_m \in \mathbb{C}$ različne lastne vrednosti endomorfizma \mathcal{A} , $a = (-1)^n$, $k_1 + k_2 + \cdots + k_m = n$. Lastne vrednosti matrike $A \in \mathbb{C}^{m \times n}$ so ničle $\lambda_1, \dots, \lambda_m$ karakterističnega polinoma $\Delta_A(\lambda)$.

Množica $\{\lambda_1, \dots, \lambda_m\}$ vseh lastnih vrednosti matrike A (oz. endomorfizma \mathcal{A}) se imenuje **spekter** matrike A (oz. endomorfizma \mathcal{A}). Oznaka $\sigma(A)$.

Število k_i , ki je red ničle λ_i v $\Delta_A(\lambda)$ se imenuje **algebraična večkratnost** lastne vrednosti λ_i .

$n \times n$ matrika ima lahko največ n lastnih vrednosti, vsota njihovih algebraičnih večkratnosti pa je enaka n .

Spomnimo se: **geometrična večkratnost** lastne vrednosti λ_i je $\dim(\ker(A - \lambda_i, I))$.

⁵⁹Oziroma pripadajoče matrike $A \in \mathbb{C}^{m \times n}$

PRIMER:

$$\begin{aligned}
 0 &= \\
 &= \Delta_A(\lambda) \\
 &= \det(A - \lambda I) \\
 &= \begin{vmatrix} 1-\lambda & 1 & 1 & 1 \\ -1 & -1-\lambda & 2 & 3 \\ 0 & 0 & 2-\lambda & 2 \\ 0 & 0 & 0 & 1-\lambda \end{vmatrix} \\
 &= (1-\lambda)(2-\lambda)(\lambda^2 - 1 + 1) \\
 &= \lambda^2(\lambda - 1)(\lambda - 2)
 \end{aligned}$$

lastne vrednosti:

0 (algebraična večkratnost 2)
 1 (algebraična večkratnost 1)
 2 (algebraična večkratnost 1).

Lastni vektorji so elementi $\ker(A - \lambda I)$

$\lambda = 0$:

(zanima nas $\ker(A)$)

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & 2 & 3 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 3 & 4 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$x_1 + x_2 + x_3 + x_4 = 0 \Rightarrow x_1 = -x_2$$

$$x_3 + x_4 = 0 \Rightarrow x_3 = 0$$

$$x_4 = 0$$

Lastni podprostor $\left\{ \begin{bmatrix} -x_2 \\ x_2 \\ 0 \\ 0 \end{bmatrix}, x_2 \in \mathbb{C} \right\}$, baza za $\ker A$ je $\left\{ \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \right\}$.

Geometrična večkratnost lastne vrednosti $\lambda = 0$ je 1 (= $\dim(\ker(A))$).

$\lambda = 1$:

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ -1 & -2 & 2 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -2 & -3 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{aligned}x_1 + 2x_2 - 2x_3 - 3x_4 &= 0 \\x_2 + x_3 + x_4 &= 0 \\x_3 + 2x_4 &= 0\end{aligned}$$

Lastni podprostor $\ker(A - I) = \left\{ \begin{bmatrix} -3x_4 \\ x_4 \\ -2x_4 \\ x_4 \end{bmatrix}, x_4 \in \mathbb{C} \right\}$, baza $\left\{ \begin{bmatrix} -3 \\ 1 \\ -2 \\ 1 \end{bmatrix} \right\}$, geometrična večkratnost

lastne vrednosti $\lambda = 1$ je 1. Podobno še za $\lambda = 2$, geometrična večkratnost $\lambda = 2$ je 1.

Izrek. Matrika A se da diagonalizirati, natanko takrat, ko sta algebraična in geometrična večkratnost vsake njene lastne vrednosti enaki.

Dokaz.

(\Rightarrow) Naj bo A podobna diagonalni matriki $D = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_m \end{bmatrix}$, kjer so $\lambda_1, \dots, \lambda_m$ (ne nujno različne) lastne vrednosti matrike A .

$$\Delta_A(\lambda) = (\lambda_1 - \lambda)(\lambda_2 - \lambda) \cdots (\lambda_m - \lambda)$$

Algebraična večkratnost lastne vrednosti λ_i je število pojavitev faktorja $\lambda_i - \lambda$ v zgornjem produktu.

$$\ker(D - \lambda_i I) = \text{Lin}\{e_j; \lambda_j = \lambda_i\}$$

$$\dim(\ker(A - \lambda_i I)) = \dim(\ker(D - \lambda_i I))$$

saj je $A = P^{-1}DP$ in $A - \lambda_i I = P^{-1}(D - \lambda_i I)P$ množenje z obrnljivo matriko ohranja rang $\Rightarrow \text{rang}(A - \lambda_i I) = \text{rang}(D - \lambda_i I) \Rightarrow \dim(\ker(A - \lambda_i I)) = \dim(\ker(D - \lambda_i I)) \Rightarrow \dim(\ker(A - \lambda_i I)) = \text{število indeksov } j, \text{ za katere je } \lambda_j = \lambda_i \Rightarrow \text{algebraična in geometrična večkratnost lastne vrednosti } \lambda_i \text{ sta enaki za vsak } i$.

(\Leftarrow) Naj bo $\Delta_A(\lambda) = (-1)^n(\lambda - \lambda_1)^{k_1}(\lambda - \lambda_2)^{k_2} \cdots (\lambda - \lambda_n)^{k_n}$, kjer so $\lambda_i \neq \lambda_j$ za $i \neq j$.

Dokazati moramo, da v \mathbb{C}^n obstaja baza iz lastnih vektorjev matrike A . Po predpostavki je $k = \dim(\ker(A - \lambda_i I))$ za vsak i .

Naj bo $\{x_1, \dots, x_k\}$ baza $\ker(A - \lambda_1 I)$, $\{x_{k_1+1}, \dots, x_{k_1+k_2}\}$ baza $\ker(A - \lambda_2 I)$, \dots , $\{x_{k_1+k_2} + \dots + k_{m-1} + 1, \dots, x_{k_1+k_2+\dots+k_m}\}$ baza $\ker(A - \lambda_n I)$.

Zadošča dokazati, da je $\{ \}$ baza \mathbb{C}^n . Ker je $k_1 + \dots + k_n = n$ zadošča dokazati, da so x_1, \dots, x_n linearno neodvisni.

Predpostavimo, da je $\sum_{j=1}^n \alpha_j x_j = 0$ za nek $\alpha_j \in \mathbb{C}$. Za vsak i definiramo

$$x_i = \sum_{j=1}^{k_i} \alpha_{k_1+\dots+k_{i-1}+j} x_{k_1+\dots+k_{i-1}+j}$$

Ker je $Ax_{k_1+\dots+k_{i-1}+j} = \lambda_i x_{k_1+\dots+k_{i-1}+j}$ za vsak j , je tudi $\Delta v_i = \lambda_i v_i$ za vsak i .

Za vsak $i = 1, \dots, m$ je $Av_i = \lambda_i v_i$, $\lambda_i \neq \lambda_j$ za $i \neq j$ in $\sum_{i=1}^m v_i = 0$. Ker so λ_i paroma različni, so lastni vektorji za te lastne vrednosti linearno neodvisni.

Torej v_1, \dots, v_m niso lastni vektorji. Torej je $v_i = 0$ za vsak i .

Za vsak i torej velja:

$$\sum_{j=1}^{k_i} \alpha_{k_1+\dots+k_{i-1}} x_{k_1+\dots+k_{i-1}+j} = 0$$

Vektorji $x_{k_1+\dots+k_{i-1}}$ so baza prostora $\ker(A - \lambda_i I)$, torej so linearno neodvisni $\Rightarrow \alpha_{k_1+\dots+k_{i-1}+j} = 0$ za $\forall j = 1, \dots, k_i$, $\forall i = 1, \dots, m \Rightarrow x_1, \dots, x_n$ so linearno neodvisni. \square

Izrek (Cayley - Hamiltonov izrek). Naj bo $p(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathcal{O}[x]$ nek polinom in $A \in \mathcal{O}^{n \times n}$. Potem lahko izračunamo $a_n A^n + a_{n-1} A^{n-1} + \dots + a_1 A + a_0 I \in \mathcal{O}^{n \times n}$. To matriko označimo s $p(A)$ in imenujemo vrednost polinoma p v matriki A . Če je $p(A) = 0$ (ničelna $n \times n$ matrika), pravimo, da je A ničla polinoma p .

Izrek (Cayley - Hamiltonov izrek). Vsaka kvadratna matrika je ničla svojega karakterističnega polinoma $\Delta_A(A) = 0$

Dokaz. Prirejenka $A - \lambda I$ ima za člene polinome v λ stopnje največ $n - 1$. Označimo $B(\lambda) = (A - \lambda I)^T$. $B(\lambda)$ lahko napišemo kot vsoto matrik, kjer so vsi neničelni členi monomi iste stopnje. Najvišjo potenco λ lahko iz vsake od teh matrik v vsoti izpostavimo in dobimo $B(\lambda) = B_0 + B_1 \lambda + \dots + B_{n-1} \lambda^{n-1}$ za neke matrike $B_0, \dots, B_{n-1} \in \mathcal{O}^{n \times n}$.

Za nek $\lambda \in \mathbb{C}$ je $B(\lambda) = (A - \lambda I)^T = {}^{60}$.

Spomnimo se $(A - \lambda I)^T (A - \lambda I) = \det(A - \lambda I) I \Rightarrow (B_0 + B_1 \lambda + \dots + B_{n-1} \lambda^{n-1})(A - \lambda I) = \Delta_A(\lambda) I$ za nek $\lambda \in \mathbb{C}$

Naj bo $\Delta_A(\lambda) = a_n \lambda^n + \dots + a_1 \lambda + a_0 \Rightarrow B_0 A + (B_1 A - B_0) \lambda + \dots + (B_{n-1} A - B_{n-2}) \lambda^n = a_0 I + (a_1 \lambda) + \dots + a_n I \lambda^n$ za vsak $\lambda \in \mathbb{C}$.

Členi matrike na desni ⁶¹ v vseh kompleksnih številih ujemajo z ustreznimi členi matrike na levi. Ker je \mathbb{C} neskončen obseg, to pomeni, da sta za vsaka i in j polinoma na (i, j) - tem mestu v levi in desni matriki enaka, kar pomeni, da imata enake koeficiente. Zato so matrični koeficienti v enakosti zgoraj na levi in na desni enaki.

$$\begin{aligned} a_0 I &= B_0 A \\ a_1 I &= B_1 A \\ &\vdots \\ a_{n-1} I &= B_{n-2} A \\ a_n I &= -B_{n-1} A \end{aligned}$$

⁶⁰dopiši

⁶¹preveri

$$\begin{aligned}
a_0 I &= B_0 A \\
a_1 A &= B_1 A^2 - B_0 A \\
a_2 A^2 &= B_2 A^3 - B_1 A^2 \\
&\vdots \\
a_n A^n &= -B_{n-1} A^n
\end{aligned}$$

62

□

Posledica. Če je $A \in \mathcal{O}^{n \times n}$ obrnljiva matrika, obstaja polinom $q(x) \in \mathcal{O}[x]$, da je $A^{-1} = q(A)$. Inverz torej vedno leži v algebri, generirani z A .

Dokaz. A obrnljiva $\Rightarrow \det A \neq 0$

$$\Delta_A(\lambda) = a_n \lambda^n + \dots + a_1 \lambda + a_0 = \det(A - \lambda I) \forall \lambda \Rightarrow \Delta_A(0) = \det A = a_0 \Rightarrow a_0 \neq 0 \Rightarrow a_0 \text{ je obrnljiv}$$

Cayley - Hamiltonov izrek:

$$\begin{aligned}
a_n A^n + a_{n-1} A^{n-1} + \dots + a_1 A + a_0 I &= 0 \\
-\frac{a_n}{a_0} A^n - \frac{a_{n-1}}{a_0} A^{n-1} &= -\frac{a_1}{a_0} A - \frac{a_0}{a_0} I
\end{aligned}$$

□

Opomba: Cayley - Hamiltonov izrek smo formulirali za matrike nad \mathbb{C} in dokazali za matrike nad neskončnim obsegom. Velja pa za matrike nad poljubnim obsegom.

Cayley - Hamiltonov izrek nam med drugim pove, da za vsako matriko $A \in \mathcal{O}^{n \times n}$ obstaja vsaj en polinom iz $\mathcal{O}[x]$, ki ima A za ničlo.⁶⁴

Definicija. Minimalni polinom matrike $A \in \mathcal{O}^{n \times n}$ je polinom v $\mathcal{O}[x]$, ki ima ničlo A in vodilni koeficient 1 in je najmanjše možne stopnje med vsemi polinomi, ki imajo A za ničlo.

Trditev. Minimalni polinom matrike A je z matriko enolično določen.

Dokaz. Recimo, da sta $p(x) = x^k + a_{n-1}x^{k-1} + \dots + a_0$ in $q(x) = x^k + b_{n-1}x^{k-1} + \dots + b_0$ minimalna polinoma za A .

$$\begin{aligned}
\Rightarrow A^k + a_{n-1}A^{k-1} + \dots + a_0 I &= \\
&= A^k + (b_{n-1} - a_{n-1})A^{k-1} + \dots + (b_0 - a_0)I \\
&= (a_{k-1} - b_{k-1})A^{k-1} + (a_{k-2} - b_{k-2})A^{k-2} + \dots + (a_0 - b_0)I = 0
\end{aligned}$$

Če v zgornji vrstici niso vsi koeficienti 0, dobimo polinom stopnje $\leq k-1$, ki ima A za matriko, kar je v protislovju z minimalnostjo k - ja. Torej je $b_{k-1} = a_{k-1}, \dots, b_0 = a_0$ □

Trditev. Naj bo $A \in \mathcal{O}^{n \times n}$ in $p \in \mathcal{O}[x]$. Če je $p(A) = 0$, potem minimalni polinom matrike A (oznaka m_A) deli p .

⁶²dopiši

⁶⁴Zato je naslednja definicija smiselna.

Dokaz. Po izreku o deljenju polinomov obstajata polinoma $q, r \in \mathcal{O}[x]$, da je $p(x) = m_A(x) \cdot q(x) + r(x)$ in je stopnja polinoma r strogo manjša od stopnje m_A .
Preslikava

$$\begin{aligned} \mathcal{O}[x] &\rightarrow \mathcal{O}^{n \times n} \\ f(x) &\mapsto f(A) \end{aligned}$$

je homomorfizem kolobarjev.

\Rightarrow v prejšnjo enačbo lahko ustavimo A namesto x

$$p(A) = m_A(A) \cdot q(A) + r(A) \Rightarrow r(A) = 0$$

Ker je stopnja r manjša od stopnje m_A in je $r(A) = 0$, mora biti r ničelni polinom.
 $\Rightarrow m_A(x) | p(x)$ □

Posledica. Minimalni polinom matrik vedno deli njemu karakteristični polinom.

Trditev. Podobni matriki imata enak minimalni polinom.

Dokaz. Naj bo $B = P^{-1}AP$, kjer je P obrnljiva matrika in $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ nek polinom. Potem je

$$\begin{aligned} p(B) &= \\ &= a_n (P^{-1}AP)^n + \dots + a_1 (P^{-1}AP) + a_0 I \\ &= a_n (P^{-1}A^n P) + \dots + a_1 (P^{-1}AP) + a_0 I \\ &= P^{-1} (a_n A^n + \dots + a_1 A + a_0 I) P \\ &= P^{-1} p(A) P \end{aligned}$$

Od tod sledi, da je $p(A) = 0 \Leftrightarrow p(B) = 0$ (ker je p obrnljiva matrika.) V posebnem primeru je $m_A(B) = 0$ in $m_B(A) = 0$. Po zadnji trditvi m_A deli m_B in m_B deli m_A . Polinoma $m_A(x)$ in $m_B(x)$ imata oba vodilni koeficient 1, zato morata biti enaka. □

Zaradi te trditve je naslednja definicija dobra.

Definicija. Minimalni polinom endomorfizma $\mathcal{A} \in \mathcal{L}(V)$ (oznaka $m_{\mathcal{A}}(x)$) je minimalni polinom poljubne matrike, ki pripada temu endomorfizmu glede na neko bazo V .

Če je $p(x) = a_n x^n + \dots + a_1 x + a_0$ polinom in $A \in \mathcal{L}(V)$, lahko izračunamo $a_n A^n + \dots + a_1 A + a_0 \text{id}_V \in \mathcal{L}(V)$ (kjer je $A^k = A \circ A \circ \dots \circ A$ ⁶⁵). Ta endomorfizem označimo s $p(A)$ in ga imenujemo vrednost polinoma p in endomorfizma \mathcal{A} . Če je $p(A) = 0$ (ničelni endomorfizem), pravimo, da je A ničla polinoma p .

Trditev. Minimalni polinom $m_{\mathcal{A}}$ endomorfizma \mathcal{A} je neničelni polinom najmanjše stopnje, za katerega je $m_{\mathcal{A}}(A) = 0$ in ima vodilni koeficient 1.

⁶⁵k - krat

Dokaz. Sledi iz dejstva, da nam izbira baze B v V določa izomorfizem algeber

$$\begin{aligned}\mathcal{L}(V) &\rightarrow \mathcal{O}^{n \times n} \\ A &\mapsto A_B^B\end{aligned}$$

⁶⁶ Natančneje razmislite sami. □

Dokazali smo, da $m_A | \Delta_A$. Zato so vse ničle (v \mathbb{C}) polinoma m_A tudi ničle polinoma Δ_A .

Trditev. Vsaka ničla karakterističnega polinoma matrike je tudi ničla njenega minimalnega polinoma.

Dokaz. $\Delta_A(x), m_A(x)$ naj bosta karakteristični in minimalni polinom matrike A . Naj bo $\alpha \in \mathbb{C}$ neka ničla polinoma $\Delta_A(x)$. Potem je α lastna vrednost matrike A in obstaja $x \neq 0$, da je $Ax = \alpha x$.

Po izreku o deljenju je $m_A(x) = (x - \alpha) \cdot q(x) + m_A(\alpha)$ za nek polinom q .

V to enakost vstavimo A namesto X . Ker je preslikava $p \mapsto p(A)$ homomorfizem algeber $\mathbb{C}[X] \rightarrow \mathbb{C}^{n \times n}$, dobimo

$$\begin{aligned}m_A(A) &= (A - \alpha I) \cdot q(A) + m_A(\alpha)I \\ 0 &= (A - \alpha I)q(A) + m_A(\alpha)I \\ &= q(A)(A - \alpha I) + m_A(\alpha)I\end{aligned}$$

⁶⁷ To enakost uporabimo na lastnem vektorju x :

$$\begin{aligned}0 &= \\ &= 0 \cdot x \\ &= q(A) \cdot (A - \alpha I)x + m_A(\alpha)x \\ &= q(A)(Ax - \alpha x) + m_A(\alpha)x \\ &= m_A(\alpha)x\end{aligned}$$

⁶⁸ □

Posledica. Če je $\Delta_A(\lambda) = (-1)^n(\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_n)^{n_k}$, kjer so λ_i paroma različni, je $m_A(\lambda) = (\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_k)^{n_k}$, kjer je $1 \leq m \leq n$ za vsak i .

