LINEARNA ALGEBRA

VEKTORJI V R^n

pojmi v ravnini
→ urejeni pari realnih števil
→ točke v ravnini
→ krajevni vektorji
→ množice paroma enakih geometrijskih vektorjev

Geometrijski vektorji:
→ usmerjena daljica med dvema točkama
→ začetna točka: **rep**
→ končna točka: **glava**
→ dva vektorja sta enaka če sta vzporedna in imata enako dolžino in smer

Krajevni vektorji:
→ izberemo neko točko kot **izhodišče**
→ postavimo rep v izhodišče
→ vsak geometrijski enak **natanko enemu** krajevnemu
→ natančno določen z glavo
→ če koordinatni sistem so **koordinate** glava

koordinate geometrijskega vektorja enakega krajevnemu $(x_1, \ldots, x_n) \to (y_1, \ldots, y_n)$ $(y_1 - x_1, \ldots, y_n - x_n)$

realna števila so skalarji in vektorji so krajevni vektorji

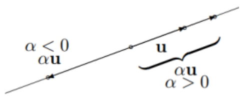
Operacije nad vektorji:
1. **vsota** in **razlika** dveh vektorjev
2. produkt **vektorja** s **skalarjem**
3. **skalarni** produkt
4. **vektorski** produkt
5. **mešani** produkt

1. $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$

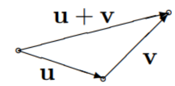
2. $\alpha(x_1, \ldots, x_n) := (\alpha x_1, \ldots, \alpha x_n)$

poznamo paralelogramsko in trikotniško pravilo

Označimo $\mathbf{0} := (0, \ldots, 0)$



če je α negativna potem vektor prezrcalimo čez izhodišče



ker obe operaciji po komponentah jih lahko izpeljemo iz lastnosti realnih števil

Lastnosti vsote
- $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$,
- $(\mathbf{x} + \mathbf{y}) + \mathbf{z} = \mathbf{x} + (\mathbf{y} + \mathbf{z})$
- $\mathbf{x} + \mathbf{0} = \mathbf{x}$,
- $\mathbf{x} + (-\mathbf{x}) = \mathbf{0}$.

Lastnosti množenja s skalarjem
- $\alpha(\mathbf{x} + \mathbf{y}) = \alpha\mathbf{x} + \alpha\mathbf{y}$,
- $(\alpha + \beta)\mathbf{x} = \alpha\mathbf{x} + \beta\mathbf{x}$,
- $(\alpha\beta)\mathbf{x} = \alpha(\beta\mathbf{x})$,
- $1\mathbf{x} = \mathbf{x}$, $0\mathbf{x} = \mathbf{0}$.

Linearna kombinacija:

Vektor $\mathbf{v} \in \mathbb{R}^n$ je **linearna kombinacija** vektorjev $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{R}^n$, če obstajajo taki skalarji $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$, da velja

$$\mathbf{v} = \alpha_1\mathbf{v}_1 + \ldots + \alpha_m\mathbf{v}_m \in \mathbb{R}^n.$$

→ ali je linearna kombinacija: rešimo n linearnih enačb z m neznankami

Linearna neodvisnost:
→ vektorji so **linearno odvisni** če je eden enak **linearni kombinaciji** ostalih
→ če to ne drži so linearno neodvisni
→ en vektor: ni enak 0
→ dva vektorja: nista na isti premici skozi **izhodišče !**
→ trije vektorji: niso na isti ravnini skozi izhodišče

IZREK: Vektorji so linearno neodvisni natanko tedaj ko ima enačba ima samo eno rešitev in ta je **trivialna**

$$\alpha_1\mathbf{v}_1 + \ldots + \alpha_m\mathbf{v}_m = \mathbf{0}$$

$$\alpha_1 = \ldots = \alpha_m = 0$$

DOKAZ:
Očitno je to vedno rešitev – ali **edina**? Predpostavimo da ni. potem za nek α_i velja **da ni nič**. Torej bi lahko i-ti vektor izrazili z linearno kombinacijo ostalih in bi bil **linearno odvisen** →←

V drugo smer velja: če so linearno odvisni lahko enega **izrazimo** z linearno kombinacijo ostalih. In bi bila α_i enaka -1

$$\mathbf{v}_i = \beta_1\mathbf{v}_1 + \ldots + \beta_{i-1}\mathbf{v}_{i-1} + \beta_i\mathbf{v}_{i+1} + \ldots + \beta_{m-1}\mathbf{v}_m$$

$$\alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1} \quad \alpha_i = -1$$

$$\alpha_{i+1} = \beta_i, \ldots, \alpha_m = \beta_{m-1}$$

DOKAZ:
Predpostavimo, da so linearno neodvisni in obratno, da se da na **dva** načina.

$$\mathbf{v} = \alpha_1\mathbf{v}_1 + \ldots + \alpha_m\mathbf{v}_m = \beta_1\mathbf{v}_1 + \ldots + \beta_m\mathbf{v}_m$$

Če prenesemo vektorje na drugo stran dobimo:

$$\mathbf{0} = \mathbf{v} - \mathbf{v} = (\alpha_1 - \beta_1)\mathbf{v}_1 + \ldots + (\alpha_m - \beta_m)\mathbf{v}_m$$

Ker so vektorji **linearno neodvisni** obstaja samo trivialna rešitev torej $\alpha_i - \beta_i = 0$
To pomeni da je αi **enak** βi za vsak i, obstaja torej kvečjemu ena rešitev.

Obratno, če se da **vsak** vektor izraziti na največ en način mora to veljati tudi za vektor **0**. Potem je vsaka α enaka 0 torej so vektorji linearno neodvisni.

$$\alpha_1\mathbf{v}_1 + \ldots + \alpha_m\mathbf{v}_m = \mathbf{0} = 0\mathbf{v}_1 + \ldots + 0\mathbf{v}_m$$

POSLEDICA: vektorji $v_1,..,v_m$ so linearno neodvisni natanko tedaj ko se da **vsak** vektor iz R^n na **največ en** način izraziti kot linearna kombinacija $v_1,..,v_m$

Ogrodje:
→ vektorji $\mathbf{v_1},..,\mathbf{v_m} \in \mathbf{R^n}$
→ vsak vektor iz R^n lahko na **vsaj en** način izraziti kot njihova **linearna kombinacija**

Baza:
→ vektorji $\mathbf{v_1},..,\mathbf{v_m} \in \mathbf{R^n}$
→ so **ogrodje**
→ so **linearno neodvisni**

vsaka baza v $\mathbf{R^n}$ ima natanko **n** elementov

Norma:
→ $x = (x_1,..,x_n) \in R^n$
→ norma je **skalar**
→ **geometrijski pomen**: po Pitagorovem izreku je to **oddaljenost** x od izhodišča
→ razdalja med dvema točkama || x – y ||

$$\|\mathbf{x}\| = \sqrt{\sum_{i=1}^{n} x_i^2}$$

$\|\mathbf{x}\| \geq 0$ za vsak $\mathbf{x} \in \mathbb{R}^n$

$\|\alpha\mathbf{x}\| = |\alpha|\|\mathbf{x}\|$

$\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$

3. → $\mathbf{x} = (\mathbf{x_1},..,\mathbf{x_n})$ in $\mathbf{y} = (\mathbf{y_1},..,\mathbf{y_n})$
→ **skalarni produkt** je skalar

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i y_i$$

$\langle \mathbf{x}, \mathbf{x} \rangle = \|\mathbf{x}\|^2$ $\quad \langle \alpha\mathbf{x} + \beta\mathbf{y}, \mathbf{z} \rangle = \alpha\langle \mathbf{x}, \mathbf{z} \rangle + \beta\langle \mathbf{y}, \mathbf{z} \rangle$

$\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$ $\quad \langle \mathbf{x}, \alpha\mathbf{y} + \beta\mathbf{z} \rangle = \alpha\langle \mathbf{x}, \mathbf{y} \rangle + \beta\langle \mathbf{x}, \mathbf{z} \rangle$

TRDITEV: Naj bo φ **kot** med vektorjema. Potem velja

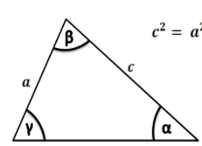
$$\langle \mathbf{x}, \mathbf{y} \rangle = \|\mathbf{x}\| \, \|\mathbf{y}\| \cos\phi$$

DOKAZ:
V sinusni izrek vstavimo **a** je $\|x\|$ in **b** je $\|y\|$ in **c** je $\|x - y\|$ in **γ = φ**

$$\|\mathbf{x} - \mathbf{y}\|^2 = \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 - 2\|\mathbf{x}\|\|\mathbf{y}\| \cos\phi$$

$$\langle \mathbf{x} - \mathbf{y}, \mathbf{x} - \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{x} \rangle + \langle \mathbf{y}, \mathbf{y} \rangle - \langle \mathbf{x}, \mathbf{y} \rangle - \langle \mathbf{y}, \mathbf{x} \rangle = \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 - 2\langle \mathbf{x}, \mathbf{y} \rangle$$

$$c^2 = a^2 + b^2 - 2ab\cos\gamma$$



POSLEDICA: vektorja sta **pravokotna** ko njun **skalarni produkt 0**

DOKAZ: Če sta oba vektorja **neničelna** je skalarni produkt lahko 0 le kadar je **kosinus** kota med njima 0, torej **pravi kot**

POSLEDICA: $|\langle \mathbf{x}, \mathbf{y}\rangle| \leq \|\mathbf{x}\|\,\|\mathbf{y}\|$

DOKAZ: Oceno pomnožimo z ||x|| ||y|| $-1 \leq \cos\phi \leq 1$

Cauchy-Schwartzova neenakost

POSLEDICA: $\|\mathbf{x}+\mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$

DOKAZ: Cauchy-Schwartzovo neenakost pomnožimo z 2 prištejemo $||x||^2$ + $||y||^2$ in korenimo

$$|\|\mathbf{x}\| - \|\mathbf{y}\|| \leq \|\mathbf{x}+\mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$$

4.

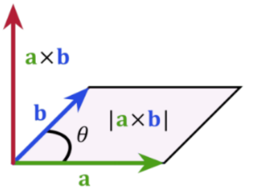
5.

v R^3 definiramo **vektorski produkt**

$$\mathbf{u} \times \mathbf{v} = \begin{bmatrix} x_2y_3 - x_3y_2 \\ x_3y_1 - x_1y_3 \\ x_1y_2 - x_2y_1 \end{bmatrix}$$

→ ne moremo posplošiti
→ v R^2 podoben vnanji produkt
→ **geometrijsko**: ploščina **paralelograma** ki ga oklepata x in y

$$(x_1, x_2) \wedge (y_1, y_2) = x_1y_2 - x_2y_1$$



Lastnosti vektorskega produkta:

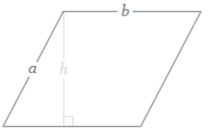
$$(\mathbf{u}+\mathbf{v})\times\mathbf{w} = \mathbf{u}\times\mathbf{v} + \mathbf{v}\times\mathbf{w}$$
$$\mathbf{u}\times(\mathbf{v}+\mathbf{w}) = \mathbf{u}\times\mathbf{v} + \mathbf{u}\times\mathbf{w}$$
$$(\alpha\mathbf{u})\times\mathbf{v} = \alpha(\mathbf{u}\times\mathbf{v}) = \mathbf{u}\times(\alpha\mathbf{v})$$
$$\mathbf{u}\times\mathbf{u} = \mathbf{0}$$
$$\mathbf{u}\times\mathbf{0} = \mathbf{0}$$
$$\mathbf{u}\times\mathbf{v} = -\mathbf{v}\times\mathbf{u}$$
$$(\alpha\mathbf{u}+\beta\mathbf{v})\times\mathbf{w} = \alpha(\mathbf{u}\times\mathbf{w}) + \beta(\mathbf{v}\times\mathbf{w})$$
$$(\mathbf{u}\times\mathbf{v})\times\mathbf{w} = \langle\mathbf{u},\mathbf{w}\rangle\mathbf{v} - \langle\mathbf{v},\mathbf{w}\rangle\mathbf{u}$$

DOKAZ:
Ploščina paralelograma je $h_b \cdot b$ in višino lahko zapišemo kot sinφ · a. Sledi da je ploščina sinφ · a · b. Uporabimo pravila za mešani produkt in dobimo

$$\|\mathbf{u}\times\mathbf{v}\|^2 = \langle\mathbf{u}\times\mathbf{v}, \mathbf{u}\times\mathbf{v}\rangle = \langle(\mathbf{u}\times\mathbf{v})\times\mathbf{u}, \mathbf{v}\rangle$$
$$\langle(\mathbf{u}\times\mathbf{v})\times\mathbf{u}, \mathbf{v}\rangle = \langle\langle\mathbf{u},\mathbf{u}\rangle\mathbf{v} - \langle\mathbf{v},\mathbf{u}\rangle\mathbf{u}, \mathbf{v}\rangle$$
$$\langle\mathbf{u},\mathbf{u}\rangle\langle\mathbf{v},\mathbf{v}\rangle - \langle\mathbf{v},\mathbf{u}\rangle\langle\mathbf{u},\mathbf{v}\rangle = \|\mathbf{u}\|^2\|\mathbf{v}\|^2 - \langle\mathbf{u},\mathbf{v}\rangle^2$$
$$\|\mathbf{u}\times\mathbf{v}\|^2 = \|\mathbf{u}\|^2\|\mathbf{v}\|^2 - \|\mathbf{u}\|^2\|\mathbf{v}\|^2\cos^2\varphi$$

Če upoštevamo: $\|\mathbf{u}\|^2\|\mathbf{v}\|^2(1-\cos^2\varphi)$ = $\|\mathbf{u}\|^2\|\mathbf{v}\|^2\sin^2\varphi$

$$\|\mathbf{u}\times\mathbf{v}\| = \|\mathbf{u}\|\|\mathbf{v}\|\sin\varphi$$!

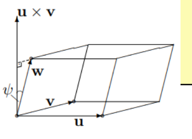


vektor skalarnega produkta leži na premici skozi izhodišče ki je **pravokotna** tako na **x** kot na **y**

smer določimo s **pravilom desnega vijaka**

Lastnosti mešanega produkta:

$$\langle\mathbf{u}\times\mathbf{v}, \mathbf{w}\rangle = \langle\mathbf{u}, \mathbf{v}\times\mathbf{w}\rangle$$
$$\langle\mathbf{u}\times\mathbf{v}, \mathbf{w}\times\mathbf{z}\rangle = \langle\mathbf{u},\mathbf{w}\rangle\langle\mathbf{v},\mathbf{z}\rangle - \langle\mathbf{u},\mathbf{z}\rangle\langle\mathbf{v},\mathbf{w}\rangle$$
$$(\mathbf{u}\times\mathbf{v})\times\mathbf{w} + (\mathbf{v}\times\mathbf{w})\times\mathbf{u} + (\mathbf{w}\times\mathbf{u})\times\mathbf{v} = 0$$



v R^3 definiramo **mešani produkt**
→ prostornina **paralepipeda**
→ kot med **x × y** in **z**
→ 3 krat 3 **determinanta**

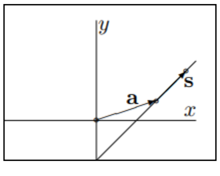
$$[\mathbf{x},\mathbf{y},\mathbf{z}] = \|\mathbf{x}\times\mathbf{y}\|\,\|\mathbf{z}\|\,\cos\theta$$
$$[\mathbf{x},\mathbf{y},\mathbf{z}] = \langle\mathbf{x}\times\mathbf{y}, \mathbf{z}\rangle$$

Premice ravnine in hiperravnine v R^n

Premice:
→ podamo z **točko** na premici in **vektorjem** v **smeri** premice
→ to je **parametrična enačba** premice
→ parameter **t** $x_1 = x_{01} + tp_1, \ldots, x_n = x_{0n} + tp_n$

$$\mathbf{r} = \mathbf{r}_0 + t\mathbf{p}$$

premica podana po **komponentah**



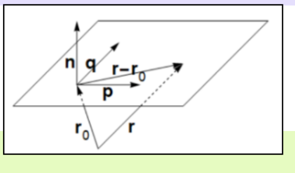
normala premice ignore deljenje z 0

$$t = \frac{x_1 - x_{01}}{p_1} = \ldots = \frac{x_n - x_{0n}}{p_n}$$

Ravnine:
→ podamo z eno **točko** in dvema **linearno neodvisnima vektorjema**
→ s **točko** na ravnini in neničelno **normalo** točka mora zadoščati **normalni enačbi**

$$\mathbf{r} = \mathbf{r}_0 + s\mathbf{p} + t\mathbf{q} \qquad \langle\mathbf{n}, \mathbf{r}-\mathbf{r}_0\rangle = 0$$

→ prvi način deluje tudi v R^n
→ drugi način se ne posploši enačba določa **hiperravnino** torej **n – 1** razsežno množico



DOKAZ:
Ploščina **paralelograma** je **||x × y||**.
Višina je **||z||** · **cosφ** ker je x × y **pravokoten** tako na y kot x lahko višino izračunamo na ta način.
Volumen je **višina** pomnožena z **ploščino** osnovne ploskve torej:
||x × y|| · **||z||** · **cosφ**

hiperravnine v **eni** dimenziji so **točke** v **dveh premice** v **treh ravnine** v štirih pa trirazsežne množice

hiperravnine so množice rešitev **netrivialnih lineranih** enačb v **n** spremenljivkah

SISTEMI LINEARNIH ENAČB

→ linearna enačba v n spremenljivkah
→ a_i in b so **realna** števila
→ x_i so **spremenljivke**
→ če a_i vse 0 je to **trivialna** enačba
→ trivialna: množica rešitev $\mathbf{R^n}$ če je b **nič**
→ trivialna: množica rešitev **{ }** če b **ni nič**

IZREK: če je enačba netrivialna je njena rešitev **hiperravnina** v $\mathbf{R^n}$

2**x** = 1 ni enaka 2**x** + 0**y** = 1 množica rešitev prve je **točka** v R druge pa **premica** v R^2

Sistem linearnih enačb:
→ **m** enačb v **n** spremenljivkah
→ rešitev je taka n-terica realnih števil ki ustreza vsem m spremenljivkam
→ rečemo m × n sistem

$$\begin{aligned} a_{1,1}x_1 + \ldots + a_{1,n}x_n &= b_1 \\ \vdots \qquad\qquad \vdots \quad &\quad \vdots \\ a_{m,1}x_1 + \ldots + a_{m,n}x_n &= b_m \end{aligned}$$

DOKAZ:
Če je enačba netrivialna obstaja tak i da lahko zapišemo:

$$a_1x_1 + \ldots + a_i(x_i - \frac{b}{a_i}) + \ldots + a_nx_n = 0.$$

vektor je neničelen saj a_i ni nič. $\mathbf{n} := (a_1, \ldots, a_i, \ldots, a_n)$
Definiramo še vektor r in dobimo enačbo hiperravnine

$$\mathbf{r} := (x_1, \ldots, x_i, \ldots, x_n) \qquad \langle\mathbf{n}, \mathbf{r}-\mathbf{r}_0\rangle = 0.$$

Vzamemo poljubno ravnino v $\mathbf{R^n}$ potem obstaja tak neničelen vektor n in tak r_0 da je hiperravnina množica rešitev vektorske enačbe

$$\mathbf{r}_0 = (c_1, \ldots, c_n) \quad \mathbf{n} = (a_1, \ldots, a_n)$$

Če razpišemo dobimo

$$a_1x_1 + \ldots + a_nx_n = b \qquad \langle\mathbf{n}, \mathbf{r}-\mathbf{r}_0\rangle = 0$$
$$b = a_1c_1 + \ldots + a_nc_n$$

TRDITEV: če so vsi koeficienti in vse desne strani enake **nič** potem je rešitev sistema $\mathbf{R}^n$

TRDITEV: če **niso** vsi koeficienti nič potem je rešitev **presek hiperravnin** v R^n

prazna množica je presek vzporednih hiperravnin

DOKAZ:
Množica rešitev **sistema** je **presek** množic **rešitev** enačb. Množice rešitev netrivialnih enačb so hiperravnine. Če so torej vse **netrivialne** je to gotovo presek. Kaj če je enačba **trivialna**? Če ima za rešitev **prazno** množico je rešitev prazna množica, torej drži. Če je rešitev R^n to **ne vpliva** na rešitev sistema.

Klasifikacija sistemov:

glede na **velikost**:

→ **kvadratni**: število spremenljivk in enačb enako
→ **predoločeni**: enačb je več kot spremenljivk
→ **poddoločeni**: več spremenljivk kot enačb

glede na **rešljivost**:

→ **nerešljive**: množica rešitev prazna
→ **enolično** rešljive: množica rešitev en element
→ **neenolično** rešljive: več kot ena rešitev

glede na **obliko** desne strani:

→ **homogeni**: vse desne strani 0
→ **nehomogeni**: niso vse desne strani 0

če sta **x** in **y** dve rešitvi je tudi: $(1-t)\mathbf{x}+t\mathbf{y}$

kvadraten sistem po navadi enolično, **predoločen** nerešljiv in **poddoločen** neenolično

Algebraični pomen:

$$(b_1,\dots,b_n) = (a_{1,1}x_1+\dots+a_{1,n}x_n,\dots,a_{m,1}x_1+\dots+a_{m,n}x_n)$$

$$= x_1(a_{1,1},\dots,a_{m,1})+\dots+x_n(a_{1,n},\dots,a_{m,n})$$

→ to je razvoj v linearno kombinacijo

$$\mathbf{b} = x_1\mathbf{a}_1+\dots+x_n\mathbf{a}_n$$

→ vektor **b**: **vektor desnih strani**
→ vektorji **a**: **stolpci** sistema
→ množica rešitev **vsi** možni **razvoji** vektorja desnih strani po stolpcih

1. METODA REŠEVANJA:
Izločanje spremenljivk

→ iz prve enačbe **izločimo** spremenljivko
→ **vstavimo** v ostale enačbe
→ dobimo sistem z eno enačbo in eno spremenljivko **manj**
→ postopek **ponavljamo** dokler ne zmanjka enačb oz spremenljivk
→ če **zmanjka enačb** potem sistem **rešljiv**
→ če zmanjka spremenljivk preverimo če je katera **protislovna**
→ izraz za zadnjo izraženo spremenljivko **vstavimo** v ostale

homogen sistem je **vedno rešljiv** ker ima **trivialno** rešitev, neenolično rešljiv vedno kadar **poddoločen**

2. METODA REŠEVANJA:
Gaussova metoda za reševanje sistemov

- zamenjamo **vrstni red**
- **pomnožimo** z neničelno **konstanto**
- k eni **prištejemo večkratnik** druge

$$\left[\begin{array}{ccc|c} a_{1,1} & \dots & a_{1,n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m,1} & \dots & a_{m,n} & b_m \end{array}\right]$$

razširjena matrika sistema

→ množica rešitev sistema se ne spremeni če uporabimo eno od **elementarnih vrstičnih transformacij**
→ ker se s spremenljivkami nič ne dogaja jih ne pišemo
→ napišemo razširjeno matriko sistema
→ izvedemo naslednje korake:

- poiščemo prvi stolpec z **neničelnim** elementom
- označimo stolpec z $\mathbf{j_1}$
- če je $\mathbf{a_{1,\,j1}}$ nič in $\mathbf{a_{r,\,j1}}$ ni nič **zamenjamo** vrstici
- prvo vrstico delimo z $\mathbf{a_{1,\,j1}}$ tako da zdaj tam **1**
- od vsake vrstice razen prve **odštejemo** z $\mathbf{a_{i,\,j1}}$ **pomnoženo** prvo vrstico torej so vsi elementi v $\mathbf{j_1}$ stolpcu 0 razen prvega

$$\left[\begin{array}{cccccccc|c} 0 & \dots & 0 & 1 & a'_{1,j_1+1} & \dots & a'_{1,n} & & b'_1 \\ 0 & \dots & 0 & 0 & a'_{2,j_1+1} & \dots & a'_{2,n} & & b'_2 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & a'_{m,j_1+1} & \dots & a'_{m,n} & & b'_m \end{array}\right]$$

→ ignore prvo vrstico in korake **ponovimo** na vseh ostalih vrsticah
→ spet ignoriramo drugo vrstico in tako naprej tretjo in **ponavljamo**

$$\left[\begin{array}{ccccccccccccccccc|c} 0 & \dots & 0 & 1 & \times & \dots & \times & \times & \times & \dots & \times & \times & \times & \dots & \times & \times & \dots & \times \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & \times & \dots & \times & \times & \times & \dots & \times & \times & \dots & \times \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & \times & \dots & \times & \times & \dots & \times \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & \dots & \times \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & \times \end{array}\right]$$

→ dobimo **vrstično stopničasto formo sistema**
→ x označuje neko število ki je lahko neničelno
→ taka forma ima k neničelnih vrstic začetne enke teh pa so **pivoti**
→ z zadnjim pivotom **uničimo** vse elemente **nad** njim
→ nadaljujemo do prvega kjer ni nič za uničit
→ dobimo **reducirano vrstično stopničasto formo**
→ iz nje lahko izpišemo enačbe

$$\left[\begin{array}{ccccccccccccccccc|c} 0 & \dots & 0 & 1 & \times & \dots & \times & 0 & \times & \dots & \times & 0 & \times & \dots & \times & 0 & \dots & \times \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & \times & \dots & \times & 0 & \times & \dots & \times & 0 & \dots & \times \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & \times & \dots & \times & 0 & \dots & \times \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & \dots & \times \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & \times \end{array}\right]$$

če dobimo na koncu v **vrstični stopničasti** formi kjerkoli obliko: [**0** … **0** | **x**] in x **ni nič** potem je sistem **nerešljiv** in **končamo**

nehomogen: ne nujno homogen

Homogeni sistemi:

→ ima vsaj eno **trivialno** rešitev
→ **linearna kombinacija** dveh rešitev je spet rešitev
→ splošna rešitev nehomogenega sistema je **vsota partikularne** rešitve nehomogenega in **splošne** rešitve pripadajočega **homogenega** sistema

1. DOKAZ:
Dokazujemo z **popolno indukcijo** po številu vrstic. Dokažimo najprej za enačbo kjer je spremenljivk več ali enako 2 vrstica pa samo ena. Če je $\mathbf{a_n}$ **nič** potem je (**0,…,0,1**) netrivialna rešitev. Če **ni nič** potem je (**0,…,0,** $\mathbf{-a_n}$**,** $\mathbf{a_{n-1}}$) netrivialna rešitev. Recimo da to drži za vse sisteme z **m** – **1** enačbami. Vzemimo poljuben homogen sistem z **m** vrsticami in **n** > **m** stolpci. Če so vsi **koeficienti nič** je netrivialna rešitev (**0,…,0,1**). Če to ne drži **izpostavimo** eno spremenljivko in jo vstavimo v preostalih m – 1 enačb. Sedaj imamo m – 1 enačb z n – 1 spremenljivkami za kar lahko uporabimo **indukcijsko predpostavko**.

2. DOKAZ:
Vzamemo **dve rešitvi** sistema ena spremenljivke označene z **s** in druge z **t**. Preverimo če je **linearna kombinacija** res rešitev:

$$a_{1,1}(\alpha s_1+\beta t_1)+\dots+a_{1,n}(\alpha s_n+\beta t_n) =$$
$$= \alpha(a_{1,1}s_1+\dots+a_{1,n}s_n)+\beta(a_{1,1}t_1+\dots+a_{1,n}t_n) = 0$$
$$\vdots$$
$$a_{m,1}(\alpha s_1+\beta t_1)+\dots+a_{m,n}(\alpha s_n+\beta t_n) =$$
$$= \alpha(a_{m,1}s_1+\dots+a_{m,n}s_n)+\beta(a_{m,1}t_1+\dots+a_{m,n}t_n) = 0$$

3. DOKAZ:
Možico rešitev **nehomogenega** sistema dobimo tako, da za p **premaknemo** množico rešitev pripadajočega **homogenega**. Dokaz zelo očiten, vidimo, da če tako kot pri prejšnjem dokazu samo **prištejemo** rešitve dobimo rešitev nehomogenega sistema in obratno če **odštejemo**.