PRIMER:

$$\begin{aligned}A &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \\ \Delta_A(\lambda) &= \begin{bmatrix} -\lambda & 1 & 0 \\ 0 & -\lambda & 0 \\ 0 & 0 & -\lambda \end{bmatrix} = -\lambda^3 \Rightarrow m_A(\lambda) = \lambda^k \text{ za nek } k \leq 3 \\ A &\neq 0 \Rightarrow m_A(\lambda) \neq \lambda \\ A^2 &= 0 \Rightarrow m_A(\lambda) = \lambda^2\end{aligned}$$

⁶⁶ker je izomorfizem, imata hkrati ničle

⁶⁷ $m_A(A) = 0$, ker je to minimalni polinom matrike A

⁶⁸0 je $m_A(\alpha)x$ in ker je $x \neq 0$, je $m_A(\alpha) = 0$

8.2 Korenski podprostor

Definicija. Naj bo $A \in \mathcal{L}(V)$. Vektorski podprostor $W \subseteq V$ je **invarianten**, če za vsak $x \in W$ velja $Ax \in W$. Včasih pišemo tudi $A(W) \subseteq W$.

PRIMER:

1. $\{0\}, V$ sta vedno invariantna podprostora
2. $\ker A$ in $\operatorname{im} A$ sta invariantna podprostora

$$x \in \ker A \Rightarrow Ax = 0 \in \ker A$$

$$x \in \operatorname{im} A \Rightarrow Ax \in \operatorname{im} A$$

3. vsak lasten podprostor endomorfizma je invarianten

$$\begin{aligned} x \in \ker(A - \lambda I) &\Rightarrow \\ &\Rightarrow (A - \lambda I)(Ax) \\ &= A(Ax) - \lambda(Ax) \\ &= A(\lambda x) - \lambda(Ax) \\ &= \lambda(Ax) - \lambda(Ax) \\ &= 0 \\ &\Rightarrow Ax \in \ker(A - \lambda I) \end{aligned}$$

4. $A : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ naj bo rotacija za kot $\frac{\pi}{2}$ okrog z -osi. Invariantna podprostora sta gotovo z -os in ravnina $z = 0$

Naj bo $W \subseteq V$ invarianten podprostor za endomorfizem $\mathcal{A} \in \mathcal{L}(V)$. Potem je $Ax \in W$ za vsak $x \in W$. To pomeni, da zožitev $A|_W$ slika $W \rightarrow W$. Zožitev je očitno linearna, torej $A|_W \in \mathcal{L}(W)$.

Trditev. Naj bo $V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$, kjer so W_1, \dots, W_k invariantni podprostori za endomorfizem $\mathcal{A} \in \mathcal{L}(V)$. Potem obstaja neka baza prostora V , da je matrika endomorfizma

$$\mathcal{A} \text{ v tej bazi bločno diagonalna. Natančneje, enaka je } A = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix}. \text{ kjer je } A_i$$

matrika, ki pripada zožitvi $A|_{W_i}$ za vsak i .

Pravimo, da je A **direktna vsota** matrik A_1, \dots, A_k in pišemo $A = A_1 \oplus \cdots \oplus A_k$. Podobno, če označimo $A_i = A|_{W_i}$, pišemo $A = A_1 \oplus \cdots \oplus A_k$ in govorimo o direktni vsoti endomorfizmov.

Dokaz. Za vsak i naj bo $A_i = A|_{W_i}$ in A_i matrika endomorfizma $\mathcal{A} \in \mathcal{L}(V)$ glede na neko bazo $B_i = \{v_1^{(i)}, \dots, v_n^{(i)}\}$ prostora W . Vemo, da je $B = B_1 \cup B_2 \cdots \cup B_n$ baza za $V = W_1 \oplus \cdots \oplus W_k$.

Naj bo A matrika endomorfizma \mathcal{A} glede na bazo B . Potem velja:

$$\begin{aligned} W_1 &= Av_1^{(i)} * v_1^{(i)} + *v_2^{(i)} + \dots = A_1 v_1^{(i)} \\ &\vdots \end{aligned}$$

$$^{69} \text{ Potem je } \begin{bmatrix} A_1 & & & \\ 0 & A_2 & & \\ \vdots & \vdots & \ddots & \\ 0 & 0 & & A_k \end{bmatrix} \quad \square$$

$B_1 = \{\vec{k}\}$ je baza za W_1 , $B_2 = \{\vec{i}, \vec{j}\}$ pa je baza za W_2 . $\mathbb{R}^3 = W_1 \oplus W_2$ in $B = \{\vec{k}, \vec{i}, \vec{j}\}$ je baza \mathbb{R}^3 .

A naj bo matrika preslikave A glede na bazo B .

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

Ali vedno obstajajo "majhni" invariantni podprostorji za $A \in \mathcal{L}(V)$, katerih direktna vsota je V ?

Do konca poglavja o korenskih podprostorih fiksirajmo oznake.

$V \cdots n$ - razsežen kompleksen vektorski prostor

$A \in \mathcal{L}(V)$

$\lambda_1 \cdots \lambda_k$ različne vrednosti endomorfizma A

$$\Delta_A(\lambda) = (-1)^n (\lambda - \lambda_1 - I)^{n_1} \cdots (\lambda - \lambda_k)^{n_k}$$

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

Definicija. Vektorski podprostor $W_i = \ker(A - \lambda_i \text{id}_V)^{m_i}$ prostora V je korenski podprostor za endomorfizem \mathcal{A} , ki pripada lastni vrednosti λ_i .

To je res vektorski podprostor, ki vsebuje lastni podprostor ($\ker(A - \lambda_i \text{id}_V) \subseteq \ker(A - \lambda_i \text{id}_V)^m$).

V posebnem primeru je $W_i \neq \{0\}$, ker je λ_i lastna vrednost.

Trditev. W_i je invarianten podprostor za A .

Dokaz.

$$x \in W_i \Rightarrow (A - \lambda_i \text{id}_V)^{m_i} x = 0 \Rightarrow (A - \lambda_i \text{id}_V)^{m_i} Ax = A(A - \lambda_i \text{id}_V)^{m_i} x = 0 \Rightarrow \ker(A - \lambda_i \text{id}_V)^{m_i} = W_i$$

□

⁶⁹prepiši

Izrek. Naj bo $d(x)$ največji skupni delitelj polinomov $p_1(x) \cdots p_k(x) \in \mathcal{O}[x]$. Potem obstajajo polinomi $q_1(x), \dots, q_k(x) \in \mathcal{O}[x]$, da je $p_1(x)q_1(x) + \cdots + p_k(x)q_k(x) = d(x)$.

Dokaz pri Algebri 2.

Opomba:

Podobno velja za \mathbb{Z} . Če je $d \in \mathbb{Z}$ največji skupni delitelj števil $a_1, \dots, a_n \in \mathbb{Z}$, potem obstajajo $b_1, \dots, b_k \in \mathbb{Z}$, da je $a_1b_1 + \cdots + a_kb_k = d$.

Poseben primer:

$k = 2$: $a_1b_1 + a_2b_2 = d$. b_1 in b_2 lahko poiščemo z Evklidovim algoritmom. Tudi $q_1(x)$ in $q_2(x)$ iz izreka v primeru $k = 2$ lahko poiščemo z Evklidovim algoritmom. Nasploh imata kolobarja $\mathbb{Z} \in \mathcal{O}[x]$ podobne aritmetične lastnosti. Vzrok za to je osnovni izrek o deljenju.

Več pri Algebri 2.

Izrek. $V = W_1 \oplus \cdots \oplus W_k$.

Dokaz. Za vsak $i = 1, \dots$ definiramo polinom $p_i(\lambda) = \prod_{j \neq i} (\lambda - \lambda_j)^{m_j} m_A(\lambda) = (\lambda - \lambda_1)^{m_1} \cdots (\lambda - \lambda_k)^{m_k} \Rightarrow p_i(\lambda) = \frac{m_A(\lambda)}{(\lambda - \lambda_i)^{m_i}}$. Polinomi $p_1(\lambda) \cdots p_k(\lambda)$ nimajo skupne ničle, zato so tuji (nimajo nekonstantnega skupnega delitelja).

Po zadnjem izreku obstajajo polinomi $q_1(\lambda) \cdots q_k(\lambda) \in \mathbb{C}[\lambda]$, da je $p_1(\lambda)q_1(\lambda) + \cdots + p_k(\lambda)q_k(\lambda) = 1$

V to enakost vstavimo A namesto λ (to lahko naredimo, ker je $p \mapsto p(A)$ homomorfizem algeber $\mathbb{C}[\lambda] \rightarrow \mathcal{L}(V)$). Dobimo

$$p_1(A)q_1(A) + \cdots + p_k(A)q_k(A) = id_V$$

Naj bo $x \in V$ poljuben. Dokazati želimo, da se x lahko na enoličen način zapiše v obliko $x = x_1 + \cdots + x_k$, kjer je $x_i \in W_i$ za vsak i .

Definirajmo $x_i = p_i(A)q_i(A)x$ za vsak i .

Velja:

$$x = id_V(x) = \sum_{i=1}^k p_i(A)q_i(A)x = \sum_{i=1}^k x_i$$

Dokažimo, da res velja $x_i \in W_i$, za vsak i .

$$\begin{aligned} W_i &= \ker(A - \lambda_i id_V)^{m_i} \\ (A - \lambda_i id_V)^{m_i} x_i &= \\ &= (A - \lambda_i id_V)^{m_i} p_i(A)q_i(A)x \\ &= m_A(A)q_i(A)x \\ &= 0 \\ &\Rightarrow x_i \in W_i \forall i \\ &\Rightarrow V = W_1 + \cdots + W_n \end{aligned}$$

Dokazati moramo še enoličnost razcepa $x = x_1 + \dots + x_k$. Naj bo še $x = y_1 + \dots + y_k$, kjer je $y_i \in W_i$ za vsak i in velja $z_1 + z_2 + \dots + z_n = 0$.

Če je $i \neq j$, je $p_i(A)z_j = \prod_{l \neq j} (A - \lambda_l id_v)^{m_j}$ ⁷¹

Dokažimo še, da je $p_i(A)z_i = 0$ za vsak i .

$$\begin{aligned} 0 &= p_i(A)(z_1 + \dots + z_k) \\ &= p_i(A)z_i \end{aligned} \quad \text{⁷²}$$

Dokazali smo torej, da je $p_i(A)z_j = 0$ za vsaka i in j .

$$\begin{aligned} z_i &= \\ &= id_v(z_i) \\ &= \sum_{j=1}^k p_j(A)q_j(A)z_i \\ &= \sum_{j=1}^k q_j(A)p_j(A)z_i = 0 \quad \forall i \end{aligned}$$

Torej je $y_i = x_i$ za vsak i .

$$\Rightarrow V = W_1 \oplus \dots \oplus W_k$$

□

Posledica. V neki bazi prostora V (ki je unija baz korenskih podprostorov W_i) endomorfizmu \mathcal{A} pripada matrika $A =$

$$\begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix}, \text{ kjer za vsak } i \text{ matrika } A_i \text{ pripada začetni}$$

$A|_{W_i}$.

Zanima nas še, kako so povezani m_{A_i} z m_A in Δ_{A_i} z Δ_A in ali so A_i podobne kakšni lepi matriki.

LEMA:

$$\det \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_k \end{bmatrix} = (\det A_1)(\det A_2) \dots (\det A_k), \text{ če so } A_1, \dots, A_k \text{ poljubne (ne nujno enako} \\ \text{velike) kvadratne matrike. Dokaz morda na vajah.}$$

Spomnimo se: $\Delta_A(\lambda) = (-1)^n(\lambda - \lambda_1)m_1 \dots (\lambda - \lambda_k)^{m_k}$, $m_A(\lambda) = (\lambda - \lambda_1)^{m_1} \dots (\lambda - \lambda_k)^{m_k}$

Izrek. Naj bo $A = A|_{W_i}$ za vsak i . Potem za vsak $i = 1, \dots, k$ velja $\Delta_{A_i}(\lambda) = (-1)^n(\lambda - \lambda_i)^{n_i}$ in $m_A(\lambda) = (\lambda - \lambda_i)^{m_i}$.

⁷¹prepiši, ker se mega slabo vidi

Dokaz. A_i naj bo matrika endomorfizma A_i , zapisana v neki bazi prostora W_i , A pa naj bo matrika endomorfizma \mathcal{A} , zapisana glede na unijo teh baz.

$$\text{Potem je } A = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix}.$$

$$\Delta_A(\lambda) = \Delta_A(\lambda) = \det(A - \lambda I) = \det(A_1 - \lambda I) \cdots \det(A_k - \lambda I) = \Delta_{A_1}(\lambda) \cdots \Delta_{A_k}(\lambda)$$

$$\text{Vemo } \Delta_A(\lambda) = (-1)^n (\lambda - \lambda_1)^{m_1} \cdots (\lambda - \lambda_k)^{m_k}.$$

$$\text{Naj bo } x_i \in W_i \text{ poljuben. Potem je } (A_i - \lambda_i \text{id}_{W_i})^{m_i} x_i = (A - \lambda_i \text{id}_V)^{m_i} x_i = 0$$

To pomeni, da je endomorfizem $(A_i - \lambda_i \text{id}_{W_i})^{m_i} \in L(W_i)$ ničeln. Zato je A_i ničla polinoma $(\lambda - \lambda_i)^{m_i}$.

$$\Rightarrow m_{A_i}(\lambda) | (\lambda - \lambda_i)^{m_i}$$

Torej je $m_{A_i} = (\lambda - \lambda_i)^{S_i}$ za nek $1 \leq S_i \leq m_i$ in $\Delta_{A_i}(\lambda) = (-1)^{t_i} (\lambda - \lambda_i)^{t_i}$ za nek $t_i \geq S_i$ (Δ_{A_i} in m_{A_i} imata enake ničle.)

$$\text{Za vsak } i \text{ je } \Delta_{A_i}(\lambda) = (\lambda - \lambda_i)^{t_i} (-1)^{t_i}.$$

$$\begin{aligned} \Delta_A(\lambda) &= \Delta_{A_1}(\lambda) \cdots \Delta_{A_k}(\lambda) \\ &= (-1)^n (\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_k)^{n_k} \\ &= (-1)^{t_1 + \cdots + t_k} (\lambda - \lambda_1)^{t_1} \cdots (\lambda - \lambda_k)^{t_k} \end{aligned}$$

$$\Rightarrow t_i = m_i \text{ za vsak } i \Rightarrow \Delta_{A_i}(\lambda) = (-1)^n (\lambda - \lambda_i)^{n_i} \text{ za vsak } i$$

Definirajmo polinom $p(\lambda) = (\lambda - \lambda_1)^{s_1} \cdots (\lambda - \lambda_k)^{s_k}$. Radi bi dokazali, da je $p(A) = 0$. Naj bo $x \in V$ poljuben vektor. Potem obstajajo (enolični) $x_1 \in W_1 \cdots x_k \in W_k$, da je $x = x_1 + \cdots + x_k$.

$$\begin{aligned} p(A)x &= \\ &= (A - \lambda_1 \text{id}_V)^{s_1} \cdots (A - \lambda_k \text{id}_V)^{s_k} \\ &= \sum_{i=1}^k \prod_{j=1}^k (A - \lambda_j \text{id}_V)^{s_j} x_i \\ &= \sum_{i=1}^k \prod_{j \neq i}^k (A - \lambda_j \text{id}_V)^{s_j} (A - \lambda_i \text{id}_V)^{s_i} x_i \\ &= \sum_{i=1}^k \prod_{j \neq i}^k (A - \lambda_j \text{id}_V)^{s_j} (A - \lambda_i \text{id}_{W_i})^{s_i} \\ &= \sum_{i=1}^k \prod_{j \neq i}^k (A - \lambda_j \text{id}_V)^{s_j} m_{A_i}(A_i) x_i = 0. \end{aligned}$$

Torej je $p(A)x = 0$ za vsak $x \in V : p(A)$ je ničelni endomorfizem. Z drugimi besedami: A je ničla polinoma $p_i \Rightarrow m_A | p_i$

$$(\lambda - \lambda_1)^{m_1} \dots (\lambda - \lambda_k)^{m_k} | (\lambda - \lambda_1)^{s_1} \dots (\lambda - \lambda_k)^{s_k}$$

$\Rightarrow m_i \leq s_i$ za vsak i . Vemo pa že, da je $s_i \leq m_i \Rightarrow s_i = m_i$ za vsak $i \Rightarrow m_{A_i}(\lambda) = (\lambda - \lambda_i)^{m_i}$ za vsak i .

□

Posledica. $A_i \in \mathbb{C}^{n_i \times n_i}$ (kjer je n_i algebraična večkratnost lastne vrednosti λ za endomorfizem \mathcal{A}).

Posledica. Geometrična večkratnost lastne vrednosti je manjša ali enaka algebraični.

Dokaz. $\ker(A - \lambda id) \subseteq \ker(A - \lambda_i id)^{m_i} = W_i$

$$\Rightarrow \dim(\ker(A - \lambda_i id)) \leq \dim W_i = n_i$$

□

8.3 Jordanova kanonična forma

Vemo, da je vsak endomorfizem direktna vsota zožitev na korenske podprostore in da imajo te zožitve samo eno lastno vrednost. ⁷³

Če želimo poiskati čim lepšo matriko za endomorfizem \mathcal{A} je dovolj obravnavati primer, ko ima A eno samo lastno vrednost. Fiksirajmo oznake (do preklica):

V naj bo n - razsežen vektorski prostor nad \mathbb{C}

- $A \in \mathcal{L}(V)$ naj bo endomorfizem z eno samo lastno vrednostjo $\rho \in \mathbb{C}$
- $\Delta_A(\lambda) = (-1)^n (\lambda - \rho)^n$
- $m_A(\lambda) = (\lambda - \rho)^r$ za nek $1 \leq r \leq n$
- $r = 1$ ni zanimiv primer, saj je tedaj $A = \rho id$. Zato bomo običajno predpostavili $r \geq 2$.
- $m_A(\lambda) = (\lambda - \rho)^r \Rightarrow (A - \rho id_v) = 0, (A - \rho id_v)^{r-1} \neq 0$ ⁷⁴

Potem je $B^r = 0$ in $B^{r-1} \neq 0$. Takemu endomorfizmu pravimo **nipolenten** endomorfizem, številu r pa **indeks nilpotentnosti** (to je najmanjše število, za katerega je $B^r = 0$)

$$\Delta_B(\lambda) = (-1)^n \lambda^n, m_B(\lambda) = \lambda^r$$

Če endomorfizmu B pripada matrika B v neki bazi, v tej isti bazi endomorfizmu $\mathcal{A} = B + \rho I$. Zato bomo obravnavali B namesto A .

Za vsak $i = 0, 1, \dots$ označimo $V_i = \ker B^i$. To so vektorski podprostor v V , za katere velja:

⁷³smo že dokazali

⁷⁴ $(A - \rho id_v)^1 = id$

1. $V_i = V$, če je $i \geq r$
2. $\{0\} = V_0 \subseteq V_1 \subseteq \dots \subseteq V_r = V$
3. $x \in V_i \Leftrightarrow Bx \in V_{i-1}$ za $i \geq 1$

Dokaz. 1. Če je $i \geq r$, je $B' = B^{i-r}B^r = 0 \Rightarrow V_i = \ker B' = V$

2. $B^0 = id \Rightarrow \ker(id_v) = \{0\} \Rightarrow V_i = \ker B'$. Če je $x \in \ker B'$ je $B'x = 0 \Rightarrow B^{i+1}x = 0 \Rightarrow x \in \ker B^{i+1} = V_{i+1}$

3. $x \in V_i \Leftrightarrow B'x = 0 \Leftrightarrow B^{i-1}(Bx) = 0 \Leftrightarrow Bx \in \ker(B^{i-1}) = V_{i-1}$

□

LEMA:

Naj bo $i \geq 2$ in naj bo $V = \{v_1, \dots, v_k\} \subseteq V_i$ linearno neodvisna množica, za katero velja $\text{Lin}V \cap V_{i-1} = \{0\}$. Potem je množica $B(V) = \{Bv_1, \dots, Bv_k\}$ linearno neodvisna podmnožica V_{i-1} , za katero velja $\text{Lin}(B(V)) \cap V_{i-2} = \{0\}$

Dokaz. $B(V) \subseteq V_{i-1}$ sledi iz lastnosti (3).

Naj bo $\alpha_1 Bv_1 + \dots + \alpha_k Bv_k \in V_{i-2}$. Potem je

$$\begin{aligned}
 B^{i-2}(\alpha_1 Bv_1 + \dots + \alpha_k Bv_k \in V_{i-2}) &= 0 \\
 B^{i-1}(\alpha_1 v_1 + \dots + \alpha_k v_k) & \\
 \Rightarrow \alpha_1 v_1 + \dots + \alpha_k v_k \in \ker(B^{i-1}) &= V_{i-1} \cap \text{Lin}V = {}^{75} = \{0\} \\
 \Rightarrow \alpha_1 v_1 + \dots + \alpha_k v_k &= 0 \\
 \Rightarrow \text{Lin}(B(V)) \cap V_{i-2} &= \{0\}
 \end{aligned}$$

Dokažimo še linearno neodvisnost Bv_1, \dots, Bv_k .

Naj bo

$$\begin{aligned}
 \alpha_1 Bv_1 + \dots + \alpha_k Bv_k &= 0 \in V_{i-2} \\
 B(\alpha_1 v_1 + \dots + \alpha_k v_k) &= 0^{76} \\
 \Rightarrow \alpha_1 = \dots = \alpha_k &= 0
 \end{aligned}$$

□

Posledica. $\{0\} = V_0 \subset V_1 \subset \dots \subset V_r = V$.

Dokaz. Z "obratno" indukcijo.

$$B^{r-1} \neq 0 \Rightarrow \ker(B^{r-1}) \neq V = V_r$$

Neko bazo prostora V_{r-1} lahko z množico $V \neq 0$ dopolnimo do baze V_r . V je linearno neodvisna in po konstrukciji je $\text{Lin}V \cap V_{r-1} = \{0\}$, saj je $V_r = V_{r-1} \oplus \text{Lin}V$.

Po lemi je $B(V)$ linearno neodvisna in $\text{Lin}B(V) \cap V_{r-2} = \{0\}$ in $B(V) \subseteq V_{r-1} \Rightarrow V_{r-2} \subset V_{r-1}$ ⁷⁷.

Predpostavimo, da za nek i velja $V_i \subset V_{i+1}$. Potem neko bazo prostora V_i lahko z množico V' dopolnimo do baze prostora V_{i+1} . Potem je $\text{Lin}V' \cap V_i = \{0\}$. Tedaj po lemi obstaja linearno neodvisna množica $V'' = B(V') \subseteq V_i$, da je $\text{Lin}(B(V')) \cap V_{i-1} = \{0\}$.

□

8.4 Konstrukcija Jordanove baze

Po zadnji posledici obstaja linearno neodvisna množica $V_r = \{v_1^r, \dots, v_{s_r}^r\} \subseteq V_r = V$, da za $U_r := \text{Lin}V_r$ velja $V_r = V_{r-1} \oplus U_r$.⁷⁸ Po zadnji lemi je množica $B(V_r) = \{v_1^{(r-1)}, \dots, v_{s_r}^{(r-1)}\} \subseteq V_{r-1}$ linearno neodvisna in $\text{Lin}(B(V_r)) \cap V_{r-2} = \{0\}$.

Če vektorje iz $B(V_r)$ dodamo bazi prostora V_{r-2} dobimo linearno neodvisne vektorje v V_{r-1} . Te lahko dopolnimo do baze prostora V_{r-1} .

Bazo za V_{r-1} torej lahko dobimo tako, da bazi za V_{r-1} dodamo neko linearno neodvisno množico V_{r-1} , ki vsebuje $B(V_r)$.

$V_{r-1} = \{v_1^{(r-1)}, \dots, v_{s_r}^{(r-1)}, \dots, v_{s_{r-1}}^{(r-1)}\}$ je linearno neodvisna in velja $\text{Lin}V_{r-1} \cap V_{r-2} = \{0\}$.

Definiramo $U_{r-1} = \text{Lin}V_{r-1}$. Potem je $U_{r-1} \oplus V_{r-2} = V_{r-1}$.

Po lemi je $B(V_{r-1}) \subseteq V_{r-2}$ linearno neodvisna množica in velja $\text{Lin}B(V_{r-1}) \cap V_{r-2} = \{0\}$. Postopek nadaljujemo. Na vsakem koraku dobimo podprostor U_i v V_i , da je $U_i \oplus V_{i-1} = V_i$. $V_0 = \{0\} \Rightarrow U_1 = V_1$.

U_i je baza za U_i za vsak i .

$$\begin{aligned} V &= \\ &= V_r = U_r \oplus V_{r-1} \\ &= U_r \oplus U_{r-1} \oplus V_{r-2} \\ &= \dots \\ &= U_r \oplus U_{r-1} \oplus \dots \oplus U_1 \oplus V_0 \end{aligned} \quad ^{79}$$

Unija baz V_i je baza za V .

$$V_i = \{v_1^{(i)}, \dots, v_{s_i}^{(i)}\} \text{ in } B_{v_j}^{(i)} = v_j^{(i-1)}$$

⁷⁷kjer je \subset je ubistvu subset z neq spodaj

⁷⁸preseki $V_r = V_{r-1} \oplus U_r$ je 0

Bazo za V uvedemo na naslednji način:

$$V = \{v_1^{(1)}, \dots, v_1^{(r)}, v_2^{(2)} \dots, v_2^{(r)} \dots\}$$

Zapišimo matriko:

$$\begin{aligned} v_1^{(1)} &\in V_1 = \ker B^1 \\ Bv_1^{(1)} &= 0 \\ Bv_1^{(2)} &= v_1^{(1)} \\ &\vdots \\ Bv_1^{(r)} &= v_1^{(r-1)} \end{aligned}$$

Dobimo matriko:

$$\begin{aligned} Bv_2^{(1)} &= 0 \\ Bv_2^{(2)} &= v_2^{(1)} \\ &\vdots \\ Bv_2^{(*)} &= v_2^{(*-1)} \end{aligned}$$

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & 0 & 1 & & \vdots & \vdots & \vdots \\ & & & \ddots & & & \\ & & & & 1 & & \\ 0 & \cdots & & & 0 & 0 & \cdots \\ & & & & 0 & 1 & \\ & & & & & & \ddots \\ & & & & & & 1 \\ & & & & & & 0 \\ & & & & & & \ddots \\ & & & & & & 0 & 1 \\ & & & & & & & \ddots \\ & & & & & & & 1 \\ & & & & & & & 0 \end{bmatrix}$$

Na ta način urejeno bazo V imenujemo **Jordanova baza** endomorfizma B , matriko, ki smo jo dobili, pa **Jordanova matrika** nilpotenta B .

Označimo jo z $J(B)$. Je bločno diagonalna z bloki $J_k = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix}$ po diagonalni.

Takim blokom pravimo **Jordanove celice** za lastno vrednost 0.

$\Rightarrow J(B)$ je direktna vsota Jordanovih celic ($J_1 = 0$).

Pri tem velikosti celic po diagonali naraščajo.⁸⁰ Najnižja je velikosti $r \times r$, kjer je r indeks nilpotentnosti B -ja. Njihovo število pa je enako $\dim(\ker B) =$ geometrična večkratnost lastne vrednosti 0.

Vrnimo se k primeru, ko ima endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ eno samo lastno vrednost ρ .

Če definiramo $B = \mathcal{A} \circ \text{pid}_v$, potem je B nilpotenten. Jordanova baza za \mathcal{A} je ista kot Jordanova baza za B .

\Rightarrow Jordanova baza za $\mathcal{A} : J(A) = J(B) + \rho I$

$\Rightarrow J(A)$ je direktna vsota Jordanovih celic oblike

$$J_t^{81}(\rho) = \begin{bmatrix} \rho & 1 & & & \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & \ddots & \ddots \\ & & & & \ddots & 1 \\ & & & & & \rho \end{bmatrix}$$

kjer je ρ lastna vrednost.

Število teh celic je enako geometrični večkratnosti lastne vrednosti ρ . Velikosti celic po diagonali ne naraščajo, velikost največje celice je enaka stopnji minimalnega polinoma $m_{\mathcal{A}}(\lambda)$.

Obravnavajmo splošni primer, torej endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ je poljuben. Če je $V = W_1 \oplus \dots \oplus W_k$ razcep prostora V na korenske podprostore, potem vemo, da je $\mathcal{A} = \mathcal{A}_1 \oplus \dots \oplus \mathcal{A}_k$, kjer $\mathcal{A}_i = \mathcal{A}|_{W_i}$ za vsak i in \mathcal{A}_i ima le eno lastno vrednost λ_i , pri čemer je $\lambda_i \neq \lambda_j$ za $i \neq j$.

$$A = \begin{bmatrix} A_1 & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \ddots & \\ & & & & A_k \end{bmatrix}$$

če je A_i matrika endomorfizma $\mathcal{A}_i \in L(W_i)$ glede na neko bazo in A je matrika endomorfizma \mathcal{A} glede na unijo teh baz.

⁸⁰Preveri pri Izaku, kaj piše tu

⁸¹Preveri pri Izaku, kaj pomeni ta "t"?

Jordanova baza endomorfizma \mathcal{A} je (urejena) unija Jordanovih baz endomorfizma \mathcal{A} . Glede na to bazo endomorfizma \mathcal{A} pripada matrika $J(\mathcal{A}_i) \oplus \cdots \oplus J(\mathcal{A}_k)$. To je Jordanova matriko endomorfizma \mathcal{A} . Oznaka je $J(\mathcal{A})$.

$J(\mathcal{A})$ je torej direktna vsota Jordanovih celic oblike $J_t(\lambda_i) \in \mathbb{C}^{t \times t}$, kjer so $\lambda_1, \dots, \lambda_k$ vse paroma različne lastne vrednosti endomorfizma \mathcal{A} .⁸² Pri tem velja:

1. Za fiksni λ_i ima $J(\mathcal{A})$ toliko Jordanovih celic oblike $J_t(\lambda_i)$, kolikor je geometrična večkratnost lastne vrednosti λ_i .
2. Velikost največje celice oblike $J_t(\lambda_i)$, kjer je λ_i fiksni, je enaka večkratnosti ničle λ_i v minimalnem polinomu.
3. Algebraična večkratnost lastne vrednosti λ_i je enaka številu pojavitev λ_i na diagonali matrike $J(\mathcal{A})$.

PRIMER:

$$J(\mathcal{A}) = \begin{bmatrix} 1 & & & & & & & & \\ & 1 & & & & & & & \\ & & 1 & & & & & & \\ & & & 1 & & & & & \\ & & & & 1 & & & & \\ & & & & & 1 & & & \\ & & & & & & 2 & & \\ & & & & & & & 1 & \\ & & & & & & & & 2 \\ & & & & & & & & & 2 \\ & & & & & & & & & & 2 \end{bmatrix}$$

$$\Delta_{\mathcal{A}}(\lambda) = (-1)^9(\lambda - 1)^5(\lambda - 2)^4$$

$$m_{\mathcal{A}}(\lambda) = (\lambda - 1)^3(\lambda - 2)^2$$

lastne vrednosti:

- 1 (algebraična večkratnost 5, geometrična večkratnost 2, 2 celici)
- 2 (algebraična večkratnost 4, geometrična večkratnost 3, 3 celice)

Za vsak endomorfizem obstaja Jordanova baza, zato je vsaka kvadratna matrika podobna neki Jordanovi matriki. Jordanova matrika endomorfizma pa je enolično določena do vrstnega reda Jordanovih celic natančno.

Dokaz. (ideja dokaza): Število Jordanovih celic $J_t(\lambda_i)$, kjer je $t \geq s$ je enako $\dim(\ker(\mathcal{A} - \lambda_i \text{id}_v)^s) - \dim(\ker(\mathcal{A} - \lambda_i \text{id}_v)^{s-1})$, kar je odvisno le od endomorfizma \mathcal{A} . Zato matriki $J(\mathcal{A})$ pravimo tudi **Jordanova kanonična forma endomorfizma \mathcal{A}** (ki je neodvisna od baze). \square

⁸²Lahko imamo več Jordanovih celic za isto lastno vrednost.

8.5 Funkcije matrik

Vemo že:

Če je $p(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ polinom, je $p(A) = a_n A^n + a_{n-1} A^{n-1} + \dots + a_1 A + a_0 I$, kjer je A poljubna kvadratna matrika.

Vemo tudi:

Če je $A = P^{-1} J(A) P$, potem je $p(A) = P^{-1} p(J(A)) P$.

$J(A)$ je direktna vsota Jordanovih celic oblike $J_t(\lambda_i)$, kjer je λ_i lastna vrednost matrike A .

$\Rightarrow p(J(A))$ je direktna vsota matrik $p(J_t(\lambda_i))$.

Naj bo $p(X) = c_0 + c_1 X + c_2 X^2 + \dots$ polinom.

$$J_t(\rho) = \begin{bmatrix} \rho & 1 & & & \\ & \rho & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & \ddots \\ & & & & \rho & 1 \end{bmatrix} = \begin{bmatrix} \rho & & & & \\ & \rho & & & \\ & & \rho & & \\ & & & \ddots & \\ & & & & \rho \end{bmatrix} + \begin{bmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & \ddots \\ & & & & 0 & 1 \end{bmatrix} = \rho I + N$$

Za vsak $j = 0, 1, \dots, t-1$; $N^t = 0$ in $N^0 = I$

$$\begin{aligned} p(J_t(\rho)) &= p(\rho I + N) \\ &= c_0 I + c_1(\rho I + N) + c_2(\rho I + N)^2 + c_3(\rho I + N)^3 + \dots \\ &\stackrel{83}{=} c_0 I + (c_1 \rho I + c_1 N) + (c_2 \rho^2 I + 2c_2 \rho N + c_2 N^2) + (c_3 \rho^3 I + 3c_3 \rho^2 N + 3c_3 \rho N^2 + c_3 N^3) + \dots \\ &= I(c_0 + c_1 \rho + c_2 \rho^2 + c_3 \rho^3 + \dots) + (c_1 + 2c_2 \rho + 3c_3 \rho^2 + \dots)N + \dots \\ &= Ip(\rho) + Np'(\rho) + \frac{1}{2!}N^2p''(\rho) + \frac{1}{3!}p'''(\rho)N^3 + \dots \\ &= \begin{bmatrix} p(\rho) & p'(\rho) & \frac{1}{2}p''(\rho) & \dots & \frac{1}{(t-1)!}p^{(t-1)}(\rho) \\ & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & \ddots & \frac{1}{2}p''(\rho) \\ & & & & \ddots & p'(\rho) \\ & & & & & p(\rho) \end{bmatrix} \end{aligned}$$

Definicija. Naj bo $D \subseteq \mathbb{C}$ odprta množica, ki vsebuje ρ in naj bo $f : D \rightarrow \mathbb{C}$ funkcija, ki

jo je mogoče razviti v Taylorjevo vrsto okrog ρ :⁸⁴

$$\begin{aligned} f(z) &= \\ &= f(\rho) + f'(\rho)(z - \rho) + \frac{1}{2}f''(\rho)(z - \rho)^2 + \frac{1}{3!}f'''(\rho)(z - \rho)^3 + \dots \\ &= \sum_{j=0}^{\infty} \frac{1}{j!} f^{(j)}(\rho)(z - \rho)^{(j)} \end{aligned}$$

Definiramo

$$\begin{aligned} f(J_t(\rho)) &= f(\rho I + N) \\ &= \sum_{j=0}^{\infty} \frac{1}{j!} f^{(j)}(\rho)(\rho I + N - \rho I)^{(j)} \\ &= \sum_{j=0}^{t-1} \frac{1}{j!} f^{(j)}(\rho) N^j \\ &= \begin{bmatrix} f(\rho) & f'(\rho) & \frac{1}{2}f''(\rho) & \dots & \frac{1}{(t-1)!}f^{(t-1)}(\rho) \\ & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & \frac{1}{2}f''(\rho) \\ & & & \ddots & f'(\rho) \\ & & & & f(\rho) \end{bmatrix} \end{aligned}$$

Definicija. Naj bo f kompleksna funkcija, ki jo je mogoče v okolici spektra matrike $A \in \mathbb{C}$ razviti v Taylorjevo vrsto in naj bo $A = P^{-1}J(A)P$ in $J(A) = J_{t_1}(\rho_1) \oplus \dots \oplus J_{t_l}(\rho_l)$, kjer so ρ_1, \dots, ρ_l ne nujno različne lastne vrednosti matrike A .

Potem definirajmo

$$\begin{aligned} f(J(A)) &= f(J_{t_1}(\rho_1)) \oplus \dots \oplus f(J_{t_l}(\rho_l)) \\ f(A) &= P^{-1}f(J(A))P \end{aligned}$$

Opomba:

- Definicija se ujema s prejšnjo definicijo na polinomih.
- Če je $\rho_i \neq \rho_j$ za izračun $f(J_{t_i}(\rho_i))$ uporabimo drug razvoj v Taylorjevo vrsto kot za izračun $f(J_{t_j}(\rho_j))$.
- Pri Analizi 2 bomo take funkcije imenovali holomorfne funkcije.⁸⁶
- Pri funkcionalni analizi bomo funkcije matrike definirali še na druge načine (kot npr. z vrsto, integralom). Te se ujemajo z zgornjo definicijo.
- Da se pokazati, da za vsako funkcijo f kot v definiciji in vsako matriko A obstaja polinom p (ki je odvisen od f in od A), da je $f(A) = p(A)$

⁸⁴To pomeni, da vrsta konvergira in njena vsota je enaka $f(z)$ za vsak $z \in D$.

⁸⁶To so tiste funkcije, ki se jih da odvajati v \mathbb{C}

- Jordanova baza ni enolična. Kljub temu je definicija dobra, saj se s pomočjo prejšnje opombe (5) da pokazati, da

$$P^{-1}f(J(A))P = Q^{-1}f(J(A))Q$$

Naj bo F algebra vseh funkcij, ki jih je mogoče v okolici spektra matrike $A \in \mathbb{C}^{n \times n}$ razviti v Taylorjevo vrsto in $\Phi : F \rightarrow \mathbb{C}^{n \times n}$ ⁸⁷preslikava, definirana s predpisom $\Phi(f) = f(A)$. Potem velja:

1. $\Phi(\alpha f + \beta g) = \alpha \Phi(f) + \beta \Phi(g)$ za vsaka $f, g \in F$ in $\alpha, \beta \in \mathbb{C}$
2. $\Phi(f \cdot g) = \Phi(f) \cdot \Phi(g)$ za vsaka $f, g \in F$
3. $\Phi(1) = I$, kjer je 1 konstantna funkcija
4. $\Phi(id) = A$, kjer $id : z \mapsto z$

(brez dokaza)

PRIMER:

$$J = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\begin{array}{ll} f(x) = \sin(x) & g(x) = \cos(x) \\ f'(x) = \cos(x) & g'(x) = -\sin(x) \\ f''(x) = -\sin(x) & g''(x) = -\cos(x) \end{array}$$

Edina lastna vrednost J je 0.

$$\begin{array}{ll} f(0) = 0 & g(0) = 1 \\ f'(0) = 1 & g'(0) = 0 \\ f''(0) = 0 & g''(0) = -1 \end{array}$$

$$\sin J = f(0)I + f'(0)J + \frac{1}{2}f''(0)J^2 = J$$

$$\cos J = g(0)I + g'(0)J + \frac{1}{2}g''(0)J^2 = I - \frac{1}{2}J^2 = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix} - \begin{bmatrix} & & \frac{1}{2} \\ & & \\ & & \end{bmatrix} = \begin{bmatrix} 1 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\cos^2 J + \sin^2 J = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = I$$

⁸⁷ Φ je homomorfizem algeber.