Predoločeni sistemi:

$(a_{1,1}x_1 + \ldots + a_{1,n}x_n, \ldots, a_{m,1}x_1 + \ldots + a_{m,n}x_n)$

$(b_1, \ldots, b_m)$

→ več enačb kot spremenljivk
→ običajno **nerešljiv**
→ posplošimo definicijo rešitve tako da sistem **posplošeno rešljiv**

če je sistem običajno rešljiv potem se rešitvi **ujemata**

rešitvi rečemo tudi rešitev po **metodi najmanjših kvadratov** ker minimizira izraz

$$(a_{1,1}x_1 + \ldots + a_{1,n}x_n - b_1)^2 + \ldots + (a_{m,1}x_1 + \ldots + a_{m,n}x_n - b_m)^2$$

Podoločeni sistemi:

→ manj neznank kot enačb
→ lahko tudi **nerešljiv**

TRDITEV: če je poddoločen sistem rešljiv potem ima **neskončno** rešitev

DOKAZ:
Vsak poddoločen **homogen** sistem ima **neskončno** rešitev in če je **h** množica rešitev tega sistema, **p** pa rešitev nehomogenega pripadajočega sistema potem je tudi **p** + **h** rešitev tega sistema

Posplošena rešitev:

→ to je taka n-terica realnih števil da je vektor **desnih** strani **najbližje** vektorju **levih** strani
→ predelamo v vektorsko obliko
→ geometrijsko je minimizacija izraza enaka **pravokotni projekciji** vektorja **b** na množico vseh **linearnih kombinacij** vektorjev $\mathbf{a}_1, \ldots \mathbf{a}_n$
→ poiskati moramo take skalarje x, da je vektor $x_1\mathbf{a}_1 + \ldots + x_n\mathbf{a}_n - \mathbf{b}$ pravokoten na vektorje $\mathbf{a}_1, \ldots \mathbf{a}_n$
→ če pogoje za pravokotnost razpišemo dobimo **sistem** linearnih enačb

$$\|x_1\mathbf{a}_1 + \ldots + x_n\mathbf{a}_n - \mathbf{b}\|^2$$

$\mathbf{a}_1 = (a_{1,1}, \ldots, a_{m,1})$ $\mathbf{a}_n = (a_{1,n}, \ldots, a_{m,n})$

$\mathbf{b} = (b_1, \ldots, b_m)$

$$\langle x_1\mathbf{a}_1 + \ldots + x_n\mathbf{a}_n - \mathbf{b}, \mathbf{a}_1\rangle = \ldots$$
$$= \langle x_1\mathbf{a}_1 + \ldots + x_n\mathbf{a}_n - \mathbf{b}, \mathbf{a}_n\rangle = 0$$

$$\begin{array}{ccc} \langle\mathbf{a}_1,\mathbf{a}_1\rangle x_1 + \ldots + \langle\mathbf{a}_n,\mathbf{a}_1\rangle x_n & = & \langle\mathbf{b},\mathbf{a}_1\rangle \\ \vdots \quad\quad \vdots & & \vdots \\ \langle\mathbf{a}_1,\mathbf{a}_n\rangle x_1 + \ldots + \langle\mathbf{a}_n,\mathbf{a}_n\rangle x_n & = & \langle\mathbf{b},\mathbf{a}_n\rangle \end{array}$$

Regresijska premica:

→ taka premica **y** = **ax** + **b**
→ najbolje se prilega točkam $(\mathbf{x_1}, \mathbf{y_1}), \ldots, (\mathbf{x_n}, \mathbf{y_n})$
→ če bi iskana premica šla skozi vse dane točke bi koeficienta zadoščala **m** × **2** sistemu:
$\mathbf{a}x_1 + \mathbf{b} = y_1$ in $\mathbf{a}x_2 + \mathbf{b} = y_2$
→ to se skoraj nikoli ne zgodi ko m več od 2
→ uporabimo **posplošeno rešitev**

$$(ax_1 + b - y_1)^2 + \ldots + (ax_m + b - y_m)^2$$

$$\|a(x_1, \ldots, x_m) + b(1, \ldots, 1) - (y_1, \ldots, y_m)\|^2$$

→ iščemo tak a in b da bo izraz **minimalen**
→ točke pravokotno projiciramo na ravnino $\mathbf{R}^{\mathbf{m}}$
→ vemo da mora biti vektor pravokoten na $(\mathbf{x_1}, \ldots, \mathbf{x_n})$ in $(\mathbf{1}, \ldots, \mathbf{1})$

$$\langle a(x_1, \ldots, x_m) + b(1, \ldots, 1) - (y_1, \ldots, y_m), (x_1, \ldots, x_m)\rangle = 0$$
$$\langle a(x_1, \ldots, x_m) + b(1, \ldots, 1) - (y_1, \ldots, y_m), (1, \ldots, 1)\rangle = 0$$

$$\begin{array}{ccccc} a(\sum_{i=1}^m x_i^2) & + & b(\sum_{i=1}^m x_i) & = & \sum_{i=1}^m x_i y_i \\ a(\sum_{i=1}^m x_i) & + & bm & = & \sum_{i=1}^m y_i \end{array}$$

rešitev tega sistema vstavimo v **y = ax + b**

izkaže se da je ta sistem vedno **rešljiv**, enolično ko so vektorji a_i **linearno neodvisni**

Najkrajša rešitev:

→ **geometrijsko:** pravokotna projekcija izhodišča na presek hiperravnin

Ena hiperravnina:

$\langle\mathbf{n},\mathbf{r}\rangle = b$ $\quad \mathbf{r} = t\mathbf{n}$

premica ki gre skozi **izhodišče,** iščemo njun presek. Vstavimo prvo v drugo in dobimo t. Potem vstavimo to v r in dobimo **najkrajšo rešitev**.

$$t = \frac{b}{\langle\mathbf{n},\mathbf{n}\rangle} \quad \mathbf{r} = \frac{b}{\langle\mathbf{n},\mathbf{n}\rangle}\mathbf{n}$$

Dve hiperravnini:

$\langle\mathbf{n}_1,\mathbf{r}\rangle = b_1$ in $\langle\mathbf{n}_2,\mathbf{r}\rangle = b_2$

lotimo se v dveh korakih. Najdemo ravnino ki je **pravokotna** na **presek** obeh hiperravnin in gre skozi **izhodišče**.

$$\mathbf{r} = t_1\mathbf{n}_1 + t_2\mathbf{n}_2$$

Izračunamo **presek** te z **presekom hiperravnin**. Dobimo sistem:

$$t_1\langle\mathbf{n}_1,\mathbf{n}_1\rangle + t_2\langle\mathbf{n}_1,\mathbf{n}_2\rangle = b_1$$
$$t_1\langle\mathbf{n}_2,\mathbf{n}_1\rangle + t_2\langle\mathbf{n}_2,\mathbf{n}_2\rangle = b_2$$

Rešimo t in vstavimo v enačbo ravnine. Postopek deluje tudi za **več** hiperravnin

MATRIKE

→ **matrika** velikosti **m** × **n** je urejena m-terica urejenih n-teric realnih števil
→ element prostora $(\mathbf{R}^{\mathbf{n}})^{\mathbf{m}}$
→ matrike **1** × **1** so **skalarji**
→ **m** × **1** so **stolpčni** vektorji
→ **1** × **n** so **vrstični** vektorji
→ stolpčni vektorji v matriki so **stolpci**
→ vrstični vektorji v matriki so **vrstice**

$$\alpha \begin{bmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \ldots & a_{m,n} \end{bmatrix} := \begin{bmatrix} \alpha a_{1,1} & \ldots & \alpha a_{1,n} \\ \vdots & & \vdots \\ \alpha a_{m,1} & \ldots & \alpha a_{m,n} \end{bmatrix}$$

- produkt s skalarjem je po **komponentah**
- vsota je po **komponentah**

Operacije z matrikami:

1. **produkt** matrike z **skalarjem**
2. **vsota** dveh matrik
3. **produkt** dveh matrik

$$\begin{bmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \ldots & a_{m,n} \end{bmatrix} + \begin{bmatrix} b_{1,1} & \ldots & b_{1,n} \\ \vdots & & \vdots \\ b_{m,1} & \ldots & b_{m,n} \end{bmatrix} := \begin{bmatrix} a_{1,1}+b_{1,1} & \ldots & a_{1,n}+b_{1,n} \\ \vdots & & \vdots \\ a_{m,1}+b_{m,1} & \ldots & a_{m,n}+b_{m,n} \end{bmatrix}$$

- produkt matrik **m** × **p** in **p** × **n** je matrika **m** × **n**
- za matriko **C** = **A** · **B** velja:

$$\begin{bmatrix} c_{i,j} \end{bmatrix} = \begin{bmatrix} a_{i,1} & \ldots & a_{i,n} \end{bmatrix} \begin{bmatrix} b_{1,j} \\ \vdots \\ b_{n,j} \end{bmatrix} = \begin{bmatrix} \sum_{k=1}^n a_{i,k}b_{k,j} \end{bmatrix}$$

- osnovne **lastnosti** so:

$(AB)C = A(BC)$
$(A+B)C = AC + BC$
$A(B+C) = AB + AC$
$(\lambda A)B = A(\lambda B) = \lambda(AB)$

Posebne matrike:

1. **transponiranka**
2. **ničelna** matrika
3. **identična** matrika

1. transponiranka je če **obrnemo** vsak **i,j**-ti element v **j,i**-ti element

2. ničelna matrika je taka matrika ki ima **vse** elemente **nič** če sta m in n znana pišemo kar **0**. enota za **seštevanje**, če množimo z njo ali jo **transponiramo** dobimo **ničelno** matriko

$$\begin{bmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \ldots & a_{m,n} \end{bmatrix}^T := \begin{bmatrix} a_{1,1} & \ldots & a_{m,1} \\ \vdots & & \vdots \\ a_{1,n} & \ldots & a_{m,n} \end{bmatrix}$$

3. identična matrika je taka kvadratna matrika ki ima po glavni **diagonali same enke** in drugje **nič**. označimo z $\mathbf{I_n}$ in je enota za **množenje**. če jo transponiramo spet **identična** matrika

$$A\mathbf{x} = \mathbf{b}$$

$$\begin{bmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \ldots & a_{m,n} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{1,1}x_1 + \ldots + a_{1,n}x_n \\ \vdots \\ a_{m,1}x_1 + \ldots + a_{m,n}x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

z matriko lahko zapišemo tudi **sistem enačb**

Gaussova metoda v matričnem zapisu

→ definiramo **elementarne** matrike
→ elementarne **transformacije** zapišemo z njimi
→ uporabljamo transformacije dokler ne dobimo matrike oblike **stopničaste reducirano forme**

Posplošena rešitev sistema v matričnem zapisu

→ kadar je sistem **Ax** = **b** nerešljiv
→ poiščemo tak $\mathbf{x}_0$ ki **minimizira** izraz || Ax – b ||
→ **vektorski** zapis napišemo v **matričnem** $A^T A\mathbf{x} = A^T\mathbf{b}$

$$\begin{bmatrix} \langle \mathbf{a}_1, \mathbf{a}_1\rangle & \dots & \langle \mathbf{a}_1, \mathbf{a}_n\rangle \\ \vdots & \ddots & \vdots \\ \langle \mathbf{a}_n, \mathbf{a}_1\rangle & \dots & \langle \mathbf{a}_n, \mathbf{a}_n\rangle \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \langle \mathbf{a}_1, \mathbf{b}\rangle \\ \vdots \\ \langle \mathbf{a}_n, \mathbf{b}\rangle \end{bmatrix}$$

Najkrajša rešitev sistema v matričnem zapisu

→ kadar je sistem **Ax** = **b** neenolično rešljiv

TRDITEV: **najkrajša** rešitev sistema **Ax** = **b** je enaka $\mathbf{A^T}$ $\mathbf{y_0}$ kjer je $\mathbf{y_0}$ **poljubna** rešitev $\mathbf{AA^T}$ **y** = **b**

DOKAZ:

Naj bo $\mathbf{x}_0$ poljubna rešitev sistema **Ax** = **b** in $\mathbf{y}_0$ poljubna rešitev sistema $\mathbf{AA^T}$ **y** = **b,** pokažemo da || $\mathbf{x}_0$ || ≥ || $\mathbf{A^T}$ **y** ||

Najprej pokažemo da sta $\mathbf{x}_0$ - $\mathbf{A^T}$ **y** in $\mathbf{A^T}$ **y pravokotna** in nato uporabimo **Pitagorov** izrek:

$$\langle \mathbf{x}_0 - A^T\mathbf{y}_0, A^T\mathbf{y}_0\rangle = (\mathbf{x}_0 - A^T\mathbf{y}_0)^T A^T\mathbf{y}_0 =$$
$$= (A(\mathbf{x}_0 - A^T\mathbf{y}_0))^T\mathbf{y}_0 = (\mathbf{b}-\mathbf{b})^T\mathbf{y}_0 = 0$$

$$\|\mathbf{x}_0\|^2 = \|\mathbf{x}_0 - A^T\mathbf{y}_0 + A^T\mathbf{y}_0\|^2 =$$
$$\|\mathbf{x}_0 - A^T\mathbf{y}_0\|^2 + \|A^T\mathbf{y}_0\|^2 \geq \|A^T\mathbf{y}_0\|^2$$

Iz česar sledi tudi zelena **neenakost**, prav tako pa tudi da je res vseeno katero rešitev vzamemo.

Elementarne matrike:

→ identični matriki **i**-ti vrstici **prištejemo α**-kratnik **j**-te vrstice $E_{i,j}(\alpha)$
→ v identični matriki **zamenjamo i**-to in **j**-to vrstico $P_{i,j}$
→ v identični matriki **množimo** i-to vrstico z **β** $E_i(\beta)$

Elementarne transformacije:

→ če **i**-ti enačbi prištejemo **α**-kratnik **j**-te enačbe $E_{i,j}(\alpha)A\mathbf{x} = E_{i,j}(\alpha)\mathbf{b}$
→ če **zamenjamo** dve enačbi $P_{i,j}A\mathbf{x} = P_{i,j}\mathbf{b}$
→ če **pomnožimo i**-to enačbo z **β** $E_i(\beta)A\mathbf{x} = E_i(\beta)\mathbf{b}$

TRDITEV: **posplošene** rešitve sistema **Ax** = **b** so enake **običajnim** rešitvam sistema $\mathbf{A^T}$ **Ax** = $\mathbf{A^T}$ **b**

DOKAZ:

Naj bo $\mathbf{x}_0$ tak da velja **matrični zapis**. uporabili bomo formulo ⟨**c**, **d**⟩ = $\mathbf{c^T}$ **d**. Potem velja slednja formula ki pa je po predpostavki **nič**. Uporabimo **Pitagorov izrek** ki dokaže, da izrek res minimizira **Ax** = **b**

$$\langle A(\mathbf{x}-\mathbf{x}_0), A\mathbf{x}_0 - \mathbf{b}\rangle = (A(\mathbf{x}-\mathbf{x}_0))^T(A\mathbf{x}_0 - \mathbf{b}) = (\mathbf{x}-\mathbf{x}_0)^T A^T(A\mathbf{x}_0 - \mathbf{b})$$

$$\|A\mathbf{x}-\mathbf{b}\|^2 = \|A(\mathbf{x}-\mathbf{x}_0) + A\mathbf{x}_0 - \mathbf{b}\|^2 = \|A(\mathbf{x}-\mathbf{x}_0)\|^2 + \|A\mathbf{x}_0 - \mathbf{b}\|^2$$

$\|A\mathbf{x}-\mathbf{b}\| \geq \|A\mathbf{x}_0 - \mathbf{b}\|$ $\mathbf{c} := A\mathbf{x}_0 - \mathbf{b}$ $\mathbf{d} := A\mathbf{z}$

V drugo stran: recimo da je $\mathbf{x}_0$ tak, da je **posplošena rešitev** sistema. Torej za vsak x velja zadnja enačba zgoraj. Pokažimo, da sta c in d **pravokotna**.

Po predpostavki je $\|\mathbf{c}+t\mathbf{d}\| \geq \|\mathbf{c}\|$ za vsak $t \in \mathbb{R}$. Če $\langle \mathbf{c}, \mathbf{d}\rangle \neq 0$, potem za $t_0 := -\frac{\langle \mathbf{c},\mathbf{d}\rangle}{\langle \mathbf{d},\mathbf{d}\rangle}$ velja $t_0\mathbf{d} \neq 0$. Po definiciji t_0 je $\langle \mathbf{c}+t_0\mathbf{d}, \mathbf{d}\rangle = 0$, torej je $\|\mathbf{c}+t_0\mathbf{d}\|^2 + \|-t_0\mathbf{d}\|^2 = \|\mathbf{c}\|^2$, kar nam da protislovje $\|\mathbf{c}+t_0\mathbf{d}\| < \|\mathbf{c}\|$.

Iz **pravokotnosti c** in **d** sledi

$$\langle A^T(A\mathbf{x}_0-\mathbf{b}), \mathbf{z}\rangle = (A^T(A\mathbf{x}_0-\mathbf{b}))^T\mathbf{z} = (A\mathbf{x}_0-\mathbf{b})^T A\mathbf{z} = \mathbf{c}^T\mathbf{d} = 0$$

$\mathbf{z} = A^T(A\mathbf{x}_0 - \mathbf{b})$ → $\mathbf{z} = \mathbf{0}$ → $A^TA\mathbf{x}_0 = A^T\mathbf{b}$

primerjava matričnega in vektorskega zapisa: **Ax** = **b** lahko zapišemo kot

$\langle \mathbf{n}_1, \mathbf{x}\rangle = b_1 \quad \dots \quad \langle \mathbf{n}_m, \mathbf{x}\rangle = b_m$

$\mathbf{x} = y_1\mathbf{n}_1 + \dots + y_m\mathbf{n}_m$

$\mathbf{n_i}$ so transponirane vrstice matrike A in rešitev iščemo z spodnjo enačbo in to **vstavimo** v zgornjo

dobimo sistem ki je v matričnem zapisu $\mathbf{AA^T}$ **y** = **b**

$$\begin{bmatrix} \langle \mathbf{n}_1, \mathbf{n}_1\rangle & \dots & \langle \mathbf{n}_1, \mathbf{n}_m\rangle \\ \vdots & \ddots & \vdots \\ \langle \mathbf{n}_m, \mathbf{n}_1\rangle & \dots & \langle \mathbf{n}_m, \mathbf{n}_m\rangle \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

Obrnljive matrike

Inverz matrike:

→ inverz **kvadratne** matrike **A** je **kvadratna** matrika B da velja **A** · **B** = **I**
→ matrika ima lahko **največ en** inverz
→ ničelna matrika nima inverza
→ označimo: $\mathbf{A}^{-1}$
→ nimajo vse inverza
→ najdemo tako da **A razširimo** na desno z **I** iste velikosti
→ matrika **obrnljiva** če ima inverz

dokaz za en inverz

$$B_1 = IB_1 = (B_2A)B_1 = B_2(AB_1) = B_2I = B_2$$

DOKAZ:

Naj bodo E_1 do E_n take **elementarne** matrike da ima S = $E_n \cdots E_1 \cdot A$ **reducirano stopničsto formo**. Ločimo dva primera, če ima S **ničelno** vrstico ni obrnljiva sledi da tudi A ni obrnljiva. Če nima ničelne vrstice potem je enaka identični matriki torej $A^{-1} = E_n \cdots E_1$:

$$[A|I] \xrightarrow{E_1} [E_1A|E_1] \xrightarrow{E_2} \dots \xrightarrow{E_n} [E_n\cdots E_1A|E_n\cdots E_1] = [I|A^{-1}]$$

Torej ima ravno takrat ko je enaka **produktu elementarnih matrik**.

TRDITEV: A je poljubna **n** × **n** matrika in C poljubna **n** × **n obrnljiva** matrika.
→ če stolpci A **linearno neodvisni** tudi stolpci **CA**
→ če stolpci A **ogrodje** tudi stolpci **CA**

DOKAZ 1:

$CA\mathbf{x} = 0$ $\quad A\mathbf{x} = C^{-1}(CA\mathbf{x})$

$C^{-1}\mathbf{0} = \mathbf{0}$ $\quad \mathbf{x} = \mathbf{0}$

DOKAZ 2:

obstaja tak **x** da: $A\mathbf{x} = C^{-1}\mathbf{b}$ če **pomnožimo** z C: $CA\mathbf{x} = \mathbf{b}$

→ vsako **n** × **n** matriko lahko napišemo kot **A** = [$\mathbf{a_1}$...$\mathbf{a_n}$]
→ $\mathbf{a_i}$ so **stolpci** matrike
→ za vsako **n** × **n** matriko **C** velja

$$CA = C[\mathbf{a}_1 \dots \mathbf{a}_n] = [C\mathbf{a}_1 \dots C\mathbf{a}_n]$$

$$A\mathbf{x} = A\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = x_1\mathbf{a}_1 + \dots + x_n\mathbf{a}_n$$

za vsak stolpčni vektor

TRDITEV:
→ stolpci **A** so **linearno neodvisni** natanko ko za vsak **x** ∈ R^n ki zadošča **Ax** = **0** velja **x** = **0**
→ stolpci so **ogrodje** natanko ko za vsak **b** ∈ R^n obstaja **x** ∈ R^n da velja **Ax** = **b**

DOKAZ 2:

Iz dokaza gor da so stolpci **ogrodje** če obstajajo x da velja:

$$\mathbf{b} = x_1\mathbf{a}_1 + \dots + x_n\mathbf{a}_n$$

DOKAZ 1:

Gre direktno iz dokaza gor da so stolpci **linearno neodvisni** če

$$x_1\mathbf{a}_1 + \dots + x_n\mathbf{a}_n = 0$$

in če za vsak x za katerega velja zgornja enačba velja

$$x_1 = \dots = x_n = 0$$

TRDITEV: če je kvadratna matrika **reducirana vrstična stopničasta forma** ekvivalentno:
→ stolpci A **linearno neodvisni**
→ stolpci A **ogrodje**
→ A je **identična** matrika

DOKAZ:
Iz **tretje** trditve sledita **prve dve**. Če zadnja **ni identična** matrika potem stolpci **niso linearno neodvisni** in **ogrodje**. Dokaz. Če ni identiteta potem ima stopnico **daljšo** od **1** ker je stolpec ki je na drugem mestu v drugi stopnici **linearna kombinacija prejšnjih** stolpcev stolpci niso linearno neodvisni. In ker je ena daljša od 1 stopnišče **ne pride** do **konca** torej je zadnja vrstica **ničelna**. Zato ni ogrodje.

POSLEDICA: za vsako kvadratno matriko so enakovredne trditve:
→ stolpci A **linearno neodvisni**
→ stolpci A **ogrodje**
→ A je produkt **elementarnih** matrik

DOKAZ:
Identična matrika ima po stolpce **linearno neodvisne** in so **ogrodje** ker so elementarne matrike **obrnljive** in lahko I zapišemo kot njihov **produkt**. V drugo smer po **Gaussovi metodi** obstajajo elementarne matrike z katerimi spravimo matriko A v **reducirano vrstično formo** in ker so stolpci neodvisni so tudi stolpci dobljene matrike neodvisni po prejšnji trditvi. To pa pomeni da je dobljena matrika **identična** in torej produkt elementarnih matrik.

POSLEDICA: za vsako kvadratno matriko so enakovredne trditve:
→ A je **obrnljiva**
→ obstaja matrika **B** da **AB** = **I**
→ stolpci A so **ogrodje**

DOKAZ:
Po prejšnji posledici iz prve trditve sledi zadnja saj je matrika **obrnljiva** natanko tedaj **ko produkt elementarnih** matrik. Za iz druge v tretjo dokažemo da obstaja x da **Ax** = **b** in za x vzamemo **x** = **Bb**

TRDITEV: **transponiranka** obrnljive matrike je obrnljiva

DOKAZ:
Ker A obrnljiva velja $AA^{-1} = A^{-1}A = I$
$$(A^{-1})^T A^T = A^T (A^{-1})^T = I^T = I$$
in velja $(A^T)^{-1} = (A^{-1})^T$

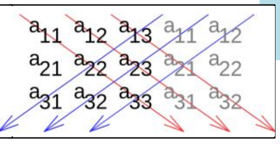
P O V Z E T E K

naslednje trditve so ekvivalentne:
→ matrika A je **obrnljiva**
→ obstaja matrika **B** da je **AB** = **BA** = **I**
→ stolpci A so **ogrodje**
→ stolpci A so linearno **neodvisni**
→ A je **produkt elementarnih** matrik
→ za vsak **b** obstaja **x** da velja **Ax** = **b**
→ za vsak **x** ki zadošča **Ax** = **0** je **x** = **0**
→ **vrstična kanonična forma** za A je **I**
→ matrika $\mathbf{A^T}$ je **obrnljiva**

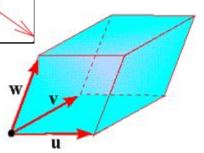
DETERMINANTE

→ vsaki kvadratni matriki priredimo **realno število** ki mu rečemo **determinanta**
→ **det** [**a**] = **a** če je matrika **1** × **1**
→ za matriko **n** × **n** označimo z $A_{i,j}$ matriko ki jo dobimo če **zbrišemo vrstico** i in **stolpec** j velikosti **n – 1** × **n – 1**

formulo za determinanto **3** × **3** si zapomnimo: pozitivne so **rdeče** negativne so **modre**

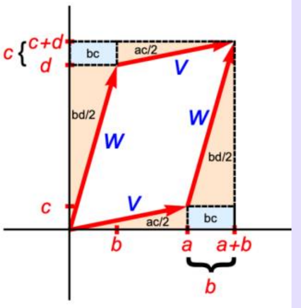


→ determinanto lahko razvijemo po **stolpcu** ali po **vrstici**
→ razvoj po **vrstici i**:
$$\det A = \sum_{k=1}^{n} a_{i,k}(-1)^{i+k} \det A_{i,k}$$
→ razvoj po **stolpcu j**:
$$\det A = \sum_{k=1}^{n} a_{k,j}(-1)^{k+j} \det A_{k,j}$$



po navadi razvijemo po tistem stolpcu oziroma vrstici ki ima **največ ničel**

determinanta v splošnem **ni linearna** spodaj obravnavamo **vrstice** trditve veljajo tudi za **stolpce**



Geometrijski pomen:
→ absolutna vrednost **2** × **2** det je enaka **ploščini paralelograma**, ki ga razpenjata stolpca matrike
$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc$$
$$\mathbf{v} = \begin{bmatrix} a \\ c \end{bmatrix} \quad \mathbf{w} = \begin{bmatrix} b \\ d \end{bmatrix}$$
$$(a+b)(c+d) - 2bc - 2\frac{ac}{2} - 2\frac{bd}{2} = ad - bc = \det A.$$
→ **predznak** povezan z **orientacijo** če bi **w** ležal na drugi strani **v** bi bila determinanta negativna
→ determinanta **3** × **3** je enaka **volumnu** paralepipeda kar je enako **mešanemu produktu**
→ recimo da so stolpci **u v w**
$$u_1(v_2w_3 - v_3w_2) - v_1(u_2w_3 - u_3w_2) + w_1(u_2v_3 - u_3v_2)$$
$$\langle \mathbf{u} \times \mathbf{v}, \mathbf{w} \rangle = (u_2v_3 - u_3v_2)w_1 + (u_3v_1 - u_1v_3)w_2 + (u_1v_2 - u_2v_1)w_3$$

TRDITEV: determinanta je **linearna** v vsaki **vrstici** in pa **stolpcu**
$$\det \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,n} \\ \beta b_{i,1} + \gamma c_{i,1} & \cdots & \beta b_{i,n} + \gamma c_{i,n} \\ a_{i+1,1} & \cdots & a_{i+1,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} = \beta \det \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,n} \\ b_{i,1} & \cdots & b_{i,n} \\ a_{i+1,1} & \cdots & a_{i+1,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} + \gamma \det \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,n} \\ c_{i,1} & \cdots & c_{i,n} \\ a_{i+1,1} & \cdots & a_{i+1,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix}$$

TRDITEV: če dve vrstici **zamenjamo** se determinanti spremeni **predznak**
$$\det P_{i,j}A = -\det A$$

DOKAZ:
Determinanto razvijemo po iti vrstici in dobimo:
$$\det A(\beta,\gamma) = \sum_{k=1}^{n}(-1)^{i+k}(\beta b_{i,k} + \gamma c_{i,k}) \det A_{i,k}$$
$$\beta \sum_{k=1}^{n}(-1)^{i+k} b_{i,k} \det A_{i,k} + \gamma \sum_{k=1}^{n}(-1)^{i+k} c_{i,k} \det A_{i,k}$$
$$\det A(\beta,\gamma) = \beta \det A(1,0) + \gamma \det A(0,1)$$

DOKAZ:
Dokažemo **induktivno**. Najprej dokažemo za matriko **2** × **2**.
$$\det \begin{bmatrix} a_{2,1} & a_{2,2} \\ a_{1,1} & a_{1,2} \end{bmatrix} = a_{1,2}a_{2,1} - a_{1,1}a_{2,2} = -\det \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix}$$
Predpostavimo da velja za **n – 1** × **n – 1**. Vzamemo **n** × **n** matriko A in poljubna **različna i** in **j**. Za poljuben **k** različen od i in j lahko det $\mathbf{P_{i,j}}$ **A** izračunamo tako da jo razvijemo po kti vrstici. Upoštevamo indukcijsko predpostavko in **izpostavimo -1** in determinanto **razvijemo** kot **det A** in dobimo želeno formulo.

POSLEDICA: če ima matrika dve **vrstici enaki** je njena determinanta **0**

TRDITEV:
Če v matriki A eni **vrstici prištejemo večkratnik druge** vrstice potem se njena determinanta **ne spremeni**

$\det(E_{i,j}(\alpha)A) = \det A$

DOKAZ:
Po prejšnji **posledici** in **prvi trditvi** o linearnosti

$$\det(E_{i,j}(\alpha)A) = \det \begin{bmatrix} \vdots & & \vdots \\ a_{i,1}+\alpha a_{j,1} & & a_{i,n}+\alpha a_{j,n} \\ \vdots & & \vdots \\ a_{j,1} & & a_{j,n} \\ \vdots & & \vdots \end{bmatrix} =$$

$$= \det \begin{bmatrix} \vdots & \vdots \\ a_{i,1} & a_{i,n} \\ \vdots & \vdots \\ a_{j,1} & a_{j,n} \\ \vdots & \vdots \end{bmatrix} + \alpha \det \begin{bmatrix} \vdots & \vdots \\ a_{j,1} & a_{j,n} \\ \vdots & \vdots \\ a_{j,1} & a_{j,n} \\ \vdots & \vdots \end{bmatrix} =$$

$$= \det A + \alpha \cdot 0 = \det A$$

Gaussova metoda za računanje determinant

→ matriko hočemo s pomočjo elementarnih vrstičnih transformacij pripeljati do **reducirane vrstične stopničaste** forme
→ upoštevati moramo prejšnje trditve
→ če vrstici **zamenjamo**: spremenimo **predznak**
→ če **prištejemo** večkratnik: se ne zgodi **nič**
→ če **vrstico pomnožimo** z številom: celo **determinanto pomnožimo**
→ reducirana vrstična forma je **zgornje trikotna**

TRDITEV:
determinanta **zgornje trikotne** matrike je enaka **produktu** elementov na glavni **diagonali**

DOKAZ:
Večkrat uporabimo formulo za razvoj po **prvi vrstici**:

$$\det \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ 0 & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{n,n} \end{bmatrix} = a_{1,1} \det \begin{bmatrix} a_{2,2} & \dots & a_{2,n} \\ \vdots & \ddots & \vdots \\ 0 & \dots & a_{n,n} \end{bmatrix} =$$

$$= a_{1,1}a_{2,2} \det \begin{bmatrix} a_{3,3} & \dots & a_{3,n} \\ \vdots & \ddots & \vdots \\ 0 & \dots & a_{n,n} \end{bmatrix} = \ldots = a_{1,1}a_{2,2}\cdots a_{n,n}.$$

TRDITEV:
za kvadratni matriki velja
det AB = det A · det B

DOKAZ:
V spodnje formule vstavimo namesto B identično matriko.
Vidimo da trditev velja če je A **elementarna** matrika.

$$\det(E_{i,j}(\alpha)B) = \det B, \quad \det(P_{i,j}B) = -\det B, \quad \det(E_i(\beta)B) = \beta \det B$$

$$\det(E_{i,j}(\alpha)) = 1, \quad \det(P_{i,j}) = -1, \quad \det(E_i(\beta)) = \beta.$$

$$\det(E_{i,j}(\alpha)B) = \det E_{i,j}(\alpha)\det B, \quad \det(P_{i,j}B) = \det P_{i,j}\det B, \quad \det(E_i(\beta)B) = \det E_i(\beta)\det B.$$

Vidimo da velja tudi če ima matrika A v neki vrstici same **ničle** ker ima potem tudi AB same ničle in je determinanta **0**.
V splošnem obstaja **S** = **E$_n$** · · · **E$_1$** · **A** da ima S reducirano vrstično stopničasto obliko. Ločimo dva primera. Če ima S **ničelno vrstico** je potem determinanta A **0** in AB prav tako.

$$\det E_n \cdots \det E_1 \det AB = \det(E_n \cdots E_1 A)B = \det SB = 0$$

$$\det E_n \cdots \det E_1 \det A = \det E_n \cdots E_1 A = \det S = 0.$$

Če nima ničelne vrstice potem je S **identična** matrika

$$\det E_n \cdots \det E_1 \det AB = \det(E_n \cdots E_1 A)B = \det IB = \det B$$

$$\det E_n \cdots \det E_1 \det A = \det E_n \cdots E_1 A = \det I.$$

TRDITEV:
matrika je **obrnljiva** kadar njena determinanta **ni nič**

DOKAZ:
Če je obrnljiva obstaja taka matrika **B** da velja **AB** = **I det I** pa je enaka **1**. V drugo smer če determinanta ni nič lahko izberemo elementarne matrike da je **S** = **E$_n$** · · · **E$_1$** · **A** reducirana vrstična stopničasta forma. Ker so elementarne matrike **obrnljive** determinanta **ni nič**. Po predpostavki determinanta A ni nič torej tudi **det S ni nič**. Torej ne more imeti ničelne vrstice in je po tem takem **identiteta**.