9 PROSTORI S SKALARNIM PRODUKTOM

9.1 Osnovne lastnosti

V celotnem poglavju o skalarnem produktu bo F obseg realnih ali kompleksnih števil.

Definicija. Naj bo V vektorski prostor nad F . Skalarni produkt na V je preslikava

$$V \times V \rightarrow F$$

$$(x, y) \mapsto \langle x, y \rangle$$

za katero veljajo naslednje lastnosti:

- linearnost v prvem faktorju

$$\langle \alpha x + \beta y, z \rangle = \alpha \langle x, z \rangle + \beta \langle y, z \rangle$$

- poševna simetričnost

$$\langle y, x \rangle = \overline{\langle x, y \rangle}$$

- pozitivna definitnost

$$\langle x, x \rangle \geq 0$$

za vsak $x \in V$, pri čemer je $\langle x, x \rangle = 0 \Leftrightarrow x = 0$ ⁸⁸

Realen vektorski prostor s skalarnim produktom se imenuje **evklidski prostor**, kompleksen vektorski prostor s skalarnim produktom pa **unitaren vektorski prostor**.

Lema. V vektorskem prostoru s skalarnim produktom velja:

1. $\langle x, 0 \rangle = \langle 0, x \rangle = 0$ za vsak $x \in V$
2. $\langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle$ za vsak $x, y, z \in V$
3. $\langle x, \alpha y \rangle = \overline{\alpha} \langle x, y \rangle$ za vsak $\alpha \in F$ za vsak $x, y \in V$

Dokaz.

1.

$$\begin{aligned} \langle 0, x \rangle &= \\ &= \langle 0 \cdot x, x \rangle \\ &= 0 \cdot \langle x, x \rangle \\ &= 0 \end{aligned}$$

$$\begin{aligned} \langle x, 0 \rangle &= \\ &= \overline{\langle 0, x \rangle} \\ &= 0 \end{aligned}$$

⁸⁸V \mathbb{C} to pomeni: $\langle x, x \rangle$ je realno število in ≥ 0

2.

$$\begin{aligned}
 \langle x, y + z \rangle &= \\
 &= \overline{\langle y + z, x \rangle} \\
 &= \overline{\langle y, x \rangle + \langle z, x \rangle} \\
 &= \overline{\langle y, x \rangle} + \overline{\langle z, x \rangle} \\
 &= \langle x, y \rangle + \langle x, z \rangle
 \end{aligned}$$

3.

$$\begin{aligned}
 \langle x, \alpha y \rangle &= \\
 &= \overline{\langle \alpha y, x \rangle} \\
 &= \overline{\alpha \langle y, x \rangle} \\
 &= \overline{\alpha} \overline{\langle y, x \rangle} \\
 &= \overline{\alpha} \langle x, y \rangle
 \end{aligned}$$

□

Posledica. V evklidskem prostoru je skalarni produkt bilinearen funkcional. V unitarnem prostoru pa je skalarni produkt linearen v 1. faktorju ter aditiven in poševno homogen v 2. faktorju.

PRIMER:

1. \mathbb{R}^3 nad \mathbb{R} . Če je $x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$, $y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$ s predpisom $\langle x, y \rangle = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$ definiran standardni skalarni produkt na \mathbb{R}^n

2. \mathbb{C}^n nad \mathbb{C}

$$\langle x, y \rangle = x_1 \overline{y_1} + x_2 \overline{y_2} + \cdots + x_n \overline{y_n}$$

Standardni skalarni produkt na \mathbb{C}^n

3. $C[a, b]$ nad \mathbb{R} je vektorski prostor vseh realnih zveznih funkcij na intervalu $[a, b]$.

$$\langle f, g \rangle = \int_a^b f(x)g(x)dx$$

je skalarni produkt na $C[a, b]$.⁸⁹

Definicija. Norma vektorja $x \in V$ je število $\|x\| = \sqrt{\langle x, x \rangle}$. Ker je $\langle x, x \rangle \geq 0$ za vsak x je definicija smiselna.

Lastnosti norme:

1. $\|x\| \geq 0$ za vsak $x \in V$ in $\|x\| = 0 \Leftrightarrow x = 0$

⁸⁹Za drugi del zadnjega aksioma potrebujemo zveznost.

2. $||\alpha x|| = |\alpha| ||x||$ za vsak $\alpha \in F$ in $x \in V$

3. *trikotniška neenakost*

$$||x + y|| \leq ||x|| + ||y|| \text{ za vse } x, y \in V$$

Dokaz.

1. *Očitno.*

$$2. ||\alpha x|| = \sqrt{\langle \alpha x, \alpha x \rangle} = \sqrt{\alpha \bar{\alpha} \langle x, x \rangle} = |\alpha| ||x||$$

3. *Kasneje.*

□

(1),(2),(3) so aksiomi normiranega prostora, torej je $(V, || \cdot ||)$ normiran prostor.

Trditev. V prostoru s skalarnim produktom velja:

1. *Pitagorov izrek:* Če je $\langle x, y \rangle = 0$, potem je $||x + y||^2 = ||x||^2 + ||y||^2$

2. *paralelogramska enakost:*

$$||x + y||^2 + ||x - y||^2 = 2(||x||^2 + ||y||^2)$$

Dokaz.

1.

$$\begin{aligned} ||x + y||^2 &= \\ &= \langle x + y, x + y \rangle \\ &= \langle x, x \rangle + \langle x, y \rangle + \langle y, x \rangle + \langle y, y \rangle \\ &= ||x||^2 + ||y||^2 \end{aligned}$$

2.

$$\begin{aligned} ||x + y||^2 + ||x - y||^2 &= \\ &= \langle x + y, x + y \rangle + \langle x - y, x - y \rangle \\ &= \langle x, x \rangle + \langle x, y \rangle + \langle y, x \rangle + \langle y, y \rangle + \\ &\quad \langle x, x \rangle - \langle x, y \rangle - \langle y, x \rangle + \langle y, y \rangle \\ &= 2(\langle y, y \rangle + \langle x, x \rangle) \\ &= 2(||x||^2 + ||y||^2) \end{aligned}$$

□

Da se pokazati, da paralelogramska enakost karakterizira normirane prostore s skalarnim produktom:

V normiranem prostoru lahko uvedemo skalarni produkt tako, da bo $\|x\|^2 = \langle x, x \rangle$ natanko takrat, ko velja paralelogramska enakost.

Definicija. V vektorskem prostoru s skalarnim produktom definiramo razdaljo s predpisom $d(x, y) = \|x - y\|$.

Lastnosti razdalje:

$$1. \quad d(x, y) \geq 0, d(x, y) = 0 \Leftrightarrow x = y$$

$$2. \quad d(x, y) = d(y, x)$$

3. trikotniška neenakost

$$d(x, z) \leq d(x, y) + d(y, z)$$

Dokaz.

1. Očitno.

2. Očitno.

3.

$$\begin{aligned} d(x, z) &= \\ &= \|x - z\| \\ &= \|x - y + y - z\| \\ &\leq \|x - y\| + \|y - z\| \\ &= d(x, y) + d(y, z) \end{aligned}$$

□

(1), (2), (3) so aksiomi metričnega prostora. (V, d) je torej metričen prostor.

Izrek. (Cauchy, Schwarz, Bunjakaski)

V vektorskem prostoru V s skalarnim produktom za vsaka $x, y \in V$ velja $|\langle x, y \rangle| \leq \|x\| \|y\|$. Enakost velja natanko takrat, ko sta x in y linearno odvisna.

Dokaz. Za vsaka $\alpha, \beta \in F$ velja

$$\langle \alpha x + \beta y, \alpha x + \beta y \rangle \geq 0$$

$$|\alpha|^2 \|x\|^2 + \alpha \beta \langle x, y \rangle + \beta \bar{\alpha} \langle x, y \rangle + |\beta|^2 \|y\|^2 \geq 0$$

za vsaka $\alpha, \beta \in F$ in $x, y \in V$. Vzamemo $\alpha = \|y\|^2$ in $\beta = -\langle x, y \rangle$.

Dobimo

$$\|y\|^4 \|x\| - \|y\|^2 \langle \overline{x, y} \rangle \langle x, y \rangle - \langle x, y \rangle \|y\|^2 \langle \overline{x, y} \rangle + |\langle x, y \rangle|^2 \|y\| \geq 0$$

za vse $x, y \in V$.

$$||y||^2(||x|| \cdot ||y||^2 | \langle x, y \rangle |^2) \geq 0$$

za vse $x, y \in V$.

Če je $||y|| = 0$, potem je $y = 0 \Rightarrow \langle x, y \rangle = 0 = ||x|| \cdot ||y||$

Če je $||y|| = 0$, potem je $||x||^2 ||y||^2 \geq | \langle x, y \rangle |^2$. Neenakost je s tem dokazana.

Ugotoviti moramo še, kdaj velja enakost.

Če je $y = 0$, že vemo, da enakost velja, vektorja x in y pa sta v tem primeru očitno linearno odvisna.

Predpostavimo, da je $y \neq 0$ in $||x|| \cdot ||y|| = | \langle x, y \rangle |$. Potem iz zgornjega dokaza sledi, da je $||\alpha x + \beta y||^2 = 0$, kjer je $\alpha = ||y||^2$ in $\beta = - \langle x, y \rangle$

$\Rightarrow \alpha x + \beta y = 0, \alpha = ||y||^2 \neq 0 \Rightarrow x$ in y sta linearno odvisna.

Obratno, naj bosta x in y linearno odvisna in dokažimo, da je $||x|| ||y|| = | \langle x, y \rangle |$. Primer, ko je $y = 0$, smo že obravnavali, zato naj bo $y \neq 0$. Ker sta x in y linearno odvisna, obstaja $x \in F$, da je $x = \lambda y (y \neq 0)$

$$\begin{aligned} \Rightarrow ||x|| \cdot ||y|| &= ||\lambda y|| \cdot ||y|| = |\lambda| ||y||^2 \\ | \langle x, y \rangle | &= | \langle \lambda y, y \rangle | = |\lambda| ||y||^2 \end{aligned}$$

□

PRIMER:

CSB v F^n s standardnim skalarnim produktom:

$$| \sum_{j=1}^n x_j \overline{y_j} | \leq \sqrt{\sum_{j=1}^n |x_j|^2} \sqrt{\sum_{j=1}^n |y_j|^2}$$

To neenakost je dokazal Cauchy. Schwarz in Binjakovski sta neenakost dokazala v $C[a, b]$.

$$(\int_a^b f(x)g(x)dx) \leq (\int_a^b f(x)^2 dx)(\int_a^b g(x)^2 dx)$$

Posledica. *Trikotniška neenakost:*

V vektorskem prostoru V s skalarnim produktom velja $||x+y|| \leq ||x|| + ||y||$ za vse $x, y \in V$.

Dokaz.

$$\begin{aligned}
\|x + y\|^2 &= \\
&= \langle x + y, x + y \rangle \\
&= \|x\|^2 + \langle x, y \rangle + \langle y, x \rangle + \|y\|^2 \\
&= \|x\|^2 + 2\Re \langle x, y \rangle + \|y\|^2 \\
&\leq \|x\|^2 + 2|\langle x, y \rangle| + \|y\|^2 \\
&\leq \|x\|^2 + 2\|x\| \cdot \|y\| + \|y\|^2 \\
&= (\|x\| + \|y\|)^2
\end{aligned}$$

□

Naj bo V evklidski prostor (nad \mathbb{R}). Potem za $x, y \neq 0$ in CSB sledi $-1 \leq \frac{\langle x, y \rangle}{\|x\| \cdot \|y\|} \leq 1$. Zato obstaja enoličen $\varphi \in [0, \pi]$, da je $\frac{\langle x, y \rangle}{\|x\| \cdot \|y\|} = \cos \phi$. Definiramo, da je kot med neničelnima vektorjema x in y enak $\arccos \frac{\langle x, y \rangle}{\|x\| \cdot \|y\|}$.

Ta definicija se ujema z znanim dejstvom, da v \mathbb{R}^3 velja

$$\langle x, y \rangle = \|x\| \cdot \|y\| \cos \varphi$$

kjer je φ kot med x in y .

Definicija. Vektorja x in $y \in V$, kjer je V prostor s skalarnim produktom, sta **pravokotna**, kadar je $x \cdot y = 0$ ⁹¹

Ta definicija se sklada z definicijo kota, pri čemer dovolimo, da je kakšen od kotov enak 0.

Trditev. $x = 0 \Leftrightarrow \langle x, y \rangle = 0$ za vsak $y \in V$.

Dokaz. \Rightarrow Že vemo.

\Leftarrow Ker je $\langle x, y \rangle = 0$ za vsak y , je v posebnem primeru $\langle x, x \rangle = 0 \Rightarrow x = 0$. □

Definicija. $M \subseteq V$ je **ortogonalna množica**, če za vsaka različna $x, y \in M$ velja $x \perp y$.

Trditev. Ortogonalna množica, ki ne vsebuje vektorja 0, je linearno neodvisna.

Dokaz. Naj bo $\alpha_1 x_1 + \dots + \alpha_m x_m = 0$ za neke $x_1, \dots, x_m \in M$ in $\alpha_1, \dots, \alpha_m \in F$. Naj bo $j \in \{1, \dots, m\}$ poljuben. Zgornjo enakost skalarno pomnožimo z x_j .

$$\begin{aligned}
0 &= \\
&= \langle 0, x_j \rangle \\
&= \left\langle \sum_{k=1}^m \alpha_k x_k, x_j \right\rangle \\
&= \sum_{k=1}^m \alpha_k \langle x_k, x_j \rangle \stackrel{92}{=} \\
&= \alpha_j \|x_j\|^2 \stackrel{93}{=} \\
&\Rightarrow \alpha_j = 0
\end{aligned}$$

□

⁹¹Oziroma $\langle x, y \rangle = 0$. Oznaka $x \perp y$.

Posledica. V n - razsežnem vektorskim prostoru s skalarnim produktom ima ortogonalna množica lahko največ $n + 1$ elementov.

Definicija. Množica $M \subseteq V$ je **ortonormirana**, kadar je **ortogonalna** in velja $\|x\| = 1$ za vsak $x \in M$.

Trditev. Če je M ortogonalna množica in $0 \notin M$, potem je množica vseh vektorjev oblike $\{\frac{x}{\|x\|}; x \in M\}$ ortonormirana.

Dokaz.

$$\begin{aligned} \left\langle \frac{x}{\|x\|}, \frac{y}{\|y\|} \right\rangle &= \\ &= \frac{1}{\|x\| \cdot \|y\|} \langle x, y \rangle \\ &= 0 \end{aligned}$$

$$\begin{aligned} \left\| \frac{x}{\|x\|} \right\| &= \\ &= \frac{1}{\|x\|} \cdot \|x\| \\ &= 1 \end{aligned}$$

□

Posledica. V n - razsežnem vektorskem prostoru s skalarnim produktom ima ortonormirana množica lahko največ n elementov.

10 ORTOGONALIZACIJA

Izrek. (Gram - Schmidtova ortogonalizacija)

Naj bo V vektorski prostor s skalarnim produktom in $x_1, \dots, x_m \in V$ linearno neodvisni vektorji. Potem obstajajo taki linearno neodvisni paroma pravokotni vektorji $y_1, \dots, y_m \in V$, da je $\text{Lin}\{x_1, \dots, x_k\} = \text{Lin}\{y_1, \dots, y_k\}$ za vsak $k = 1, \dots, m$.

Dokaz. Vektorje y_1, \dots, y_m konstruirani postopoma z indukcijo na k .

$k = 1$

Vzamemo $y_1 = x_1$

$k \rightarrow k + 1$

Denimo, da smo že konstruirali linearno neodvisne in paroma pravokotne vektorje y_1, \dots, y_m , da za vsak $j = 1, \dots, m$ velja $\text{Lin}\{x_1, \dots, x_j\} = \text{Lin}\{y_1, \dots, y_j\}$.

Vektor y_{k+1} iščemo v obliki $y_{k+1} = x_{k+1} - \alpha_1 y_1 - \dots - \alpha_k y_k$.

Ta vektor bo pravokoten na y_i ($1 \leq i \leq k$) natanko takrat, ko bo

$$\begin{aligned} 0 &= \langle y_{k+1}, y_i \rangle \\ &= \langle x_{k+1}, y_i \rangle - \sum_{j=1}^k \alpha_j \langle y_j, y_i \rangle \\ &= \langle x_{k+1}, y_i \rangle - \alpha_i \|y_i\|^2 \\ &\Leftrightarrow \alpha_i = \frac{\langle x_{k+1}, y_i \rangle}{\|y_i\|^2} \end{aligned}$$

Če torej definiramo $\alpha_i = \frac{\langle x_{k+1}, y_i \rangle}{\|y_i\|^2}$ za $i = 1, \dots, k$, potem bo $y_{k+1} \perp y_i$ za nek $i = 1, \dots, k$.

Dokazati moramo še, da je $\text{Lin}\{x_1, \dots, x_{k+1}\} = \text{Lin}\{y_1, \dots, y_{k+1}\}$ ⁹⁵

Ker je $\text{Lin}\{x_1, \dots, x_j\} = \text{Lin}\{y_1, \dots, y_j\}$ za $j = 1, \dots, k$ po induksijski predpostavki, zadošča dokazati, da je $y_{k+1} \in \text{Lin}\{x_1, \dots, x_k\}$ in $x_{k+1} \in \text{Lin}\{y_1, \dots, y_k\}$.

Ker je $\text{Lin}\{x_1, \dots, x_k\} = \text{Lin}\{y_1, \dots, y_k\}$ obstajajo $\beta_1, \dots, \beta_k \in F$, da je $\sum_{j=1}^k \alpha_j y_j = \sum_{j=1}^k \beta_j x_j$. ⁹⁶

$$\Rightarrow y_{k+1} = x_{k+1} - \sum_{j=1}^k \alpha_j y_j = x_{k+1} - \sum_{j=1}^k \beta_j x_j \in \text{Lin}\{x_1, \dots, x_{k+1}\}$$

in

$$x_{k+1} = y_{k+1} + \sum_{j=1}^k \alpha_j y_j \in \text{Lin}\{y_1, \dots, y_{k+1}\}$$

□

⁹⁵Od tod bo zaradi $\dim \text{Lin}\{x_1, \dots, x_{k+1}\}$ sledilo tudi, da so y_1, \dots, y_{k+1} linearno neodvisni.

⁹⁶Za α_j konstruirana zgoraj.

Posledica. Za linearno neodvisne vektorje $x_1, \dots, x_m \in V$ obstaja ortonormirana množica $\{y_1, \dots, y_m\} \subseteq V$, da je $\text{Lin}\{x_1, \dots, x_k\} = \text{Lin}\{y_1, \dots, y_k\}$ za vsak $k = 1, \dots, m$.

Dokaz. Množico iz posledice normiramo (y_j zamenjamo z $\frac{y_j}{\|y_j\|} \forall j$) in dobimo ortonormirano množico. Pri tem se linearne ogrinjače ne spremenijo. \square

Posledica. Vsak končnorazsežen vektorski prostor s skalarnim produktom ima ortonormirano bazo.