TRDITEV: determinanta **transponiranke** matrike je **enaka** determinanti **matrike**

DOKAZ:

Iz $P_{i,j}^T = P_{i,j}$ sledi $\det P_{i,j}^T = \det P_{i,j}$.
Iz $E_i(\beta)^T = E_i(\beta)$ sledi $\det E_i(\beta)^T = \det E_i(\beta)$.
Iz $E_{i,j}(\alpha)^T = E_{j,i}(\alpha)$ sledi $\det E_{i,j}(\alpha)^T = 1 = \det E_{i,j}(\alpha)$

Izberemo elementarne matrike da **S** = **E$_n$** · · · **E$_1$** · **A** in ločimo:
Če ima S **ničelno vrstico** ima transponiranka ničelni stolpec in je determinanta 0. Če je nima potem je **identiteta** torej je **enaka** svoji **transponiranki** in ima enako determinanto.

$$\det S = \det(E_n \cdots E_1 A) = \det E_n \cdots \det E_1 \det A$$

$$\det E_i^T = \det E_i \neq 0$$

$$\det S^T = \det(E_n \cdots E_1 A)^T = \det(A^T E_1^T \cdots E_n^T) = \det A^T \det E_1^T \cdots \det E_n^T$$

ista formula velja za **spodnje** bločne matrike ker lahko izpeljemo z **transponiranjem**

Bločno trikotna matrika

$$\begin{bmatrix} a_{1,1} & \dots & a_{1,m} & b_{1,1} & \dots & b_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,m} & b_{m,1} & \dots & b_{m,n} \\ 0 & \dots & 0 & c_{1,1} & \dots & c_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & c_{n,1} & \dots & c_{n,n} \end{bmatrix} = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$$

TRDITEV: determinanta **bločno trikotne matrike je det A · det C**

DOKAZ:

$$\begin{bmatrix} A & B \\ 0 & C \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & C \end{bmatrix} \begin{bmatrix} A & B \\ 0 & I \end{bmatrix} \qquad \begin{bmatrix} A & B \\ 0 & I \end{bmatrix} = E \begin{bmatrix} A & 0 \\ 0 & I \end{bmatrix}$$

$$\det \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} = \det \begin{bmatrix} I & 0 \\ 0 & C \end{bmatrix} \det \begin{bmatrix} A & B \\ 0 & I \end{bmatrix}$$

S pomočjo **elementarnih transformacij** dobimo:

$$E = E_{1,m+1}(b_{1,1}) \cdots E_{m,m+1}(b_{m,1}) E_{1,m+n}(b_{1,n}) \cdots E_{m,m+n}(b_{m,n})$$

$$\det \begin{bmatrix} I_m & 0 \\ 0 & C \end{bmatrix} = \det \begin{bmatrix} I_{m-1} & 0 \\ 0 & C \end{bmatrix} = \ldots = \det \begin{bmatrix} I_1 & 0 \\ 0 & C \end{bmatrix} = \det C$$

$$\det \begin{bmatrix} A & 0 \\ 0 & I_n \end{bmatrix} = \det \begin{bmatrix} A & 0 \\ 0 & I_{n-1} \end{bmatrix} = \ldots = \det \begin{bmatrix} A & 0 \\ 0 & I_1 \end{bmatrix} = \det A$$

SCHUROV KOMPLEMENT
→ **A B C** in **D** velikosti: **m × m** | **m × n** | **n × m** | **n × n**
→ če je **D** obrnljiva: **det D det (A − B · D^{-1}C)**
→ če je **A** obrnljiva: **det A det (D − C · A^{-1}B)**

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

DOKAZ: SCHUROV KOMPLEMENT

Če je **D obrnljiva** matrika velja:

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} A - BD^{-1}C & B \\ 0 & D \end{bmatrix} \begin{bmatrix} I_m & 0 \\ D^{-1}C & I_n \end{bmatrix}$$

$$\det \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \det \begin{bmatrix} A - BD^{-1}C & B \\ 0 & D \end{bmatrix} \det \begin{bmatrix} I_m & 0 \\ D^{-1}C & I_n \end{bmatrix} = \det(A - BD^{-1}C) \det D \det I_m \det I_n$$

Če je matrika **A obrnljiva**:

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} I_m & 0 \\ CA^{-1} & I_n \end{bmatrix} \begin{bmatrix} A & B \\ 0 & D - CA^{-1}B \end{bmatrix}$$

$$\det \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \det \begin{bmatrix} I_m & 0 \\ CA^{-1} & I_n \end{bmatrix} \det \begin{bmatrix} A & B \\ 0 & D - CA^{-1}B \end{bmatrix} = \det I_m \det I_n \det A \det(D - CA^{-1}B)$$

CARMEROVO PRAVILO

$$x_i = \frac{\det A_i(\mathbf{b})}{\det A}$$

→ **eksplicitna formula** za rešitev sistema enačb **Ax** = **b**
→ A je **kvadratna** matrika z neničelno determinanto
→ **n** je število stolpcev matrike
→ $\mathbf{A_i}$(**b**) je matrika ki jo dobimo če iti **stolpec** zamenjamo z vektorjem **b**

DOKAZ: CARMEROVO PRAVILO

$\mathbf{a_1}, \dots \mathbf{a_n}$ so stolpci matrike A. Definiramo še matriko $\mathbf{I_i}(\mathbf{x})$ kjer so $\mathbf{e_n}, \dots, \mathbf{e_1}$ stolpci identične matrike I in **x** je rešitev sistema **Ax** = **b**

$$A_i(\mathbf{b}) = \begin{bmatrix} \mathbf{a}_1 & \dots & \mathbf{a}_{i-1} & \mathbf{b} & \mathbf{a}_{i+1} & \dots & \mathbf{a}_n \end{bmatrix}$$

$$I_i(\mathbf{x}) = \begin{bmatrix} \mathbf{e}_1 & \dots & \mathbf{e}_{i-1} & \mathbf{x} & \mathbf{e}_{i+1} & \dots & \mathbf{e}_n \end{bmatrix}$$

Opazimo da velja:

$$\begin{aligned} A\, I_i(\mathbf{x}) &= A \begin{bmatrix} \mathbf{e}_1 & \dots & \mathbf{e}_{i-1} & \mathbf{x} & \mathbf{e}_{i+1} & \dots & \mathbf{e}_n \end{bmatrix} \\ &= \begin{bmatrix} A\mathbf{e}_1 & \dots & A\mathbf{e}_{i-1} & A\mathbf{x} & A\mathbf{e}_{i+1} & \dots & A\mathbf{e}_n \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{a}_1 & \dots & \mathbf{a}_{i-1} & \mathbf{b} & \mathbf{a}_{i+1} & \dots & \mathbf{a}_n \end{bmatrix} \\ &= A_i(\mathbf{b}) \end{aligned}$$

$\det A \det I_i(\mathbf{x}) = \det A_i(\mathbf{b})$ z razvojem $\mathbf{I_i}(\mathbf{x})$ po iti vrstici dobimo $\mathbf{x_i}$

Formula za inverz matrike

$$A^{-1} = \frac{1}{\det A} \tilde{A}^T$$

→ je kvadratna matrika A det **ni 0**
→ vsak element $\mathbf{a_{i,j}}$ v matriki **zamenjamo** z njegovim kofaktorjem $(-1)^{i+j}$ **det** $\mathbf{A_{i,j}}$
→ dobimo **kofaktorsko matriko** matrike A
→ oznaka: **Ã**

DOKAZ

Matrika $\mathbf{A^{-1}}$ je rešitev enačbe **AX** = **I** naj bodo $\mathbf{x_1}, \dots, \mathbf{x_n}$ stolpci potem velja da so $\mathbf{Ax_1} = \mathbf{e_1}, \dots, \mathbf{Ax_n} = \mathbf{e_n}$ kjer so e stolpci v identičnim matriki. vzamemo poljubna i in j in izračunamo element tako da uporabimo Carmerovo pravilo.

$$x_{i,j} = i\text{-ti element vektorja } \mathbf{x}_j = \frac{\det A_i(\mathbf{e}_j)}{\det A}$$

Determinanto **B** = $\mathbf{A_i}(\mathbf{e_j})$ razvijemo po i stolpcu. Če upoštevamo da je $\mathbf{B_{k,i}} = \mathbf{A_{k,i}}$ dobimo spodnjo formulo.

$$\det B = \sum_{k=1}^{n} (-1)^{k+i} b_{k,i} \det B_{k,i}$$

$$b_{k,i} = k\text{-ti element } \mathbf{e}_j = \begin{cases} 0 & k \neq j \\ 1 & k = j \end{cases}$$

$$\det A_i(\mathbf{e}_j) = (-1)^{i+j} \det A_{j,i}$$

$$x_{i,j} = (-1)^{i+j} \frac{\det A_{j,i}}{\det A} = \frac{1}{\det A} (\text{kofaktor } a_{j,i})$$

Torej formula drži.

Permutacije

→ označimo za vsak **naraven n** množico $\mathbf{N_n}$ = { **1**, **2**, **3**, … , **n** }
→ za vsako preslikavo **σ** : $\mathbf{N_n}$ → $\mathbf{N_n}$ so ekvivalentne lastnosti:

- σ je **injektivna** torej slika **različne** elemente **v različne** elemente
- σ je **surjektivna** torej je **vsak** element **slika** nekega elementa
- σ je **bijektivna** ker je injektivna in surjektivna

→ preslikavi ki zadošča tem pogojem pravimo **permutacija** množice $\mathbf{N_n}$
→ množici vseh preslikav $\mathbf{N_n}$ označimo z $\mathbf{S_n}$
→ naj bo $\mathbf{e_i}$ stolpčni vektor velikosti n ki ima na i mestu **enko** drugje pa **nič**
→ vsaki permutaciji iz $\mathbf{S_n}$ lahko priredimo matriko

$$P_\sigma := \begin{bmatrix} \mathbf{e}_{\sigma(1)} & \mathbf{e}_{\sigma(2)} & \dots & \mathbf{e}_{\sigma(n)} \end{bmatrix}$$

→ determinanti te matrike pravimo **signatura** permutacije **sgn(σ)** := **det** $\mathbf{P_\sigma}$
→ signatura je vedno med **-1** in **1** in sgn(**σ** ∘ **τ**) = sgn(**σ**) sgn(**τ**)

Eksplicitno izražene determinante

$$\det A = \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\, a_{1,\pi(1)} a_{2,\pi(2)} \cdots a_{n,\pi(n)}$$

DOKAZ

$$P_\sigma^T P_\sigma = \begin{bmatrix} \mathbf{e}_{\sigma(1)}^T \\ \mathbf{e}_{\sigma(2)}^T \\ \vdots \\ \mathbf{e}_{\sigma(n)}^T \end{bmatrix} \begin{bmatrix} \mathbf{e}_{\sigma(1)} & \mathbf{e}_{\sigma(2)} & \dots & \mathbf{e}_{\sigma(n)} \end{bmatrix} = \begin{bmatrix} \langle \mathbf{e}_{\sigma(1)}, \mathbf{e}_{\sigma(1)} \rangle & \langle \mathbf{e}_{\sigma(1)}, \mathbf{e}_{\sigma(2)} \rangle & \dots & \langle \mathbf{e}_{\sigma(1)}, \mathbf{e}_{\sigma(n)} \rangle \\ \langle \mathbf{e}_{\sigma(2)}, \mathbf{e}_{\sigma(1)} \rangle & \langle \mathbf{e}_{\sigma(2)}, \mathbf{e}_{\sigma(2)} \rangle & \dots & \langle \mathbf{e}_{\sigma(2)}, \mathbf{e}_{\sigma(n)} \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle \mathbf{e}_{\sigma(n)}, \mathbf{e}_{\sigma(1)} \rangle & \langle \mathbf{e}_{\sigma(n)}, \mathbf{e}_{\sigma(2)} \rangle & \dots & \langle \mathbf{e}_{\sigma(n)}, \mathbf{e}_{\sigma(n)} \rangle \end{bmatrix} = I$$

$$(\det P_\sigma)^2 = \det P_\sigma^T \det P_\sigma = \det P_\sigma^T P_\sigma = \det I = 1$$

je dokaz **prve** trditve in dokaz **druge** trditve: $P_\sigma \mathbf{e}_i = \mathbf{e}_{\sigma(i)}$

$$\begin{aligned} P_\sigma P_\tau &= P_\sigma \begin{bmatrix} \mathbf{e}_{\tau(1)}, \mathbf{e}_{\tau(2)}, \dots, \mathbf{e}_{\tau(n)} \end{bmatrix} \\ &= \begin{bmatrix} P_\sigma \mathbf{e}_{\tau(1)}, P_\sigma \mathbf{e}_{\tau(2)}, \dots, P_\sigma \mathbf{e}_{\tau(n)} \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{e}_{\sigma(\tau(1))}, \mathbf{e}_{\sigma(\tau(2))}, \dots, \mathbf{e}_{\sigma(\tau(n))} \end{bmatrix} \\ &= P_{\sigma \circ \tau} \end{aligned}$$

determinanto uporabimo na obeh straneh in dobimo formulo

DOKAZ

Vsako vrstico izrazimo s spodnjo formulo. Upoštevamo linearnost determinante

$$\begin{bmatrix} a_{i,1} & a_{i,2} & \dots & a_{i,n} \end{bmatrix} = \sum_{j=1}^{n} a_{i,j} \mathbf{e}_j^T$$

$$\det A = \det \begin{bmatrix} \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \end{bmatrix} \\ \vdots \\ \begin{bmatrix} a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{bmatrix} \end{bmatrix} = \det \begin{bmatrix} \sum_{j_1=1}^{n} a_{i,j_1} \mathbf{e}_{j_1}^T \\ \vdots \\ \sum_{j_n=1}^{n} a_{i,j_n} \mathbf{e}_{j_n}^T \end{bmatrix} =$$

$$= \sum_{j_1=1}^{n} \dots \sum_{j_n=1}^{n} a_{i,j_1} \cdots a_{i,j_n} \det \begin{bmatrix} \mathbf{e}_{j_1}^T \\ \vdots \\ \mathbf{e}_{j_n}^T \end{bmatrix} = \sum_{(j_1, \dots, j_n) \in (\mathbb{N}_n)^n} a_{i,j_1} \cdots a_{i,j_n} \det \begin{bmatrix} \mathbf{e}_{j_1}^T \\ \vdots \\ \mathbf{e}_{j_n}^T \end{bmatrix}$$

Če sta dve izmed števil j_i enaki potem determinanta nič. Če pa so vsa različna potem je funkcija ki slika k v j_k injektivna in spada v množico permutacij

$$\begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} \in S_n$$

$$\det \begin{bmatrix} \mathbf{e}_{j_1}^T \\ \vdots \\ \mathbf{e}_{j_n}^T \end{bmatrix} = \det \begin{bmatrix} \mathbf{e}_{j_1} & & \mathbf{e}_{j_n} \end{bmatrix} = \operatorname{sgn} \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$$

$$\det A = \sum_{\begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} \in S_n} \operatorname{sgn} \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} a_{i,j_1} \cdots a_{i,j_n}$$

ALGEBRSKE STRUKTURE

O S N O V E :

- **I.** **operacija:** funkcija iz **M** × **M** → **M**
- **II.** **grupoid**: urejen par funkcije in množice M: (**M**, **·**)
- **III.** **polgrupa:** če je grupoid in je operacija **asociativna** za vsak element iz množice
- **IV.** **komutativna polgrupa:** polgrupa z **komutativno** operacijo za vsak element množice
- **V.** **monoid**: polgrupa z **enoto**
- **VI.** **grupa:** monoid kjer je vsak element **obrnljiv**
- **VII.** **Abelova grupa:** **komutativna** grupa

I. operacije pišemo kot abstraktno **množenje** oz. **kompozitum**

III. asociativnost: (**ab**) **c** = **a** (**bc**) členi so neodvisni od postavitve oklepajev

IV. komutativnost: **ab** = **ba**

VI. obrnljivost: če obstaja tak element b da velja **ab** = **ba** = **e** elementu rečemo **inverz** in označimo z a^{-1}

desni inverz: a**b** = **e**
levi inverz: **b**a = **e**

V. enota: za vsak element velja **xe** = **ex** = **x**

desna enota: **xe** = **x**
leva enota: **ex** = **x**

TRDITEV:
- vsak **grupoid** ima največ **eno enoto**
- v vsakem **monoidu** ima vsak element največ **en inverz**

DOKAZ
- Predpostavimo da imamo **dve enoti** in dobimo da sta enoti **enaki**. Torej je **vsaka leva** enaka **vsaki desni** in vsaka desna vsaki levi. Grupoid nima drugih levih ali desnih enot. Če **nima desne** enote ima lahko **več levih** in **več desnih** enot če **nima leve** tho.
- Isto rečemo da imamo **dva inverza** in vidimo da sta **enaka**. Analogno velja da vsak levi enak vsakemu desnemu torej ni levih in desnih inverzov. Again enako če **nima desnega** lahko **več levih** in obratno.

Podstrukture
→ množica **N** je **podmnožica** M
→ struktura je **podstruktura** če operacija **zaprta** na N
→ **podgrupoid:** operacija zaprta na N
→ **podpolgrupa:** če podgrupoid
→ **podmonoid**: če podpolgrupa in **vsebuje enoto**
→ monoid in podmonoid imata lahko različno enoto
→ **podgrupa**: podmonoid in vsebuje **vsak** svoj **inverz**

TRDITEV:
struktura je **podgrupa** natanko tedaj ko **H** podmnožica **G** in za poljubna elementa **a** in **b** iz **H** velja $\mathbf{ab^{-1}}$ **pripada H**

DOKAZ
Pokažimo da ustreza vsem trem trditvam ki so potrebne da je struktura podgrupa. Če **namesto b** vstavimo **a** dobimo da **enota** spada **v H**. Če **namesto a** vstavimo **enoto** vidimo da vsak **inverz b v H**. Dokažemo še da je operacija **notranja** tako da **namesto b** vstavimo $\mathbf{b^{-1}}$ dobimo **ab** pripada **H**.

Lastnosti končnih grup
→ **lagrangeov izrek**: moč podgrupe deli moč grupe
→ **red elementa:** najmanjša potenca da element nanjo enota
→ vsak element končne grupe ima končen red
→ končen **red deli moč** končne **grupe**
→ struktura je podgrupa grupe natanko tedaj ko operacija **zaprta**

če taka potenca ne obstaja je red neskončen

Dokaz za red pri **DS2**

DOKAZ LAGRANGEOVEGA IZREKA
H podgrupa končne grupe. Za vsak element g grupe G velja:

$$g \circ H := \{g \circ h \mid h \in H\} \qquad G = \bigcup_{g \in G} g \circ H$$

Za vsak g je moč množice gH enaka moči množice H. Če imata dve taki množici neprazen presek sta enaki. Preslikava gH je bijektivna. Surjektivna je iz definicije injektivna pa iz spodnjega zapisa. To je dokaz 1. trditve.

$$h_1 = g^{-1} \circ (g \circ h_1) = g^{-1} \circ (g \circ h_2) = h_2$$

Druga trditev pride iz tega da predpostavimo da imata neprazen presek dve taki množici in vidimo da sta enaki.

HOMOMORFIZMI $f\colon M_1 \to M_2$

$$f(x \circ_1 y) = f(x) \circ_2 f(y)$$

→ preslikave ki ohranjajo strukturo
→ **homomorfizem grupoidov** za vsaka x in y velja formula
→ **polgrupe:** iz polgrupe v polgrupo
→ **monoid:** iz monoida v monoid in enoto preslika v enoto
→ **grupe:** iz grupe v slika v grupo, inverze v inverze slik elementov in enoto v enoto

$$f(e_1) \circ_2 f(e_1) = f(e_1 \circ_1 e_1) = f(e_1) = e_2 \circ_2 f(e_1)$$

→ **kompozitum** homomorfizmov je homomorfizem

IZOMORFIZEM
→ bijektivni homomorfizem
→ dve strukturi sta izomorfni če obstaja homomorfizem iz ene v drugo
→ v bistvu samo **preimenovanje** elementov
→ ustrezno preimenujemo tudi **produkte**
→ **inverz** izomorfizma spet **izomorfizem**

CAYLEYEV IZREK:
Vsaka grupa je izomorfna kaki **podgrupi** v kaki grupi **permutacij**

DOKAZ
Dokaz: Naj bo $(G,*)$ grupa in naj bo $(\mathcal{P}(G),\circ)$ grupa vseh permutacij množice G. Ideja je, da konstruiramo injektiven homomorfizem grup ϕ iz $(G,*)$ v $(\mathcal{P}(G),\circ)$. Potem je $\phi(G)$ podgrupa v $(\mathcal{P}(G),\circ)$ in ϕ je bijektiven homomorfizem grup iz $(G,*)$ v $(\phi(G),\circ_{\phi(G)})$. Torej sta grupi $(G,*)$ in $(\phi(G),\circ_{\phi(G)})$ izomorfni.

Za vsak $g \in G$ lahko definiramo preslikavo $\phi_g\colon G \to G$, $\phi_g(x) = g * x$. Pokažimo, da je ϕ_g permutacija množice G. Če je $\phi_g(x) = \phi_g(y)$, potem je $x = g^{-1} * (g * x) = g^{-1} * (g * y) = y$, torej je ϕ_g injektivna. Iz $x = g * (g^{-1} * x) = \phi_g(g^{-1} * x)$ sledi, da je ϕ_g surjektivna.

Preslikavo $\phi\colon G \to \mathcal{P}(G)$ definirajmo z $\phi(g) := \phi_g$. Pokažimo najprej, da je ϕ injektivna. Iz $\phi_g = \phi_h$ sledi $g = \phi_g(e) = \phi_h(e) = h$. Pokažimo še, da je ϕ homomorfizem, se pravi, da je $\phi_{g*h} = \phi_g \circ \phi_h$ za vsaka $g, h \in G$. To sledi iz $\phi_{g*h}(x) = (g*h)*x = g*(h*x) = \phi_g(\phi_h(x)) = (\phi_g \circ \phi_h)(x)$.

TRDITEV:
če imamo homomorfizem monoidov in je element a **obrnljiv** v prvem monoidu potem je obrnljiv tudi v drugem monoidu. Velja: $\mathbf{f(a)^{-1} = f(a^{-1})}$

DOKAZ
Ker slika preslikava enoto v enoto in je element obrnljiv obstaja tak element da velja **a · b = b · a = e**
Po definiciji homomorfizma velja:

$$f(a) \circ_2 f(b) = f(a \circ_1 b) = f(e_1) = e_2$$

$$f(b) \circ_2 f(a) = f(b \circ_1 a) = f(e_1) = e_2$$

Bigrupoidi
→ množica z **dvema** operacijama **·** in **+**
→ če med operacijama ni veze obravnavamo vsakega posebej
→ povezava **distributivnosti**
→ **polkolobar:** distributiven digrupoid kjer seštevanje **komutativna polgrupa**
→ **kolobar:** polkolobar ampak seštevanje **Abelova grupa**

Lastnosti kolobarjev (**M**, **+**, **·**)
→ **asociativnost:** če (**M**, **·**) asociativen grupoid
→ **komutativnost:** če (**M**, **·**) komutativen grupoid
→ **kolobar z enoto:** če ima grupoid (**M**, **·**) enoto

Podkolobarji
→ **N** podmnožica **M**
→ (**N**, **+**) podgrupa (**M**, **+**)
→ (**N**, **·**) podgrupoid (**M**, **·**)
→ oziroma če za vsaka x in y iz N velja **x – y** in **x · y** pripada N
→ podkolobar v kolobar tako da dodamo skrčitve operaciji
→ isto **podpolkolobar** in **podbigrupoid** samo zahtevamo samo zaprtost

HOMOMORFIZMI KOLOBARJEV

- → taka preslikava da ustreza:
  $f(x +_1 y) = f(x) +_2 f(y)$ $f(x \cdot_1 y) = f(x) \cdot_2 f(y)$
- → bijektivni homomorfizem je **izomorfizem**
- → pri **kolobarjih z enoto** multiplikativna **enota v** multiplikativno **enoto**
- → **kompozitum** dveh homomorfizmov oz. izomorfizmov je spet homomorfizem oz. izomorfizem
- → **inverz** izomorfizma je **izomorfizem**

Kolobarji v Z_n in F[x]/(p)

oba sta bolj opisana spodaj pod primeri

Kolobar Z_n

- → množica od **0** do **n – 1**
- → operaciji seštevanja in množenja sta po **modulu**
- → **mod n** je ostanek pri seštevanju oz množenju z n
- → **komutativen** in **asociativen** kolobar z enoto
- → aditivna enota: **0**
- → multiplikativna enota: **1**
- → aditivni inverz: **n – x**
- → **obseg:** kadar n praštevilo
- → preslikava iz Z v Z_n je **homomorfizem**

ni **obseg** zato ker bi če ne obstajala taka elementa da **x y = 0** oz. taka polinoma da **p q = 0**

konstantni in **linearni** polinomi so nerazcepni

Kolobarji F[x]/(p)

- → množica **polinomov** z spremenljivko **x** in koeficienti iz F
- → **F**[**x**] **komutativen** in **asociativen** kolobar z enoto
- → **F**[**x**]/(**p**) je množica vseh polinomov iz **F**[**x**] nižje stopnje od p
- → množenje definiramo kot **ostanek pri deljenju** polinoma s polinomom p
- → preslikava iz prvega v drugega je **homomorfizem**
- → polinom je **razcepen** če obstajata polinoma **k** in **q** da velja **p** = **k q**
- → polinom ki ni razcepen je **nerazcepen**
- → **obseg:** kadar polinom p nerazcepen

Polja z P^n elementi

- → vzamemo praštevilo p in naravno število n
- → dokažemo da v $\mathbf{Z_p}$[**x**] obstaja nerazcepen polinom **q**(**x**) stopnje n
- → potem je $\mathbf{Z_p}$[**x**] / **q**(**x**) polje z $\mathbf{p^n}$ elementi
- → vsako **končno polje** je **izomorfno** enemu od zgornjih polj
- → dve končni polji z **enakim številom** elementov sta izomorfni

Obsegi in polja

- → v obsegih lahko elemente tudi delimo
- → množica neničelnih elementov je **grupa** za množenje
- → **polje:** komutativen obseg
- → drugačna definicija: **asociativen** kolobar z **enoto** kjer je vsak neničelen element **obrnljiv**
- → **podobseg:** taka podmnožica ki je zaprta za odštevanje in deljenje
- → **podpolje:** komutativen podobseg
- → imamo **homomorfizem** polj in obsegov ki slika iz obsega v obseg
- → bijektivni homomorfizem je **izomorfizem**
- → **inverz** izomorfizma je **izomorfizem**
- → če je **f** : **K** → **L** homomorfizem potem je **f** (**K**) **podobseg** v **L** in če je homomofrizem bijektiven je to izomorfizem torej je **K podobseg** v **L**

TRDITEV:
vsak homomorfizem obsegov je **injektiven**

DOKAZ

Dokaz: Recimo, da je $f: K \to L$ homomorfizem obsegov in da je $f(a_1) = f(a_2)$ za neka $a_1, a_2 \in K$. Radi bi pokazali, da je $a_1 = a_2$. Označimo $a := a_1 - a_2$. Potem je $f(a) = f(a_1) - f(a_2) = 0_L$.
Če $a_1 \neq a_2$, potem je $a \neq 0$, torej obstaja tak b iz K, da je $ab = 1_K$
Odtod sledi, da je $0_L = 0_L f(b) = f(a)f(b) = f(ab) = f(1_K) = 1_L$, kar je protislovje. Torej je res $a_1 = a_2$.

Linearna diofantska enačba

če sta števili **a** in **b tuji** potem obstajata števili **x** in **y** da velja
ax + **by** = **1**

DOKAZ

Brez škode lahko predpostavimo da sta števili naravni. Po izreku o deljenju z ostankom obstajajo taka naravna števila k da velja:

$$a_1 = k_1 a_2 + a_3 \quad \text{kjer } a_3 < a_2$$
$$a_2 = k_2 a_3 + a_4 \quad \text{kjer } a_4 < a_3$$
$$\vdots$$
$$a_{n-1} = k_{n-1} a_n + a_{n+1} \quad \text{kjer } a_{n+1} < a_n$$
$$a_n = k_n a_{n+1}$$

Ker se ostanek manjša je ostankov **končno** mnogo. Ker sta števili tuji velja da je $\mathbf{a_{n+1}}$ enak **1**. Dokažemo da za vsak **m** od **1** do **n** obstaja:

$$a_1 x_m + a_2 y_m = a_{m+1}$$

Za m je 1 lahko vzamemo x je **0** in y je **1**. Z indukcijo pridemo do:

$$x_m = x_{m-2} - k_{m-1} x_{m-1} \qquad y_m = y_{m-2} - k_{m-1} y_{m-1}$$

Dobimo: $a_1 x_n + a_2 y_n = a_{n+1} = 1$
Iz tega dobimo dokaz za kdaj je obseg polje za prejšnja kolobarja.

VEKTORSKI PROSTORI

- → **vektorski prostor** je podan nad **poljem**
- → podan je z tremi podatki
- → elementom množice V pravimo **vektorji**
- → elementom množice F pravimo **skalarji**
- → operacija seštevanja je **vsota vektorjev**
- → množenje je **produkt vektorja z skalarjem**
- → produkt ima večjo prednost kot vsota
- → če je F samo kolobar potem **modul**

lahko definiramo tudi kot **Abelovo grupo** (**V**, **+**) skupaj z **homomorfizmom kolobarjev** z enoto iz **F** v **End**(**V**, **+**) oz. **kolobar endomorfizmov** Abelove grupe (**V**, **+**)

- neprazna **množica V**
- taka operacija **+** nad **V** da je (**V**, **+**) **Abelova grupa**
- preslikavo **·** : **V** × **F** → **V**

$\alpha \cdot (u + v) = (\alpha \cdot u) + (\alpha \cdot v)$ za vse $\alpha \in F$ in $u, v \in V$
$(\alpha \oplus \beta) \cdot v = (\alpha \cdot v) + (\beta \cdot v)$ za vse $\alpha, \beta \in F$ in $v \in V$
$(\alpha \odot \beta) \cdot v = \alpha \cdot (\beta \cdot v)$ za vse $\alpha, \beta \in F$ in $v \in V$
$1 \cdot v = v$ za vse $v \in V$

Vektorski podprostori

- → **V** je vektorski prostor nad **F**
- → **U** je neprazna **podmnožica V**
- → natanko ko za dva elementa **x** in **y** iz **U** in skalarja **α** in **ß** iz **F** velja da **α x** + **ß y** pripada **U** je to vektorski **podprostor**
- → vsak vektorski podprostor je **prostor**
- → če **W** podprostor **U** je tudi podprostor **V**

enakovreden pogoj če velja da **α x** pripada U in **x** + **y** pripada U

TRDITEV:
vsak vektorski podprostor vsebuje **ničelni vektor**

DOKAZ

Enota Abelove grupe V naj bo **0**. vzamemo poljuben element iz U **u**. Po definiciji velja:

Iz $0_V + 0u = 0u = (0+0)u = 0u + 0u$ sledi $0_V = 0u \in U$.

TRDITEV:
Naj bodo $\mathbf{U_1}$ do $\mathbf{U_k}$ podprostori **V** potem je tudi njihov **presek** in **vsota** vektorski **podprostor**

vsota je množica **vseh možnih vsot** vseh vektorjev tako da vsak vektor iz **enega** podprostora

DOKAZ ZA PRESEK

Dokaz za presek: Vzemimo $w, z \in U_1 \cap \ldots \cap U_k$ in $\alpha, \beta \in F$. Radi bi dokazali, da $\alpha w + \beta z \in U_1 \cap \ldots \cap U_k$. Za vsak $i = 1, \ldots, k$ je U_i tak podprostor v V, ki vsebuje tako w kot z, torej vsebuje tudi $\alpha w + \beta z$. Ker $\alpha w + \beta z$ leži v vseh U_i, leži tudi v preseku.

DOKAZ ZA VSOTO

Dokaz za vsoto: Vzemimo $w, z \in U_1 + \ldots + U_k$ in $\alpha, \beta \in F$. Radi bi dokazali, da $\alpha w + \beta z \in U_1 + \ldots + U_k$. Po definiciji vsote podprostorov lahko w in z izrazimo kot $w = w_1 + \ldots + w_k$ in $z = z_1 + \ldots + z_k$, kjer $w_i, z_i \in U_i$ za vsak $i = 1, \ldots, k$. Ker so vsi U_i podprostori v V velja $\alpha w_i + \beta z_i \in U_i$ za vsak $i = 1, \ldots, k$. Odtod sledi

$$\alpha w + \beta z = (\alpha w_1 + \beta z_1) + \ldots + (\alpha w_k + \beta z_k) \in U_1 + \ldots + U_k$$

Baze

→ V naj bo **vektorski prostor**
→ vektorji od $\mathbf{v_1}$ do $\mathbf{v_n}$ so ogrodje če se da vsak vektor iz **V** na **vsaj en** način izraziti kot **linearna kombinacija** v_1 ,.., v_n
→ vektorji od $\mathbf{v_1}$ do $\mathbf{v_n}$ so **linearno neodvisni** če se da vsak vektor iz V izraziti na **največ en** način
→ vektorji so **baza** če se jih da izraziti na **natanko en** način torej so **linearno neodvisni** in so **ogrodje**
→ vektorji $\mathbf{v_1}$ do $\mathbf{v_n}$ so ogrodje natanko tedaj ko njihova **linearna ogrinjača** enaka **V**

Obstoj baze

→ vektorski prostor je končno razsežen če ima **ogrodje**
→ če ima ogrodje z **n** elementi nima pa ogrodja z **n – 1** elementi je **n razsežen**
→ vsak končno razsežen vektorski prostor ima **bazo**
→ če je vektorski prostor n razsežen ima baza **n elementov**
→ vsako ogrodje ima **podmnožico** ki je **baza**
→ prostor je n razsežen natanko tedaj ko ima baza n elementov

TRDITEV:
Podmnožica S vektorskega prostora je **baza** natanko tedaj ko je **ogrodje** in ko **nobena** prava **podmnožica** v **S ni ogrodje**

DOKAZ

Dokaz: Če je S ogrodje in če nobena prava podmnožica v S ni ogrodje, potem za vsak $v \in S$ velja $v \notin \mathrm{Lin}(S \setminus \{v\})$ (sicer bi iz $v \in \mathrm{Lin}(S \setminus \{v\})$ in $S \setminus \{v\} \subseteq \mathrm{Lin}(S \setminus \{v\})$ sledilo $S \subseteq \mathrm{Lin}(S \setminus \{v\})$, odtod pa bi sledilo $\mathrm{Lin}\, S \subseteq \mathrm{Lin}(S \setminus \{v\})$, torej bi bila prava podmnožica $S \setminus \{v\}$ ogrodje.) Odtod po karakterizaciji linearno neodvisnih množic sledi, da je S linearno neodvisna. Torej je S baza. Dokaz v obratno smer je podoben.

trivialni vektorski prostor je { 0 } in je **0 razsežen**. Njegova baza je **prazna** množica. **Lin**{ } = { **0** }

METODA ZA ISKANJE:

→ iščemo bazo nad **podmnožico** F^n
→ vzamemo matriko [$\mathbf{v_1} \ldots \mathbf{v_n}$]
→ z **Gaussovo metodo** v reducirano vrstično stopničasto formo R
→ če ima R ničelno vrstico potem ni ogrodje
→ če nima ničelne vrstice potem **pivotni stolpci** indeksi stolpcev v originalni matriki ki sestavljajo **bazo**

POSLEDICA: če je V **n razsežen** prostor velja:
→ če so vektorji u linearno **neodvisni** je **m ≤ n**
→ če so vektorji u **ogrodje** potem **m ≥ n**
→ če so vektorji u **baza** potem **m = n**

DOKAZ

Dokaz: Recimo, da so vektorji $v_1, \ldots, v_m$ linearno neodvisni, in da vektor v_{m+1} ne leži v njihovi linearni ogrinjači. Vzemimo take $\alpha_1, \ldots, \alpha_m, \alpha_{m+1}$, da velja $\alpha_1 v_1 + \ldots + \alpha_m v_m + \alpha_{m+1} v_{m+1} = 0$. Radi bi dokazali, da velja $\alpha_1 = \ldots, \alpha_m = \alpha_{m+1} = 0$. Ločimo dva primera.

Če je $\alpha_{m+1} \neq 0$, potem velja $v_{m+1} = \frac{-1}{\alpha_{m+1}}(\alpha_1 v_1 + \ldots + \alpha_m v_m)$, kar je v nasprotju s predpostavko, da v_{m+1} ne leži v linearni ogrinjači $v_1, \ldots, v_m$.