Dokaz. V prejšnji posledici za $\{x_1, \dots, x_m\}$ vzamemo bazo prostora V . Potem bo $\{y_1, \dots, y_m\}$ tudi baza. Po konstrukciji je ortonormirana. \square

Posledica. Vsako ortonormirano podmnožico končnorazsežnega vektorskega prostora s skalarnim produktom lahko dopolnimo do ortonormirane baze tega prostora.

Dokaz. Naj bo x_1, \dots, x_m ortonormirana podmnožica prostora V . Potem je linearno neodvisna in jo lahko dopolnimo do neke baze $\{x_1, \dots, x_m, x_{m+1}, \dots, x_n\}$ prostora V .

Na tej bazi izvedemo Gram - Schmidtov postopek za normiranje.

Dobimo ortonormirano bazo $\{y_1, \dots, y_n\}$, pri čemer je $y_1 = x_1, \dots, y_m = x_m$ ⁹⁷ \square

Lema. Naj bo v_1, \dots, v_m ortonormirana baza prostora V in $x \in V$. Potem velja:

1. $x = \sum_{j=1}^n \langle x, v_j \rangle v_j$
2. Če je še $y \in V$, velja $\langle x, y \rangle = \sum_{j=1}^n \langle x, v_j \rangle \langle y, v_j \rangle$ ⁹⁸

Dokaz.

1.

$$x = \sum_{j=1}^n \alpha_j v_j$$

Enakost skalarno pomnožimo z v_k .

$$\langle x, v_k \rangle = \sum_{j=1}^n \alpha_j \langle v_j, v_k \rangle \stackrel{99}{=} \alpha_k \text{ za vsak } k.$$

2. Po točki 1. je tudi $y = \sum_{j=1}^n \langle y, v_j \rangle v_j$

$$\begin{aligned} \Rightarrow \langle x, y \rangle &= \\ &= \left\langle \sum_{j=1}^n \langle x, v_j \rangle v_j, \sum_{j=1}^n \langle y, v_j \rangle v_j \right\rangle \stackrel{100}{=} \\ &= \sum_{j,k=1}^n \langle x, v_j \rangle \langle y, v_k \rangle \langle v_j, v_k \rangle \\ &= \sum_{j,k=1}^n \langle x, v_j \rangle \langle y, v_j \rangle \end{aligned}$$

⁹⁷Preveri.

⁹⁸Preveri indekse.

⁹⁹ $\langle v_j, v_k \rangle = \delta_{jk}$

□

Definicija. Vektorski prostor V_1 nad \mathcal{F} s skalarnim produktom \langle, \rangle_1 je izomorfen vektorskemu prostoru V_2 nad \mathcal{F} , s skalarnim produktom \langle, \rangle_2 , kadar obstaja tak izomorfizem vektorskih prostorov $\mathcal{F} : V_1 \rightarrow V_2$, da za vsaka $x, y \in V_1$ velja

$$\langle \mathcal{F}(x), \mathcal{F}(y) \rangle_2 = \langle x, y \rangle_1$$

Vektorska prostora s skalarnima produktoma sta izomorfna natanko takrat, ko sta izomorfna kot vektorska prostora, poleg tega pa mora izomorfizem ohranjati skalarni produkt.

Izomorfnost vektorskih prostorov je ekvivalenčna relacija.

Izrek. n - razsežen vektorski prostor na \mathcal{F} s skalarnim produktom je izomorfen \mathcal{F}^n s standardnim skalarnim produktom.

Dokaz.

$n = 0$ je očitno.

Za $n \geq 1$ v V lahko izberemo ortonormirano bazo v_1, \dots, v_n . Ortonormirana baza je baza,

zato že vemo, da je s predpisom $\mathcal{F}(\alpha_1 v_1 + \dots + \alpha_n v_n) = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}$ dobro definiran izomorfizem

vektorskih prostorov $\mathcal{F} : V \rightarrow \mathcal{F}^n$, potrebno je dokazati le, da ta izomorfizem ohranja skalarni produkt.

$$\begin{aligned} \langle x, y \rangle &= \\ &= \sum_{i=1}^n \langle x, v_i \rangle_v \cdot \langle \overline{y}, \overline{v_i} \rangle_v \\ &= \left\langle \begin{bmatrix} \langle x, v_1 \rangle_v \\ \vdots \\ \langle x, v_n \rangle_v \end{bmatrix} \cdot \begin{bmatrix} \langle y, v_1 \rangle_v \\ \vdots \\ \langle y, v_n \rangle_v \end{bmatrix} \right\rangle_{\mathcal{F}^n} \\ &= \langle \mathcal{F}(\sum_{j=1}^n \langle x, v_j \rangle_v v_j), \mathcal{F}(\sum_{j=1}^n \langle y, v_j \rangle_v v_j) \rangle_{\mathcal{F}^n} \\ &= \langle \mathcal{F}(x), \mathcal{F}(y) \rangle_{\mathcal{F}^n} \end{aligned}$$

□

Posledica. Končnorazsežna vektorska prostora s skalarnim produktom¹⁰¹ sta izomorfna kot prostora s skalarnima produktoma natanko takrat, ko imata isto razsežnost.

¹⁰¹Nad istim obsegom.

Definicija.

- Množici $M, N \subseteq V$ sta **pravokotni**,¹⁰² kadar velja $\langle x, y \rangle = 0$ za vse $x \in M$ in $y \in N$.
- Naj bodo $V_1, V_2, \dots, V_n \subseteq V$ podprostorji V in $V = V_1 + \dots + V_n$. Vsota $V_1 + \dots + V_n$ je pravokotna, kadar je $V_i \perp V_j$ za $i \neq j$.

Trditev. Pravokotna vsota je direktna.

Dokaz. Dokazati je potrebno, da je mogoče vsak $x \in V$ zapisati v obliki $x = x_1 + \dots + x_k$, kjer je $x_j \in V_j$ za vsak j na enoličen način.

Ker je $V = V_1 + \dots + V_k$, obstoj takega zapisa že imamo, dokazati je treba le še enoličnost.

Recimo, da je $x = x_1 + \dots + x_k = y_1 + \dots + y_k$, kjer $x_i, y_i \in V_i$ za vsak i .

$$0 = x_1 - y_1 + \dots + x_k - y_k$$

Naj bo j poljuben. Zgornjo enakost skalarno pomnožimo z $x_j - y_j$:

$$\begin{aligned} 0 &= \\ &= \sum_{i=1}^k \langle x_i - y_i, x_j - y_j \rangle^{103} \\ &= \|x_j - y_j\|^2 \\ &\Rightarrow y_j = x_j \end{aligned}$$

Oznaka za pravokotno vsoto: $V = V_1 \oplus \dots \oplus V_k$.

Treba je posebej poudariti ali ta oznaka pomeni pravokotno vsoto ali "le" direktno.

Definicija. Naj bo $M \subseteq V$ poljubna množica. Množico $M^\perp = \{x \in V; \langle x, y \rangle = 0 \text{ za vsak } y \in M\}$ imenujemo **pravokotni**¹⁰⁴ **komplement množice** M .

Če je $x \in V$, namesto $\{x\}^\perp$ pišemo x^\perp .

Posebna primera: $0^\perp = V, V^\perp = \{0\}$.

Trditev. M^\perp je vedno vektorski prostor.

Dokaz. Naj bosta $x, y \in M^\perp$ in $\alpha, \beta \in \mathcal{F}$. Dokazati želimo $\alpha x + \beta y \in M^\perp$. Če je $z \in M$ poljuben, je

$$\begin{aligned} \langle \alpha x + \beta y, z \rangle &= \\ &= \alpha \langle x, z \rangle + \beta \langle y, z \rangle \\ &= \alpha \cdot 0 + \beta \cdot 0 \\ &= 0 \\ &\Rightarrow \alpha x + \beta y \in M^\perp \end{aligned}$$

¹⁰²Oznaka: $M \perp N$.

¹⁰³ $0 \in V_j$

¹⁰⁴Ortogonalni.

□

Trditev. Naj bo $\{x_1, \dots, x_n\}$ ortonormirana baza za V in $1 \leq m \leq n$. Naj bo $V_1 = \text{Lin}\{v_1, \dots, v_m\}$ in $V_2 = \text{Lin}\{v_{m+1}, \dots, v_n\}$. Potem je $V = V_1 \oplus V_2$,¹⁰⁵ $V_1 = V_2^\perp$ in $V_2^\perp = V_1$.

Dokaz. Vemo že, da je $V = V_1 + V_2$ direktna vsota. Dokazati moramo še, pravokotnost. Naj bosta $x \in V_1$ in $y \in V_2$ poljubna. Potem je

$$x = \sum_{i=1}^m \alpha_i v_i \text{ in } y = \sum_{i=1}^m \beta_i v_i \text{ za neke } \alpha_i, \beta_i \in \mathcal{F}$$

$$\begin{aligned} \Rightarrow \langle x, y \rangle &= \\ &= \left\langle \sum_{i=1}^m \alpha_i v_i, \sum_{i=m+1}^n \beta_i v_i \right\rangle \\ &= \sum_{i=1}^m \sum_{j=m+1}^n \alpha_i \overline{\beta_j} \langle v_i, v_j \rangle \\ &= 0 \end{aligned}$$

$V_1 \perp V_2$. Dokazali smo tudi, da je $V_1 \subseteq V_2^\perp$ in $V_2 \subseteq V_1^\perp$. Dokazati je treba le še, da je $V_1^\perp \subseteq V_2$.¹⁰⁶ Naj bo $x \in V_1^\perp$. Potem je $x = \sum_{i=1}^m \langle x, v_i \rangle v_i$.

$$x \in V_1^\perp \Rightarrow \langle x, v_i \rangle = 0 \text{ za } i = 1, \dots, m$$

$$\Rightarrow x = \sum_{i=m+1}^n \langle x, v_i \rangle v_i \in V_2$$

□

Posledica. Naj bo W vektorski podprostor prostora V s skalarnim produktom. Potem je $V = W \oplus W^\perp$ ¹⁰⁷ in $W^{\perp\perp} = W$.¹⁰⁸

Dokaz. Za $W = \{0\}$ in $W = V$ je to očitno. Sicer pa izberimo ortonormirano bazo $\{v_1, \dots, v_n\}$ za W in jo dopolnimo do ortonormirane baze $\{v_1, \dots, v_m, \dots, v_n\}$ vektorskega prostora V . Po prejšnji trditvi je $\text{Lin}\{v_{m+1}, \dots, v_n\} = W^\perp$ in $W^{\perp\perp} = W$ in $V = W \oplus W^\perp$. □

Posledica. $\dim W + \dim W^\perp = \dim V$

Definicija. Naj bo W podprostor prostora s skalarnim produktom in $x \in V$. Če je $x = x_1 + x_2$, kjer je $x_1 \in W$ in $x_2 \in W^\perp$, potem vektor x_1 imenujemo **pravokotna projekcija** vektorja x za podprostor W .

¹⁰⁵Pravokotna vsota.

¹⁰⁶In zaradi simetrije tudi $V_2^\perp \subseteq V_1$.

¹⁰⁷Pravokotna vsota.

¹⁰⁸Involucija.

Ker je vsota $V = W \oplus W^\perp$ direktna ¹⁰⁹ pravokotna projekcija vsakega vektorja na W obstaja in je enolična.

Iz prejšnje trditve in njene posledica tudi vidimo, kako pravokotno projekcijo dobimo:

Če je $x = \sum \alpha_i v_i$, kjer je $\{v_1, \dots, v_n\}$ ortonormirana baza za V , pri čemer je $\{v_1, \dots, v_m\}$ ortonormirana baza za W in $v_i \in W^\perp$ za $i > m$, potem je pravokotna projekcija x na W enaka $\sum_{i=1}^m \alpha_i v_i = \sum_{i=1}^m \langle x, v_i \rangle v_i$.

Definirajmo preslikavo

$$P : V \rightarrow V$$

$$x \mapsto \sum_{i=1}^m \langle x, v_i \rangle v_i$$

$\text{im} P = W$ in za $x \in W$ velja $P(x) = x$.

$$x = P(x)^{110} + (x - P(x))^{111}$$

$$\ker P = W^\perp$$

P je **projektor** na W vzdolž W^\perp . Pravimo mu pravokotni projektor na podprostor W .

10.1 Preslikave na prostorih s skalarnim produktom

10.1.1 Reprezentacija linearnih funkcionalov na vektorskih prostorih s skalarnim produktom

Naj bo V vektorski prostor s skalarnim produktom in $z \in V$. Definiramo preslikavo

$$\varphi_z : V \rightarrow \mathcal{F}$$

$$x \mapsto \langle x, z \rangle$$

Lema. φ_z je linearen funkcional.

Dokaz.

$$\begin{aligned} \varphi_z(\alpha x + \beta y, z) &= \\ &= \langle \alpha x + \beta y, z \rangle \\ &= \alpha \langle x, z \rangle + \beta \langle y, z \rangle \\ &= \alpha \varphi_z(x) + \beta \varphi_z(y) \end{aligned}$$

□

¹⁰⁹Celo pravokotna.

¹¹⁰ $P(x) \in W$

¹¹¹ $x - P(x) \in W^\perp$

Ali so to vsi linearni funkcionali na V ?

Zaradi leme lahko definiramo preslikavo

$$\Phi : V \rightarrow V^*$$

$$z \mapsto \varphi_z^{112}$$

Izrek. Preslikava $\Phi : V \rightarrow V^*$, definirana s predpisom $\Phi(z) = \varphi_z$ je **poševni izomorfizem**, kar pomeni, da je **aditivna**, **poševno homogena** bijekcija.

Dokaz.

1. aditivnost

$$\begin{aligned}\Phi(z_1 + z_2)(x) &= \\ &= \langle x, z_1 + z_2 \rangle \\ &= \langle x, z_1 \rangle + \langle x, z_2 \rangle \\ &= \Phi(z_1)(x) + \Phi(z_2)(x) \\ &= (\Phi(z_1) + \Phi(z_2))(x) \text{ za vsak } x \in V\end{aligned}$$

$$\Phi(z_1 + z_2) = \Phi(z_1) + \Phi(z_2) \text{ za vsak } z_1, z_2 \in V$$

2. poševna homogenost

$$\begin{aligned}\Phi(\alpha z)x &= \\ &= \langle x, \alpha z \rangle \\ &= \bar{\alpha} \langle x, z \rangle \\ &= \bar{\alpha}(\Phi(z)(x)) \\ &= (\bar{\alpha}\Phi(z))x \text{ za vsak } x \in V\end{aligned}$$

$$\Rightarrow \Phi(\alpha z) = \bar{\alpha}\Phi(z) \text{ za vsak } z \in V \text{ in vsak } \alpha \in F$$

3. injektivnost

Naj bo $\Phi(z_1) = \Phi(z_2)$. To pomeni, da je $\Phi(z_1)x = \Phi(z_2)x$ za vsak $x \in V$.

$$\langle x, z_1 \rangle = \langle x, z_2 \rangle \text{ za vsak } x \in V$$

$$\langle x, z_1 - z_2 \rangle = 0 \text{ za vsak } x \in V \Rightarrow z_2 = z_1^{113}$$

4. surjektivnost

Naj bo $\varphi \in V^*$. Iščemo $z \in V$, da bo $\varphi = \varphi_z$, torej $\varphi(x) = \langle x, z \rangle$ za vsak $x \in V$.

¹¹² = $x \mapsto \langle x, z \rangle$

¹¹³ Spomnimo se: edini vektor, ki je pravokoten na vse vektorje je enak 0 ali pa vzamemo $x = z_1 - z_2$

Če je $\varphi = 0$, lahko vzamemo $z = 0$.

Naj bo torej $\varphi \neq 0$. Potem je φ surjektiven in $\dim(\ker \varphi) = n - 1$ ¹¹⁴ Naj bo $V = \ker \varphi$

$$\dim U^\perp = n - (n - 1) = 1$$

\Rightarrow obstaja $v \in V$, da je $U^\perp = \text{Lin}\{v\}$.

Naj bo $x \in V$ poljuben. Vemo, da je $V = U \oplus U^\perp$.¹¹⁵ To pomeni, da obstajata enolična $y \in U$ in $\alpha \in F$, da je $x = y + \alpha v$

$$\Rightarrow \langle x, v \rangle = \langle y, v \rangle$$
¹¹⁶

Brez škode za splošnost lahko privzamemo, da je $\|v\| = 1$.

$$\Rightarrow \alpha = \langle x, v \rangle \Rightarrow x = y + \langle x, v \rangle v$$

$$\varphi(x) = \varphi(y) + \varphi(\langle x, v \rangle v) = \langle x, v \rangle \varphi(v) = \langle x, \overline{\varphi(v)} \rangle, v \rangle$$

Če vzamemo $z = \overline{\varphi(v)}$, bo $\varphi(x) = \langle x, z \rangle$ za vsak $x \in V$, torej $\varphi = \varphi_z$.

□

Posledica. (Riesrov izrek o reprezentaciji linearnih funkcionalov na prostorih s skalarnim produktom)

Za vsak $\varphi \in V^*$ obstaja natanko en $z \in V$, da je $\varphi(x) = \langle x, z \rangle$ za vsak $x \in V$.¹¹⁹

Če imamo na V skalarni produkt, pa je V poševno izomorfen V^* ($V^* \cong V$ za $F = \mathbb{R}$) in ta poševni izomorfizem ni odvisen od izbire baze.

10.2 Hermitsko adjungirana preslikava

Spomnimo se: če je $\mathcal{A} : U \rightarrow V$, pri čemer je \mathcal{A} linearna, potem je dualna preslikava $\mathcal{A}^d : V^* \rightarrow U^*$, definirana s predpisom $\mathcal{A}^d(\varphi) = \varphi \circ \mathcal{A}$.

$$\begin{array}{ccc} U & \xrightarrow{\mathcal{A}} & V \\ & \searrow \varphi \circ \mathcal{A} & \downarrow \varphi \\ & & F \end{array}$$

¹¹⁴Kjer je $n = \dim V$.

¹¹⁵Pravokotna vsota.

¹¹⁶0, ker je $y \in U, v = U^\perp$ ($y \cdot v = 0$)

¹¹⁷0, ker je $y \in \ker \varphi$

¹¹⁸ $\langle x, v \rangle \varphi(v) \in F$

¹¹⁹Opomba: Če je $\dim V < \infty$ velja $V \cong V^*$, kar pomeni, da je izomorfizem odvisen od izbire baze.

Definicija. Naj bosta $\Phi_u : U \rightarrow U^*$ in $\Phi_v : V \rightarrow V^*$ poševna izomorfizma iz prejšnjega izreka. Preslikava $\mathcal{A}^* : V \rightarrow U$, definirana s predpisom

$$\mathcal{A}^* = \Phi_u^{-1} \circ \mathcal{A}^d \circ \Phi_v$$

se imenuje **hermitsko adjungirana preslikava** preslikave \mathcal{A} .

To je torej enolična¹²⁰ preslikava, za katero komutira diagram

$$\begin{array}{ccc} V^* & \xrightarrow{\mathcal{A}^d} & U^* \\ \Phi_v \uparrow & & \uparrow \Phi_u \\ V & \xrightarrow{\mathcal{A}^*} & U \end{array}$$

Trditev. \mathcal{A}^* je linearna preslikava.

Dokaz. Dokaz doma.¹²¹

Lema. Če za linearni preslikavi $\mathcal{A}, \mathcal{B} : U \rightarrow V$ velja $\langle \mathcal{A}x, y \rangle = \langle \mathcal{B}x, y \rangle$ za vsak $x \in U$ in vsak $y \in V$, potem je $\mathcal{A} = \mathcal{B}$.