Če je $\alpha_{m+1} = 0$, potem velja $\alpha_1 v_1 + \ldots + \alpha_m v_m = 0$. Ker so vektorji $v_1, \ldots, v_m$ linearno neodvisni, je $\alpha_1 = \ldots, \alpha_m = 0$.

Linearna ogrinjača

→ **V** je vektorski prostor nad **F**
→ $\mathbf{v_1}$ do $\mathbf{v_k}$ so vektorji iz **V**
→ vektor v je linearna kombinacija teh vektorjev če obstajajo taki **skalarji** iz **F** da velja:

$$v = \alpha_1 v_1 + \ldots + \alpha_k v_k$$

→ **množico vseh** linearnih kombinacij označimo **Lin** {$\mathbf{v_1}$,…, $\mathbf{v_k}$ }

TRDITEV:
Za vsako **končno podmnožico S** v vektorskem prostoru **V** je njena linearna ogrinjača **Lin** { **S** } vektorski **podprostor** v **V**

DOKAZ

Dokaz: Če $u_1, u_2 \in \mathrm{Lin}\{v_1, \ldots, v_k\}$ in $\gamma_1, \gamma_2 \in F$, potem bi radi dokazali, da $\gamma_1 u_1 + \gamma_2 u_2 \in \mathrm{Lin}\{v_1, \ldots, v_k\}$. Izberimo take skalarje $\alpha_1, \ldots, \alpha_n$ in $\beta_1, \ldots, \beta_n$, da je $u_1 = \alpha_1 v_1 + \ldots + \alpha_k v_k$ in $u_2 = \beta_1 v_1 + \ldots + \beta_k v_k$. Sledi $\gamma_1 u_1 + \gamma_2 u_2 = (\gamma_1 \alpha_1 + \gamma_2 \beta_1) v_1 + \ldots + (\gamma_1 \alpha_k + \gamma_2 \beta_k) v_k \in \mathrm{Lin}\{v_1, \ldots, v_k\}$.

Karakterizacije linearne neodvisnosti

V naj bo **vektorski prostor** in vektorji od $\mathbf{v_1}$ do $\mathbf{v_n}$ iz V
1. vektorji so **linearno neodvisni**
2. za vse velja za skalarje:

$$\alpha_1 v_1 + \ldots + \alpha_n v_n = 0 \qquad \alpha_1 = \ldots = \alpha_n = 0$$

3. nobeden od vektorjev se **ne da** izraziti kot **linearna kombinacija** preostalih

DOKAZ

dokaz iz 1 v 2: recimo da so vektorji linearno neodvisni. Potem se da vektor **0** na **največ en** način izraziti kot njihova linearna kombinacija. Ena izmed teh je da so **vsi skalarji 0**. Ker so linearno neodvisni je to **edina**.

dokaz iz 2 v 1: recimo da velja formula $\boldsymbol{\alpha_1} \mathbf{v_1} + \ldots + \boldsymbol{\alpha_n} \mathbf{v_n} = \mathbf{0}$ potem sledi da so skalarji 0. Vzamemo vektor v ki se da na **dva** načina izraziti kot linearna kombinacija zgornjih vektorjev. Prvi način je

$\mathbf{v} = \boldsymbol{\beta_1} \mathbf{v_1} + \ldots + \boldsymbol{\beta_n} \mathbf{v_n}$ in drugi način: $\mathbf{v} = \boldsymbol{\gamma_1} \mathbf{v_1} + \ldots + \boldsymbol{\gamma_n} \mathbf{v_n}$
Ko oba načina odštejemo dobimo:

$$0 = v - v = (\beta_1 - \gamma_1) v_1 + \ldots + (\beta_n - \gamma_n) v_n$$

Po predpostavki sledi da je $\boldsymbol{\beta_i} - \boldsymbol{\gamma_i} = \mathbf{0}$ torej sta skalarja **enaka**. Obstaja torej **največ en** način da izrazimo vektor v torej so vektorji **linearno neodvisni**.

dokaz iz 2 v 3: recimo da velja 2 in ne velja 3. Potem lahko nek vektor izrazimo kot linearna kombinacija ostalih.

$$v_i = \alpha_1 v_1 + \ldots + \alpha_{i-1} v_{i-1} + \alpha_{i+1} v_{i+1} + \ldots + \alpha_n v_n$$

$$\alpha_1 v_1 + \ldots + \alpha_{i-1} v_{i-1} + (-1) v_i + \alpha_{i+1} v_{i+1} + \ldots + \alpha_n v_n = 0$$

Ampak potem vidimo da je to **protislovje**

dokaz iz 3 v 2: recimo da velja 3 ampak ne velja 2. Potem obstajajo **neničelni skalarji** da linearna kombinacija **0**. Potem lahko pri neničlnem skalarju izrazimo vektor z preostalimi kar pa je **protislovje**.

TRDITEV:
Če so $\mathbf{u_1}$ do $\mathbf{u_m}$ **linearno neodvisni** vektorji v V in so vektorji od $\mathbf{v_1}$ do $\mathbf{v_n}$ ogrodje za V potem je **m manjši** ali enak **n**

DOKAZ

Vsak u vektor **razvijemo** po vektorjih v

$$u_1 = \alpha_{1,1} v_1 + \ldots + \alpha_{1,n} v_n$$
$$\vdots$$
$$u_m = \alpha_{m,1} v_1 + \ldots + \alpha_{m,n} v_n$$

Pa recimo da je **m večji** od **n**. Ker ima vsak **poddoločen homogen sistem netrivialno** rešitev obstajajo taki ne vsi ničelni skalarji x da velja:

$$\alpha_{1,1} x_1 + \ldots + \alpha_{m,1} x_m = 0$$
$$\vdots$$
$$\alpha_{1,n} x_1 + \ldots + \alpha_{m,n} x_m = 0$$

$$\sum_{i=1}^{m} x_i u_i = \sum_{i=1}^{m} x_i(\alpha_{i,1} v_1 + \ldots + \alpha_{i,n} v_n)$$
$$= (\sum_{i=1}^{m} \alpha_{i,1} x_i) v_1 + \ldots + (\sum_{i=1}^{m} \alpha_{i,n} x_i) v_n$$
$$= 0 v_1 + \ldots + 0 v_n = 0$$

Ker so vektorji u linearno neodvisni sledi da so x ničelni kar pa je v **protislovju**.

Dopolnitev linearno neodvisne množice do baze

→ vzamemo linearno neodvisne vektorje $\mathbf{v_1}$ do $\mathbf{v_n}$
→ če vektor $\mathbf{v_{n+1}}$ ne leži v linearni ogrinjači potem so tudi vektorji od $\mathbf{v_1}$ do $\mathbf{v_{n+1}}$ linearno neodvisni

TRDITEV:
V **n razsežnostnem** prostoru je vsaka **linearno neodvisna** množica z **n elementi baza**

DOKAZ

Če so vektorji $\mathbf{v_1}$ do $\mathbf{v_n}$ linearno neodvisni **niso** pa **baza**, potem **niso ogrodje**. Torej obstaja tak vektor $\mathbf{v_{n+1}}$ da ne leži v linearni ogrinjači. Potem so vektorji s tem vektorjem še vedno linearno neodvisni. Ampak n razsežnostni prostor ima ogrodje z n elementi. Linearno **neodvisna** množica mora imeti **manj** elementov kot **ogrodje** kar je **protislovje**.

BAZE REVIEW & RAZSEŽNOSTI REVIEW

Za vsako podmnožico S v n-razsežnem prostoru V so ekvivalentne trditve:

- S je baza.
- S je linearno neodvisna in je ogrodje.
- S je linearno neodvisna in ima n elementov.
- S je ogrodje in ima n elementov.
- S je linearno neodvisna in nima nobene prave linearno neodvisne nadmnožice.
- S je ogrodje in nima nobene prave podmnožice, ki bi bila ogrodje.

Za vsak vektorski prostor V so ekvivalentne naslednje trditve:

- V je n-razsežen.
- V ima ogrodje z n elementi, nima pa ogrodja z $n-1$ elementi.
- V ima bazo z n elementi.
- V ima linearno neodvisno množico z n elementi, nima pa linearno neodvisne množice z $n+1$ elementi.

Razsežnosti podprostora

→ V **končno razsežni** prostor
→ razsežnost označimo z **dim V**
→ če ni končno razsežnost potem dimenzija **neskončna**

→ **minimum** moči **ogrodij** za V
→ **moč** katerekoli **baze** za V
→ **maksimum** moči linearno **neodvisnih** množic v V

TRDITEV:
U vektorski **podprostor V** potem je **dim U** manjša od **dim V**

DOKAZ

Dokaz: Naj bo $n = \dim V$. Če $\dim U = +\infty$ ali če $\dim U > n$, potem U nima ogrodja z $\leq n$ elementi. Torej obstajajo taki $u_1, u_2, \ldots, u_{n+1} \in U$ da $u_1 \notin \mathrm{Lin}\{\}$, $u_2 \notin \mathrm{Lin}\{u_1\}$, $u_3 \notin \mathrm{Lin}\{u_1, u_2\}$, $\ldots, u_{n+1} \notin \mathrm{Lin}\{u_1, \ldots, u_n\}$. Po Trditvi 3 od zadnjič odtod sledi, da so vektorji $u_1, u_2, \ldots, u_{n+1}$ linearno neodvisni v U (in zato tudi linearno neodvisni v V). Toda vsaka linearno neodvisna množica v V ima največ n elementov. To je protislovje.

$$U_1 + \ldots + U_n := \{u_1 + \ldots + u_n \mid u_1 \in U_1, \ldots, u_n \in U_n\}$$

VSOTA VEKTORSKIH PROSTOROV

→ dobimo vektorski **prostor**

1. **interna direktna** vsota
2. **eksterna direktna** vsota

če za vse vektorje $\mathbf{w_1}$ in $\mathbf{v_1}$ iz $\mathbf{U_1}$ in $\mathbf{w_n}$ in $\mathbf{v_n}$ iz $\mathbf{U_n}$ ki ustrezajo:

$$v_1 + \ldots + v_n = w_1 + \ldots + w_n$$

velja $\mathbf{v_1} = \mathbf{w_1}$ in $\mathbf{v_n} = \mathbf{w_n}$

množica vseh n teric $\mathbf{u_1}$ do $\mathbf{u_n}$ kjer $\mathbf{u_i}$ pripada $\mathbf{U_i}$ uporabimo znak $\oplus$

→ vsota $\mathbf{U_1} + \ldots + \mathbf{U_n}$ je **direktna**
→ če $\mathbf{u_1} + \ldots + \mathbf{u_n} = \mathbf{0}$ v prostoru V so vsi **ničelni**
→ če so vsi $\mathbf{u_{i,1}}$ do $\mathbf{u_{i,mi}}$ baza v $\mathbf{U_i}$ potem so vsi skupaj **baza** za vsoto prostorov

$$\dim(U_1 + \ldots + U_n) = \dim U_1 + \ldots + \dim U_n$$

$$(U_1 + \ldots + U_i) \cap U_{i+1} = \{0\}$$

→ zgornja formula velja za vse i od **1** do **n – 1**

velja za 3 podprostore tudi podobna formula:

$$\dim(U_1 + U_2 + U_3) = \dim U_1 + \dim U_2 + \dim U_3 - \dim(U_1 \cap U_2) - \dim(U_1 \cap U_3) - \dim(U_2 \cap U_3) + \dim(U_1 \cap U_2 \cap U_3)$$

TRDITEV:
če imamo dva **podprostora** velja naslednja formula

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$$

DOKAZ

Dokaz: Naj bo $f_1, \ldots, f_k$ baza za podprostor $U_1 \cap U_2$. Naj bo $g_1, \ldots, g_l$ njena dopolnitev do baze za U_1 in naj bo $h_1, \ldots, h_m$ njena dopolnitev do baze za U_2. Dokazali bomo, da je $f_1, \ldots, f_k, g_1, \ldots, g_l, h_1, \ldots, h_m$ baza za $U_1 + U_2$. Potem je $\dim(U_1 + U_2) = k + l + m$, $\dim(U_1 \cap U_2) = k$, $\dim U_1 = k + l$ in $\dim U_2 = k + m$. Torej formula v trditvi drži.

Pokažimo najprej, da so $f_1, \ldots, f_k, g_1, \ldots, g_l, h_1, \ldots, h_m$ ogrodje za $U_1 + U_2$. Po definiciji vsote dveh podprostorov lahko vsak vektor $u \in U_1 + U_2$ izrazimo kot $u = u_1 + u_2$, kjer $u_1 \in U_1$ in $u_2 \in U_2$. Ker je $f_1, \ldots, f_k, g_1, \ldots, g_l$ baza za U_1, lahko izrazimo u_1 kot linearno kombinacijo $f_1, \ldots, f_k, g_1, \ldots, g_l$. Ker je $f_1, \ldots, f_k, h_1, \ldots, h_m$ baza za U_2, lahko izrazimo u_2 kot linearno kombinacijo $f_1, \ldots, f_k, h_1, \ldots, h_m$. Torej lahko u izrazimo kot linearno kombinacijo $f_1, \ldots, f_k, g_1, \ldots, g_l, h_1, \ldots, h_m$

Pokažimo še, da so $f_1, \ldots, f_k, g_1, \ldots, g_l, h_1, \ldots, h_m$ linearno neodvisni. Če $\alpha_1 f_1 + \ldots + \alpha_k f_k + \beta_1 g_1 + \ldots + \beta_l g_l + \gamma_1 h_1 + \ldots + \gamma_m h_m = 0$, potem $\alpha_1 f_1 + \ldots + \alpha_k f_k + \beta_1 g_1 + \ldots + \beta_l g_l = (-\gamma_1) h_1 + \ldots + (-\gamma_m) h_m$ leži v $U_1 \cap U_2$ (ker leva stran leži v U_1, desna pa v U_2.) Torej obstajajo taki skalarji $\delta_1, \ldots, \delta_k$, da je $(-\gamma_1) h_1 + \ldots + (-\gamma_m) h_m = \delta_1 f_1 + \ldots + \delta_k f_k$. Ker je $f_1, \ldots, f_k, h_1, \ldots, h_m$ baza za U_2, odtod sledi $\gamma_1 = \ldots = \gamma_m = 0$ (in $\delta_1 = \ldots = \delta_k = 0$). Sledi $\alpha_1 f_1 + \ldots + \alpha_k f_k + \beta_1 g_1 + \ldots + \beta_l g_l = 0$. Ker je $f_1, \ldots, f_k, g_1, \ldots, g_l$ baza za U_1, odtod sledi $\alpha_1 = \ldots = \alpha_k = 0$ in $\beta_1 = \ldots = \beta_l = 0$. Dokaz linearne neodvisnosti je s tem končan.

POSLEDICA: enačaj velja natanko tedaj ko **presek** podprostorov **0**

DOKAZ

dokaz iz 1 v 2: recimo da **velja prva** trditev potem vzamemo tak $\mathbf{u_i}$ iz $\mathbf{U_i}$ da velja $\mathbf{u_1} + \ldots + \mathbf{u_n} = \mathbf{0}$ ker v U spada tudi **ničelni vektor** in velja $\mathbf{0} + \ldots + \mathbf{0} = \mathbf{0}$ torej res velja tudi druga trditev.

dokaz iz 2 v 1: recimo da **velja druga** trditev. Potem vzamemo take da velja $\mathbf{w_i}$ in $\mathbf{v_i}$ iz $\mathbf{U_i}$ da velja $\mathbf{w_1} + \ldots + \mathbf{w_n} = \mathbf{v_1} + \ldots + \mathbf{v_n}$ iz tega pa dobimo da $(\mathbf{w_1} - \mathbf{v_1}) + \ldots + (\mathbf{w_n} - \mathbf{v_n}) = \mathbf{0}$ Torej res drži prva trditev.

dokaz iz 2 v 3: recimo da **velja 2** in vektorji od **i,1** do **i,mi** so **baza** $\mathbf{U_i}$. Vsak vektor iz vsote izrazimo z $\mathbf{u_1} + \ldots + \mathbf{u_n}$ vsakega izmed teh pa lahko izrazimo z prej omenjeno bazo. Ti vektorji so potem ziher **ogrodje**. Dokažemo še da so linearno **neodvisni**. Ker so baze podprostorov i linearno neodvisne in velja trditev 2 sledi da so res linearno neodvisni.

dokaz iz 3 v 4: upoštevamo da **razsežnost enaka moči** baze

dokaz iz 4 v 5: če n krat uporabimo posledico **dimenzijske formule** dobimo

$$\dim(U_1 + \ldots + U_n) \leq \dim(U_1 + \ldots + U_{n-1}) + \dim U_n \leq \leq (\dim(U_1 + \ldots + U_{n-2}) + \dim U_{n-1}) + \dim U_n \leq \ldots \ldots \leq \dim U_1 + \ldots + \dim U_n$$

kjer pa je **enačaj** ker velja trditev 4. Torej mora biti **presek prazen**

dokaz iz 5 v 2: recimo da velja 5. Vzamemo tak $\mathbf{u_i}$ iz $\mathbf{U_i}$ da velja $\mathbf{u_1} + \ldots + \mathbf{u_n} = \mathbf{0}$ od kjer sledi da $\mathbf{u_1} + \ldots + \mathbf{u_{n-1}} = -\mathbf{u_n}$ pripada preseku iz formule 5 ki pa je po predpostavki enak 0.
Torej je $\mathbf{u_1} + \ldots + \mathbf{u_{n-1}} = \mathbf{0}$ in $\mathbf{u_n} = \mathbf{0}$ nadaljujemo naprej in dobimo da so res vsi vektorji ničelni torej velja trditev 2.

$$[v]_{\mathcal{B}} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} \qquad [v]_{\mathcal{C}} = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{bmatrix}$$

Prehod na novo bazo

→ **B** vektorji $\mathbf{u_i}$ so stara baza
→ **C** vektorji $\mathbf{w_i}$ so nova baza
→ n razsežnostni prostor

$$v = \beta_1 u_1 + \ldots + \beta_n u_n$$

$$v = \gamma_1 w_1 + \ldots + \gamma_n w_n$$

→ skonstruiramo tako **prehodno matriko** da velja

$$[v]_{\mathcal{C}} = P_{\mathcal{C} \leftarrow \mathcal{B}} [v]_{\mathcal{B}}$$

→ vsak element iz **stare** baze lahko **razvijemo** po **novi** bazi
→ **skalarje** iz i razvoja zložimo v **stolpec i** in ne v vrstico i!

$$u_1 = \alpha_{1,1} w_1 + \ldots + \alpha_{1,n} w_n$$
$$\vdots$$
$$u_n = \alpha_{n,1} w_1 + \ldots + \alpha_{n,n} w_n$$

$$P_{\mathcal{C} \leftarrow \mathcal{B}} = \begin{bmatrix} \alpha_{1,1} & \ldots & \alpha_{n,1} \\ \vdots & & \vdots \\ \alpha_{1,n} & \ldots & \alpha_{n,n} \end{bmatrix}$$

$$P_{\mathcal{C} \leftarrow \mathcal{B}} = \begin{bmatrix} [u_1]_{\mathcal{C}} & \ldots & [u_n]_{\mathcal{C}} \end{bmatrix}$$

PREHODNE MATRIKE:

→ za vsak vektor velja formula $[v]_{\mathcal{C}} = P_{\mathcal{C} \leftarrow \mathcal{B}} [v]_{\mathcal{B}}$
→ če imamo **tri baze** velja: $P_{\mathcal{D} \leftarrow \mathcal{B}} = P_{\mathcal{D} \leftarrow \mathcal{C}} P_{\mathcal{C} \leftarrow \mathcal{B}}$
→ $(P_{\mathcal{C} \leftarrow \mathcal{B}})^{-1} = P_{\mathcal{B} \leftarrow \mathcal{C}}$ $\quad P_{\mathcal{C} \leftarrow \mathcal{B}} = \begin{bmatrix} w_1 & \ldots & w_n \end{bmatrix}^{-1} \begin{bmatrix} u_1 & \ldots & u_n \end{bmatrix}$
→ za vektorski prostor $\mathbf{F^n}$ velja zgornja formula

LINEARNE PRESLIKAVE

- → vzamemo da **U** in **V** vektorska prostora nad istim poljem **F**
- → preslikave med vektorskimi prostori ki **ohranjajo strukturo** torej ohranjajo **vsoto** in **produkt** z skalarjem
- → to so **homomorfizmi** vektorskih prostorov
- → preslikava L : U → V je **aditivna** če velja: $L(u_1 + u_2) = L(u_1) + L(u_2)$
- → preslikava L : U → V je **homogena** če velja: $L(\alpha u) = \alpha L(u)$
- → preslikava L : U → V je **linearna** če je aditivna in homogena

Aditivna preslikava je **homomorfizem Abelovih grup** (**U**, **+**) v (**V**, **+**)

Namesto **L**(**u**) pišemo kar **Lu**

DOKAZ

$$\begin{aligned} P_{\mathcal{D}\leftarrow\mathcal{C}}P_{\mathcal{C}\leftarrow\mathcal{B}} &= P_{\mathcal{D}\leftarrow\mathcal{C}}\left[\, [u_1]_{\mathcal{C}} \;\; \ldots \;\; [u_n]_{\mathcal{C}} \,\right] \\ &= \left[\, P_{\mathcal{D}\leftarrow\mathcal{C}}[u_1]_{\mathcal{C}} \;\; \ldots \;\; P_{\mathcal{D}\leftarrow\mathcal{C}}[u_n]_{\mathcal{C}} \,\right] \\ &= \left[\, [u_1]_{\mathcal{D}} \;\; \ldots \;\; [u_n]_{\mathcal{D}} \,\right] \\ &= P_{\mathcal{D}\leftarrow\mathcal{B}} \end{aligned}$$

$$(P_{\mathcal{C}\leftarrow\mathcal{B}})^{-1} = P_{\mathcal{B}\leftarrow\mathcal{C}}$$

Dokaz: Če uporabimo Izrek 2 z $\mathcal{D} = \mathcal{B}$, dobimo $P_{\mathcal{B}\leftarrow\mathcal{C}}P_{\mathcal{C}\leftarrow\mathcal{B}} = P_{\mathcal{B}\leftarrow\mathcal{B}}$. Po definiciji prehodne matrike je $P_{\mathcal{B}\leftarrow\mathcal{B}}$ identična matrika. Odtod sledi, da je $P_{\mathcal{C}\leftarrow\mathcal{B}}$ obrnljiva matrika in da velja

Dokaz: Naj bo $\mathcal{S}$ standardna baza F^n. Potem je $[v]_{\mathcal{S}} = v$ za vsak $v \in F^n$. Iz formule (7) sledi $P_{\mathcal{S}\leftarrow\mathcal{B}} = \left[\, [u_1]_{\mathcal{S}} \;\; \ldots \;\; [u_n]_{\mathcal{S}} \,\right] = \left[\, u_1 \;\; \ldots \;\; u_n \,\right]$. Podobno dokažemo $P_{\mathcal{S}\leftarrow\mathcal{C}} = \left[\, w_1 \;\; \ldots \;\; w_n \,\right]$. Po izrekih 2 in 3 je

$$P_{\mathcal{C}\leftarrow\mathcal{B}} = P_{\mathcal{C}\leftarrow\mathcal{S}}P_{\mathcal{S}\leftarrow\mathcal{B}} = \left[\, w_1 \;\; \ldots \;\; w_n \,\right]^{-1}\left[\, u_1 \;\; \ldots \;\; u_n \,\right]$$

TRDITEV:
Preslikava je **linearna** natanko tedaj ko velja

$$L(\alpha_1 u_1 + \alpha_2 u_2) = \alpha_1 L u_1 + \alpha_2 L u_2$$

DOKAZ

Če je L **aditivna** potem velja

$$L(\alpha_1 u_1 + \alpha_2 u_2) = L(\alpha_1 u_1) + L(\alpha_2 u_2)$$

Če je L **homogena** potem velja

$$L(\alpha_1 u_1) = \alpha_1 L u_1 \qquad L(\alpha_2 u_2) = \alpha_2 L u_2$$

Dokažemo še da preslikava res linearna.

$$L(u_1 + u_2) = L(1 \cdot u_1 + 1 \cdot u_2) = 1 \cdot Lu_1 + 1 \cdot Lu_2 = Lu_1 + Lu_2$$

$$L(\alpha u) = L(\alpha \cdot u + 0 \cdot u) = \alpha \cdot Lu + 0 \cdot Lu = \alpha Lu$$

Posplošitve linearnih preslikav $L(\alpha u) = \phi(\alpha)L(u)$

- → **U** vektorski prostor nad **F** in **V** vektorski prostor nad **K**
- → preslikava **φ** : **F** → **K** je **homomorfizem** polj
- → preslikava **L** : **U** → **V** je **φ** - **homogena** če velja formula zgoraj
- → preslikava **L** : **U** → **V** je **linearna** če je homogena in aditivna
- → bijektivna linearna preslikava je **linearni izomorfizem**

Opomba: Naj bosta U in V vektorska prostora nad poljem F in naj bo K podpolje v F. Preslikava $L\colon U \to V$ je K-**homogena**, če velja $L(\alpha u) = \alpha Lu$ za vsak $\alpha \in K$ in vsak $u \in U$. Preslikava $L\colon U \to V$ je K-**linearna**, če je aditivna in K-homogena.

TRDITEV: **inverzna** preslikava od linearnega **izomorfizma** je linearni izomorfizem

TRDITEV: Kompozitum dveh linearnih **izomorfizmov** je linearni **izomorfizem**

Če U in V **nista** vektorska prostora **nad isto** množico potem **ne moremo** definirati linearne preslikave lahko pa definiramo **posplošeno**

DOKAZ

Dokaz: Naj bosta U in V vektorska prostora nad poljem F in naj bo $L\colon U \to V$ bijektivna linearna preslikava. Radi bi pokazali, da je tudi njena inverzna preslikava $L^{-1}\colon V \to U$ linearna.

Za vsaka vektorja $v_1, v_2 \in V$ in vsaka skalarja $\alpha_1, \alpha_2 \in F$ velja

$$\begin{aligned} &L(\alpha_1 L^{-1}v_1 + \alpha_2 L^{-1}v_2) = L(\alpha_1 u_1 + \alpha_2 u_2) = \alpha_1 Lu_1 + \alpha_2 Lu_2 = \\ &= \alpha_1 L(L^{-1}v_1) + \alpha_2 L(L^{-1}v_2) = \alpha_1 v_1 + \alpha_2 v_2 = L(L^{-1}(\alpha_1 v_1 + \alpha_2 v_2)) \end{aligned}$$

kjer je $u_1 = L^{-1}v_1$ in $u_2 = L^{-1}v_2$. Ker je L injektivna preslikava, sledi

$$\alpha_1 L^{-1}v_1 + \alpha_2 L^{-1}v_2 = L^{-1}(\alpha_1 v_1 + \alpha_2 v_2)$$

Torej je L^{-1} res linearna preslikava.

katerakoli **enako razsežna** vektorska prostora nad istim poljem sta linearno izomorfna

DOKAZ

Pokažemo da je **kompozitum** dveh linearnih preslikav **linearna preslikava**.

$$\begin{aligned} &(K \circ L)(\alpha_1 u_1 + \alpha_2 u_2) = K(L(\alpha_1 u_1 + \alpha_2 u_2)) = K(\alpha_1 Lu_1 + \alpha_2 Lu_2) = \\ &= \alpha_1 K(Lu_1) + \alpha_2 K(Lu_2) = \alpha_1 (K \circ L)u_1 + \alpha_2 (K \circ L)u_2 \end{aligned}$$

linearno izomorfna sta prostora če obstaja linearni izomorfizem iz **enega** v **drugega**

Matrika linearne preslikave

- → imamo preslikavo **L** : **U** → **V**
- → iz vsakega prostora izberemo **bazo**
- → razvijemo vektorje **preslikane** iz **U** po bazi **V**
- → **skalarje** zložimo v matriko
- → iz i **vrstice** zložimo v i **stolpec**

$$\begin{aligned} Lu_1 &= \alpha_{1,1}v_1 + \ldots + \alpha_{1,m}v_m \\ &\;\vdots \\ Lu_n &= \alpha_{n,1}v_1 + \ldots + \alpha_{n,m}v_m \end{aligned}$$

$$[L]_{\mathcal{C}\leftarrow\mathcal{B}} := \begin{bmatrix} \alpha_{1,1} & \ldots & \alpha_{n,1} \\ \vdots & & \vdots \\ \alpha_{1,m} & \ldots & \alpha_{n,m} \end{bmatrix}$$

Lastnosti linearnih preslikav

Naj bo $L\colon U \to V$ linearna preslikava in naj bo u element U. Naj bo $\mathcal{B}$ baza za U in $\mathcal{C}$ baza za V. Potem velja $[Lu]_{\mathcal{C}} = [L]_{\mathcal{C}\leftarrow\mathcal{B}}[u]_{\mathcal{B}}$.

Naj bodo U, V in W vektorski prostori nad istem poljem in naj bosta $L\colon U \to V$ in $K\colon V \to W$ linearni preslikavi. Naj bo $\mathcal{B}$ baza za U, $\mathcal{C}$ baza za V in $\mathcal{D}$ baza za W. Potem velja $[K \circ L]_{\mathcal{D}\leftarrow\mathcal{B}} = [K]_{\mathcal{D}\leftarrow\mathcal{C}}[L]_{\mathcal{C}\leftarrow\mathcal{B}}$

Naj bo $L\colon U \to V$ linearna preslikava. Naj bosta $\mathcal{B}$ in $\mathcal{B}'$ bazi za U ter $\mathcal{C}$ in $\mathcal{C}'$ bazi za V. Potem velja $[L]_{\mathcal{C}'\leftarrow\mathcal{B}'} = P_{\mathcal{C}'\leftarrow\mathcal{C}}[L]_{\mathcal{C}\leftarrow\mathcal{B}}(P_{\mathcal{B}'\leftarrow\mathcal{B}})^{-1}$

DOKAZ

Dokaz: Razvijmo vektor u po bazi $\mathcal{B} = \{u_1, \ldots, u_n\}$. Dobimo

$$u = \beta_1 u_1 + \ldots + \beta_n u_n$$

Ker je L linearna preslikava, iz (6) sledi

$$Lu = \beta_1 Lu_1 + \ldots + \beta_n Lu_n$$

Za vsak $i = 1, \ldots, n$ razvijmo Lu_i po bazi $\mathcal{C} = \{v_1, \ldots, v_m\}$. Dobimo

$$Lu_i = \alpha_{i,1}v_1 + \ldots + \alpha_{i,m}v_m$$

Če razvoje (8) vstavimo v razvoj (7), dobimo

$$\begin{aligned} Lu &= \beta_1(\alpha_{1,1}v_1 + \ldots + \alpha_{1,m}v_m) + \ldots + \beta_n(\alpha_{n,1}v_1 + \ldots + \alpha_{n,m}v_m) \\ &= (\beta_1\alpha_{1,1} + \ldots + \beta_n\alpha_{n,1})v_1 + \ldots + (\beta_1\alpha_{1,m} + \ldots + \beta_n\alpha_{n,m})v_m \end{aligned}$$

$$[Lu]_{\mathcal{C}} = \begin{bmatrix} \beta_1\alpha_{1,1} + \ldots + \beta_n\alpha_{n,1} \\ \vdots \\ \beta_1\alpha_{1,m} + \ldots + \beta_n\alpha_{n,m} \end{bmatrix} = $$

$$= \begin{bmatrix} \alpha_{1,1} & \ldots & \alpha_{n,1} \\ \vdots & & \vdots \\ \alpha_{1,m} & \ldots & \alpha_{n,m} \end{bmatrix} \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = [L]_{\mathcal{C}\leftarrow\mathcal{B}}[u]_{\mathcal{B}}$$

DOKAZ

Dokaz: Naj bo $\mathcal{B} = \{u_1, \ldots, u_n\}$. Po formuli (4) velja

$$\begin{aligned} [K \circ L]_{\mathcal{D}\leftarrow\mathcal{B}} &= \left[\, [(K \circ L)u_1]_{\mathcal{D}} \;\; \ldots \;\; [(K \circ L)u_n]_{\mathcal{D}} \,\right] \\ &= \left[\, [K(Lu_1)]_{\mathcal{D}} \;\; \ldots \;\; [K(Lu_n)]_{\mathcal{D}} \,\right] \end{aligned}$$

$$[K(Lu_i)]_{\mathcal{D}} = [K]_{\mathcal{D}\leftarrow\mathcal{C}}[Lu_i]_{\mathcal{C}}$$

$$\begin{aligned} [K \circ L]_{\mathcal{D}\leftarrow\mathcal{B}} &= \left[\, [K]_{\mathcal{D}\leftarrow\mathcal{C}}[Lu_1]_{\mathcal{C}} \;\; \ldots \;\; [K]_{\mathcal{D}\leftarrow\mathcal{C}}[Lu_n]_{\mathcal{C}} \,\right] = \\ &= [K]_{\mathcal{D}\leftarrow\mathcal{C}}\left[\, [Lu_1]_{\mathcal{C}} \;\; \ldots \;\; [Lu_n]_{\mathcal{C}} \,\right] = [K]_{\mathcal{D}\leftarrow\mathcal{C}}[L]_{\mathcal{C}\leftarrow\mathcal{B}} \end{aligned}$$

- → **Ker L** = { **0** }
- → **n** (**L**) = **0**
- → **L injektivna**

DOKAZ

Dokaz: Najprej zapišemo L kot $\mathrm{id}_V \circ L \circ \mathrm{id}_U$. Po izreku 2 velja

$$[\mathrm{id}_V \circ L \circ \mathrm{id}_U]_{\mathcal{C}'\leftarrow\mathcal{B}'} = [id_V]_{\mathcal{C}'\leftarrow\mathcal{C}}[L]_{\mathcal{C}\leftarrow\mathcal{B}}[id_U]_{\mathcal{B}\leftarrow\mathcal{B}'}$$

Upoštevajmo še $[id_V]_{\mathcal{C}'\leftarrow\mathcal{C}} = P_{\mathcal{C}'\leftarrow\mathcal{C}}$ in $[id_U]_{\mathcal{B}\leftarrow\mathcal{B}'} = P_{\mathcal{B}\leftarrow\mathcal{B}'} = (P_{\mathcal{B}'\leftarrow\mathcal{B}})^{-1}$

Jedro:

- → **kernel** oz **null space** $\mathrm{Ker}\, L = \{u \in U \mid Lu = 0\}$
- → **ničnost**: $n(L) = \dim \mathrm{Ker}\, L$

ang: **nullity**

TRDITEV:
jedro linearne preslikave **L** : **U** → **V** je **vektorski podprostor** v **U**

DOKAZ

Dokazujemo da vsaka dva vektorja iz **jedra** in za vsaka dva **skalarja** iz F velja definicija vektorskega prostora.

$$L(\alpha_1 u_1 + \alpha_2 u_2) = \alpha_1 L u_1 + \alpha_2 L u_2 = \alpha_1 0 + \alpha_2 0 = 0$$

Slika: $\mathrm{Im}\, L = \{Lu \mid u \in U\}$

to je spet **vektorski podprostor**

Rang: $\mathrm{r}(L) = \dim \mathrm{Im}\, L$

preslikava je ničelna če dobimo nič za vsako **sliko**

→ **r (L) = dim V**
→ **Im L = V**
→ **L** je **surjektivna**

IZREK: n(L) + r(L) = dim U

DOKAZ

Dokaz: Naj bo $w_1, \ldots, w_k$ baza za $\mathrm{Ker}\, L$ in naj bo $u_1, \ldots, u_l$ njena dopolnitev do baze U. Velja torej $\dim \mathrm{Ker}\, L = k$ in $\dim U = k + l$. Dokazati moramo še, da velja $\dim \mathrm{Im}\, L = l$.