Dokaz. Naj bo $x \in U$ poljuben. Potem je $\langle \mathcal{A}x - \mathcal{B}x, y \rangle = 0$ za vsak $y \in V$. Zato je $\mathcal{A}x = \mathcal{B}x$.¹²² □

Trditev. Naj bo \mathcal{A} linearna preslikava, $\mathcal{A} : U \rightarrow V$. Potem je $\langle \mathcal{A}x, y \rangle_V = \langle x, \mathcal{A}^*y \rangle_U$ za vsak $x \in U$ in vsak $y \in V$. Poleg tega je \mathcal{A}^* edina linearna preslikava iz V v U s to lastnostjo.

Dokaz.

$$\begin{aligned} \langle x, \mathcal{A}^*y \rangle_U &= \\ &= \langle x, (\Phi_U^{-1} \circ \mathcal{A}^d \circ \Phi_V)(y) \rangle_U \\ &= \langle x, \Phi_U^{-1}(\mathcal{A}^d(\Phi_V(y))) \rangle_U \\ &= (\Phi_U(\Phi_U^{-1} \circ \mathcal{A}^d \circ \Phi_V(y)))(x) \\ &= (\mathcal{A}^d \circ \Phi_V(y))(x) \\ &= \Phi_V(y)(\mathcal{A}x) \\ &= \langle \mathcal{A}x, y \rangle_V \end{aligned}$$

¹²³ enoličnost:

Če je $\mathcal{B} : V \rightarrow U$ linearna preslikava, za katero velja $\langle \mathcal{A}x, y \rangle_V = \langle x, \mathcal{B}y \rangle_U$ za vsak $x \in U$ in za vsak $y \in V$. Potem velja $\langle \mathcal{B}y, x \rangle_U = \langle \mathcal{A}^d y, x \rangle_U$ za vsak $x \in U$ in vsak $y \in V$. Po lemi je $\mathcal{B} = \mathcal{A}^*$. □

¹²⁰Enolična je zato, ker sta Φ_v in Φ_u bijekciji.

¹²¹Dopiši.

¹²²Ker je bil x poljuben, torej je $\mathcal{A} = \mathcal{B}$.

¹²³Preveri.

Posledica. Naj bosta U in V prostora s skalarnim produktom. Če so $\mathcal{A}, \mathcal{B}, \mathcal{C}$ linearne preslikave med ustreznimi prostori s skalarnim produktom, potem velja

$$1. \langle \mathcal{A}^*x, y \rangle_V = \langle x, \mathcal{A}y \rangle_U \text{ za vse } x \in U \text{ in } y \in V, \text{ če } \mathcal{A} : V \rightarrow U.$$

$$2. \mathcal{A}^{**} = \mathcal{A}^{124}$$

$$3. (\mathcal{A} + \mathcal{B})^* = \mathcal{A}^* + \mathcal{B}^*$$

$$4. (\alpha\mathcal{A})^* = \overline{\alpha}\mathcal{A}$$

$$5. (\mathcal{AC})^* = \mathcal{C}^*\mathcal{A}^*$$

Dokaz.

1.

$$\begin{aligned} \langle \mathcal{A}^*x, y \rangle_V &= \\ &= \langle \overline{y}, \mathcal{A}^*x \rangle_V \\ &= \langle \mathcal{A}y, x \rangle_U \\ &= \langle x, \mathcal{A}y \rangle_U \end{aligned}$$

$$2. \langle \mathcal{A}^*x, y \rangle_V \stackrel{125}{=} \langle x, \mathcal{A}^{**}y \rangle \text{ za vse } x \in U \text{ in } y \in V. \text{ Po lemi je } \mathcal{A}^{**} = \mathcal{A}.$$

$$3. \text{Napravite sami}^{126}$$

$$4. \text{Napravite sami}^{127}$$

5.

$$\begin{aligned} \langle (\mathcal{AC})^*x, y \rangle &= \\ &= \langle x, \mathcal{AC}y \rangle \\ &= \langle x, \mathcal{A}(\mathcal{C}(y)) \rangle \\ &= \langle \mathcal{A}^*x, \mathcal{C}y \rangle \\ &= \langle \mathcal{C}^*\mathcal{A}^*x, y \rangle \end{aligned}$$

$$\forall x, \forall y \Rightarrow (\mathcal{A} \circ \mathcal{C})^* = \mathcal{C}^*\mathcal{A}^*$$

□

Trditev. Naj bo \mathcal{A} linearna preslikava. $\mathcal{A} : U \rightarrow V$.¹²⁸ Potem je $U = \ker \mathcal{A} \oplus \operatorname{im} \mathcal{A}^*$ ¹²⁹ in $\operatorname{im} \mathcal{A}^* = (\ker \mathcal{A})^\perp$.

¹²⁴Če je $\mathcal{A} \in \mathcal{L}(V)$, je preslikava $\mathcal{A} \rightarrow \mathcal{A}^*$ involucija.

¹²⁵ $\langle x, \mathcal{A}y \rangle_U$

¹²⁶Dopiši.

¹²⁷Dopiši.

¹²⁸ U, V sta vektorska prostora s skalarnim produktom.

¹²⁹Pravokotna vsota.

Dokaz. Vemo, da je $V = \ker \mathcal{A} \oplus (\ker \mathcal{A})^\perp$ pravokotna vsota. Dokazati je treba, da je $\operatorname{im} \mathcal{A}^* = (\ker \mathcal{A})^\perp$.

Naj bo $x \in \ker \mathcal{A}$ in $y \in \operatorname{im} \mathcal{A}^*$. Potem obstaja $z \in V$, da je $y = \mathcal{A}^* z$

$$\begin{aligned} \langle x, y \rangle &= \\ &= \langle x, \mathcal{A}^* z \rangle \\ &= \langle \mathcal{A} x, z \rangle \\ &= 0 \text{ za vsak } x \in \ker \mathcal{A} \text{ in vsak } y \in \operatorname{im} \mathcal{A}^* \end{aligned}$$

$$\Rightarrow \operatorname{im} \mathcal{A}^* \subseteq (\ker \mathcal{A})^\perp$$

Obratno, naj bo $u \in (\operatorname{im} \mathcal{A}^*)^\perp$. Potem je $\langle u, \mathcal{A}^* v \rangle = 0$ za vsak $v \in V$.

$$\begin{aligned} \langle \mathcal{A} u, v \rangle &= 0 \\ \Rightarrow \mathcal{A} u \text{ mora biti } 0 &\Rightarrow u \in \ker \mathcal{A} \\ \Rightarrow (\operatorname{im} \mathcal{A}^*)^\perp &\subseteq \ker \mathcal{A} \\ &= (\ker \mathcal{A})^\perp \subseteq \operatorname{im} \mathcal{A}^* \end{aligned}$$

□

Posledica. $\operatorname{rang} \mathcal{A}^* = \operatorname{rang} \mathcal{A}$

Dokaz. Dokazali smo, da je $U = \ker \mathcal{A} \oplus \operatorname{im} \mathcal{A}^*$.¹³⁰

$$\Rightarrow \dim U = \dim \ker \mathcal{A} + \operatorname{rang} \mathcal{A}^*$$

Vemo pa tudi, da je $U = \dim(\operatorname{im} \mathcal{A}) + \operatorname{rang} \mathcal{A}$.

$$\Rightarrow \operatorname{rang} \mathcal{A}^* = \operatorname{rang} \mathcal{A}$$

□

Trditev. Naj bo $\mathcal{A} \in \mathcal{L}(V)$ in $U \subseteq V$ podprostor. Potem je U invarianten za \mathcal{A} natanko takrat, ko je U^\perp invarianten za \mathcal{A}^* .

Dokaz. \Rightarrow Naj bo U invarianten za \mathcal{A} in $x \in U^\perp$. Radi bi dokazali, da je $\mathcal{A}^* x \in U^\perp$.

Naj bo $y \in U$ poljuben. Potem je $\mathcal{A} y \in U$.

$$\Rightarrow \langle \mathcal{A}^* x, y \rangle = \langle x, \mathcal{A} y \rangle = 0^{131}$$

Ker je bil $y \in U$ poljuben, je $\mathcal{A}^* x \in U^\perp$.

\Leftarrow Naj bo U^\perp invarianten za \mathcal{A}^* . Potem je $U = U^{\perp\perp}$ invarianten za $\mathcal{A}^{**} = \mathcal{A}$. □

¹³⁰Kjer je $\mathcal{A} \in L(U, W)$.

¹³¹ $x \in U^\perp, \mathcal{A} y \in U$

Izrek. Naj bosta U in V oba evklidska ali unitarna prostora in $\mathcal{A} \in L(U, V)$. Naj bo $\{u_1, \dots, u_m\}$ ortonormirana baza za U in $\{v_1, \dots, v_n\}$ ortonormirana baza za V . Glede na ti dve bazi naj preslikavi \mathcal{A} pripada matrika $A = [a_{ij}]_{1 \leq i \leq m, 1 \leq j \leq n}$. Potem velja

1. $a_{ij} = \langle \mathcal{A}u_j, v_i \rangle$ za vsaka $i = 1, \dots, m$ in $j = 1, \dots, n$.

2. Preslikava $\mathcal{A}^* \in \mathcal{L}(V, U)$ glede na bazi $\{v_1, \dots, v_n\}$ in $\{u_1, \dots, u_m\}$ pripada matrika $A^H = [b_{ij}]_{1 \leq i \leq m, 1 \leq j \leq n}$, kjer je $b_{ij} = \overline{a_{ij}}$ za vsaka i in j velja $A^H = \overline{A^T}$. Matriko A^H imenujemo **hermitska transponiranka** matrike A .¹³²

Dokaz.

1.

$$\begin{aligned} \mathcal{A}u_i &= a_{1i}v_1 + a_{2i}v_2 + \dots + a_{ni}v_n \\ \langle \mathcal{A}u_i, v_j \rangle &= \\ &= \sum_{k=1}^n \langle a_{ki}v_k, v_j \rangle \\ &= \sum_{k=1}^n a_{ki} \langle v_k, v_j \rangle^{133} \\ &= a_{ji} \end{aligned}$$

2.

$$\begin{aligned} b_{ij} &= \\ &= \langle \mathcal{A}^*v_j, u_i \rangle \\ &= \overline{\langle u_i, \mathcal{A}^*v_j \rangle} \\ &= \overline{\langle \mathcal{A}u_i, v_j \rangle} \\ &= a_{ij} \end{aligned}$$

□

10.3 Normalni endomorfizmi

V naj bo evklidski ali unitaren prostor in $\mathcal{A} \in \mathcal{L}(V)$. Vemo, da se da \mathcal{A} diagonalizirati \Leftrightarrow obstaja baza sestavljena iz lastnih vektorjev endomorfizma \mathcal{A} .

Kdaj se da \mathcal{A} diagonalizirati v ortonormirani bazi?

Kdaj obstaja ortonormirana baza za V , sestavljena iz lastnih vektorjev za \mathcal{A} ?

Recimo, da se endomorfizem \mathcal{A} da diagonalizirati v neki ortonormirani bazi. Naj bo A pripadajoča diagonalna matrika.

¹³²Opomba: Če A identificiramo s preslikavo $F^m \rightarrow F^n, x \mapsto Ax$, potem je A^H matrika preslikave A^* , glede na standardni bazi prostorov F^n in F^m .

Ker je baza ortonormirana v tej isti bazi endomorfizmu \mathcal{A}^* pripada matrika A^H , ki je tudi diagonalna.

Diagonalne matrike komutirajo $\Rightarrow AA^H = A^H A$.

Enako velja tudi za preslikavi $\Rightarrow A \circ A^H = A^H \circ A$.

Definicija. $\mathcal{A} \in \mathcal{L}(V)$ je **normalen endomorfizem**, kadar je $\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A}$.

$A \in \mathbb{C}^{n \times n}$ je **normalna matrika**, kadar je $AA^H = A^H A$. Normalnemu endomorfizmu glede na ortonormirano bazo priprada normalna matrika.

Posledica. Vsak endomorfizem, ki se da diagonalizirati v ortonormirani bazi, je normalen.

Trditev. $\mathcal{A} \in \mathcal{L}(V)$ je normalen endomorfizem natanko takrat, ko velja $\langle \mathcal{A}x, \mathcal{A}y \rangle = \langle \mathcal{A}^*x, \mathcal{A}^*y \rangle$ za vsaka $x, y \in V$.

Dokaz. \Rightarrow

$$\begin{aligned} \langle \mathcal{A}^*x, \mathcal{A}^*y \rangle &= \\ &= \langle \mathcal{A}\mathcal{A}^*x, y \rangle \\ &= {}^{134} \langle \mathcal{A}^*\mathcal{A}x, y \rangle \\ &= \langle \mathcal{A}x, \mathcal{A}y \rangle \end{aligned}$$

\Leftarrow Predpostavimo $\langle \mathcal{A}x, \mathcal{A}y \rangle {}^{135} = \langle \mathcal{A}^*x, \mathcal{A}^*y \rangle {}^{136}$ za vse $x, y \in V$. Vemo, da od tod sledi $\mathcal{A}^*\mathcal{A} = \mathcal{A}\mathcal{A}^*$. \square

Posledica. Naj bo $\mathcal{A} \in \mathcal{L}(V)$ normalen endomorfizem. Potem velja

1. $\|\mathcal{A}^*x\| = \|\mathcal{A}x\|$ za vsak $x \in V$
2. $\ker \mathcal{A}^* = \operatorname{im} \mathcal{A}$
3. $\mathcal{A} - \alpha \operatorname{id}_V$ je normalen za vsak $\alpha \in F$
4. za $\alpha \in F$ in $x \in V$ velja

$$\mathcal{A}x = \alpha x \Leftrightarrow \mathcal{A}^*x = \bar{\alpha}x$$

5. $\delta(\mathcal{A}^*) = \{\alpha \in F, \bar{\alpha} \in \delta(\mathcal{A})\} = \overline{\delta(\mathcal{A})}$

6. Lastna vektorja, ki pripadata različnim lastnim vrednostima preslikave \mathcal{A} , sta pravokotna.

Dokaz.

1. V trditev vstavimo $y = x$.
2. Sledi iz 1.

¹³⁵ $= \langle \mathcal{A}^*\mathcal{A}x, y \rangle$

¹³⁶ $= \langle \mathcal{A}\mathcal{A}^*x, y \rangle$

3.

$$\begin{aligned}
 (\mathcal{A} - \alpha id_v)^*(\mathcal{A} - \alpha id_v) &= \\
 &= (\mathcal{A}^* - \bar{\alpha} id_v)(\mathcal{A} - \alpha id_v) \\
 &= \mathcal{A}^* \mathcal{A} - \alpha \mathcal{A}^* - \bar{\alpha} \mathcal{A} + \|\alpha\|^2 id_v \\
 &= \mathcal{A} \mathcal{A}^* \dots \\
 &= (\mathcal{A}^* - \bar{\alpha} id_v)(\mathcal{A} - \alpha id_v)
 \end{aligned}$$

4.

$$\begin{aligned}
 \mathcal{A}x = \alpha x &\Leftrightarrow x \in \ker(\mathcal{A} - \alpha id_v)^{137} \\
 \Leftrightarrow {}^{138} x &\in \ker(\mathcal{A} - \alpha id_v)^* = \ker(\mathcal{A}^* - \bar{\alpha} id_v) \\
 &\Leftrightarrow \mathcal{A}^* x = \bar{\alpha} x
 \end{aligned}$$

5. Sledi iz 4.

6. Naj bo $\mathcal{A}x_1 = \lambda_1 x_1$ in $\mathcal{A}x_2 = \lambda_2 x_2$, kjer je $\lambda_1 \neq \lambda_2$.

$$\begin{aligned}
 \lambda_1 \langle x_1, x_2 \rangle &= \\
 &= \langle \lambda_1 x_1, x_2 \rangle \\
 &= \langle \mathcal{A}x_1, x_2 \rangle \\
 &= \langle x_1, \mathcal{A}^* x_2 \rangle \\
 &= {}^{139} \langle x_1, \bar{\lambda}_2 x_2 \rangle \\
 &= \lambda_2 \langle x_1, x_2 \rangle
 \end{aligned}$$

$$\lambda_1 \neq \lambda_2 \Rightarrow \langle x_1, x_2 \rangle = 0$$



□

Izrek. Naj bo $\mathcal{A} \in \mathcal{L}(V)$ normalen endomorfizem. Če je $\mathcal{F} = \mathbb{C}$ ali če je $\mathcal{F} = \mathbb{R}$ in ima karakteristični polinom $\Delta_{\mathcal{A}}(\lambda)$ same realne ničle, potem se da \mathcal{A} diagonalizirati v ortonormirani bazi.

Dokaz. Z indukcijo na $n = \dim V$.

$n = 1$ Očitno.

$n \rightarrow n + 1$:

Predpostavimo, da je $\dim V = n + 1 \geq 2$ in da izrek velja za vse n - razsežne prostore s skalarnim produktom.

Predpostavka izreka nam pove, da ima $\Delta_{\mathcal{A}}(\lambda)$ vse ničle v \mathcal{F} . Ničle $\Delta_{\mathcal{A}}(\lambda)$ so lastne vrednosti endomorfizma \mathcal{A} , zato v V obstaja vsaj en lastni vektor za \mathcal{A} .

$\mathcal{A}v_1 = \lambda_1 v_1$, kjer je $v_1 \in V, \lambda_1 \in \mathcal{F}$.¹⁴⁰

Ker je v_1 lastni vektor za \mathcal{A} , je $\text{Lin}\{v_1\}$ invarianten podprostor za \mathcal{A} .

Vemo, da od tod sledi, da je v_1^\perp invarianten podprostor za \mathcal{A}^* . Očitno je $\dim V_1^\perp = \dim V - 1 = n$.

$\mathcal{A}v_1 = \lambda_1 v_1 \Rightarrow \mathcal{A}^*v_1 = \overline{\lambda_1}v_1$, kjer je \mathcal{A} normalen. Torej je $\text{Lin}\{v_1\}$ invarianten podprostor tudi za \mathcal{A}^* in zato je v_1^\perp invarianten podprostor za \mathcal{A} . Zožitev endomorfizma \mathcal{A} in \mathcal{A}^* na v_1^\perp sta endomorfizma n - razsežnega prostora v_1^\perp .

Očitno zožitvi \mathcal{A} in \mathcal{A}^* na v_1^\perp tudi komutirata.

$\Rightarrow \mathcal{A}|_{v_1^\perp}$ je normalen.

Ničle karakterističnega polinoma zožitve $\mathcal{A}|_{v_1^\perp}$ so tudi ničle $\Delta_{\mathcal{A}}(\lambda)$, torej vse ležijo v \mathcal{F} .

Po indukcijski predpostavki obstaja ortonormirana baza $\{v_1, \dots, v_{n+1}\}$ prostora v_1^\perp v kateri je matrika zožitve $\mathcal{A}|_{v_1^\perp}$ diagonalna.

Potem pa se \mathcal{A} diagonalizira v ortonormirani bazi $\{v_1, \dots, v_{n+1}\}$ prostora V .

Posledica. Za $A \in \mathbb{C}^{n \times n}$ velja $A^H A = A A^H$ natanko takrat, ko obstaja ortonormirana baza \mathbb{C}^n , sestavljena iz lastnih vektorjev matrike A .

Izrek (Schunov izrek). Naj bo V unitaren prostor¹⁴¹ in $\mathcal{A} \in \mathcal{L}(V)$. Potem obstaja ortonormirana baza prostora V , glede na katero je matrika za \mathcal{A} zgornje trikotna.