Zadošča dokazati, da je $Lu_1, \ldots, Lu_l$ baza za $\mathrm{Im}\, L$. Vzemimo poljuben $v \in \mathrm{Im}\, L$ in izberimo tak u, da je $v = Lu$. Razvijo u po bazi za U:

$$u = \alpha_1 w_1 + \ldots + \alpha_k w_k + \beta_1 u_1 + \ldots + \beta_l u_l$$

Ker je L linearna in ker je $Lw_1 = \ldots = Lw_k = 0$, odtod sledi

$$Lu = \alpha_1 Lw_1 + \ldots + \alpha_k Lw_k + \beta_1 Lu_1 + \ldots + \beta_l Lu_l = \beta_1 Lu_1 + \ldots + \beta_l Lu_l$$

Torej so $Lu_1, \ldots, Lu_l$ ogrodje za $\mathrm{Im}\, L$.
Pokažimo sedaj, da so vektorji $Lu_1, \ldots, Lu_l$ linearno neodvisni. Če je $\beta_1 Lu_1 + \ldots + \beta_l Lu_l = 0$, potem $\beta_1 u_1 + \ldots + \beta_l u_l \in \mathrm{Ker}\, L$. Ker je $w_1, \ldots, w_k$ baza za $\mathrm{Ker}\, L$, obstajajo taki $\gamma_1, \ldots, \gamma_l \in F$, da je

$$\beta_1 u_1 + \ldots + \beta_l u_l = \gamma_1 w_k + \ldots + \gamma_l w_k$$

Ker je $w_1, \ldots, w_k, u_1, \ldots, u_l$ baza za U, odtod sledi $\beta_1 = \ldots = \beta_l = 0$.

IZREK: Slika **matrike** je enaka linearni **ogrinjači** njenih stolpcev. Rang matrike je enak **maksimalnemu** številu linearno **neodvisnih stolpcev** te matrike.

POSLEDICA: Za vsako linearno preslikavo **L** : **U** → **V** obstaja taka baza **B** za **U** in taka baza **C** za **V**, da velja formula in je **I** identična matrika velikosti **r(L)**.

$$[L]_{\mathcal{C} \leftarrow \mathcal{B}} = \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}$$

DOKAZ

Dokaz: Naj bodo $w_1, \ldots, w_k$ in $u_1, \ldots, u_l$ kot v dokazu osnovne formule. Naj bo $z_1, \ldots, z_s$ dopolnitev $Lu_1, \ldots, Lu_l$ do baze za V. Vzemimo

$$\mathcal{B} = \{u_1, \ldots, u_l, w_1, \ldots, w_k\} \quad \text{in} \quad \mathcal{C} = \{Lu_1, \ldots, Lu_l, z_1, \ldots, z_s\}$$

Linearni ogrinjači vrstic matrike A pravimo **vrstični prostor** matrike A in jo označimo z **RowA** dobimo da **Transponiramo ColA**

Linearni ogrinjači stolpcev matrike A pravimo **stolpčni prostor** matrike A in jo označimo z **ColA.** Dokazali smo da je **ImA** = **ColA**

TRDITEV: imamo
L : **U** → **V** in **K** : **V** → **W**
n(K ∘ L) ≤ n(K) + n(L)

elementi $\mathbf{F^n}$ so **stolpčni** vektorji

Slika matrike:
→ A m × n matrika z F elementi
→ priredimo ji lahko linearno preslikavo

$L_A \colon F^n \to F^m \quad L_A v = Av$

$\mathrm{Ker}\, A := \mathrm{Ker}\, L_A \quad \mathrm{Im}\, A := \mathrm{Im}\, L_A$

$\mathrm{Ker}\, A = \{v \in F^n \mid Av = 0\}$

$\mathrm{Im}\, A = \{Av \mid v \in F^n\}$

DOKAZ

Če so vektorji **a** stolpci matrike **A.** $\boldsymbol{\alpha_1, \ldots, \alpha_n}$ so komponente vektorja v. $\mathbf{Av} = \boldsymbol{\alpha_1 a_1} + \ldots + \boldsymbol{\alpha_n a_n}$

$$\mathrm{Im}\, A = \{\alpha_1 \mathbf{a}_1 + \ldots + \alpha_n \mathbf{a}_n \mid \alpha_1, \ldots, \alpha_n \in F\} = \mathrm{Lin}\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$$

Izberimo take stolpce $\mathbf{a_{i1}, \ldots, a_{ir}}$, ki so linearno neodvisni in ki zadoščajo
Lin { $\boldsymbol{\alpha_1, \ldots, \alpha_n}$ } = **Lin** { $\mathbf{a_{i1}, \ldots, a_{ir}}$ }. Potem so stolpci $\mathbf{a_{i1}, \ldots, a_{ir}}$ baza podprostora **ImA.** Rang matrike **A** je enak **r** oz. **maksimalnemu** številu linearno neodvisnih stolpcev matrike **A**.

DOKAZ

Uporabimo osnovni izrek za **linearno preslikavo**.

$\tilde{L} \colon \mathrm{Ker}\,(K \circ L) \to \mathrm{Ker}\, K, \quad \tilde{L}(u) = L(u)$

$\mathrm{n}(\tilde{L}) + \mathrm{r}(\tilde{L}) = \dim \mathrm{Ker}\,(K \circ L) \quad \mathrm{Ker}\, \tilde{L} \subseteq \mathrm{Ker}\, L$

$\mathrm{n}(\tilde{L}) = \dim \mathrm{Ker}\, \tilde{L} \leq \dim \mathrm{Ker}\, L = \mathrm{n}(L) \quad \mathrm{Im}\, \tilde{L} \subseteq \mathrm{Ker}\, K$

$\mathrm{r}(\tilde{L}) = \dim \mathrm{Im}\, \tilde{L} \leq \dim \mathrm{Ker}\, K = \mathrm{n}(K)$

TRDITEV: naj bosta **A** in **B** **m** × **n** matriki nad poljem **F**

→ če sta **A** in **B stolpčno ekvivalentni** potem imata enak stolpčni **prostor**, enako **sliko**, **enak rang** in enako **ničnost**

→ če sta **A** in **B vrstično ekvivalentni** potem imata enak vrstični **prostor**, enako **jedro**, enak **rang** in enako **ničnost**

TRDITEV: vsaka matrika **ranga r** je ekvivalentna matriki $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$

DOKAZ

Dokaz: Naj bo A $m \times n$ matrika nad F. Po Posledici 1 obstajata taka baza $\mathcal{B}$ za F^n in taka baza $\mathcal{C}$ za F^m, da velja

$$[L_A]_{\mathcal{C} \leftarrow \mathcal{B}} = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$$

Naj bosta $\mathcal{S}_n$ in $\mathcal{S}_m$ standardni bazi za F^n in F^m. Potem je

$$A = [L_A]_{\mathcal{S}_m \leftarrow \mathcal{S}_m} = P_{\mathcal{S}_m \leftarrow \mathcal{C}} [L_A]_{\mathcal{C} \leftarrow \mathcal{B}} P_{\mathcal{B} \leftarrow \mathcal{S}_n} = P_{\mathcal{S}_m \leftarrow \mathcal{C}} \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} P_{\mathcal{B} \leftarrow \mathcal{S}_n}$$

kjer sta $P_{\mathcal{S}_m \leftarrow \mathcal{C}}$ in $P_{\mathcal{B} \leftarrow \mathcal{S}_n}$ obrnljivi matriki. Torej je $A \sim \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$.

Ekvivalentnost matrik:

→ **stolpčna**: matriki A in B če dobimo **eno** iz **druge** s pomočjo elementarnih stolpčnih transformacij. Drugače če obstaja **obrnljiva matrika** Q da veja **B** = **AQ**

→ **vrstično**: matriki A in B če dobimo **eno** iz **druge** s pomočjo elementarnih vrstičnih transformacij. Drugače če obstaja **obrnljiva matrika** P da veja **B** = **PA**

→ **ekvivalentni matriki**: ko obstajata obrnljivi matriki da velja **B** = **PAQ** torej lahko uporabljamo vrstične in stolpčne transformacije. Natanko tedaj ko imata **enak rang** in **enako velikost**

Računsko: matriko s pomočjo **elementarnih vrstičnih transformacij** prevedemo v **reducirano** stolpčno formo **R**. Potem matriko R pomočjo **elementarnih stolpčnih transformacij** prevedemo v **željeno obliko**

DOKAZ

Dokaz: Če sta A in B stolpčno ekvivalentni, potem obstaja taka obrnljiva matrika Q, da je $B = AQ$. Pokažimo najprej, da velja $\mathrm{Im}\, AQ = \mathrm{Im}\, A$.

Za vsak $v \in F^n$ so ekvivalentne trditve: (a) $v \in \mathrm{Im}\, AQ$, (b) $v = AQu$ za nek $u \in F^n$, (c) $v = Au'$ za nek $u' \in F^n$, (d) $v \in \mathrm{Im}\, A$. Ekvivalentnost med (b) in (c) sledi iz obrnljivosti matrike Q.

Iz $\mathrm{Im}\, A = \mathrm{Im}\, B$ sledi $\mathrm{r}(A) = \dim \mathrm{Im}\, A = \dim \mathrm{Im}\, B = \mathrm{r}(B)$. Po osnovni formuli odtod sledi $\mathrm{n}(A) = n - \mathrm{r}(A) = n - \mathrm{r}(B) = \mathrm{n}(B)$.

Če sta matriki A in B vrstično ekvivalentni, potem obstaja taka obrnljiva matrika P, da velja $B = PA$. Pokažimo, da je $\mathrm{Ker}\, PA = \mathrm{Ker}\, A$. Za vsak $v \in F^n$ je $Av = 0$ ekvivalentno s $PAv = 0$ zaradi obrnljivosti matrike P.

Iz $\mathrm{Ker}\, A = \mathrm{Ker}\, B$ sledi $\mathrm{n}(A) = \dim \mathrm{Ker}\, A = \dim \mathrm{Ker}\, B = \mathrm{n}(B)$. Po osnovni formuli je torej $\mathrm{r}(A) = n - \mathrm{n}(A) = n - \mathrm{n}(B) = \mathrm{r}(B)$.

Zveza med **KerA** in **RowA**: vektor iz $\mathbf{F^n}$ je v **KerA** natanko ko je **pravokoten** na vse **vrstice** matrike **A** torej ko je **pravokoten** na **RowA**. **KerA** je **ortogonalni komplement**
$\mathrm{Im}\, A^T = (\mathrm{Row}\, A)^T$

TRDITEV: Za vsako matriko **A** je $\mathbf{r(A) = r(A^T)}$

→ **stolpčni rang**: rang matrike A enak maksimalnemu številu **linearno neodvisnih stolpcev** matrike A

→ **vrstični rang**: rang matrike A enak maksimalnemu številu **linearno neodvisnih vrstic** matrike A

DOKAZ

Dokaz: Ekvivalentnost matrik A in B označimo z $A \sim B$. Dokažimo najprej $A \sim A$. To sledi iz $A = I_m A I_n$ in obrnljivosti matrik I_m in I_n.

Če je $A \sim B$, potem je $B = PAQ$ za obrnljivi matriki P, Q. Odtod sledi $A = P^{-1} B Q^{-1}$, kjer sta tudi P^{-1}, Q^{-1} obrnljivi. Torej je $B \sim A$.

Če je $A \sim B$ in $B \sim C$, potem je $B = P_1 A Q_1$ in $C = P_2 B Q_2$ za neke obrnljive matrike P_1, Q_1, P_2, Q_2. Odtod sledi, da je $C = P_2 P_1 A Q_1 Q_2$ in da sta matriki $P_2 P_1$ in $Q_1 Q_2$ obrnljivi. Torej je $A \sim C$

DOKAZ

Dokaz: Če je A $m \times n$ matrika ranga r, potem po Trditvi 9 obstajata taki obrnljivi matriki P in Q, da velja $A = P \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} Q$

$$A^T = Q^T \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}^T P^T$$

Ker sta P in Q obrnljivi matriki, sta tudi P^T in Q^T obrnljivi. Po Trditvi 7 odtod sledi

$$\mathrm{r}(A^T) = \mathrm{r}(Q^T \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}^T) = \mathrm{r}(\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}^T) = r$$

$$\mathrm{r}(A) = r = \mathrm{r}(A^T)$$

Recimo da sta **A** in **B ekvivalentni** matriki. Potem obstajata taki obrnljivi matriki **P** in **Q**, da velja **B** = **PAQ.** Ker so vse **obrnljive** matrike **kvadratne**, je matrika **PAQ** enake velikosti kot matrika A. Torej sta **A** in **B** enake **velikosti**. Velja **r**(**PAQ**) = **r**(**PA**) = **r**(**A**). Torej imata **A** in **B** enak **rang**. Recimo sedaj, da imata matriki A in B enako velikost **m** × **n** in enak rang r.

Opomba: Matrika $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ je velikosti $m \times n$, matrika $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}^T$ pa je velikosti $n \times m$. Imata pa obe enak rang r.

Podobnost matrik:

Podobnost je **ekvivalenčna** relacija

Ko obstajata obrnljiva matrika **P** da velja **B** = **PAP⁻¹**

TRDITEV: Podobni matriki imata enako **determinanto**

DOKAZ

Dokaz: $\det PAP^{-1} = \det P \det A \det P^{-1} = \det A \det PP^{-1} = \det A$.

Opomba: Odtod sledi, da je za vsako linearno preslikavo $L\colon V \to V$ vrednost izraza $\det[L]_{\mathcal{B}\leftarrow\mathcal{B}}$ neodvisna od izbire baze $\mathcal{B}$. To vrednost vzamemo za definicijo $\det L$.

DOKAZ

Dokaz: Ker je $A = IAI^{-1}$, kjer je I identična matrika, je A podobna A.

Če je matrika A podobna matriki B, potem je $B = PAP^{-1}$ za neko obrnljivo matriko P. Odtod sledi, da je $A = P^{-1}BP = P^{-1}B(P^{-1})^{-1}$ in da je matrika P^{-1} obrnljiva. Torej je tudi matrika B podobna matriki A.

Če je matrika A podobna matriki B in če je matrika B podobna matriki C, potem velja $B = PAP^{-1}$ in $C = QBQ^{-1}$ za obrnljivi matriki P in Q. Odtod sledi $C = QPAP^{-1}Q^{-1} = (QP)A(QP)^{-1}$ in da je matrika QP obrnljiva. Torej je matrika A podobna matriki C.

pridružena matrika polinoma $p(x) = x^n - \sum_{i=0}^{n-1} \alpha_i x^i$.

Preproste matrike:

→ **diagonalne matrike**: ni vsaka kvadratna matrika diagonalna
→ **zgornje trikotne matrike**: vsaka kvadratna matrika lahko
→ **Jordanske kanonične forme**: posebni primeri zgornje trikotnih matrik, vsaka kompleksna matrika
→ **Frobeniusove kanonične forme**: bločno diagonalne matrike iz polinomov in vsaka matrika podobna taki

iz **podobnosti** sledi **ekvivalentnost** matrik ne velja pa obratno

Kadar govorimo o **invariantnih podprostorih** matrike **A** ∈ **Mn**(**F**) imamo v mislih **invariantne podprostore** pripadajo če **linearne** preslikave $\mathbf{L_A} : \mathbf{F^n} \to \mathbf{F^n}$, $\mathbf{v} \to \mathbf{Av}$

TRDITEV: Naj bo **V** vektorski prostor nad **F** in naj bo **L** : **V** → **V** linearna preslikava. Za vsaka **polinoma p**(**x**), **q**(**x**) ∈ **F**[**x**] sta **podprostora** Ker **q**(**L**) in **Imq**(**L**) invariantna za **p**(**L**)

INVARIANTNI PODPROSTORI:

→ naj bo **L** : **V** → **V** linearna preslikava
→ vektorski **podprostor W**
→ **W** je **invarianten** za **L** če za vsak **w** ∈ **W** velja **Lw** ∈ **W**
→ Če ima linearna preslikava **invarianten podprostor**, potem ji lahko priredimo **matriko** z **veliko ničlami**
→ **direktna vsota:** podprostori W_i in so W_i invariantni za L. B_i je baza prostora $\mathbf{W_i}$ in **B** je **unija** vseh baz. Obstajajo matrike $\mathbf{A_1}, \dots, \mathbf{A_k}$ velikosti $\mathbf{dimW_i}$ da velja

DOKAZ

Dokaz: V dokazu bomo uporabili, da je

$$p(L) \circ q(L) = q(L) \circ p(L)$$

kar sledi iz $L^r \circ L^s = L^{r+s} = L^s \circ L^r$ z direktnim računom.

Če je $v \in \operatorname{Ker} q(L)$, potem je $q(L)v = 0$. Odtod sledi $p(L)(q(L)v) = 0$. Po prvem odstavku odtod sledi $q(L)(p(L)v) = 0$. Torej je $p(L)v \in \operatorname{Ker} q(L)$.

Če je $v \in \operatorname{Im} q(L)$, potem obstaja tak $u \in V$, da je $v = q(L)u$. Odtod sledi $p(L)v = p(L)(q(L)v) = q(L)(p(L)v) = q(L)u'$, kjer je $u' = p(L)v$ element V. Odtod sledi, da je $p(L)v \in \operatorname{Im} q(L)$.

TRDITEV: Naj bo **L**: **V** → **V** linearna preslikava in naj bo **W** **invarianten podprostor** za L. Izberimo bazo $\mathbf{w_1}, \dots, \mathbf{w_k}$ za **W** in jo dopolnimo do **baze B** za **V**. Potem je **[L]B ← B** bločno zgornje trikotna matrika.

$$[L]_{\mathcal{B}\leftarrow\mathcal{B}} = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$$

za neko **k** × **k** matriko **A** in neki matriki **B** in **v**

$$[L]_{\mathcal{B}\leftarrow\mathcal{B}} = \begin{bmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_k \end{bmatrix}$$

ENORAZSEŽNI INVARIANTNI PODPROSTORI:

→ vsaka invariantna preslikava **L** : **V** → **V** kjer je V netrivialen vektorski prostor nad C
→ naslednje trditve so **enakovredne**:

- **L** ima **enorazsežen invarianten** podprostor
- obstaja neničeln **v** ∈ **V** in tak **λ** ∈ **C**, da je **Lv** = **λv**
- obstaja neničeln **v** ∈ **V** in tak **λ** ∈ **C**, da je (**L** − **λ id**) **v** = **0**
- obstaja tak **λ** ∈ **C**, da je **Ker**(**L** − **λ id**) 6= { **0** }
- obstaja tak **λ** ∈ **C**, da linearna preslikava **L** − **λ id** ni injektivna
- obstaja tak **λ** ∈ **C**, da linearna preslikava **L** − **λ id** ni obrnljiva
- obstaja tak **λ** ∈ **C**, da velja det (**L** − **λ id**) = **0**

→ ker smo v **kompleksnih** številih: **det**(**L** − **λ id**) = **0** vsaj eno **netrivialno rešitev**

DOKAZ

Dokaz: Naj bodo $v_1, \dots, v_l \in V$ taki vektorji, da je $w_1, \dots, w_k, v_1, \dots, v_l$ baza za V. Označimo to bazo z $\mathcal{B}$. Ker je W invarianten podprostor za L, so $Lw_1, \dots, Lw_k$ v W. Torej lahko $Lw_1, \dots, Lw_k$ razvijemo po $w_1, \dots, w_k$:

$$Lw_1 = \alpha_{1,1}w_1 + \ldots + \alpha_{1,k}w_k$$
$$\vdots$$
$$Lw_k = \alpha_{k,1}w_1 + \ldots + \alpha_{k,k}w_k$$

Vektorje $Lv_1, \dots, Lv_l$ razvijmo po bazi $w_1, \dots, w_k, v_1, \dots, v_l$

$$Lv_1 = \beta_{1,1}w_1 + \ldots + \beta_{1,k}w_k + \gamma_{1,1}v_1 + \ldots + \gamma_{1,l}v_l$$
$$\vdots$$
$$Lv_l = \beta_{l,1}w_1 + \ldots + \beta_{l,k}w_k + \gamma_{l,1}v_1 + \ldots + \gamma_{l,l}v_l$$

Označimo $\mathcal{B} = \{w_1, \dots, w_k, v_1, \dots, v_l\}$. Potem je

$$[L]_{\mathcal{B}\leftarrow\mathcal{B}} = \begin{bmatrix} \alpha_{1,1} & \dots & \alpha_{k,1} & \beta_{1,1} & \dots & \beta_{l,1} \\ \vdots & & \vdots & \vdots & & \vdots \\ \alpha_{1,k} & \dots & \alpha_{k,k} & \beta_{1,k} & \dots & \beta_{l,k} \\ 0 & \dots & 0 & \gamma_{1,1} & \dots & \gamma_{l,1} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & \gamma_{1,l} & \dots & \gamma_{l,l} \end{bmatrix}$$

Če sta dve matriki kongruentni, potem sta očitno tudi **ekvivalentni**. Obratno ni res.

Recimo matriki [**1**] in [**−1**] sta **ekvivalentni** nista pa **kongruentni**.

Kongurentnost matrik

→ **A** in **B** sta **kongurentni** če velja $\mathbf{B} = \mathbf{PAP^T}$.

ekvivalentnost

podobnost ↗̸ ↗ ↖ ↖̸ kongruentnost

Če v definiciji **ekvivalentnosti** matrik in **podobnosti** matrik **zamenjamo obrnljive** matrike z **ortogonalnimi** matrikami, potem dobimo definiciji **ortogonalne ekvivalentnosti** matrik in **ortogonalne podobnosti** matrik

Ortogonalnost:

→ **kvadratna matrika** je **ortogonalna** če velja $\mathbf{I} = \mathbf{PP^T}$.
→ matriki A in B sta **ortogonalno ekvivalentni** če obstajata **ortogonalni matriki P** in **Q**.

$B = PAQ^{-1}$ $(\Leftrightarrow B = PAQ^T)$ $\qquad$ $B = PAP^{-1}$ $(\Leftrightarrow B = PAP^T)$

→ matriki A in B sta **ortogonalno podobni** če obstaja **ortogonalna matrika P**

ekvivalentnost

↗ ↑ ↖

ortogonalna ekvivalentnost $\qquad$ podobnost $\qquad$ kongruentnost

↖ ↑ ↗

ortogonalna podobnost

LASTNE VREDNOSTI

Diagonalna ali **zgornje trikotna** matrika

Lastni problem:

→ **kvadratno** matriko iščemo čim **preprostejšo** matriko ki ji je **podobna**
→ vemo da pomaga če ima matrika **invariantni prostor**
→ kdaj ima **enorazsežen invariantni** prostor
→ obstaja enorazsežen podprostor v $\mathbf{F^n}$ ki je **invarianten** za **A** (1)
→ obstaja tak **skalar λ** ∈ **F** in tak neničeln **vektor v** ∈ $\mathbf{F^n}$ da velja **Av** = **λv** (2)

DOKAZ

Dokaz: Če velja (2), potem je očitno $\operatorname{Lin}\{v\}$ enorazsežen invarianten podprostor za A. Torej velja (1).

Če velja (1), potem obstaja tak neničeln vektor $v \in F^n$, da je podprostor $\operatorname{Lin}\{v\}$ invarianten za A. Ker je $Av \in \operatorname{Lin}\{v\}$, obstaja tak skalar $\lambda \in F$, da velja $Av = \lambda v$. Torej velja (2).

LASTNA VREDNOST:

→ **A** ∈ **Mn**(**F**) je dana matrika
→ **Av** = **λv**
→ iščemo **skalar λ** ∈ **F** in vektor **v** ∈ $\mathbf{F}^n$
→ ta enačba je **lastni problem**
→ **trivialna** rešitev: **ničelni vektor**
→ če je par netrivialna rešitev potem je **λ lastna vrednost** in **v** pa **lastni vektor**
→ matrika A ima **enorazsežen invarianten podprostor** natanko tedaj, ko ima kako **lastno vrednost**

ENAKOVREDNE TRDITVE

- **λ** je **lastna vrednost** matrike **A**
- **Ker**(**A − λI**) ≠ { **0** }
- matrika **A − λI ni obrnljiva**
- **det**(**A − λI**) = **0**

DOKAZ

Enačbo lahko zapišemo tudi v obliki (**A− λI**)**v** = **0**

$(A - \lambda I)v = Av - \lambda Iv = Av - \lambda v$

Torej je **prva** točka **ekvivalentna** z **drugo.**
Druge trditve iz obrnljivosti matrik.

KARAKTERISTIČNI POLINOM:

→ **A** ∈ **Mn**(**F**) je dana matrika
→ to je polinom $\mathbf{p_A}$(**x**) = **det** (**A − xI**)
→ **I** je **identična** matrika velikosti **n**
→ če je lastna vrednost **λ m** kratna **ničla** potem je njena **algebraična večkratnost** enaka **m**

TRDITEV: **Skalar λ** ∈ **F** je **lastna vrednost** matrike **A** ∈ **Mn**(**F**) natanko tedaj, ko je **λ ničla karakterističnega polinoma** matrike **A**

DOKAZ

V nadaljevanju se bomo omejili na primer **F** = **C**
Osnovni izrek algebre pravi, da ima vsak **nekonstanten** polinom s **kompleksnimi koeficienti** vsaj eno kompleksno ničlo. Od tod sledi, da ima vsaka **kompleksna kvadratna matrika** vsaj eno **lastno vrednost**.
Karakteristični polinom lahko razcepimo na **linearne faktorje**:

$p_A(x) = (-1)^n (x - \lambda_1)^{n_1} \cdots (x - \lambda_k)^{n_k}$

kjer so $\boldsymbol{\lambda_1,\ldots,\lambda_k}$ vse paroma **različne lastne vrednosti** matrike **A.** Naravna števila $\mathbf{n_1,\ldots,n_k}$ očitno zadoščajo $\mathbf{n_1} + \ldots + \mathbf{n_k}$ = **n**. To so **algebraične večkratnosti** lastnih vrednost $\boldsymbol{\lambda_1,\ldots,\lambda_k}$

TRDITEV: matriki **A** in **B** sta **podobni** torej je **det**(**A − xI**) = **det**(**B − xI**).
Torej imata **A** in **B** enake lastne vrednosti z **enakimi algebraičnimi večkratnostnmi**

DOKAZ

Dokaz: Če je $A = PBP^{-1}$, potem je $A - xI = P(B - xI)P^{-1}$. Torej je $\det(A - xI) = \det P \det(B - xI) \det P^{-1} = \det P \det P^{-1} \det(B - xI) = \det(PP^{-1}) \det(B - xI) = \det I \det(B - xI) = \det(B - xI)$.

TRDITEV: naj bosta **A** in **B podobni** matriki in **λ** lastna vrednost za **A** in geometrijsko večkratnostjo **m**. Potem sta **m** in **λ enake** za **B**

DOKAZ

Naj bosta A in B podobni matriki in naj bo λ lastna vrednost za A. Po Trditvi 4 je λ tudi lastna vrednost za B. Poglejmo kakšna je zveza med lastnima podprostoroma $\mathrm{Ker}\,(A - \lambda I)$ in $\mathrm{Ker}\,(B - \lambda I)$.

Naj bo P taka obrnljiva matrika, da velja $B = PAP^{-1}$. Potem velja

$$
\begin{aligned}
\mathrm{Ker}\,(B - \lambda I) &= \mathrm{Ker}\,P(A - \lambda I)P^{-1} \\
&= \{v \in F^n \mid P(A - \lambda I)P^{-1}v = 0\} \\
&= \{v \in F^n \mid (A - \lambda I)P^{-1}v = 0\} \\
&= \{Pw \mid w \in F^n, (A - \lambda I)w = 0\} \\
&= \{Pw \mid w \in \mathrm{Ker}\,(A - \lambda I)\} \\
&= P\,\mathrm{Ker}\,(A - \lambda I)
\end{aligned}
$$

Odtod sledi, da podprostora $\mathrm{Ker}\,(A - \lambda I)$ in $\mathrm{Ker}\,(B - \lambda I)$ nista nujno enaka. Sta pa enaki njuni dimenziji.

Velja namreč

$$\dim \mathrm{Ker}\,(B - \lambda I) = \mathrm{n}(B - \lambda I) = \mathrm{n}(P(A - \lambda I)P^{-1}) =$$

$$= \mathrm{n}(P(A - \lambda I)) = \mathrm{n}(A - \lambda I) = \dim \mathrm{Ker}\,(A - \lambda I)$$

ker se ničnost ohranja pri vrstični in stolpčni ekvivalenci matrik.