Dokaz. V Jordanovi bazi je matrika za \mathcal{A} zgornje trikotna. Na Jordanovi bazi izvedemo Gramm - Schmidtov postopek za normiranje. Dobimo ortonormirano bazo v kateri je matrika z \mathcal{A} zgornje trikotna.

10.4 Sebi adjungirani endomorfizmi

Definicija. Endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ je sebi adjungiran, kadar je $\mathcal{A}^* = \mathcal{A}$.

Očitno je vsak sebi adjungiran endomorfizem normalen.

Naj bo A^{142} matrika, ki pripada endomorfizmu \mathcal{A} glede na neko ortonormirano bazo.

Velja $\mathcal{A}^* = \mathcal{A} \Leftrightarrow A^H = A$.

Definicija. Matrika $A \in \mathbb{C}^{n \times n}$ je **hermitska**, kadar je $A^H = A$. Matrika $A \in \mathbb{R}^{n \times n}$ je **simetrična**, kadar je $A^T = A$.

¹⁴⁰Brez škode za splošnost lahko privzamemo $\|v_1\| = 1$.

¹⁴¹Nad \mathbb{C} .

¹⁴² $\in \mathbb{C}^{n \times n}$

Trditev. Endomorfizem \mathcal{A} je sebi adjungiran natanko takrat, ko velja $\langle \mathcal{A}x, y \rangle = \langle x, \mathcal{A}y \rangle$ za vse $x, y \in V$.

Dokaz.

(\Rightarrow) Predpostavimo $\mathcal{A} = \mathcal{A}^*$.

$$\langle \mathcal{A}x, y \rangle = \langle x, \mathcal{A}^*y \rangle = \langle x, \mathcal{A}y \rangle$$

(\Leftarrow) Naj bo $\langle \mathcal{A}x, y \rangle = \langle x, \mathcal{A}y \rangle$ za vse $x, y \in V$. Potem je $\langle \mathcal{A}x, y \rangle = \langle \mathcal{A}^*x, y \rangle$ za vse $x, y \in V$. Potem vemo, da mora biti $\mathcal{A} = \mathcal{A}^*$. \square

Trditev. Naj bo $\mathcal{A} \in \mathcal{L}(V)$ sebi adjungiran endomorfizem. Če je $\langle \mathcal{A}x, x \rangle = 0$ za vsak $x \in V$, potem je $\mathcal{A} = 0$.

Dokaz. Po predpostavki je $0 = \langle \mathcal{A}(x+y), x+y \rangle$ za vse $x, y \in V$.

$$\begin{aligned} 0 &= \\ &= \langle \mathcal{A}x, x \rangle + \langle \mathcal{A}x, y \rangle + \langle \mathcal{A}y, x \rangle + \langle \mathcal{A}y, y \rangle^{143} \\ &= \langle \mathcal{A}x, y \rangle + \langle \mathcal{A}y, x \rangle^{144} \\ &= \langle \mathcal{A}x, y \rangle + \langle y, \mathcal{A}x \rangle \\ &= 2 \langle \mathcal{A}x, \mathcal{A}x \rangle \\ &= 2\|\mathcal{A}x\|^2 \text{ za vsak } x \in V \Rightarrow \mathcal{A} = 0 \end{aligned}$$

\square

Izrek. Vse ničle karakterističnega polinoma sebi adjungiranega endomorfizma so realne.

Dokaz.

1. $\mathcal{F} = \mathbb{C}$

$$\Delta_{\mathcal{A}}(\alpha) = 0 \Rightarrow \alpha \text{ je lastna vrednost za } \mathcal{A}$$

$$\text{Obstaja torej } v \neq 0, \text{ da je } \mathcal{A}v = \alpha v$$

$$\Rightarrow \mathcal{A}^*v = \bar{\alpha}v =^{145} \mathcal{A}v$$

$$\mathcal{A}v = \alpha v$$

$$\mathcal{A}v = \bar{\alpha}v$$

$$(\alpha - \bar{\alpha})v = 0$$

$$\Rightarrow \alpha - \bar{\alpha} = 0$$

$$\alpha = \bar{\alpha}$$

$$\Rightarrow \alpha \in \mathbb{R}$$

¹⁴⁴0 po predpostavki

¹⁴⁴ $\mathcal{A} = \mathcal{A}^*$

¹⁴⁵ $\mathcal{A}^* = \mathcal{A}$

2. $\mathcal{F} = \mathbb{R}$

Endomorfizmu \mathcal{A} naj glede na neko ortonormirano bazo pripada matrika A . Ker je $\mathcal{A}^* = \mathcal{A}$, je $A^T = A^H = A \in \mathbb{R}^{n \times n}$.

Seveda je $A \in \mathbb{C}^{n \times n}$ in ustreza endomorfizmu $\mathcal{A} : x \mapsto \mathcal{A}x$ kompleksnega vektorskega prostora \mathbb{C}^n s standardnim skalarnim produktom glede na standardno bazo¹⁴⁶ prostora \mathbb{C}^n .

$A^H = A \Rightarrow \mathcal{A} : \mathbb{C}^n \rightarrow \mathbb{C}^n$ je sebi adjungirana preslikava.

Po točki (1) ima $\Delta_{\mathcal{A}}(\lambda)$ same realne ničle.

$\Delta_{\mathcal{A}}(\lambda) = \Delta_A(\lambda) \Rightarrow \Delta_A(\lambda)$ ima same realne ničle.

□

Posledica. Če je $\mathcal{A} \in \mathcal{L}(V)$ sebi adjungiran je $\delta(\mathcal{A}) \subseteq \mathbb{R}$.

Izrek. Endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ je sebi adjungiran natanko takrat, ko se da diagonalizirati v ortonormirani bazi in ima vse lastne vrednosti realne.

Dokaz.

(\Rightarrow) To velja po prejšnji trditvi in izreku o diagonalizaciji normalnih endomorfizmov.

(\Leftarrow) Naj bo A diagonalna matrika endomorfizma v neki ortonormirani bazi.¹⁴⁷ Po predpostavki je A realna matrika $\Rightarrow A^H = A \Rightarrow \mathcal{A}^* = \mathcal{A}$ □

Če je V kompleksen vektorski prostor s skalarnim produktom in $\mathcal{A} \in \mathcal{L}(V)$ poljuben endomorfizem, potem obstajata enolično določena sebi adjungirana endomorfizma $\mathcal{B}, \mathcal{C} \in \mathcal{L}(V)$, da je $\mathcal{A} = \mathcal{B} + i\mathcal{C}$.


$$\mathcal{B} = \frac{1}{2}(\mathcal{A} + \mathcal{A}^*) \quad \mathcal{C} = \frac{1}{2i}(\mathcal{A} - \mathcal{A}^*)$$

Običajno endomorfizmu $\frac{1}{2}(\mathcal{A} + \mathcal{A}^*)$ rečemo **realni del** endomorfizma \mathcal{A} , $\frac{1}{2i}(\mathcal{A} - \mathcal{A}^*)$ pa **imaginarni del** endomorfizma \mathcal{A} .¹⁴⁸

10.5 Pozitivno (semi)definitni endomorfizmi

Definicija. Endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ je:

1. **pozitivno semidefiniten**, kadar je sebi adjungiran in velja $\langle \mathcal{A}x, x \rangle \geq 0$ za vsak $x \in V$

¹⁴⁶Standardna baza je seveda tudi ortonormirana 

¹⁴⁷Ki obstaja po predpostavki.

¹⁴⁸Analogno: $z = \operatorname{Re}(z) + i\operatorname{Im}(z)$ za $z \in \mathbb{C}$.

2. **pozitivno definiten**, kadar je sebi adjungiran in velja $\langle Ax, x \rangle > 0$ za vsak $x \in V \setminus \{0\}$
3. **negativno semidefiniten**, kadar je sebi adjungiran in velja $\langle Ax, x \rangle \leq 0$ za vsak $x \in V$
4. **negativno definiten**, kadar je sebi adjungiran in velja $\langle Ax, x \rangle < 0$ za vsak $x \in V \setminus \{0\}$

A je negativno (semi)definiten $\Leftrightarrow -A$ pozitivno (semi)definiten. Zato bomo obravnavali le pozitivno (semi)definitne endomorfizme.

Izrek. Endomorfizem $A \in \mathcal{L}(V)$ je pozitivno semidefiniten/definiten natanko takrat, ko je sebi adjungiran in ima same nenegativne/strogo pozitivne lastne vrednosti.

Dokaz.

(\Rightarrow) Naj bo $Ax = \alpha x$ za nek $x \neq 0$.

Potem je $\langle Ax, x \rangle = \langle \alpha x, x \rangle = \alpha \|x\|^2$

$\Rightarrow \alpha \geq 0$ če je A pozitivno semidefiniten

$\alpha > 0$ če je A pozitivno definiten

(\Leftarrow) Naj bo A sebi adjungiran in naj ima nenegativne/strogo pozitivne lastne vrednosti.

Ker je A sebi adjungiran se diagonalizira v neki ortonormirani bazi, torej obstaja ortonormirana baza $\{v_1, \dots, v_n\}$ za V in obstajajo števila $\alpha_1, \dots, \alpha_n \in \mathbb{R}$, ki so po predpostavki nenegativna/strogo pozitivna, da je $Av_1 = \alpha_1 v_1, \dots, Av_n = \alpha_n v_n$.

Naj bo $x \in V$ poljuben. x razvijamo po bazi:

$$x = \sum_{j=1}^n \beta_j v_j$$

$$\begin{aligned} \langle \mathcal{A}x, x \rangle &= \\ &= \langle \mathcal{A}(\sum_{j=1}^n \beta_j v_j), \sum_{j=1}^n \beta_j v_j \rangle \\ &= {}^{149} \langle \sum_{j=1}^n \beta_j \mathcal{A}v_j, \sum_{j=1}^n \beta_j v_j \rangle \\ &= \langle \sum_{j=1}^n \alpha_j \beta_j v_j, \sum_{j=1}^n \beta_j v_j \rangle \\ &= \sum_{j=1}^n \beta_j \alpha_j \overline{\beta_j} \langle v_j, v_j \rangle {}^{150} \\ &= \sum_{j=1}^n |\beta_j|^2 \alpha_j \\ &\geq 0 \end{aligned}$$

Ta izraz je strogo pozitiven v drugem primeru, če je $x \neq 0$.¹⁵¹

□

Izrek. Sebi adjungiran endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ je pozitivno definiten natanko takrat, ko njegov karakteristični polinom $\Delta_{\mathcal{A}}(\lambda) = a_n \lambda^n + \dots + a_0$ zadošča pogoju

$$(-1)^k a_k > 0 \text{ za vsak } k = 0, \dots, n$$

Dokaz.

$(\Rightarrow) \Delta_{\mathcal{A}}(\lambda) = (-1)^n (\lambda - \lambda_1) \dots (\lambda - \lambda_n)$, kjer je $\lambda_j > 0$ za vsak j .

Odpravimo oklepaje in vsak člen a_k pomnožimo z $(-1)^k$.

$$\begin{aligned} a_0 &= \lambda_1 \lambda_2 \dots \lambda_n > 0 \\ -a_1 &= \lambda_1 \lambda_2 \dots \lambda_{n-1} + \lambda_1 \lambda_2 \dots \lambda_{n-2} \lambda_n + \dots + \lambda_2 \lambda_3 \dots \lambda_n \\ &\vdots \\ (-1)^k a_k &= \lambda_1 \dots \lambda_{n-k} + \lambda_1 \lambda_2 \dots \lambda_{n-k+1} + \dots + \lambda_{k+1} \lambda_{k+2} \dots \lambda_n > 0 \\ (-1)^{n-1} a_{n-1} &= \lambda_1 + \dots + \lambda_n > 0 \\ (-1)^n a_n &= 1 > 0 \end{aligned}$$

(\Leftarrow) Predpostavimo, da je $(-1)^k a_k > 0$ za vsak $k = 0, \dots, n$.

¹⁴⁹Linearnost \mathcal{A} .

¹⁵⁰ δ_{ji}

¹⁵¹Torej $\beta_j \neq 0$ za nek j .

Ker je \mathcal{A} po predpostavki izreka sebi adjungiran zadošča dokazati, da ima same pozitivne lastne vrednosti.

Denimo, da to ni res. Lastne vrednosti za \mathcal{A} so realne, zato obstaja $\alpha \leq 0$, da je $\Delta_{\mathcal{A}}(\alpha) = 0$.

$$0 = \Delta_{\mathcal{A}}(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n > 0$$

Prišli smo do protislovja. □

Izrek. Naj bo $\Delta_{\mathcal{A}}(\lambda) = a_0 + a_1\lambda_1 + \cdots + a_n\lambda^n$ karakteristični polinom sebi adjungiranega endomorfizma \mathcal{A} . Potem je \mathcal{A} pozitivno semidefiniten natanko takrat, ko obstaja $m \in \{0, \dots, n\}$, da je $a_k = 0$ za $k < m$ in $(-1)^k a_k > 0$ za $k \geq m$.

Dokaz. Doma. ¹⁵²

Spomnimo se:

Minor reda k matrike A je determinanta pomatrike matrike A , ki jo dobimo tako, da v A izberemo k vrstic in k stolpcev. Podmatriko sestavljajo elementi na križiščih teh vrstic in stolpcev.

Če vzamemo istoležne vrstice in stolpce, dobimo **glavni minor**.

Če vzamemo prvih k vrstic in prvih k stolpcev dobimo **vodilni minor**.

PRIMER:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Glavni minorji reda 1 so diagonalni elementi.

Vodilni minorji reda 1: $\det(a_{11}) = |a_{11}| = a_{11}$

Glavni minorji reda 2:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}, \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix}, \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix}$$

Vodilni minor reda 2:

$$\begin{vmatrix} a_{31} & a_{12} \\ a_{21} & a_{23} \end{vmatrix}$$

Trditev. Naj bo A pozitivno semidefinitna matrika in naj bo A' matrika, ki jo dobimo tako, da v A izbrišemo nekaj vrstic in istoležnih stolpcev. Potem je A' tudi pozitivno semidefinitna.

Dokaz. Pri brisanju iz istoležnih stolpcev se očitno ohranja hermitskost matrike.

Naj bo I množica indeksov vrstic in stolpcev, ki smo jih izbrisali. $|I|$ je moč I .

¹⁵²Dopiši.

Dokazati je treba, da je $\langle A'x', x' \rangle \geq 0$ ¹⁵³ za vsak $x' \in \mathcal{F}^{n-|I|}$.

$x \in \mathcal{F}^n$ naj bo tak vektor, da ima komponente indeksirane z indeksi iz I enake 0, če pa te komponente izbrišemo pa dobimo x' .

Če je $x' \neq 0$ je tudi $x \neq 0$.

$$\langle A'x', x' \rangle = \langle Ax, x \rangle \geq 0$$

154

To velja za poljuben $x' \in \mathcal{F}^{n-|I|}$, zato je A' pozitivno (semi)definiten. □

Izrek (Sylvestrov kriterij). *Hermitska matrika je pozitivno definitna natanko takrat, ko so vsi njegovi vodilni minorji strogo pozitivni.*

Dokaz.

(\Rightarrow) Sledi iz prejšnje trditve in dejstva, da je determinanta produkt lastnih vrednosti.

(\Leftarrow) Izrek bomo v to smer dokazali z indukcijo na velikosti matrike.

Za 1×1 matrike je to očitno.

Predpostavimo, da izrek velja za vse $n \times n$ matrike in naj bo $A(n+1) \times (n+1)$ matrika ($n \geq 1$).

A' naj bo taka matrika, ki jo dobimo, če v A izbrišemo zadnjo vrstico in stolpec.

A' je seveda hermitska in vsi vodilni minorji so strogo pozitivni.

Po indukcijski predpostavki je A' pozitivno definitna.

Recimo, da A ni pozitivno definitna. Potem ima vsaj eno lastno vrednost, ki je manjša ali enaka 0.

Po predpostavki je $\det A > 0$. Zato ima A vsaj dve negativni lastni vrednosti. Ker je mogoče A diagonalizirati v ortonormirani bazi, obstajata torej pravokotna vektorja $u, v \in \mathbb{C}^n$, da je $Au = \alpha u$ in $Av = \beta v$, kjer sta $\alpha, \beta < 0$.¹⁵⁵

Obstajata $\lambda, \mu \in \mathbb{C}$, ne oba 0, da ima $x = \lambda u + \mu v$ ničelno zadnjo komponento.

¹⁵³Oz. > 0 za pozitivno definitnost.

¹⁵⁴Dopiši.

¹⁵⁵ α ni nujno različen od β .

$x' \in \mathbb{C}^{n-1}$ naj bo vektor, ki ga dobimo tako, da v x izbrišemo zadnjo komponento.¹⁴⁹

$$\begin{aligned}
 \langle A'x', x' \rangle &= \\
 &= \langle Ax, x \rangle \\
 &= \langle A(\lambda u + \mu v), \lambda u + \mu v \rangle \\
 &= \langle \lambda Au + \mu Av, \lambda u + \mu v \rangle \\
 &= \langle \lambda \alpha u + \mu \beta v, \lambda u + \mu v \rangle \\
 &= \langle \lambda \alpha u, \lambda u \rangle + \langle \lambda \alpha u, \mu v \rangle + \langle \mu \beta v, \lambda u \rangle + \langle \mu \beta v, \mu v \rangle \\
 &= |\lambda|^2 \alpha \|u\|^2 + 0 + 0 + |\mu|^2 \beta \|v\|^2 \\
 &< 0
 \end{aligned}$$

To je v protislovju z dejstvom, da je A' pozitivno definitna.

\Rightarrow vse lastne vrednosti so pozitivne. □

Izrek. Hermitska matrika je pozitivno semidefinitna natanko takrat, ko so vsi njeni glavni minorji nenegativni.

Dokaz. Brez dokaza.

10.6 Unitarni endomorfizem

Definicija. Endomorfizem \mathcal{A} vektorskega prostora V s skalarnim produktom je **unitaren**, kadar je $\mathcal{A}^* \mathcal{A} = \mathcal{A} \mathcal{A}^* = id_V$.

Matrika $A \in \mathbb{C}^{n \times n}$ je **unitarna**, kadar je $A^H A = A A^H = I$. Realna matrika $A \in \mathbb{R}^{n \times n}$ je **ortogonalna**, kadar je $A^T A = A A^T = I$.

Unitarnemu endomorfizmu glede na ortonormirano bazo pripada unitarna¹⁵⁵ oz. ortogonalna¹⁵⁶ matrika.

Trditev. Za $\mathcal{A} \in \mathcal{L}(V)$ so ekvivalentne trditve:

1. \mathcal{A} je unitaren.
2. $\mathcal{A} \mathcal{A}^* = id_V$
3. $\mathcal{A}^* \mathcal{A} = id_V$
4. $\langle \mathcal{A}x, \mathcal{A}y \rangle = \langle x, y \rangle$ za vse $x, y \in V$.¹⁵⁷
5. $\|\mathcal{A}x\| = \|x\|$ za vsak $x \in V$. \mathcal{A} je **izometrija**, kar pomeni, da \mathcal{A} ohranja dolžine.

¹⁴⁹ $x' \neq 0$.

¹⁵⁵Nad \mathbb{C} .

¹⁵⁶Nad \mathbb{R} .

¹⁵⁷To pomeni, da je \mathcal{A} avtomorfizem vektorskega prostora V s skalarnim produktom \Rightarrow ohranja dolžine in kote.

Dokaz. Vemo že, da je $(1) \Leftrightarrow (2) \Leftrightarrow (3)$, ko ima endomorfizem končnorazsežnega vektorskega prostora levi inverz natanko takrat, ko ima desni inverz.

$$(1) \Rightarrow (4) \quad \langle \mathcal{A}x, \mathcal{A}y \rangle = \langle x, \mathcal{A}^* \mathcal{A}y \rangle = \langle x, y \rangle$$

$$(4) \Rightarrow (5) \quad \text{Vzamemo } y = x$$

$$(5) \Rightarrow (3) \quad \text{Po predpostavki za vsak } x \in V \text{ velja } \langle x, x \rangle = \langle \mathcal{A}x, \mathcal{A}x \rangle = \langle \mathcal{A}^* \mathcal{A}x, x \rangle$$

$$\begin{aligned} &\Rightarrow 0 = \\ &= \langle \mathcal{A}^* \mathcal{A}x, x \rangle - \langle x, x \rangle \\ &= \langle \mathcal{A}^T \mathcal{A}x - x, x \rangle \\ &= \langle (\mathcal{A}^* \mathcal{A} - id_V)x, x \rangle \end{aligned}$$

Naj bo \mathcal{B} sebi adjungiran. Velja $\langle \mathcal{B}x, x \rangle = 0$ za vsak $x \in V$. Vemo, da od tod sledi $\mathcal{B} = 0$, torej $\mathcal{A}\mathcal{A}^* = id_V$. \square

Trditev. Za $\mathcal{A} \in \mathcal{L}(V)$ so ekvivalentne trditve:

1. \mathcal{A} je unitaren.
2. \mathcal{A} vsako ortonormirano bazo slika v ortonormirano množico
3. \mathcal{A} vsaj eno ortonormirano bazo slika v ortonormirano bazo. ¹⁶⁰

Dokaz.

$(1) \Rightarrow (2)$ Naj bo $\{v_1, \dots, v_k\}$ ortonormirana množica. Potem za vsaka i in j velja

$$\langle \mathcal{A}v_i, \mathcal{A}v_j \rangle = \langle v_i, v_j \rangle = \delta_{ij} \Rightarrow$$

$\{\mathcal{A}v_i, \dots, \mathcal{A}v_k\}$ je ortonormirana množica.

$(7) \Rightarrow$ strožji del (3) Naj bo $\{v_1, \dots, v_n\}$ ortonormirana baza. Potem je $n = \dim V$. Po (2) je $\{\mathcal{A}v_1, \dots, \mathcal{A}v_n\}$ ortonormirana množica. Ker je ortonormirana, je linearno neodvisna. Ker ima n elementov, je baza.

$(3) \Rightarrow (1)$ Naj bo $\{v_1, \dots, v_n\}$ ortonormirana baza, za katero je $\{\mathcal{A}v_1, \dots, \mathcal{A}v_n\}$ ortonormirana baza. Dokazali bomo, da \mathcal{A} ohranja skalarni produkt.

Naj bosta $x, y \in V$ poljubna:

$$x = \sum_{i=1}^n \alpha_i v_i \quad y = \sum_{i=1}^n \beta_i v_i$$

¹⁶⁰ $\Leftrightarrow \mathcal{A}$ vsako ortonormirano bazo slika v ortonormirano bazo.

$$\begin{aligned}
\langle \mathcal{A}x, \mathcal{A}y \rangle &= \\
&= \langle \mathcal{A} \sum_{i=1}^n \alpha_i v_i, \mathcal{A} \sum_{i=1}^n \beta_i v_i \rangle \\
&= \langle \sum_{i=1}^n \alpha_i \mathcal{A}v_i, \sum_{i=1}^n \beta_i \mathcal{A}v_i \rangle \\
&= \sum_{i,j=1}^n \alpha_i \overline{\beta_j} \langle \mathcal{A}v_i, \mathcal{A}v_j \rangle \\
&= \sum_{i,j=1}^n \alpha_i \overline{\beta_j} \delta_{ij} \\
&= \sum_{i,j=1}^n \alpha_i \overline{\beta_j} \langle v_i, v_j \rangle \\
&= \langle \sum_{i=1}^n \alpha_i v_i, \sum_{j=1}^n \beta_j v_j \rangle \\
&= \langle x, y \rangle
\end{aligned}$$

□

Posledica. Matrika $A \in \mathcal{F}^{n \times n}$ je unitarna,¹⁵⁰ ko njeni stolpci tvorijo ortonormirano bazo. Isto velja za vrstice.

Dokaz.

Stolpci so slike elementov standardne baze, ki je ortonormirana.

A je unitarna $\Leftrightarrow AA^H = I \Leftrightarrow A^H$ unitarna.

Rezultat v vrsticah je zato ekvivalenten rezultatu za stolpce A^H .¹⁵¹

□

Trditev. Unitarni endomorfizmi prostora V tvorijo grupo za kompozitum.¹⁵²

Dokaz. • Notranja binarna operacija

Naj bosta \mathcal{A}, \mathcal{B} unitarna:

$$(\mathcal{A}\mathcal{B})(\mathcal{A}\mathcal{B})^* = \mathcal{A}\mathcal{B}\mathcal{B}^*\mathcal{A}^* = \mathcal{A}\mathcal{A}^* = id_V$$

$\Rightarrow \mathcal{A} \circ \mathcal{B}$ je unitarna.

• Asociativnost:

Kompozitum je asociativen.

¹⁵⁰ Ali ortogonalna.

¹⁵¹ Konjugiranje na ortogonalnost ne vpliva, prav tako ne na dolžino.

¹⁵² \Rightarrow Unitarne oz. ortogonalne matrike tvorijo grupo za matrično množenje.

- *Enota:*

Je kar id_V ¹⁵³ in ta je seveda unitarna.

- *Inverz:*

Če je \mathcal{A} unitaren, je $\mathcal{A}\mathcal{A}^* = id_V$.

$$\Rightarrow \mathcal{A}^{-1} = \mathcal{A}^* \quad ^{154}$$

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

$$\Rightarrow \mathcal{A}^* \text{ je unitaren.}$$

□

Trditev. *Spekter unitarnega endomorfizma je vsebovan v enotski krožnici kompleksne ravnine.*

Dokaz. *Naj bo λ lastna vrednost. Potem obstajajo $x \in V, x \neq 0$, da je $\mathcal{A}x = \lambda x$.*

$$\langle \mathcal{A}x, \mathcal{A}x \rangle = \langle \lambda x, \lambda x \rangle = |\lambda|^2 \langle x, x \rangle = |\lambda|^2 \|x\|^2$$

$$\langle \mathcal{A}x, \mathcal{A}x \rangle = \langle x, x \rangle = \|x\|^2 \quad ^{155} \Rightarrow |\lambda|^2 = 1 \Rightarrow |\lambda| = 1$$

Izrek. *Naj bo V unitaren vektorski prostor¹⁵⁶ in $\mathcal{A} \in \mathcal{L}(V)$. Potem je \mathcal{A} unitaren endomorfizem natanko takrat, ko se da diagonalizirati v ortonormirani bazi in so vse njegove lastne vrednosti po absolutni vrednosti enake 1.*

Dokaz.

(\Rightarrow) *Sledi iz izreka o diagonalizaciji normalnih endomorfizmov iz prejšnje trditve.*

(\Leftarrow) *Naj bo A diagonalna matrika, ki v neki ortonormirani bazi pripada endomorfizmu \mathcal{A} .*

$$A = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix} \text{ in po predpostavki velja } |\lambda_i| = 1 \text{ za vsak } i$$

$$AA^H = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix} \begin{bmatrix} \overline{\lambda_1} & & & \\ & \overline{\lambda_2} & & \\ & & \ddots & \\ & & & \overline{\lambda_n} \end{bmatrix} = \begin{bmatrix} \lambda_1 \overline{\lambda_1} & & & \\ & \lambda_2 \overline{\lambda_2} & & \\ & & \ddots & \\ & & & \lambda_n \overline{\lambda_n} \end{bmatrix} = I$$

□

¹⁵³Enota za o.

¹⁵⁴To pove, da je \mathcal{A} obrnljiv.

¹⁵⁶Nad \mathbb{C} .

PRIMER:

$n \times n$ ortogonalne matrike ¹⁵⁷

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad AA^T = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} a^2 + b^2 & ac + bd \\ ac + bd & c^2 + d^2 \end{bmatrix}$$

$$AA^T = I$$

$$\Rightarrow a^2 + b^2 = 1$$

$$ac + bd = 0$$

$$c^2 + d^2 = 1$$

$\exists \varphi, \psi \in [0, 2\pi)$, da je $a = \cos \varphi, b = \sin \varphi, c = \cos \psi, d = \sin \psi$

$$ac + bd = \cos \varphi \cos \psi + \sin \varphi \sin \psi = \cos(\varphi - \psi) = 0$$

$$\varphi - \psi = \frac{\pi}{2} + k\pi$$

$$\varphi = \psi \pm \frac{\pi}{2}$$

158

Definicija. Naj bosta $A, B \in \mathcal{F}^{n \times n}$.

1. B je **unitarno podobna** A , kadar obstaja unitarna matrika $U \in \mathbb{C}^{n \times n}$, da je $B = U^H A U$.¹⁵⁹
2. $B \in \mathbb{R}^{n \times n}$ je **ortogonalno podobna** $A \in \mathbb{R}^{n \times n}$, kadar obstaja ortogonalna matrika $Q \in \mathbb{R}^{n \times n}$, da je $B = Q^T A Q$.¹⁶⁰

Trditev. Unitarna podobnost in ortogonalna podobnost sta ekvivalenčni relaciji.

Dokaz. Dokaz je enak kot pri ekvivalentnosti matrik.

Če je $B = U^H A U$, potem stolpci U tvorijo ortonormirano bazo, v kateri endomorfizmu \mathcal{A} pripada matrika B . Obratno, če endomorfizmu \mathcal{A} v neki ortonormirani bazi pripada matrika B , potem vektorji te baze določajo unitarno matriko U , da je $B = U^H A U$.

¹⁵⁷ $\mathbb{R}^{2 \times 2}$

¹⁵⁸Dopiši še en primer.

¹⁵⁹ $= U^{-1} A U$.

¹⁶⁰ $= Q^{-1} A Q$.

Iz izreka o diagonalizaciji v ortonormirani bazi sledi:

Izrek.

- Vsaka matrika $A \in \mathbb{C}^{n \times n}$ je unitarno podobna neki zgornje trikotni matriki.
- $A \in \mathbb{C}^{n \times n}$ je normalna \Leftrightarrow unitarno podobna diagonalni matriki.
- $A \in \mathbb{C}^{n \times n}$ je hermitska \Leftrightarrow je unitarno podobna realni diagonalni matriki.
- $A \in \mathbb{R}^{n \times n}$ je simetrična \Leftrightarrow je ortogonalno podobna realni diagonalni matriki.
- $A \in \mathbb{C}^{n \times n}$ je unitarna \Leftrightarrow je unitarno podobna diagonalni matriki z lastnimi vrednostmi po absolutni vrednosti 1.

10.7 Kvadratni funkcionali

Definicija. Preslikava $\mathcal{B} : V \times W \rightarrow \mathcal{O}$ je **bilinearen funkcional**,¹⁶¹ kadar velja:

$$\begin{aligned}\mathcal{B}(\lambda x + \mu y, z) &= \lambda \mathcal{B}(x, z) + \mu \mathcal{B}(y, z) \text{ in} \\ \mathcal{B}(x, \lambda z + \mu w) &= \lambda \mathcal{B}(x, z) + \mu \mathcal{B}(x, w) \text{ za vse } \lambda, \mu \in \mathcal{O}, x, y \in V \text{ in } z, w \in W\end{aligned}$$

V tem poglavju bo $\mathcal{O} = \mathbb{R}$ ¹⁶²

Naj bo $\mathcal{B} : V \times W \rightarrow \mathbb{R}$ bilinearna forma. Naj bo $\{e_1, \dots, e_n\}$ baza za V in $\{f_1, \dots, f_m\}$ baza za W . Za $x \in V$ in $y \in W$ naj bo $x = \sum_{i=1}^n x_i e_i$ in $y = \sum_{j=1}^m y_j f_j$.

$$\mathcal{B}(x, y) = \mathcal{B}\left(\sum_{i=1}^n x_i e_i, \sum_{j=1}^m y_j f_j\right) = \sum_{i=1}^n \sum_{j=1}^m x_i y_j \mathcal{B}(e_i, f_j)$$

Označimo $a_{ij} = \mathcal{B}(e_i, f_j)$. To so skalarji, odvisni of funkcionala \mathcal{B} in izbire baz.

$$\Rightarrow \mathcal{B}(x, y) = \sum_{i=1}^n \sum_{j=1}^m x_i y_j a_{ij}$$

Naj bo $V = \mathbb{R}^n$ in $W = \mathbb{R}^m$ in predpostavimo, da sta izbrani bazi standardni. Označimo $A = [a_{ij}] \in \mathbb{R}^{n \times m}$.

$$\Rightarrow \mathcal{B}(x, y) = \sum_{i=1}^n \sum_{j=1}^m a_{ij} x_i y_j = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} = x^T A y$$

Trditev. Vsaka linearna forma $\mathcal{B} : \mathbb{R}^n \times \mathbb{R}^m \rightarrow \mathbb{R}$ je definirana s predpisom $\mathcal{B}(x, y) = x^T A y$ za **neko** matriko $A \in \mathbb{R}^{n \times m}$, ki je natančno določena s formo \mathcal{B} .

¹⁶¹Ali bilinearna forma.

¹⁶²Gledali bomo le vektorske prostore.

Dokaz. Da je s predpisom $\mathcal{B}(x, y) = x^T A y$ definirana bilinearna forma, je enostavno preveriti.

Pred trditvijo smo že dokazali, da so vse linearne forme take oblike.

Ostane nam še enoličnost matrike A . Naj bo $\mathcal{B}(x, y) = x^T A y = x^T A' y$ za vsaka $x \in \mathbb{R}^n$ in $y \in \mathbb{R}^m$.

$$\Rightarrow x^T (A - A') y = 0 \text{ za vsaka } x \in \mathbb{R}^n \text{ in } y \in \mathbb{R}^m$$

$\Rightarrow \langle (A - A')y, x \rangle = 0$ za vsak $x \in \mathbb{R}^n$ in $y \in \mathbb{R}^m$, kjer smo vzeli standardni skalarni produkt na \mathbb{R}^n . Vemo, da od tod sledi $A - A' = 0 \Rightarrow A = A'$. \square

Definicija. Naj bo V vektorski prostor nad \mathbb{R} in $\mathcal{B} : V \times V \rightarrow \mathbb{R}$ bilinearen funkcional. Preslikava $\mathcal{K} : V \rightarrow \mathbb{R}$, definirana s predpisom $\mathcal{K}(x) = \mathcal{B}(x, x)$ se imenuje **kvadratni funkcional** ali **kvadratna forma** na V .

Če v V izberemo bazo $\{e_1, \dots, e_n\}$ in je $x = \sum_{i=1}^n x_i e_i$, potem je

$$\mathcal{K}(x) = \mathcal{B}(x, x) = \sum_{i,j=1}^n a_{ij} x_i x_j$$

kjer so $a_{ij} \in \mathbb{R}$ neki skalarji, odvisni od \mathcal{K} in izbire baze. Obratno je tudi res, vsak tak predpis določa kvadratni funkcional na V .

Trditev. Vsaka kvadratna forma $\mathcal{K} : \mathbb{R}^n \rightarrow \mathbb{R}$ je oblike $\mathcal{K}(x) = \langle Ax, x \rangle$, kjer je \langle, \rangle standardni skalarni produkt na \mathbb{R}^n in $A \in \mathbb{R}^{n \times n}$ **simetrična** matrika. A je enolično določena s \mathcal{K} .

Dokaz.

\mathcal{K} je res kvadratna forma

Definirajmo

$$\mathcal{B} : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$$

$$(x, y) \mapsto \langle Ax, y \rangle = x^T A y$$

To je bilinearna forma in velja $\mathcal{B}(x, x) = \langle Ax, x \rangle = \mathcal{K}(x)$ za vsak x , torej je \mathcal{K} res kvadratna forma.

Naj bo zdaj $\mathbb{R}^n \rightarrow \mathbb{R}$ poljubna kvadratna forma. Potem obstaja bilinearna forma $\mathcal{B} : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$, da je $\mathcal{K}(x) = \mathcal{B}(x, x)$ za vsak $x \in \mathbb{R}^n$. Vemo že, da je $\mathcal{B}(x, y) = x^T A y$ za neko matriko A . Torej je $\mathcal{K}(x) = \mathcal{B}(x, x) = x^T A x = \langle Ax, x \rangle$ za vsak $x \in \mathbb{R}^n$.

$$\begin{aligned} \langle \frac{1}{2}(A + A^T)x, x \rangle &= \\ &= \frac{1}{2} \langle Ax, x \rangle + \frac{1}{2} \langle A^T x, x \rangle \\ &= \frac{1}{2} \langle Ax, x \rangle + \frac{1}{2} \langle x, Ax \rangle \\ &= \langle Ax, x \rangle \end{aligned}$$

Torej A lahko zamenjamo s simetrično matriko $\frac{1}{2}(A + A^T)$ in se kvadratna forma ne spremeni.

Enoličnost: Naj bosta A in A' simetrični¹⁶³ matriki, da velja $\mathcal{K}(x) = \langle Ax, x \rangle = \langle A'x, x \rangle$ za vsak $x \in \mathbb{R}^n$.

Potem je $\langle (A - A')x, x \rangle = 0$ za vsak $x \in \mathbb{R}^n$. Ker je $A - A'$ simetrična, je $A = A'$.

Naj bo $\mathcal{K}(x) = \langle Ax, x \rangle$ kvadratna forma na \mathbb{R}^n . Zamenjamo bazo, naj bo $x = Py$, kjer je P obrnljiva matrika.¹⁶⁴

$$\mathcal{K}(x) = \langle Ax, x \rangle = \langle APy, Py \rangle = \langle P^T APy, y \rangle$$

□

Definicija. Naj bosta A in B realni simetrični matriki. Matrika B je **konvergentna** matriki A , kadar obstaja obrnljiva realna matrika P , da je $P^T AP = B$.

Konvergentni matriki pripadata isti kvadratni formi glede na različni bazi.

Trditev. Konvergentnost je ekvivalenčna relacija.

Dokaz. Dokaz je enak kot pri podobnosti, ekvivalentnosti ...

Izrek (Sylvestrov izrek o vztrajnosti). Vsaka realna simetrična matrika je konvergentna

matriki oblike $B = \begin{bmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & \ddots & & & & & & \\ & & & 1 & & & & & \\ & & & & -1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & \ddots & & \\ & & & & & & & -1 & \\ & & & & & & & & 0 \\ & & & & & & & & & \ddots \\ & & & & & & & & & & 0 \end{bmatrix}$ za neke $p, q \geq 0$.

Pri tem je p število pozitivnih, q pa število negativnih lastnih vrednosti matrike A ¹⁶⁶

Matriki $B_1 = \begin{bmatrix} Ip_1 & & \\ & Iq_1 & \\ & & 0 \end{bmatrix}$ in $\begin{bmatrix} Ip_2 & & \\ & Iq_2 & \\ & & 0 \end{bmatrix}$ sta konvergentni natanko takrat, ko je $p_1 = p_2$ in $q_1 = q_2$.

¹⁶³Tudi realni.

¹⁶⁴Prehodna matrika med dvema bazama.

¹⁶⁵To je spet kvadratna forma v y , določena z matriko $P^T AP = (P^T AP)^T$.

¹⁶⁶Štetih z večkratnostjo v karakterističnem polinomu $\Delta_A(\lambda)$.