LASTNI PODPROSTORI:

→ množica vseh **lastnih vektorjev** matrike **A**
→ pripadajo jim svoje **lastne vrednosti**
→ ta množica enaka **Ker**(**A − λI**) \ {**0**}
→ ta množica vedno **neskončna** ker neničelen **večkratnik** lastnega vektorja spet **lastni vektor**
→ vektor 0 ni **nikoli** lastni vektor
→ če vektor **0** dodamo k množici lastnih vektorjev dobimo **Ker**(**A − λI**) ki je **podprostor** v $\mathbf{C}^n$
→ **Ker**(**A − λI**) je **lastni podprostor**
→ **dimenzija** tega podprostora je **geometrijska večkratnost**

lastne podprostore **poiščemo** tako da za **vsako** lastno vrednost matrike A rešimo **homogen sistem linearnih enačb** (**A − λI**) **v** = **0** kjer komponente v **spremenljivke**

Ker so pri **diagonalni** matriki **geometrijske večkratnosti** lastnih vrednosti enake **algebraičnim večkratnostim** je to res tudi za vse matrike ki so **podobne diagonalnim**

Diagonalizacija matrik: iskanje diagonalne matrike

→ matrika **A** ima n linearno **neodvisnih** vektorjev $\mathbf{v_1,\ldots,v_n}$
→ $\boldsymbol{\lambda_1,\ldots,\lambda_k}$ so pripadajoče vrednosti

$Av_1 = \lambda_1 v_1, \ldots, Av_n = \lambda_n v_n$ $\quad P = \begin{bmatrix} v_1 & \ldots & v_n \end{bmatrix}$

→ matrika P je torej **obrnljiva**

$AP = \begin{bmatrix} Av_1 & \ldots & Av_n \end{bmatrix} = \begin{bmatrix} \lambda_1 v_1 & \ldots & \lambda_n v_n \end{bmatrix} = PD$

$$D = \begin{bmatrix} \lambda_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & \lambda_n \end{bmatrix}$$

→ razcep **A** = $\mathbf{PDP^{-1}}$ kjer je **P obrnljiva D** pa **diagonalna** matrika

→ **P obrnljiva** natanko takrat ko so vektorji $\mathbf{v_1,\ldots,v_n}$ linearno **neodvisni**
→ **stolpci** matrike **P** so linearno neodvisni vektorji
→ matrika **diagonalizacijo** natanko ko ima **n** linearno neodvisnih vektorjev

Schurov izrek:

→ ni vsaka kvadratna matrika nad C podobna neki diagonalni
→ **vedno** je podobna neki **zgornje trikotni**
→ podobna je **Jordanski kanonični formi**

DOKAZ

Dokaz bo z popolno indukcijo po velikosti matrike. Očitno trditev velja za matrike velikosti 1, ker so te že same zgornje trikotne. Recimo sedaj, da trditev velja za vse matrike velikosti $n-1$ in vzemimo poljubno matriko A velikosti n. Radi bi dokazali, da trditev velja tudi za matriko A.
Naj bo λ lastna vrednost matrike A in naj bo v_1 pripadajoči lastni vektor.
Naj bodo $v_2, \ldots, v_n$ dopolnitev v_1 do baze za F^n. Potem je matrika

$$P = \begin{bmatrix} v_1 & \ldots & v_n \end{bmatrix}$$

obrnljiva. Razvijmo vektorje $Av_2, \ldots, Av_n$ po bazi $v_1, v_2, \ldots, v_n$.

$$Av_2 = \alpha_{2,1}v_1 + \alpha_{2,2}v_2 + \ldots + \alpha_{2,n}v_n$$
$$\vdots$$
$$Av_n = \alpha_{n,1}v_1 + \alpha_{n,2}v_2 + \ldots + \alpha_{n,n}v_n$$

Potem velja

$$AP = A\begin{bmatrix} v_1 & v_2 & \ldots & v_n \end{bmatrix} = \begin{bmatrix} Av_1 & Av_2 & \ldots & Av_n \end{bmatrix}$$
$$= \begin{bmatrix} \lambda v_1 & \alpha_{2,1}v_1 + \alpha_{2,2}v_2 + \ldots + \alpha_{2,n}v_n & \ldots & \alpha_{n,1}v_1 + \alpha_{n,2}v_2 + \ldots + \alpha_{n,n}v_n \end{bmatrix}$$
$$= \begin{bmatrix} v_1 & v_2 & \ldots & v_n \end{bmatrix} \begin{bmatrix} \lambda & \alpha_{2,1} & \ldots & \alpha_{n,1} \\ 0 & \alpha_{2,2} & \ldots & \alpha_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \alpha_{2,n} & \ldots & \alpha_{n,n} \end{bmatrix} = P\begin{bmatrix} \lambda & c \\ 0 & B \end{bmatrix}$$

Po indukcijski predpostavki obstaja taka obrnljiva matrika Q velikosti $n-1$ in taka zgornje trikotna matrika T velikosti $n-1$, da velja

$$B = QTQ^{-1}$$

Odtod sledi

$$
\begin{aligned}
&\begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix}^{-1} P^{-1}AP \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix} = \\
&= \begin{bmatrix} 1 & 0 \\ 0 & Q^{-1} \end{bmatrix} \begin{bmatrix} \lambda & c \\ 0 & B \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix} = \\
&= \begin{bmatrix} \lambda & c \\ 0 & Q^{-1}B \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix} = \\
&= \begin{bmatrix} \lambda & cQ \\ 0 & Q^{-1}BQ \end{bmatrix} = \begin{bmatrix} \lambda & cQ \\ 0 & T \end{bmatrix}
\end{aligned}
$$

kar je zgornje trikotna matrika. S tem je indukcijski korak dokazan.

TRDITEV: **lastni vektorji**, ki pripadajo **paroma različnim** lastnim vrednostim, so **linearno neodvisni**

ENAKOVREDNE TRDITVE

- matrika **A** ima **diagonalizacijo**
- matrika **A** je **podobna diagonalni** matriki
- matrika A ima n linearno neodvisnih lastnih vektorjev
- **vsota lastnih podprostorov** matrike **A** je $\mathbf{C}^n$

POSLEDICA 1:
če ima **A n** paroma različnih vrednosti ima **A diagonalizacijo**

POSLEDICA 2: v**sota** vseh lastnih podprostorov matrike je **direktna**

DOKAZ TRDITVE

Dokaz. Naj bodo $\lambda_1, \dots, \lambda_k$ paroma različne lastne vrednosti matrike A in naj bodo $v_1, \dots, v_k$ pripadajoči lastni vektorji. Se pravi

$$Av_1 = \lambda_1 v_1 \quad \dots \quad Av_k = \lambda_k v_k \tag{1}$$

in $v_1, \dots, v_k$ so neničelni vektorji. Z indukcijo po j bomo pokazali, da je za vsak $j \le k$ množica $\{v_1, \dots, v_j\}$ linearno neodvisna.

Baza indukcije: Ker je $v_1 \neq 0$, je množica $\{v_1\}$ linearno neodvisna.

Indukcijski korak: Recimo, da je množica $\{v_1, \dots, v_j\}$ linearno neodvisna, kjer je $j < k$. Radi bi pokazali, da je potem tudi množica $\{v_1, \dots, v_{j+1}\}$ linearno neodvisna. Recimo, da je

$$\alpha_1 v_1 + \ldots + \alpha_j v_j + \alpha_{j+1} v_{j+1} = 0. \tag{2}$$

Če (2) pomnožimo z leve z matriko A in upoštevamo (1), dobimo

$$\alpha_1 \lambda_1 v_1 + \ldots + \alpha_j \lambda_j v_j + \alpha_{j+1} \lambda_{j+1} v_{j+1} = 0. \tag{3}$$

Če od enačbe (3) odštejemo z λ_{j+1} pomnoženo enačbo (2), dobimo

$$\alpha_1(\lambda_1 - \lambda_{j+1}) v_1 + \ldots + \alpha_j(\lambda_j - \lambda_{j+1}) v_j = 0. \tag{4}$$

Po indukcijski predpostavki odtod sledi, da je

$$\alpha_1(\lambda_1 - \lambda_{j+1}) = 0, \dots, \alpha_j(\lambda_j - \lambda_{j+1}) = 0. \tag{5}$$

Ker so $\lambda_1, \dots, \lambda_k$ paroma različne, odtod sledi $\alpha_1 = 0, \dots, \alpha_j = 0$.
Iz enačbe (2) sedaj sledi, da je $\alpha_{j+1} v_{j+1} = 0$. Odtod sledi $\alpha_{j+1} = 0$, saj je $v_{j+1} \neq 0$. Dokazali smo, da iz (2) sledi $\alpha_1 = \ldots = \alpha_{j+1} = 0$, torej so $v_1, \dots, v_{j+1}$ linearno neodvisni.

DOKAZ POSLEDICE 2

Dokaz: Naj bodo $\lambda_1, \dots, \lambda_k$ vse paroma različne lastne vrednosti matrike $A \in M_n(\mathbb{C})$. Pripadajoči lastni podprostori so potem $V_i = \operatorname{Ker}(A - \lambda_i I)$ za $i = 1, \dots, k$. Trdimo, da je vsota podprostorov $V_1, \dots, V_k$ direktna. Treba je dokazati, da so poljubni vektorji $v_1 \in V_1, \dots, v_k \in V_k$, ki zadoščajo $v_1 + \ldots + v_k = 0$, enaki nič.

DOKAZ POSLEDICE 1

Ker ima **A n** paroma **različnih** lastnih vrednosti, ima tudi **n** linearno **neodvisnih lastnih vektorjev**. Sledi da ima A **diagonalizacijo**

LEMA: za vsako **lastno vrednost λ** je njena geometrijska večkratnost **g(λ) manjša** ali **enaka** njeni algebraični večkratnosti **a(λ)**

TRDITEV: Matrika A ima **diagonalizacijo** natanko ko se za vsako lastno vrednost njena **geometrijska** in **algebraična** večkratnost **ujemata**

DOKAZ

Dokaz: Naj bo $v_1, \dots, v_m$ baza za $\operatorname{Ker}(A - \lambda I)$ in naj bo $v_{m+1}, \dots, v_n$ njena dopolnitev do baze $\mathcal{B}$ za $\mathbb{C}^n$. Običajen račun potem pokaže, da je

$$P^{-1}AP = \begin{bmatrix} \lambda I_m & B \\ 0 & C \end{bmatrix}$$

kjer je $P = \begin{bmatrix} v_1 & \dots & v_m & v_{m+1} & \dots & v_n \end{bmatrix}$ obrnljiva matrika. Sledi

$$\det(A - xI_n) = \det(\lambda I_m - xI_m)\det(C - xI_{n-m}) = (\lambda - x)^m \det(C - xI_{n-m})$$

Ker $(x - \lambda)^m$ deli karakteristični polinom, je $a(\lambda) \ge m = g(\lambda)$

TRDITEV: $\lambda_1, \dots, \lambda_k$ vse paroma **različne** lastne vrednosti matrike A. Potem ima matrika A **diagonalizacijo** natanko ko je **produkt** matrik **$A - \lambda_1 I$, ..., $A - \lambda_k I$** enak **ničelni matriki**

DOKAZ

Naj bodo $\lambda_1, \dots, \lambda_k$ vse paroma **različne lastne vrednosti.** Njen karakteristični polinom je $p_A(x) = (-1)^n (x - \lambda_1)^{n1} \dots (x - \lambda_k)^{nk}$ in n_i **algebraična** večkratnost za λ_i očitno velja $n_1 + \dots + n_k = n$. **Geometrijska** večkratnost za λ_i je $m_i := \dim \operatorname{Ker}(A - \lambda_i I)$
Matrika ima **diagonalizacijo** natanko tedaj ko $U = C^n$ kjer je **U vsota** vseh **lastnih podprostorov** matrike **A**. **dim U** = $m_1 + \dots + m_k$ torej ima diagonalizacijo natanko takrat ko $m_1 + \dots + m_k = n_1 + \dots + n_k$ in torej velja $m_i = n_i$ za vsak i.

DOKAZ

Dokaz. Označimo $L_i = A - \lambda_i I$ za $i = 1, \dots, k$. Potrebovali bomo formulo

$$\dim \operatorname{Ker}(L_1 L_2 \cdots L_k) \le \dim \operatorname{Ker}(L_1) + \dim \operatorname{Ker}(L_2) + \ldots + \dim \operatorname{Ker}(L_k). \tag{1}$$

Primer $k = 2$ formule (1) smo dokazali v prejšnjem poglavju. Za splošen k formulo (1) dokažemo z indukcijo.
Če velja $L_1 \cdots L_k = 0$, potem je $\operatorname{Ker}(L_1 \cdots L_k) = \mathbb{C}^n$, kjer je n velikost matrike A, torej je $\dim \operatorname{Ker}(L_1 \cdots L_k) = n$. Označimo z $m_i = \dim \operatorname{Ker}(L_i)$ geometrijsko večkratnost λ_i. Iz formule (1) torej sledi $n \le m_1 + \cdots + m_k$. Naj bo n_i algebraična večkratnost λ_i. Iz $n = n_1 + \ldots + n_k$ in iz $m_i \le n_i$ sledi, da je $m_i = n_i$ za vsak i. Po Trditvi 3 ima torej matrika A diagonalizacijo.

Dokažimo še drugo smer. Recimo, da ima matrika A diagonalizacijo $A = PDP^{-1}$. S permutacijo diagonalnih elementov matrike D dobimo matriko, ki ji je podobna. Zato lahko predpostavimo, da enake lastne vrednosti ležijo skupaj na diagonali D, se pravi, da je

$$D = \begin{bmatrix} \lambda_1 I_{m_1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_k I_{m_k} \end{bmatrix} \tag{2}$$

Iz (2) sledi, da je i-ti diagonalni blok matrike $D - \lambda_i I$ enak 0, torej je

$$(D - \lambda_1 I)(D - \lambda_2 I) \cdots (D - \lambda_k I) = 0. \tag{3}$$

Iz (3) izpeljemo

$$P(D - \lambda_1 I)P^{-1} P(D - \lambda_2 I)P^{-1} \cdots P(D - \lambda_k I)P^{-1} = 0 \tag{4}$$

kjer je $P(D - \lambda_i I)P^{-1} = PDP^{-1} - \lambda_i I = A - \lambda_i I$.

MINIMALNI POLINOM MATRIKE

- → **C**[**x**] množica vseh **polinomov** v x s **kompleksnimi** koeficienti
- → **M_n(C)** množica vseh **kompleksnih n** × **n** matrik

$$p(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0 \in \mathbb{C}[x]$$

- → v polinom vstavimo **matriko** namesto x
- → problem ker c_0 skalar zato ga pomnožimo z **identiteto**

$$p(A) := c_n A^n + c_{n-1} A^{n-1} + \ldots + c_1 A + c_0 I$$

iz $p(x) = p_1(x)p_2(x)$ sledi $p(A) = p_1(A)p_2(A)$

- → **minimalni polinom**: polinom **m** če je **m**(**A**) = **0** in ima m **vodilni koeficient 1** in ima m med vsemi **najnižjo stopnjo**
- → označimo do $\mathbf{m_A}$

TRDITEV: Vsaka matrika A ima **natanko en** minimalni polinom

DOKAZ

dokaz je po **korakih** ↓
vzamemo poljubno **matriko A**

2. korak Matrika A ima vsaj en minimalni polinom.

Naj bo $\mathcal{M}$ množica vseh polinomov, ki zadoščajo točkam (1) in (2) iz definicije minimalnega polinoma. Po 1. koraku je množica $\mathcal{M}$ neprazna. Vzemimo v množici $\mathcal{M}$ polinom z najnižjo stopnjo. Tak polinom potem zadošča vsem trem točkam iz definicije minimalnega polinoma.

1. korak Konstruirajmo najprej tak polinom $p \in \mathbb{C}[x]$, ki zadošča $p(A) = 0$ in ki ima vodilni koeficient enak ena.

Očitno je $M_n(\mathbb{C})$ vektorski prostor nad $\mathbb{C}$ dimenzije n^2. Ker ima množica $\{I, A, A^2, \dots, A^{n^2}\}$ en element več od dimenzije, je linearno odvisna. Obstajajo torej taki $c_0, c_1, c_2, \dots, c_{n^2} \in \mathbb{C}$, od katerih je vsaj en neničeln, da velja $\sum_{i=0}^{n^2} c_i A^i = 0$. Polinom $p(x)$ dobimo tako, da polinom $\sum_{i=0}^{n^2} c_i x^i$ delimo z njegovim vodilnim koeficientom.

4. korak Če sta m_1 in m_2 minimalna polinoma matrike A, potem je $m_1 = m_2$.

Ker je $m_2(A) = 0$, po 3. koraku m_1 deli m_2. Ker je $m_1(A) = 0$, po 3. koraku m_2 deli m_1. Torej obstaja taka konstanta $c \neq 0$, da je $m_2 = cm_1$. Ker imata oba polinoma vodilni koeficient enak 1, je $c = 1$.

3. korak Naj bo m minimalni polinom matrike A in naj bo p tak polinom, ki zadošča $p(A) = 0$. Potem m deli p.

Po izreku o deljenju z ostankom obstajata taka polinoma k in r, da velja $p = km + r$ in $\deg r < \deg m$. Ker je $m(A) = 0$ in $p(A) = 0$, je tudi $r(A) = 0$. Če bi bil r neničeln polinom, bi ga delili z vodilnim koeficientom in bi dobili tak polinom, ki zadošča točkam (1) in (2) iz definicije minimalnega polinoma in je nižje stopnje od m. To je v nasprotju s predpostavko, da m zadošča točki (3) iz definicije minimalnega polinoma. Torej je r ničeln polinom.

TRDITEV: če je $\mathbf{p_A}$(**x**) **karakteristični** polinom matrike **A** je $\mathbf{p_A}$(**A**) = **0**

DOKAZ

Dokaz: Spomnimo se formule $B^{-1} = \frac{1}{\det B} \tilde{B}^T$ za inverz matrike, kjer matriko $\tilde{B}$ dobimo tako, da v matriki B vsak element $b_{i,j}$ zamenjamo z $(-1)^{i+j} \det B_{i,j}$. (B s pobrisano i-to vrstico in j-tim stolpcem je $B_{i,j}$).
Če to formulo pomnožimo z $\det(B)B$ z leve, dobimo $\det(B)I = B\tilde{B}^T$.
Sedaj vstavimo $B = A - xI$ in dobimo $p_A(x)I = (A - xI)\widetilde{(A - xI)}^T$.
Elementi matrike $\widetilde{(A - xI)}^T$ so polinomi v x stopnje $\le n - 1$. (So namreč determinante velikosti $n - 1$, katerih elementi so polinomi stopnje ≤ 1.)

V enačbo $p_A(x)I = (A - xI)\widetilde{(A - xI)}^T$ vstavimo
$p_A(x) = c_0 + c_1 x + \ldots + c_n x^n$, kjer $c_i \in \mathbb{C}$, in
$\widetilde{(A - xI)}^T = B_0 + xB_1 + \ldots + x^{n-1} B_{n-1}$, kjer $B_i \in M_n(\mathbb{C})$.
Primerjajmo koeficiente pri potencah x^i, kjer $i = 0, 1, 2, \dots, n - 1, n$:

$$\begin{aligned} c_0 I &= AB_0 \\ c_1 I &= AB_1 - B_0 \\ c_2 I &= AB_2 - B_1 \\ &\vdots \\ c_{n-1} I &= AB_{n-1} - B_{n-2} \\ c_n I &= -B_{n-1} \end{aligned}$$

Pomnožimo i-to enačbo z A^i z leve in vse enačbe seštejmo.
Dobimo $c_0 I + c_1 A + c_2 A^2 + \ldots + c_{n-1} A^{n-1} + c_n A^n =$
$AB_0 + A(AB_1 - B_0) + A^2(AB_2 - B_1) + \ldots + A^{n-1}(AB_{n-1} - B_{n-2}) + A^n(-B_{n-1})$.
Na desni strani odpravimo oklepaje in opazimo, da se vse pokrajša.

Ker minimalni polinom $m_A(x)$ deli karakteristični polinom $p_A(x)$ in ker je $p_A(x)$ oblike $p_A(x) = (-1)^n (x - \lambda_1)^{n_1} \cdots (x - \lambda_k)^{n_k}$, je $m_A(x)$ oblike

$$m_A(x) = (x - \lambda_1)^{r_1} \cdots (x - \lambda_k)^{r_k}$$

kjer je $r_1 \le n_1, \dots, r_k \le n_k$

TRDITEV: vsaka **lastna vrednost** matrike **A** je ničla minimalnega polinoma $\mathbf{m_A}$

DOKAZ

Dokaz: Naj bo λ lastna vrednost matrike A in naj bo v pripadajoči lastni vektor. Iz $Av = \lambda v$ s popolno indukcijo izpeljemo, da velja $A^k v = \lambda^k v$ za vsak k. Če namreč velja $A^{k-1}v = \lambda^{k-1}v$ za nek k, potem je

$$A^k v = A(A^{k-1}v) = A(\lambda^{k-1}v) = \lambda^{k-1}Av = \lambda^{k-1}(\lambda v) = \lambda^k v.$$

Recimo, da je minimalni polinom oblike $m_A(x) = \sum_{i=0}^{r} c_i x^i$. Potem velja

$$0 = 0v = m_A(A)v = \sum_{i=0}^{r} c_i A^i v = \sum_{i=0}^{r} c_i \lambda^i v = m_A(\lambda)v$$

Ker je v neničeln, odtod sledi $m_A(\lambda) = 0$

TRDITEV: matrika ima **diagonalizacijo** natanko ko njen **minimalni polinom** nima večkratnih **ničel**

DOKAZ

Dokaz: Naj bodo $\lambda_1, \dots, \lambda_k$ vse paroma različne lastne vrednosti matrike A. Iz 3. razdelka vemo, da ima A diagonalizacijo natanko tedaj, ko je produkt matrik $A - \lambda_i I$ enak nič. Označimo z $m(x)$ produkt polinomov $x - \lambda_i$, se pravi $m(x) = (x - \lambda_1)\cdots(x - \lambda_k)$. Torej ima A diagonalizacijo natanko tedaj, ko je $m(A) = 0$. Po 3. koraku v dokazu Trditve 1 velja $m(A) = 0$ natanko tedaj, ko minimalni polinom $m_A(x)$ deli polinom $m(x)$. Po Trditvi 3 velja to natanko tedaj, ko je $m_A(x) = m(x)$.

TRDITEV: vektorski podprostor **U** v $\mathbf{C^n}$ je **invarianten** za matriko **A** ∈ $\mathbf{M_n(C)}$ če za vsak **u** ∈ **U** velja **Au** ∈ **U**

DOKAZ

Dokažimo invariantnost korenskega podprostora $W_i = \mathrm{Ker}(A - \lambda_i I)^{r_i}$. Za vsak $w \in W_i$ velja $(A - \lambda_i I)^{r_i} w = 0$. Če to pomnožimo z A, dobimo $A(A - \lambda_i I)^{r_i} w = 0$. Ker je $A(A - \lambda_i I)^{r_i} = (A - \lambda_i I)^{r_i} A$, odtod sledi $(A - \lambda_i I)^{r_i} Aw = 0$. Torej $Aw \in W_i$. Dokaz ostalih točk je še lažji.

TRDITEV: vsak **netrivialen invarianten podprostor** za matriko **A** vsebuje vsaj en **lastni vektor** matrike **A**

DOKAZ

Dokaz: Naj bo U netrivialen invarianten podprostor za A. Ker je $U \neq \{0\}$, ima U bazo, recimo $\mathcal{B} = \{u_1, \dots, u_m\}$. Ker je U invarianten za A, lahko definiramo linearno preslikavo $L\colon U \to U$ z $L(u) = Au$.

Naj bo $\begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix}$ lastni vektor matrike $[L]_{\mathcal{B}}$ za lastno vrednost λ. Očitno $v := x_1 u_1 + \dots + x_m u_m$ pripada U. Pokažimo, da je v lastni vektor za A. Velja namreč $[Lv]_{\mathcal{B}} = [L]_{\mathcal{B}}[v]_{\mathcal{B}} = \lambda[v]_{\mathcal{B}} = [\lambda v]_{\mathcal{B}}$. Torej je $Lv = \lambda v$.

TRDITEV: **presek dveh različnih korenskih podprostorov** matrike **A** je **trivialen**

DOKAZ

Dokaz. Ker sta korenska podprostora W_i in W_j invariantna za A, je invarianten za A tudi njun presek. Če je njun presek netrivialen, potem po Trditvi 1 vsebuje lastni vektor za A. Torej je $Av = \lambda v$ za nek neničeln $v \in W_i \cap W_j$. Odtod sledi, da za vsak polinom $p(x)$ velja $p(A)v = p(\lambda)v$. Če vzamemo $p(x) = (x - \lambda_i)^{r_i}$, dobimo $0 = (A - \lambda_i I)^{r_i} v = (\lambda - \lambda_i)^{r_i} v$, odkoder sledi $\lambda = \lambda_i$. Če pa vzamemo $p(x) = (x - \lambda_j)^{r_j}$, potem dobimo $0 = (A - \lambda_j I)^{r_j} v = (\lambda - \lambda_j)^{r_j} v$, odkoder sledi $\lambda = \lambda_j$. Torej je $\lambda_i = \lambda_j$. Odtod sledi $W_i = W_j$, kar je v nasprotju s predpostavko.

TRDITEV: vsota vseh **korenskih podprostorov** matrike **A** je enaka $\mathbf{C^n}$

DOKAZ

Dokaz: Če v oceno $n(L_1 \cdots L_k) \leq n(L_1) + \dots + n(L_k)$ iz prejšnjega poglavja, vstavimo $L_i = (A - \lambda_i I)^{r_i}$ in upoštevamo $L_1 \cdots L_k = m_A(A) = 0$ ter $n(L_i) = \dim \mathrm{Ker}(A - \lambda_i I)^{r_i} = \dim W_i$, dobimo, da velja ocena $n \leq \dim W_1 + \dots + \dim W_k$. Po opombi zgoraj (ki ste jo delali na vajah) iz Trditve 3 sledi, da je $\dim(W_1 + \dots + W_k) = \dim W_1 + \dots + \dim W_k$. Ker je torej $\dim(W_1 + \dots + W_k) \geq n$, velja $W_1 + \dots + W_k = \mathbb{C}^n$.

Korenski podprostori

→ $\boldsymbol{\lambda_1,\dots,\lambda_k}$ vse paroma **različne lastne vrednosti** matrike **A**

$p_A(x) = (-1)^n(x - \lambda_1)^{n_1} \cdots (x - \lambda_k)^{n_k}$ $\quad m_A(x) = (x - \lambda_1)^{r_1} \cdots (x - \lambda_k)^{r_k}$

→ **Ker(A − $\boldsymbol{\lambda_i}$ I)$^{\mathbf{r_i}}$** je vektorski podprostor v $\mathbf{C^n}$ $\quad 1 \leq r_1 \leq n_1, \dots, 1 \leq r_k \leq n_k$
→ pravimo da je **korenski podprostor**
→ neničelni elementi so **korenski vektorji**
→ rabimo pri konstrukciji **jordanske kanonične forme** matrike A

KORENSKI RAZCEP

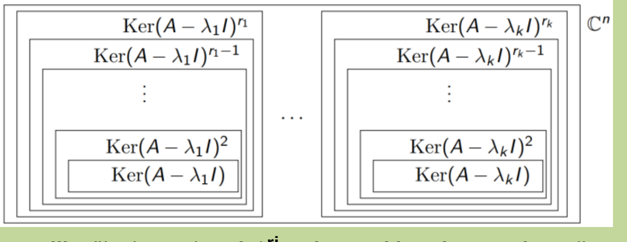
Velja $\mathrm{Ker}(A - \lambda_i I) \subset \mathrm{Ker}(A - \lambda_i I)^2 \subset \dots \subset \mathrm{Ker}(A - \lambda_i I)^{r_i} = \mathrm{Ker}(A - \lambda_i I)^{r_i+1} = \mathrm{Ker}(A - \lambda_i I)^{r_i+2} = \dots$, kjer je inkluzija stroga

$\dim \mathrm{Ker}(A - \lambda_i I)^{r_i} = n_i$, se pravi, da je dimenzija korenskega podprostora A za λ_i enaka algebraični večkratnosti λ_i.

$\mathbb{C}^n = \bigoplus_{i=1}^k \mathrm{Ker}(A - \lambda_i I)^{r_i}$, kar pomeni, da za vsak $w \in \mathbb{C}^n$ obstajajo natanko določeni $w_i \in \mathrm{Ker}(A - \lambda_i I)^{r_i}$, ki zadoščajo $w = \sum_{i=1}^k w_i$.

KORENSKI RAZCEP

→ označimo z $\mathbf{W_i}$ = **Ker(A − $\boldsymbol{\lambda_i}$I)$^{\mathbf{r_i}}$** korenski podprostor **A** za $\boldsymbol{\lambda_i}$
→ $\mathbf{V_i}$ = **Ker(A − $\boldsymbol{\lambda_i}$I)** pa lastni podprostor **A** za $\boldsymbol{\lambda_i}$
→ iz prve točke sledi da $\mathbf{V_i}$ **vsebovan** v $\mathbf{W_i}$ natanko ko $\mathbf{r_i}$ **= 1**



→ **velike** škatle **Ker(A − $\boldsymbol{\lambda_i}$I)$^{\mathbf{r_i}}$** so **korenski podprostori** matrike **A**
→ njihova **vsota** je $\mathbf{C^n}$
→ **male** škatle **Ker(A − $\boldsymbol{\lambda_i}$I)** so **lastni podprostori** matrike **A**

TRDITEV: če vektorji $\mathbf{w_1} \in \mathbf{W_1},\dots,\mathbf{w_k} \in \mathbf{W_k}$ zadoščajo $\mathbf{w_1} + \dots + \mathbf{w_k} = \mathbf{0}$ velja $\mathbf{w_1} = \dots = \mathbf{w_k} = \mathbf{0}$

DOKAZ

Dokaz: Dokazali bomo, da za vsak $i = 1, \dots, k$ velja naslednja trditev:

(T_i) **Če vektorji** $w_1 \in W_1, \dots, w_i \in W_i$ **zadoščajo** $w_1 + \dots + w_i = 0$, **potem velja** $w_1 = \dots = w_i = 0$.

Baza indukcije: Trditev (T_1) je očitna.

Indukcijski korak: Recimo, da velja trditev (T_i), kjer $i < k$. Radi bi dokazali trditev (T_{i+1}). Vzemimo take vektorje $w_1 \in W_1, \dots, w_i \in W_i, w_{i+1} \in W_{i+1}$, da velja $w_1 + \dots + w_i + w_{i+1} = 0$. Če to pomnožimo z $(A - \lambda_{i+1} I)^{r_{i+1}}$ z leve, dobimo $w_1' + \dots + w_i' + 0 = 0$. Ker je vsak korenski podprostor W_j invarianten in ker vsebuje w_j, vsebuje tudi $w_j' := (A - \lambda_{i+1} I)^{r_{i+1}} w_j$. Iz $w_1' + \dots + w_i' = 0$ torej po indukcijski predpostavki sledi, da velja $w_1' = \dots = w_i' = 0$. Zato $w_1, \dots, w_i \in W_{i+1}$. Po Trditvi 2 je $W_1 \cap W_{i+1} = \{0\}, \dots, W_i \cap W_{i+1} = \{0\}$. Odtod sledi, da je $w_1 = \dots = w_i = 0$. Odtod sledi še $w_{i+1} = 0$.

Opomba: Recimo, da je $\mathcal{B}_i$ baza za korenski podprostor W_i. Iz Trditve 3 sledi, da je $\mathcal{B}_1 \cup \dots \cup \mathcal{B}_k$ baza za vsoto $W_1 + \dots + W_k$ vseh korenskih podprostorov. Torej je $\dim(W_1 + \dots + W_k) = \dim W_1 + \dots + \dim W_k$.

$P_i := [v_{i,1} \ \dots \ v_{i,t_i}]$

Označimo $t_i := \dim W_i$ za vsak $i = 1, \dots, k$. Radi bi pokazali, da je $t_i = n_i$. Naj bo $\mathcal{B}_i = \{v_{i,1}, \dots, v_{i,t_i}\}$ baza za W_i. Ker je podprostor W_i invarianten za A, obstajajo taka števila $\alpha_{i,j,j'}$, da velja

$$\begin{aligned} Av_{i,1} &= \alpha_{i,1,1}v_{i,1} + \dots + \alpha_{i,1,t_i}v_{i,t_i} \\ &\vdots \\ Av_{i,t_i} &= \alpha_{i,t_i,1}v_{i,1} + \dots + \alpha_{i,t_i,t_i}v_{i,t_i} \end{aligned} \qquad A_i = \begin{bmatrix} \alpha_{i,1,1} & \dots & \alpha_{i,t_i,1} \\ \vdots & \ddots & \vdots \\ \alpha_{i,1,t_i} & \dots & \alpha_{i,t_i,t_i} \end{bmatrix}$$

$$A\,[P_1 \dots P_k] = [P_1 \dots P_k] \begin{bmatrix} A_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & A_k \end{bmatrix}$$

Matrike $P := [P_1 \dots P_k]$ je obrnljiva, ker je (po že dokazani točki (3) v izreku) unija baz $\mathcal{B}_i$ baza za $\mathbb{C}^n$. Označimo z A' bločno diagonalno matriko iz A_i-jev. Po formuli (1) je $A' = P^{-1}AP$, torej imata A in A' enak karakteristični polinom

$$\det(A - xI) = \det(A_1 - xI) \cdots \det(A_k - xI). \qquad (2)$$

Pokažimo, da je λ_i edina lastna vrednost matrike A_i. Potem je $\det(A_i - xI) = (\lambda_i - x)^{t_i}$. To vstavimo v formulo (2) in dobimo $t_i = n_i$. Naj bo μ_i poljubna lastna vrednost matrike A_i in naj bo $u_i \in \mathbb{C}^{t_i}$ pripadajoči lastni vektor. Potem je

$$A(P_i u_i) = (AP_i)u_i = (P_i A_i)u_i = P_i(A_i u_i) = P_i(\mu_i u_i) = \mu_i P_i u_i \qquad (3)$$

Ker je $P_i u_i$ linearna kombinacija stolpcev P_i in ker so stolpci P_i v W_i je $P_i u_i \in W_i$. Poleg tega je $P_i u_i \neq 0$, ker je $u_i \neq 0$ in ker so stolpci P_i linearno neodvisni. Po definiciji W_i je $(A - \lambda_i I)^{r_i} P_i u_i = 0$. Iz formule (3) sledi, da je $(A - \lambda_i I)^{r_i} P_i u_i = (\mu_i - \lambda_i)^{r_i} P_i u_i$. Torej je $\mu_i = \lambda_i$.

Dokaz točke (1) v izreku bomo razdelili v več korakov.

1. korak Če je $m \le m'$, potem velja $\mathrm{Ker}(A - \lambda_i I)^m \subseteq \mathrm{Ker}(A - \lambda_i I)^{m'}$.

Za vsak $v \in \mathrm{Ker}(A - \lambda_i I)^m$ velja $(A - \lambda_i I)^m v = 0$. Pomnožimo to z leve z $(A - \lambda_i I)^{m'-m}$ in dobimo $(A - \lambda_i I)^{m'} v = 0$. Torej je $v \in \mathrm{Ker}(A - \lambda_i I)^{m'}$.

2. korak Za vsak $r_i' \ge r_i$ je $\mathrm{Ker}(A - \lambda_i I)^{r_i'} = \mathrm{Ker}(A - \lambda_i I)^{r_i}$.

Označimo $W_i' := \mathrm{Ker}(A - \lambda_i I)^{r_i'}$ in $n_i' = \dim W_i'$. Po 1. koraku je $W_i \subseteq W_i'$, zato je $n_i \le n_i'$. Kot v dokazu Trditve 3 vidimo, da za poljubne $w_i' \in W_i'$, ki zadoščajo $w_1' + \ldots + w_k' = 0$, velja $w_1' = \ldots = w_k' = 0$. Kot v opombi za Trditvijo 3 odtod sledi, da je $n_1' + \ldots + n_k' = n$. Odtod in iz $n_i \le n_i'$ sledi, da je $n_i' = n_i$ za vsak i. Torej je $W_i' = W_i$ za vsak i.

3. korak Za vsak i je $\mathrm{Ker}(A - \lambda_i I)^{r_i - 1} \neq \mathrm{Ker}(A - \lambda_i I)^{r_i}$.

Če bi za nek i veljal enačaj, potem bomo pokazali, da bi polinom $m_i(x) := m_A(x)/(x - \lambda_i)$ zadoščal $m_i(A) = 0$, kar bi bilo v nasprotju z definicijo minimalnega polinoma. Vzemimo poljuben $w \in \mathbb{C}^n$.
Po Trditvi 4 obstajajo taki $w_j \in W_j$, da velja $w = \sum_{j=1}^k w_j$.
Za vsak $j \neq i$ velja $(A - \lambda_j)^{r_j} w_j = 0$, odkoder sledi $m_i(A) w_j = 0$.
Za $j = i$ pa velja $(A - \lambda_j)^{r_j - 1} w_j = 0$, torej je tudi $m_i(A) w_j = 0$.
Odtod sledi $m_i(A) w = 0$. Ker je to res za vsak $w \in \mathbb{C}^n$, je $m_i(A) = 0$.

4. korak Če velja $\mathrm{Ker}(A - \lambda_i I)^m \neq \mathrm{Ker}(A - \lambda_i I)^{m+1}$ za nek $m \ge 1$ in nek $i = 1, \ldots, k$, potem velja tudi $\mathrm{Ker}(A - \lambda_i I)^{m-1} \neq \mathrm{Ker}(A - \lambda_i I)^m$.

Predpostavimo, da velja $\mathrm{Ker}(A - \lambda_i I)^{m-1} = \mathrm{Ker}(A - \lambda_i I)^m$.
Dokazujemo, da velja $\mathrm{Ker}(A - \lambda_i I)^m = \mathrm{Ker}(A - \lambda_i I)^{m+1}$. Vzemimo poljuben $v \in \mathrm{Ker}(A - \lambda_i I)^{m+1}$. Potem $(A - \lambda_i)v \in \mathrm{Ker}(A - \lambda_i I)^m$.
Torej $(A - \lambda_i)v \in \mathrm{Ker}(A - \lambda_i I)^{m-1}$ po predpostavki. Odtod sledi, da $v \in \mathrm{Ker}(A - \lambda_i I)^m$. Torej je $\mathrm{Ker}(A - \lambda_i I)^m \supseteq \mathrm{Ker}(A - \lambda_i I)^{m+1}$.
Obratna inkluzija sledi iz 1. koraka.

Jordanska kanonična forma

KORENSKI RAZCEP

$$\begin{bmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{bmatrix} \qquad \begin{bmatrix} J_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & J_m \end{bmatrix}$$

→ **jordanska kletka** matrika oblike:
→ λ je **kompleksno** število
→ **jordanska matrika** je matrika zgoraj kjer so $J_1, \ldots, J_m$ jordanske kletke
→ **jordanska baza:** baza ki je unija jordanskih verig

TRDITEV: vsaka **kompleksna kvadratna** matrika **A** je podobna kaki **jordanski matriki J** to je jordanska kanonična forma za A

Jordanska kanonična forma ni enolična ker če **jordanske kletke** permutiramo spet dobimo **jordansko kletko**

TRDITEV: **jordanska veriga** dolžine **k** je zaporedje neničelnih vektorjev $\mathbf{v_1}, \ldots, \mathbf{v_k}$ iz $\mathbf{C^n}$ da velja:

$$(A - \lambda I)v_1 = 0,\ (A - \lambda I)v_2 = v_1, \ldots, (A - \lambda I)v_k = v_{k-1}$$

Matrika $\begin{bmatrix} v_1 & v_2 & \ldots & v_k \end{bmatrix}$ ni kvadratna.
Stolpci so linearno neodvisni.

$$A \begin{bmatrix} v_1 & v_2 & \ldots & v_k \end{bmatrix} = \begin{bmatrix} v_1 & v_2 & \ldots & v_k \end{bmatrix} \begin{bmatrix} \lambda & 1 & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & 1 \\ 0 & 0 & \ldots & \lambda \end{bmatrix}$$

$$Av_1 = \lambda v_1,\ Av_2 = v_1 + \lambda v_2,\ \ldots,\ Av_k = v_{k-1} + \lambda v_k$$

DOKAZ JORDANSKE BAZE

$$P = \begin{bmatrix} P_1 & \ldots & P_m \end{bmatrix}$$

Če uspemo najti jordansko bazo za $\mathbb{C}^n$, je dokaz izreka o jordanski kanonični formi končan. Elemente te baze namreč zložimo v matriko

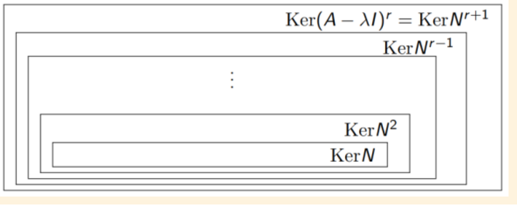
kjer so stolpci podmatrike P_i ravno elementi i-te Jordanske verige v tej bazi. Po formuli $(*)$ obstajajo take Jordanske kletke $J_1, \ldots, J_m$, da velja $AP_i = P_i J_i$ za vsak i. Odtod sledi, da velja

$$AP = P \begin{bmatrix} J_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & J_m \end{bmatrix}$$

Torej je matrika A res podobna Jordanski matriki.

Da bi našli jordansko bazo za $\mathbb{C}^n$, je dovolj dovolj poiskati jordansko bazo za vsak korenski podprostor posebej. Po izreku o korenskem razcepu je namreč $\mathbb{C}^n$ direktna vsota vseh korenskih podprostorov matrike A, torej je unija baz vseh korenskih podprostorov baza za cel prostor $\mathbb{C}^n$.

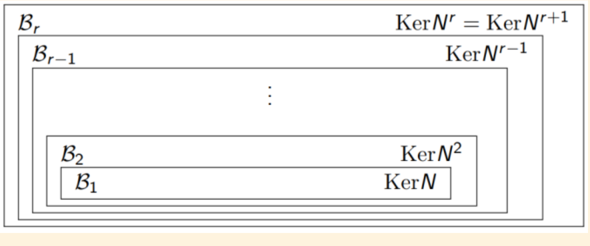
Korenski podprostor $\mathrm{Ker}(A - \lambda I)^r$, ki ustreza lastni vrednosti λ si predstavljamo kot veliko škatlo, v kateri gnezdijo majhne škatle. Najmanjša od teh škatel je lastni podprostor $\mathrm{Ker}(A - \lambda I)$ za λ.



Naj bo λ lastna vrednost matrike A. Označimo $N = A - \lambda I$. Opišimo konstrukcijo jordanske baze za korenski podprostor $\mathrm{Ker} N^r$.

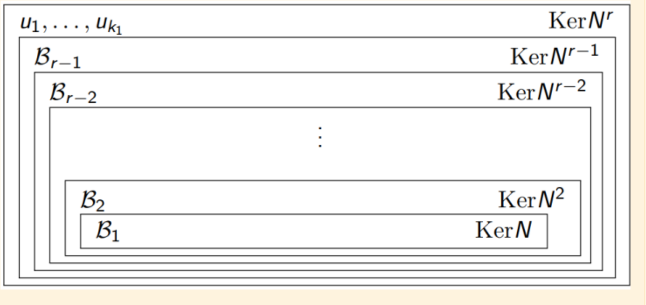
1. korak Računanje pomožnih baz.

Najprej za vsak $i = 1, \ldots, r$ izberemo poljubno bazo $\mathcal{B}_i$ za $\mathrm{Ker} N^i$.



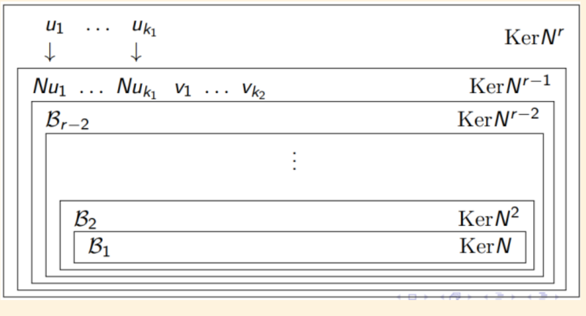
2. korak Popravljanje pomožne baze $\mathcal{B}_r$.

Najprej izberimo take elemente $u_1, \ldots, u_{k_1} \in \mathcal{B}_r$, ki dopolnijo $\mathcal{B}_{r-1}$ do baze za $\mathrm{Ker} N^r$. Potem je $\mathcal{B}_{r-1} \cup \{u_1, \ldots, u_{k_1}\}$ popravek pomožne baze $\mathcal{B}_r$.



3. korak Popravljanje pomožne baze $\mathcal{B}_{r-1}$.

Najprej vektorje $u_1, \ldots, u_{k_1} \in \mathrm{Ker} N^r$ pomnožimo z matriko N.
Dobljeni vektorji $Nu_1, \ldots, Nu_{k_1}$ ležijo v $\mathrm{Ker} N^{r-1}$.
Množica $\mathcal{B}_{r-2} \cup \{Nu_1, \ldots, Nu_{k_1}\}$ je linearno neodvisna.
Izberimo take elemente $v_1, \ldots, v_{k_2} \in \mathcal{B}_{r-1}$, ki dopolnijo linearno neodvisno množico $\mathcal{B}_{r-2} \cup \{Nu_1, \ldots, Nu_{k_1}\}$ do baze za $\mathrm{Ker} N^{r-1}$. Potem je $\mathcal{B}_{r-2} \cup \{Nu_1, \ldots, Nu_{k_1}\} \cup \{v_1, \ldots, v_{k_2}\}$ popravek pomožne baze $\mathcal{B}_{r-1}$.



4. korak Popravljanje pomožne baze $\mathcal{B}_{r-2}$.

Najprej vektorje $Nu_1, \ldots, Nu_{k_1}, v_1, \ldots, v_{k_2} \in \mathrm{Ker} N^{r-1}$ pomnožimo z N.
Dobljeni vektorji $N^2u_1, \ldots, N^2u_{k_1}, Nv_1, \ldots, Nv_{k_2}$ ležijo v $\mathrm{Ker} N^{r-2}$.
Množica $\mathcal{B}_{r-3} \cup \{N^2u_1, \ldots, N^2u_{k_1}, Nv_1, \ldots, Nv_{k_2}\}$ je LN.
Izberimo take elemente $w_1, \ldots, w_{k_3} \in \mathcal{B}_{r-2}$, ki dopolnijo LN množico $\mathcal{B}_{r-3} \cup \{N^2u_1, \ldots, N^2u_{k_1}, Nv_1, \ldots, Nv_{k_2}\}$ do baze za $\mathrm{Ker} N^{r-2}$.

$u_1 \quad \dots \quad u_{k_1}$ $\qquad \mathrm{Ker}\,N^r$

$\downarrow \qquad \downarrow$

$Nu_1 \quad \dots \quad Nu_{k_1} \quad v_1 \quad \dots \quad v_{k_2}$ $\qquad \mathrm{Ker}\,N^{r-1}$

$\downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow$

$N^2u_1 \ \dots \ N^2u_{k_1} \ Nv_1 \ \dots \ Nv_{k_2} \ w_1 \ \dots \ w_{k_3}$ $\qquad \mathrm{Ker}\,N^{r-2}$

$\vdots$

$\mathcal{B}_2$ $\qquad \mathrm{Ker}\,N^2$

$\mathcal{B}_1$ $\qquad \mathrm{Ker}\,N$

Vsak stolpec v zgornji skici nam da eno jordansko verigo. Imamo torej k_1 jordanskih verig dolžine r, k_2 jordanskih verig dolžine $r-1$, k_3 jordanskih verig dolžine $r-2$, …, k_r jordanskih verig dolžine 1. Skupaj je to $k_1 + \ldots + k_r = \dim \mathrm{Ker}\,N$ jordanskih verig. Jordanskih verig za lastno vrednost λ je torej toliko kot je njena geometrijska večkratnost.

Postopek nadaljujemo, dokler ne popravimo vseh pomožnih baz. Na koncu dobimo naslednjo skico:

$u_i \in \mathrm{Ker}\,N^r \setminus \mathrm{Ker}\,N^{r-1}$ za $i = 1, \ldots, k_1$

$\downarrow$

$Nu_i \qquad v_j \in \mathrm{Ker}\,N^{r-1} \setminus \mathrm{Ker}\,N^{r-2}$ za $j = 1, \ldots, k_2$

$\downarrow \qquad \downarrow$

$N^2u_i \qquad Nv_j \qquad w_k \in \mathrm{Ker}\,N^{r-2} \setminus \mathrm{Ker}\,N^{r-3}$

$\vdots \qquad \vdots \qquad \vdots \qquad$ za $k = 1, \ldots, k_3$

$\downarrow \qquad \downarrow \qquad \downarrow$

$N^{r-2}u_i \quad N^{r-3}v_j \quad N^{r-4}w_k \quad \dots \quad t_l \in \mathrm{Ker}\,N^2 \setminus \mathrm{Ker}\,N$

$\downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow$ za $l = 1, \ldots, k_{r-1}$

$N^{r-1}u_i \quad N^{r-2}v_j \quad N^{r-3}w_k \quad \dots \quad Nt_l \qquad z_m \in \mathrm{Ker}\,N$

za $m = 1, \ldots, k_r$

TRDITEV:

- **K** naravno število in **N** matrika
- $\mathbf{B_{k-1}}$ baza za **Ker** $\mathbf{N^{k-1}}$
- $\mathbf{B_k}$ baza za **Ker** $\mathbf{N^k}$
- $\mathbf{C_{k+1}}$ dopolnitev $\mathbf{B_k}$ do baze za **Ker** $\mathbf{N^{k+1}}$
- potem je $\mathbf{B_{k-1}} \cup \mathbf{N(C_{k+1})}$ linearno **neodvisna**
- lahko dopolnimo do **baze Ker** $\mathbf{N^k}$ s podmnožico od $\mathbf{B_k}$

DOKAZ

Dokaz: Naj bo $\mathcal{B}_{k-1} = \{e_1, \ldots, e_r\}$, $\mathcal{B}_k = \{f_1, \ldots, f_s\}$ in $\mathcal{C}_{k+1} = \{g_1, \ldots, g_t\}$. Ker je $\mathcal{C}_{k+1}$ podmnožica $\mathrm{Ker}\,N^{k+1}$, je $N(\mathcal{C}_{k+1}) := \{Ng_1, \ldots, Ng_t\}$ podmnožica $\mathrm{Ker}\,N^k$. Preverimo, da je množica $\mathcal{B}_{k-1} \cup N(\mathcal{C}_{k+1})$ linearno neodvisna. Recimo, da je

$$\alpha_1 e_1 + \ldots + \alpha_k e_k + \beta_1 Ng_1 + \ldots + \beta_t Ng_t = 0$$

Pomnožimo z N^{k-1} in upoštevajmo, da $e_1, \ldots, e_r \in \mathrm{Ker}\,N^{k-1}$. Dobimo $\beta_1 N^k g_1 + \ldots + \beta_t N^k g_t = 0$, torej $\beta_1 g_1 + \ldots + \beta_t g_t \in \mathrm{Ker}\,N^k$. Ker je $f_1, \ldots, f_s$ baza za $\mathrm{Ker}\,N^k$, lahko razvijemo

$$\beta_1 g_1 + \ldots + \beta_t g_t = \gamma_1 f_1 + \ldots + \gamma_s f_s.$$

Ker je $f_1, \ldots, f_s, g_1, \ldots, g_t$ baza za $\mathrm{Ker}\,N^{k+1}$, velja $\beta_1 = \ldots = \beta_t = 0$ (in $\gamma_1 = \ldots = \gamma_s = 0$), torej iz (1) dobimo $\alpha_1 e_1 + \ldots + \alpha_k e_k = 0$. Ker je $e_1, \ldots, e_r$ baza za $\mathrm{Ker}\,N^{k-1}$, odtod sledi $\alpha_1 = \ldots = \alpha_r = 0$. Torej je množica $\mathcal{B} := \{e_1, \ldots, e_r, Ng_1, \ldots, Ng_t\}$ res linearno neodvisna. Če je $\mathrm{Lin}\mathcal{B} = \mathrm{Ker}\,N^k$, potem končamo. Če $\mathrm{Lin}\mathcal{B} \neq \mathrm{Ker}\,N^k$ potem $\mathrm{Lin}\mathcal{B}$ ne more vsebovati vseh f_j, saj so ti baza za $\mathrm{Ker}\,N^k$. Torej obstaja tak indeks i_1, da $f_{i_1} \notin \mathrm{Lin}\mathcal{B}$. Podobno konstruiramo tak i_2, da $f_{i_2} \notin \mathrm{Lin}(\mathcal{B} \cup \{f_{i_1}\})$. S postopkom nadaljujemo dokler $\mathcal{B} \cup \{f_{i_1}, \ldots, f_{i_{s-t}}\}$ ni baza za $\mathrm{Ker}\,N^k$.

Funkcije matrik

→ poznamo **razcep** matrike **A**
→ računamo **potence** matrike **A** z **potencami** matrike **J**

$$A^n = (PJP^{-1})(PJP^{-1})\cdots(PJP^{-1}) = PJ^nP^{-1}$$

→ ker je **J bločno diagonalna** matrika sestavljena iz **Jordanskih kletk**
→ rešujemo **linearne rekurzivne enačbe**

$$\begin{bmatrix} \lambda & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \dots & \dots & \dots & \lambda \end{bmatrix}^n = \begin{bmatrix} \lambda^n & n\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \dots & \binom{n}{k-1}\lambda^{n-k+1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \binom{n}{2}\lambda^{n-2} \\ \vdots & & & \ddots & n\lambda^{n-1} \\ 0 & \dots & \dots & \dots & \lambda^n \end{bmatrix}$$

DOKAZ

Jordansko kletko lahko zapišemo v obliki **λI** + **N**, kjer je N **matrika**, ki ima na prvi **naddiagonali** same **enke**, drugod pa same **ničle**. .**Potence** matrike N izračunamo. Opazimo, da je $\mathbf{N^i}$ matrika, ki ima na naddiagonali **i** same **enke**, drugod pa same **ničle**. Ker je **N k** × **k** matrika, nima **k-te** naddiagonale, zato je $\mathbf{N^k}$ = **0**.

$$(\lambda I + N)^n = \sum_{i=1}^{n} \binom{n}{i} \lambda^{n-i} N^i = \sum_{i=1}^{k-1} \binom{n}{i} \lambda^{n-i} N^i \qquad f(x) = \sum_{n=0}^{\infty} c_n x^n$$

In vstavimo namesto **x razcep** $A = PJP^{-1}$

$$f(A) = \sum_{n=0}^{\infty} c_n A^n = \sum_{n=0}^{\infty} c_n PJ^nP^{-1} = P\Big(\sum_{n=0}^{\infty} c_n J^n\Big)P^{-1} = Pf(J)P^{-1}$$

Računanje **f** (**J**), kjer je **J jordanska matrika**, lahko prevedemo na primer, ko je **J jordanska kletka**.

$$f\left(\begin{bmatrix} \lambda & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \dots & \dots & \dots & \lambda \end{bmatrix}\right) = \begin{bmatrix} f(\lambda) & f'(\lambda) & \frac{f''(\lambda)}{2} & \dots & \frac{f^{k-1}(\lambda)}{(k-1)!} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \frac{f''(\lambda)}{2} \\ \vdots & & & \ddots & f'(\lambda) \\ 0 & \dots & \dots & \dots & f(\lambda) \end{bmatrix}$$

$$f\left(\begin{bmatrix} J_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & J_m \end{bmatrix}\right) = \begin{bmatrix} f(J_1) & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & f(J_m) \end{bmatrix}$$

VEKTORSKI PROSTORI Z SKALARNIM PRODUKTOM

Skalarni produkt nad R:

→ vektorski prostor **V**
→ preslikava ki vsakemu **paru vektorjev** **u**, **v** ∈ **V** priredi **realno število** ⟨ **u**, **v** ⟩
→ za vsak neničeln **v** ∈ **V** velja ⟨ **u**, **v** ⟩ > **0**
→ za vsaka **u**, **v** ∈ **V** velja ⟨ **u**, **v** ⟩ = ⟨ **v**, **u** ⟩
→ za vsake $\mathbf{u_1}$, $\mathbf{u_2}$, **v** ∈ **V** in $\mathbf{\alpha_1}$, $\mathbf{\alpha_2}$ ∈ **R** velja ⟨ $\mathbf{\alpha_1 u_1 + \alpha_2 u_2}$, **v** ⟩ = $\mathbf{\alpha_1}$ ⟨ $\mathbf{u_1}$, **v** ⟩ + $\mathbf{\alpha_2}$ ⟨ $\mathbf{u_2}$, **v** ⟩

Skalarni produkt nad C:

→ vektorski prostor **V**
→ preslikava ki vsakemu **paru vektorjev** **u**, **v** ∈ **V** priredi **kompleksno število** ⟨ **u**, **v** ⟩
→ za vsak neničeln **v** ∈ **V** velja ⟨ **u**, **v** ⟩ > **0** in **pripada R**
→ za vsaka **u**, **v** ∈ **V** velja ⟨ **u**, **v** ⟩ = $\overline{\langle \mathbf{v}, \mathbf{u} \rangle}$
→ za vsake $\mathbf{u_1}$, $\mathbf{u_2}$, **v** ∈ **V** in $\mathbf{\alpha_1}$, $\mathbf{\alpha_2}$ ∈ **C** velja ⟨ $\mathbf{\alpha_1 u_1 + \alpha_2 u_2}$, **v** ⟩ = $\mathbf{\alpha_1}$ ⟨ $\mathbf{u_1}$, **v** ⟩ + $\mathbf{\alpha_2}$ ⟨ $\mathbf{u_2}$, **v** ⟩

druga lastnost je **konjugirana simetričnost**

druga posledica velja tudi tukaj

prvi lastnosti pravimo **pozitivna definitnost**, drugi **simetričnost**, tretji pa **linearnost** v **prvem faktorju**

POSLEDICA:

$$\langle v, 0 \rangle = \langle 0, v \rangle = 0$$

POSLEDICA: konjugirana linearnost v **drugem** faktorju

$$\langle u, \beta_1 v_1 + \beta_2 v_2 \rangle = \bar{\beta}_1 \langle u, v_1 \rangle + \bar{\beta}_2 \langle u, v_2 \rangle$$

POSLEDICA: linearnost v **drugem** faktorju

$$\langle u, \beta_1 v_1 + \beta_2 v_2 \rangle = \beta_1 \langle u, v_1 \rangle + \beta_2 \langle u, v_2 \rangle$$

NORMA $\|v\| = \sqrt{\langle v, v \rangle}$

→ V **realen** ali **kompleksen** vektorski prostor s **skalarnim** produktom

CAUCHY SCHWARTZOVA NEENAKOST

$\rightarrow$ **V** vektorski prostor s skalarnim produktom

$$|\langle u, v\rangle| \leq \|u\|\|v\|$$

$\|v\| > 0$

$\|\alpha v\| = |\alpha|\|v\|$

$\|u+v\| \leq \|u\| + \|v\|$

Če je V vektorski prostor nad $\mathbb{R}$, potem za vsaka $u, v \in V$ velja

$$\langle u, v\rangle = \frac{1}{4}\left(\|u+v\|^2 - \|u-v\|^2\right)$$

Če je V vektorski prostor nad $\mathbb{C}$, potem za vsaka $u, v \in V$ velja

$$\langle u, v\rangle = \frac{1}{4}\sum_{k=0}^{3} i^k \|u + i^k v\|^2$$

DOKAZ

Naj bo $\alpha = \langle v, v\rangle$, $\beta = \langle u, v\rangle$ in $w = \alpha u - \beta v$.

$$0 \leq \langle w, w\rangle = \alpha\bar{\alpha}\langle u, u\rangle - \alpha\bar{\beta}\langle u, v\rangle - \beta\bar{\alpha}\langle v, u\rangle + \beta\bar{\beta}\langle v, v\rangle$$

$$\alpha\bar{\beta}\langle u, v\rangle = \beta\bar{\alpha}\langle v, u\rangle = \beta\bar{\beta}\langle v, v\rangle = |\langle u, v\rangle|^2\langle v, v\rangle = |\langle u, v\rangle|^2\|v\|^2$$

$$\alpha\bar{\alpha}\langle u, u\rangle = |\langle v, v\rangle|^2\langle u, u\rangle = \|v\|^4\|u\|^2$$

$$0 \leq \langle w, w\rangle = \|v\|^4\|u\|^2 - |\langle u, v\rangle|^2\|v\|^2$$

Če je $v \neq 0$, lahko krajšamo $\|v\|^2$ in dobimo $|\langle u, v\rangle|^2 \leq \|v\|^2\|u\|^2$

S korenjenjem potem dobimo Cauchy-Schwartzovo neenakost. Če je $v = 0$, potem Cauchy-Schwartzova neenakost očitno drži.

DOKAZ

Dokaz: Lastnost (1) sledi iz pozitivne definitnosti skalarnega produkta.

Lastnost (2) sledi iz $\|\alpha v\|^2 = \langle \alpha v, \alpha v\rangle = \alpha\bar{\alpha}\langle v, v\rangle = |\alpha|^2\|v\|^2$, kjer smo upoštevali linearnost v prvem in konjugirano linearnost v drugem faktorju.

Lastnost (3) sledi iz $\|u+v\|^2 = \langle u+v, u+v\rangle =$
$\langle u, u\rangle + \langle u, v\rangle + \langle v, u\rangle + \langle v, v\rangle = \langle u, u\rangle + 2\mathrm{Re}(\langle u, v\rangle) + \langle v, v\rangle \leq$
$\|u\|^2 + 2|\langle u, v\rangle| + \|v\|^2 \leq \|u\|^2 + 2\|u\|\|v\| + \|v\|^2 = (\|u\| + \|v\|)^2$.
Upoštevali smo, da za $z = a + ib$ velja $z + \bar{z} = 2a \leq 2\sqrt{a^2+b^2} = 2|z|$.
Uporabili smo tudi Cauchy-Schwartzovo neenakost.

DOKAZ

v **realnem** primeru velja:

$$\sum_{k=0}^{1}(-1)^k = \sum_{k=0}^{1}(-1)^{3k} = 0 \quad \text{in} \quad \sum_{k=0}^{1}(-1)^{2k} = 2.$$

$$\sum_{k=0}^{1}(-1)^k\|u + (-1)^k v\|^2 = \sum_{k=0}^{1}(-1)^k\langle u + (-1)^k v, u + (-1)^k v\rangle =$$
$$= \sum_{k=0}^{1}\Big((-1)^k\langle u, u\rangle + (-1)^{2k}\langle v, u\rangle + (-1)^{2k}\langle u, v\rangle + (-1)^{3k}\langle v, v\rangle\Big) =$$
$$= \Big(\sum_{k=0}^{1}(-1)^k\Big)\langle u, u\rangle + \Big(\sum_{k=0}^{1}(-1)^{2k}\Big)\langle v, u\rangle + \Big(\sum_{k=0}^{1}(-1)^{2k}\Big)\langle u, v\rangle +$$
$$+\Big(\sum_{k=0}^{1}(-1)^{3k}\Big)\langle v, v\rangle = 2\langle v, u\rangle + 2\langle u, v\rangle = 4\langle u, v\rangle,$$

v **kompleksnem** primeru :

$$\sum_{k=0}^{3} i^k = \sum_{k=0}^{3} i^{2k} = \sum_{k=0}^{3} i^{2k}\bar{i}^k = 0 \quad \text{in} \quad \sum_{k=0}^{3} i^k\bar{i}^k = 4.$$

$$\sum_{k=0}^{3} i^k\|u + i^k v\|^2 = \sum_{k=0}^{3} i^k\langle u + i^k v, u + i^k v\rangle =$$
$$= \sum_{k=0}^{3}\Big(i^k\langle u, u\rangle + i^{2k}\langle v, u\rangle + i^k\bar{i}^k\langle u, v\rangle + i^{2k}\bar{i}^k\langle v, v\rangle\Big) =$$
$$= \Big(\sum_{k=0}^{3} i^k\Big)\langle u, u\rangle + \Big(\sum_{k=0}^{3} i^{2k}\Big)\langle v, u\rangle + \Big(\sum_{k=0}^{3} i^k\bar{i}^k\Big)\langle u, v\rangle +$$
$$+\Big(\sum_{k=0}^{3}(i^{2k}\bar{i}^k)\Big)\langle v, v\rangle = 4\langle u, v\rangle,$$

ORTOGONALNE BAZE

- $\rightarrow$ kot med vektorjema v $\mathbf{R}^{\mathbf{n}}$ je **pravi** natanko tedaj ko **standardni skalarni produkt** enak **nič**
- $\rightarrow$ tako definiramo pravokotnost tudi drugje
- $\rightarrow$ **ničelni** vektor pravokoten na **vse**
- $\rightarrow$ **ničelni** vektor **ni** pravokoten sam **nase**
- $\rightarrow$ **množica** je **ortogonalna** če ne vsebuje ničelnega vektorja in so vektorji **paroma pravokotni**
- $\rightarrow$ **ortogonalna množica** v **V** ki je **ogrodje** je **ortogonalna baza**

TRDITEV: vsaka ortogonalna množica je **linearno neodvisna**

DOKAZ

Dokaz: Recimo, da so $v_1, \ldots, v_k$ neničelni paroma pravokotni vektorji iz V. Če je $\alpha_1 v_1 + \ldots + \alpha_k v_k = 0$ za neke skalarje $\alpha_1, \ldots, \alpha_k$, moramo pokazati, da velja $\alpha_1 = \ldots = \alpha_k = 0$. Opazimo, da za vsak i velja $0 = \langle 0, v_i\rangle =$
$= \langle \alpha_1 v_1 + \ldots + \alpha_k v_k, v_i\rangle = \alpha_1\langle v_1, v_i\rangle + \ldots + \alpha_i\langle v_i, v_i\rangle + \ldots + \alpha_k\langle v_k, v_i\rangle$.
Ker je $\langle v_1, v_i\rangle = \ldots = \langle v_{i-1}, v_i\rangle = \langle v_{i+1}, v_i\rangle = \ldots = \langle v_k, v_i\rangle = 0$, je
$0 = \alpha_i\langle v_i, v_i\rangle$. Ker je $v_i \neq 0$ za vsak i, odtod sledi $\alpha_i = 0$ za vsak i.

ORTONORMIRANE BAZE

$$\langle v_i, v_j\rangle = \begin{cases} 0 & \text{če } i \neq j \\ 1 & \text{če } i = j \end{cases}$$

- $\rightarrow$ vektorji z **normo 1** so **normirani** vektorji
- $\rightarrow$ če vsi elementi v **ortogonalni množici normirani** potem je to **ortonormirana množica**
- $\rightarrow$ ortonormirana množica ki je baza je **ortonormirana baza**

vsak element lahko **normiramo** tako da ga delimo z njegovo **normo**

Gram Schmidtova ortogonalizacija:

$\rightarrow$ če je { $\mathbf{u_1}, \ldots, \mathbf{u_n}$ } **baza** po koncu { $\mathbf{v_1}, \ldots, \mathbf{v_n}$ } **ortogonalna baza**

$$\begin{aligned}
v_1 &= u_1 \\
v_2 &= u_2 - \frac{\langle u_2, v_1\rangle}{\langle v_1, v_1\rangle}v_1 \\
v_3 &= u_3 - \frac{\langle u_3, v_1\rangle}{\langle v_1, v_1\rangle}v_1 - \frac{\langle u_3, v_2\rangle}{\langle v_2, v_2\rangle}v_2 \\
&\vdots \\
v_n &= u_n - \frac{\langle u_n, v_1\rangle}{\langle v_1, v_1\rangle}v_1 - \frac{\langle u_n, v_2\rangle}{\langle v_2, v_2\rangle}v_2 - \ldots - \frac{\langle u_n, v_{n-1}\rangle}{\langle v_{n-1}, v_{n-1}\rangle}v_{n-1}
\end{aligned}$$

DOKAZ

Ker je $v_1 = u_1 \neq 0$, je $\{v_1\}$ ortogonalna.

Recimo, da trditev drži za nek $k < n$.

$$v_{k+1} = u_{k+1} - \sum_{i=1}^{k}\frac{\langle u_{k+1}, v_i\rangle}{\langle v_i, v_i\rangle}v_i$$

dokazujemo z **indukcijo**

$$\begin{aligned}
\langle v_{k+1}, v_j\rangle &= \langle u_{k+1}, v_j\rangle - \sum_{i=1}^{k}\frac{\langle u_{k+1}, v_i\rangle}{\langle v_i, v_i\rangle}\langle v_i, v_j\rangle \\
&= \langle u_{k+1}, v_j\rangle - \frac{\langle u_{k+1}, v_j\rangle}{\langle v_j, v_j\rangle}\langle v_j, v_j\rangle = 0
\end{aligned}$$

elementi množice $\{v_1, \ldots, v_k, v_{k+1}\}$ paroma ortogonalni

Če bi veljalo $v_{k+1} = 0$, potem bi dobili

$$u_{k+1} = \sum_{i=1}^{k}\frac{\langle u_{k+1}, v_i\rangle}{\langle v_i, v_i\rangle}v_i \in \mathrm{Lin}\{v_1, \ldots, v_k\}$$

$$u_1, \ldots, u_k \in \mathrm{Lin}\{v_1, \ldots, v_k\}$$

Torej k-razsežen prostor $\mathrm{Lin}\{v_1, \ldots, v_k\}$ vsebuje linearno neodvisno množico $\{u_1, \ldots, u_k, u_{k+1}\}$, ki ima $k+1$ elementov. To je protislovje.

TRDITEV: vsak **končno** razsežen vektorski **prostor** s **skalarnim produktom** ima **ortogonalno bazo** in vsako **ortogonalno množico** lahko dopolnimo do ortogonalne baze

DOKAZ

Prvi del dokažemo tako, da vzamemo poljubno bazo in jo s **Gram-Schmidtovo ortogonalizacijo** predelamo v **ortogonalno bazo**. Drugi del pa tako da ortogonalno **množico dopolnimo** do običajne **baze** in potem spet **ortogonaliziramo**.

POSLEDICA:
vsak končno razsežen prostor ima tudi **ortonormirano bazo** do katere lahko **dopolnimo ortonormirano množico**

prednost **ortogonalnih** baz je tudi to da po tem razvoju zelo lahko razvijemo **normo**

Ortogonalna projekcija

- → **V** je vektorski **prostor** s skalarnim produktom
- → **W** vektorski **podprostor**
- → vektor **v** pripada **V**
- → vektorju iz **W** ki je **najbljižje** v pravimo **ortogonalna projekcija** na **W**

Fourierov razvoj:

- → V je vektorski prostor s skalarnim produktom
- → { $v_1, \dots, v_n$ } **ortogonalna baza**
- → veljata spodnji formuli druga za **ortonormirano**

$$v = \sum_{i=1}^{n} \frac{\langle v, v_i\rangle}{\langle v_i, v_i\rangle} v_i \qquad v = \sum_{i=1}^{n} \langle v, v_i\rangle v_i$$

DOKAZ

Dokaz: Ker je $\{v_1, \dots, v_n\}$ baza za V, obstajajo taki skalarji $\alpha_1, \dots, \alpha_n$, da velja $v = \sum_{i=1}^n \alpha_i v_i$. Če to enakost skalarno pomnožimo z v_j za nek j, dobimo $\langle v, v_j\rangle = \langle \sum_{i=1}^n \alpha_i v_i, v_j\rangle = \sum_{i=1}^n \alpha_i \langle v_i, v_j\rangle = \alpha_j \langle v_j, v_j\rangle$. Pri zadnjem enačaju smo upoštevali, da je $\langle v_i, v_j\rangle = 0$ za vse i, ki so različni od j. Odtod izrazimo $\alpha_j = \frac{\langle v, v_j\rangle}{\langle v_j, v_j\rangle}$. Sledi $v = \sum_{i=1}^n \alpha_i v_i = \sum_{i=1}^n \frac{\langle v, v_i\rangle}{\langle v_i, v_i\rangle} v_i$.

razdalja med dvema vektorjema je **norma** njune **razlike**

$$\|v - w\| > \|v - v'\|$$

Parsevalova identiteta:

- → V je vektorski prostor s skalarnim produktom
- → { $v_1, \dots, v_n$ } **ortogonalna baza**
- → veljata spodnji formuli druga za **ortonormirano**

$$\|v\|^2 = \sum_{i=1}^{n} \frac{|\langle v, v_i\rangle|^2}{\langle v_i, v_i\rangle} \qquad \|v\|^2 = \sum_{i=1}^{n} |\langle v, v_i\rangle|^2$$

- → { $w_1, \dots, w_n$ } **ortogonalna baza** podprostora **W**
- → ortogonalno projekcijo podamo z prvo formulo oz. drugo če **ortonormirana**:

$$v' = \sum_{i=1}^{k} \frac{\langle v, w_i\rangle}{\langle w_i, w_i\rangle} w_i \qquad v' = \sum_{i=1}^{k} \langle v, w_i\rangle w_i$$

uporabljamo **Pitagorov izrek**

DOKAZ

Dokaz izreka: Ker je v' linearna kombinacija vektorjev w_i iz W, je v' element W. Radi bi pokazali, da za vsak $w \in W$, ki je različen od v', velja $\|v - w\| > \|v - v'\|$. Vzemimo poljuben w iz W in ga razvijmo po bazi za W. Dobimo $w = \sum_{i=1}^k \beta_i w_i$, kjer je $\beta_i = \frac{\langle w, w_i\rangle}{\langle w_i, w_i\rangle}$ za vse i.
Pišimo $v' = \sum_{i=1}^k \alpha_i w_i$, kjer je $\alpha_i = \frac{\langle v, w_i\rangle}{\langle w_i, w_i\rangle}$ za vse i.

1.korak Dokažimo, da je vektor $v - v'$ pravokoten na vse w_i.
Velja $\langle v - v', w_j\rangle = \langle v, w_j\rangle - \langle v', w_j\rangle = \langle v, w_j\rangle - \sum_{i=1}^k \alpha_i \langle w_i, w_j\rangle = \langle v, w_j\rangle - \alpha_j \langle w_j, w_j\rangle = 0$.

2.korak Dokažimo, da je vektor $v - v'$ pravokoten na vektor $v' - w$.
Velja $\langle v - v', v' - w\rangle = \langle v - v', \sum_{i=1}^k (\alpha_i - \beta_i) w_i\rangle =$
$= \sum_{i=1}^k \overline{(\alpha_i - \beta_i)} \langle v - v', w_i\rangle = 0$ po 1. koraku.

3.korak Dokažimo, da je $\|v - w\|^2 = \|v - v'\|^2 + \|v' - w\|^2$.
To je ravno Pitagorov izrek za vektorja $a = v - v'$ in $b = v' - w$, ki sta pravokotna po 2. koraku.
Iz 3. koraka sledi, da je $\|v - w\|^2 > \|v - v'\|^2$, če je $v' \neq w$.

Ortogonalni komplement:

- → **V** je vektorski prostor s skalarnim produktom in **S** podmnožica **V**
- → vektor **v ortogonalen** na množico **S** če **skalarni produkt nič** za vsak vektor **s** iz **S**
- → množici vseh takih vektorjev pravimo **ortogonalni komplement** označimo $S^\perp$

TRDITEV: za vsak **S** je $S^\perp$ **vektorski podprostor** v **V**

DOKAZ

Dokaz: Če v_1 in v_2 pripadata $S^\perp$, je (po definiciji $S^\perp$) $\langle v_1, s\rangle = 0$ in $\langle v_2, s\rangle = 0$ za vsak $s \in S$. Potem je za vsaka skalarja α_1 in α_2 tudi $\langle \alpha_1 v_1 + \alpha_2 v_2, s\rangle = \alpha_1 \langle v_1, s\rangle + \alpha_2 \langle v_2, s\rangle = 0$ za vsak $s \in S$. Odtod sledi (spet po definiciji $S^\perp$), da je $\alpha_1 v_1 + \alpha_2 v_2 \in S^\perp$ za vsaka α_1 in α_2.

TRDITEV: $S^\perp$ = (**LinS**)$^\perp$

DOKAZ

Dokaz: Če je vektor v ortogonalen na elemente $s_1, \dots, s_k$, potem je ortogonalen tudi na vsako njihovo linearno kombinacijo, saj velja

$$\langle v, \alpha_1 s_1 + \ldots + \alpha_k s_k\rangle = \bar{\alpha}_1 \langle v, s_1\rangle + \ldots + \bar{\alpha}_k \langle v, s_k\rangle = 0 + \ldots + 0 = 0$$

ORTOGONALNI RAZCEP:
U podprostor v V potem velja:

- → **dim** $U^\perp$ **= dim V − dim U**
- → $(U^\perp)^\perp$ **= U**
- → **V = U** $\oplus$ $U^\perp$

DOKAZ

Dokaz: Naj bo $\{u_1, \dots, u_k\}$ ortogonalna baza za U in naj bo $\{v_1, \dots, v_l\}$ njena dopolnitev do ortogonalne baze za V.
Po primeru je $U^\perp = \mathrm{Lin}\{v_1, \dots, v_l\}$. Torej je $\dim U + \dim U^\perp = k + l$, kar je enako $\dim V$. To nam da prvo trditev.
Drugi del dokažemo tako, da v primeru zamenjamo bazo iz u_i z bazo iz v_j. Ker je $\{v_1, \dots, v_l\}$ ortogonalna baza za $U^\perp$, in ker je $\{u_1, \dots, u_k\}$ njena dopolnitev do ortogonalne baze za V, je $(U^\perp)^\perp = \mathrm{Lin}\{u_1, \dots, u_k\}$.
Tretji del sledi iz $V = \mathrm{Lin}\{u_1, \dots, u_k\} \oplus \mathrm{Lin}\{v_1, \dots, v_l\}$ in primera.

Opomba: Formuli $V = U \oplus U^\perp$ pravimo **ortogonalni razcep** prostora V glede na podprostor U.

To formulo lahko dokažemo tudi s pomočjo izreka o ortogonalni projekciji. Za vsak element $v \in V$ lahko izračunamo njegovo projekcijo v' na podprostor U. Iz dokaza izreka o ortogonalni projekciji vemo, da je vektor $v - v'$ pravokoten na vse vektorje podprostora U. Velja torej $v - v' \in U^\perp$. Iz $v = v' + (v - v')$ torej sledi, da je vsak element iz V vsota elementa iz U in elementa iz $U^\perp$, kar dokaže formulo $V = U + U^\perp$. Treba je preveriti še $U \cap U^\perp = \{0\}$. Vsak element $u \in U$, ki je pravokoten na vse elemente iz u, je pravokoten tudi sam nase, torej je enak nič.

Linearni funkcionali:

- → posebni primeri **linearnih preslikav**
- → **V** vektorski **prostor** nad **obsegom F**
- → to **preslikava** iz **V** v **F**

F je tudi **vektorski prostor** nad **F**

- → če **B** = { $v_1, \dots, v_n$ } **baza** v **V**
- → če **S** = { **1** } standardna **baza** v **F**
- → preslikavo predstavimo z matriko:

$$[L]_{\mathcal{S} \leftarrow \mathcal{B}} = \begin{bmatrix} L(v_1) & \dots & L(v_n) \end{bmatrix}$$

RIESZOV IZREK:
φ linearen **funkcional** in obstaja **w** da velja:

$$\phi(v) = \langle v, w\rangle$$

DOKAZ

Dokaz: Naj bo $v_1, \dots, v_n$ ortonormirana baza za V. Vzemimo poljuben $v \in V$ in ga razvijmo po tej bazi. Velja $v = \sum_{j=1}^n \langle v, v_i\rangle v_i$. Odtod sledi $\phi(v) = \sum_{i=1}^n \langle v, v_i\rangle \phi(v_i)$ zaradi linearnosti ϕ. Če upoštevamo še konjugirano linearnost skalarnega produkta v drugem faktorju, dobimo $\sum_{i=1}^n \langle v, v_i\rangle \phi(v_i) = \sum_{i=1}^n \langle v, \overline{\phi(v_i)} v_i\rangle = \langle v, \sum_{i=1}^n \overline{\phi(v_i)} v_i\rangle$. Označimo $w = \sum_{i=1}^n \overline{\phi(v_i)} v_i$ in opazimo, da ta vektor ni odvisen od v, ampak samo od ϕ in od baze. Dokazali smo, da velja $\phi(v) = \langle v, w\rangle$ za vsak $v \in V$.

Pokažimo še, da je vektor w enolično določen s funkcionalom ϕ.
Če velja $\phi(v) = \langle v, w_1\rangle$ za vsak $v \in V$ in $\phi(v) = \langle v, w_2\rangle$ za vsak $v \in V$, potem $0 = \phi(v) - \phi(v) = \langle v, w_1\rangle - \langle v, w_2\rangle = \langle v, w_1 - w_2\rangle$ za vsak $v \in V$. Vstavimo $v = w_1 - w_2$ in dobimo $\langle w_1 - w_2, w_1 - w_2\rangle = 0$. Vemo, da odtod sledi $w_1 - w_2 = 0$, se pravi $w_1 = w_2$.

ADJUNGIRANA PRESLIKAVA

→ **L : U → V linearna preslikava** med dvema vektorskima prostoroma
→ **L^* : V → U adjungirana** linearna preslikava če

$$\langle Lu, v\rangle_V = \langle u, L^*v\rangle_U$$

$\langle u_1, u_2 \rangle_U$ in $\langle v_1, v_2 \rangle_V$ označimo skalarna produkta prostora **U** in **V**

→ vsaka linearna preslikava med končnima prostoroma ima **natanko eno adjungirano** linearno preslikvo

$$A^* := (\overline{A})^T$$

Matrika adjungirane linearne preslikave:
→ **U** in **V** končno razsežna vektorska prostora s skalarnim produktom
→ **B** ortonormirana baza za **U** in **C ortonormirana baza** za **V**
→ **L: U → V** in **L^* : V → U** njena **adjungirana** linearna preslikava
→ matriko [L^*]**B** ← **C** dobimo tako da v matriki [**L**]**C** ← **B** vse elemente **konjugiramo** in dobljeno matriko **transponiramo**

DOKAZ

Dokaz: Recimo, da sta U in V končnorazsežna vektorska prostora s skalarnim produktom in da je $L\colon U \to V$ linearna preslikava.

Dokažimo najprej enoličnost: Naj bosta L^* in L' dve adjungirani linearni preslikavi linearne presklikave L. Potem za vsak $u \in U$ ter $v \in V$ velja

$$\langle Lu, v\rangle = \langle u, L^*v\rangle \quad \text{in} \quad \langle Lu, v\rangle = \langle u, L'v\rangle.$$

Če enačbi odštejemo, dobimo, da za vsak $u \in U$ in vsak $v \in V$ velja

$$\langle u, L^*v - L'v\rangle = \langle u, L^*v\rangle - \langle u, L'v\rangle = \langle Lu, v\rangle - \langle Lu, v\rangle = 0.$$

Če vstavimo $u = L^*v - L'v$, dobimo $\langle L^*v - L'v, L^*v - L'v\rangle = 0$, se pravi

$$L^*v - L'v = 0$$

za vsak $v \in V$. Torej je $L^* = L'$.

Dokažimo še obstoj adjungirane linearne preslikave.

Vzemimo poljuben vektor $v \in V$ in si oglejmo preslikavo

$$\phi(u) = \langle Lu, v\rangle_V,$$

ki slika iz U v skalarje. Preverimo najprej, da je ϕ linearen funkcional na U. To sledi iz $\phi(\alpha_1 u_1 + \alpha_2 u_2) = \langle L(\alpha_1 u_1 + \alpha_2 u_2), v\rangle_V =$
$= \langle \alpha_1 Lu_1 + \alpha_2 Lu_2, v\rangle_V = \alpha_1\langle Lu_1, v\rangle_V + \alpha_2\langle Lu_2, v\rangle_V = \alpha_1\phi(u_1) + \alpha_2\phi(u_2)$.

Po Rieszovem izreku o reprezentaciji linearnih funkcionalov obstaja natanko en vektor $w \in U$, ki zadošča $\phi(u) = \langle u, w\rangle_U$ za vsak $u \in U$. Definirajmo

$$L^*v := w.$$

Na dolgo to povemo takole: Za vsak v iz V je L^*v tak vektor iz U, da velja $\langle Lu, v\rangle_V = \langle u, L^*v\rangle_U$ za vsak $u \in U$.

S tem smo definirali preslikavo L^* iz V v U, ki zadošča

$$\langle Lu, v\rangle_V = \langle u, L^*v\rangle_U$$

za vsak $u \in U$ in vsak $v \in V$.

Vzemimo poljubna vektorja v_1 in v_2 iz V in poljubna skalarja α_1 in α_2. Po definiciji so L^*v_1, L^*v_2 in $L^*(\alpha_1 v_1 + \alpha_2 v_2)$ taki vektorji iz U, da velja

$$\langle u, L^*v_1\rangle_U = \langle Lu, v_1\rangle_V, \quad (1)$$
$$\langle u, L^*v_2\rangle_U = \langle Lu, v_2\rangle_V, \quad (2)$$
$$\langle u, L^*(\alpha_1 v_1 + \alpha_2 v_2)\rangle_U = \langle Lu, \alpha_1 v_1 + \alpha_2 v_2\rangle_V \quad (3)$$

za vsak $u \in U$. Iz (1),(2) in (3) sledi, da za vsak $u \in U$ velja

$$\begin{aligned} &\langle u, L^*(\alpha_1 v_1 + \alpha_2 v_2) - \alpha_1 L^*v_1 - \alpha_2 L^*v_2\rangle_U \\ &= \langle u, L^*(\alpha_1 v_1 + \alpha_2 v_2)\rangle_U - \bar\alpha_1\langle u, L^*v_1\rangle_U - \bar\alpha_2\langle u, L^*v_2\rangle_U \\ &= \langle Lu, \alpha_1 v_1 + \alpha_2 v_2\rangle_U - \bar\alpha_1\langle Lu, v_1\rangle_U - \bar\alpha_2\langle Lu, v_2\rangle_U \\ &= \langle Lu, \alpha_1 v_1 + \alpha_2 v_2\rangle_U - \langle Lu, \alpha_1 v_1\rangle_U - \langle Lu, \alpha v_2\rangle_U = 0 \end{aligned}$$

Če v to enakost vstavimo $u = L^*(\alpha_1 v_1 + \alpha_2 v_2) - \alpha_1 L^*v_1 - \alpha_2 L^*v_2$, dobimo

$$L^*(\alpha_1 v_1 + \alpha_2 v_2) - \alpha_1 L^*v_1 - \alpha_2 L^*v_2 = 0$$

torej je preslikava L^* res linearna.

DOKAZ

Dokaz: Naj bo $\mathcal{B} = \{u_1, \ldots, u_m\}$ in $\mathcal{C} = \{v_1, \ldots, v_n\}$. Izračunajmo matriko $[L]_{\mathcal{C}\leftarrow\mathcal{B}}$. S pomočjo Fourierovega razvoja dobimo:

$$\begin{aligned} Lu_1 &= \langle Lu_1, v_1\rangle_V v_1 + \ldots + \langle Lu_1, v_n\rangle_V v_n \\ &\vdots \\ Lu_m &= \langle Lu_m, v_1\rangle_V v_1 + \ldots + \langle Lu_m, v_n\rangle_V v_n \end{aligned}$$

Podobno s Fourierovim razvojem dobimo

$$[L]_{\mathcal{C}\leftarrow\mathcal{B}} = \begin{bmatrix} \langle Lu_1, v_1\rangle_V & \ldots & \langle Lu_m, v_1\rangle_V \\ \vdots & \ddots & \vdots \\ \langle Lu_1, v_n\rangle_V & \ldots & \langle Lu_m, v_n\rangle_V \end{bmatrix}$$

$$\begin{aligned} L^*v_1 &= \langle L^*v_1, u_1\rangle_U u_1 + \ldots + \langle L^*v_1, u_m\rangle_U u_m \\ &\vdots \\ L^*v_n &= \langle L^*v_n, u_1\rangle_U u_1 + \ldots + \langle L^*v_n, u_m\rangle_U u_m \end{aligned}$$

Opazimo, da je (i,j)-ti element matrike $[L^*]_{\mathcal{B}\leftarrow\mathcal{C}}$ enak

$$[L^*]_{\mathcal{B}\leftarrow\mathcal{C}} = \begin{bmatrix} \langle L^*v_1, u_1\rangle_U & \ldots & \langle L^*v_n, u_1\rangle_U \\ \vdots & \ddots & \vdots \\ \langle L^*v_1, u_m\rangle_U & \ldots & \langle L^*v_n, u_m\rangle_U \end{bmatrix}$$

$$\langle L^*v_j, u_i\rangle_U = \overline{\langle u_i, L^*v_j\rangle_U} = \overline{\langle Lu_i, v_j\rangle_V}$$

kar je enako konjugiranemu (j,i)-temu elementu matrike $[L]_{\mathcal{C}\leftarrow\mathcal{B}}$.
Če torej vse elemente matrike $[L]_{\mathcal{C}\leftarrow\mathcal{B}}$ konjugiramo in dobljeno matriko transponiramo, dobimo ravno matriko $[L^*]_{\mathcal{B}\leftarrow\mathcal{C}}$.

Opomba: Torej je $[L^*]_{\mathcal{B}\leftarrow\mathcal{C}} = ([L]_{\mathcal{C}\leftarrow\mathcal{B}})^*$, če sta $\mathcal{B}$ in $\mathcal{C}$ ortonormirani bazi

Lastnosti adjungiranja:

$(\alpha A + \beta B)^* = \bar\alpha A^* + \bar\beta B^*$
$(A^*)^* = A,$
$(AB)^* = B^*A^*,$
$0^* = 0,\ I^* = I.$

Iz prve lastnosti sledi na **realnih** matrikah **fiksne** velikosti adjungiranje **linearna preslikava**. Na **kompleksnih** matrikah fiksne velikosti adjungiranje **ni linearna** ampak **konjugirano linearna** preslikava

DOKAZ

Dokaz: Vemo, da za konjugiranje kompleksnih števil velja

$$\overline{z_1 + z_2} = \bar z_1 + \bar z_2, \quad \overline{z_1 z_2} = \bar z_1 \bar z_2, \quad \bar{\bar z} = z$$

Odtod sledi, da za kompleksne matrike velja

$$\overline{\alpha A + \beta B} = \bar\alpha\bar A + \bar\beta\bar B, \quad \overline{AB} = \bar A\bar B, \quad \bar{\bar A} = A$$

Upoštevajmo še lastnosti transponiranja

$$(\alpha A + \beta B)^T = \alpha A^T + \beta B^T, \quad (AB)^T = B^T A^T, \quad (A^T)^T = A$$

$$(\overline{\alpha A + \beta B})^T = (\bar\alpha\bar A + \bar\beta\bar B)^T = \bar\alpha\bar A^T + \bar\beta\bar B^T \quad (\overline{AB})^T = (\bar A\bar B)^T = \bar B^T\bar A^T$$

Če upoštevamo, da je $\bar A^T = \overline{A^T}$, potem dobimo še $\bar{\bar A}^{T^T} = A$

Podoben razmislek lahko naredimo tudi za adjungiranje linearnih preslikav.

Naj bosta U in V vektorska prostora s skalarnim produktom. Označimo z $\mathcal{L}(U,V)$ množico vseh linearnih preslikav iz U v V. To množico lahko spremenimo v vektorski prostor, če za linearni preslikavi L_1, L_2 in skalarja α_1, α_2 definiramo linearno preslikavo $\alpha_1 L_1 + \alpha_2 L_2$ s predpisom $(\alpha_1 L_1 + \alpha_2 L_2)(u) = \alpha_1 L_1(u) + \alpha_2 L_2(u)$.

Adjungiranje je preslikava $\mathcal{L}(U,V)$ v $\mathcal{L}(V,U)$. Preverimo, da zadošča

$$(\alpha_1 L_1 + \alpha_2 L_2)^* = \bar\alpha_1 L_1^* + \bar\alpha_2 L_2^* \quad (L^*)^* = L \quad (2)$$

Za vsaka $u \in U$ in $v \in V$ velja $\langle u, (\alpha_1 L_1 + \alpha_2 L_2)^*(v)\rangle =$
$= \langle(\alpha_1 L_1 + \alpha_2 L_2)(u), v\rangle = \langle \alpha_1 L_1 u + \alpha_2 L_2 u, v\rangle =$
$= \alpha_1\langle L_1 u, v\rangle + \alpha_2\langle L_2 u, v\rangle = \alpha_1\langle u, L_1^*v\rangle + \alpha_2\langle u, L_2^*v\rangle =$
$= \langle u, \bar\alpha_1 L_1^*v + \bar\alpha_2 L_2^*v\rangle = \langle u, (\bar\alpha_1 L_1^* + \bar\alpha_2 L_2^*)(v)\rangle.$
Če upoštevamo enoličnost adjungirane preslikave, odtod sledi (1).

Lastnost (1) bi lahko dokazali tudi s prehodom na matrike.

Lastnost (2) dokažemo tako, da preverimo, da sta L in $(L^*)^*$ adjungirani linearni preslikavi linearne preslikave L^*. Za vsaka $u \in U$ in $v \in V$ velja $\langle v, (L^*)^*u\rangle = \langle L^*v, u\rangle = \overline{\langle u, L^*v\rangle} = \overline{\langle Lu, v\rangle} = \langle v, Lu\rangle$.

$$(L_2 L_1)^* = L_1^* L_2^*$$

dokažemo tako, da preverimo, da sta $(L_2L_1)^*$ in $L_1^*L_2^*$ adjungirani linearni preslikavi linearne preslikave L_2L_1. Recimo, da L_1 slika iz U v V, L_2 pa iz V v W. Za vsak $u \in U$ in vsak $w \in W$ velja naslednji račun
$\langle u,(L_2L_1)^*w\rangle_U = \langle L_2L_1u,w\rangle_W = \langle L_1u,L_2^*w\rangle_V = \langle u,L_1^*L_2^*w\rangle_U$.

Seveda bi tudi lastnosti (2) in (3) lahko dokazali s prehodom na matrike.

T $\langle Lu,v\rangle_V = \langle u,L^*v\rangle_U$ U in V končno razsežna $\operatorname{Ker} L^* = (\operatorname{Im} L)^\perp$
prostora vektorska prostora s **skalarnim produktom**

$\operatorname{Ker} L^*L = \operatorname{Ker} L$

TRDITEV: **L** : **U** → **V** in sta **U** in **V** končno razsežna prostora vektorska prostora s **skalarnim produktom**

DOKAZ

Dokaz: Vzemimo poljuben $u \in U$. Če $u \in \operatorname{Ker} L$, potem je $Lu = 0$. Odtod sledi $L^*Lu = L^*0 = 0$, torej $u \in \operatorname{Ker} L^*L$.
Dokažimo še obratno. Če $u \in \operatorname{Ker} L^*L$, potem $L^*Lu = 0$. Po definiciji L^* je $\langle Lu,Lu\rangle = \langle u,L^*Lu\rangle = \langle u,0\rangle = 0$. Odtod sledi $Lu = 0$, torej je $u \in \operatorname{Ker} L$.

Oglejmo si nekaj posledic formule (6).

Če na obeh straneh formule (6) vzamemo ortogonalni komplement in upoštevamo, da po formuli (4) velja $\operatorname{Im} L^* = (\operatorname{Ker} L)^\perp$ in $\operatorname{Im} L^*L = \operatorname{Im}(L^*L)^* = (\operatorname{Ker} L^*L)^\perp$, potem dobimo

$\operatorname{Im} L^*L = \operatorname{Im} L^*$ $\quad \operatorname{Ker} LL^* = \operatorname{Ker} L^*$ $\quad \operatorname{Im} LL^* = \operatorname{Im} L$

Če v formulah (6) in (7) zamenjamo L z L^*, potem dobimo

Opomba: Pravimo, da je $L\colon V \to V$ **normalna** linearna preslikava, če velja $LL^* = L^*L$. Za normalne linearne preslikave iz (6) in (8) sledi, da je $\operatorname{Ker} L^* = \operatorname{Ker} L$, iz (7) in (9) pa sledi, da je $\operatorname{Im} L^* = \operatorname{Im} L$.

TRDITEV: naj bo **A kvadratna matrika** nad **C** in naj bo **λ** ∈ **C**. Potem je **λ** lastna vrednost za **A** natanko tedaj, ko je **$\bar{\lambda}$ lastna vrednost** za **A***

DOKAZ

Dokaz: Radi bi dokazali, da velja $\operatorname{Ker}(A-\lambda I) \neq \{0\}$ natanko tedaj, ko velja $\operatorname{Ker}(A^*-\bar{\lambda}I) \neq \{0\}$. Zadošča dokazati, da velja

$\dim \operatorname{Ker}(A-\lambda I) = \dim \operatorname{Ker}(A^*-\bar{\lambda}I)$

Označimo $B = A-\lambda I$. Iz lastnosti operacije adjungiranja sledi, da je $B^* = A^*-\bar{\lambda}I$. Torej zadošča dokazati, da je

$\dim \operatorname{Ker} B = \dim \operatorname{Ker} B^*$ Iz izreka $\operatorname{Ker} B^* = (\operatorname{Im} B)^\perp$ sledi

$\dim \operatorname{Ker} B^* = \dim(\operatorname{Im} B)^\perp$ kjer je n velikost matrike A.

Po osnovnem izreku je $\quad n - \dim \operatorname{Im} B = \dim \operatorname{Ker} B$

Oglejmo si še en dokaz, ki je bolj računski.
Najprej opazimo, da za vsako kompleksno kvadratno matriko B velja

$\det B^* = \det(\overline{B})^T = \det \overline{B} = \overline{\det B}$ Če vstavimo $B = A - x\,I$, dobimo

$\det(A^* - \bar{x}\,I) = \overline{\det(A - x\,I)}$ torej za karakteristična polinoma A in A^* velja

Opomba: Iz tega dokaza je razvidno, kako se $p_{A^*}(x)$ izraža z $p_A(x)$. Iz $p_A(x) = c_0 + c_1x + \ldots + c_nx^n$ namreč sledi, da velja $p_{A^*}(x) = \overline{p_A(\bar{x})} = \overline{c_0 + c_1\bar{x} + \ldots + c_n\bar{x}^n} = \bar{c}_0 + \bar{c}_1x + \ldots + \bar{c}_nx^n$.

TRDITEV: **lastna vektorja hermitske matrike** ki pripadata različnim **lastnim vrednostim** sta **ortogonalna** glede na standardni **skalarni produkt**

DOKAZ

Dokaz: Naj bo A hermitska matrika in naj bosta u in v njena lastna vektorja. Naj bosta λ in μ pripadajoči lastni vrednosti, se pravi

$Au = \lambda u \quad$ in $\quad Av = \mu v$ Po prejšnji trditvi sta λ in μ realni števili

$\langle Au,v\rangle = \langle \lambda u,v\rangle = \lambda\langle u,v\rangle$ Ker je A hermitska matrika, velja

$\langle u,Av\rangle = \langle u,\mu v\rangle = \bar{\mu}\langle u,v\rangle = \mu\langle u,v\rangle$ $\quad \langle Au,v\rangle = \langle u,A^*v\rangle = \langle u,Av\rangle$

$\lambda\langle u,v\rangle = \mu\langle u,v\rangle$ $\quad \langle u,v\rangle = 0$

DOKAZ

Dokaz: Vzemimo poljuben vektor $v \in V$. Opazimo, da velja $L^*v = 0$ natanko tedaj, ko je $\langle u,L^*v\rangle = 0$ za vsak $u \in U$. Po definiciji L^* velja to natanko tedaj, ko je $\langle Lu,v\rangle = 0$ za vsak $u \in U$. Po definiciji $\operatorname{Im} L$ velja to natanko tedaj, ko je $\langle w,v\rangle = 0$ za vsak $w \in \operatorname{Im} L$. Po definiciji ortogonalnega komplementa velja to natanko tedaj, ko je $v \in (\operatorname{Im} L)^\perp$.

Oglejmo si nekaj preprostih posledic formule (1). $\quad \operatorname{Im} L = (\operatorname{Ker} L^*)^\perp$

Če na obeh straneh (1) uporabimo ortogonalni komplement in upoštevamo, da je $((\operatorname{Im} L)^\perp)^\perp = \operatorname{Im} L$, dobimo

Če v formuli (1) zamenjamo L z L^*, dobimo $\quad \operatorname{Ker} L = (\operatorname{Im} L^*)^\perp$

Če v formuli (2) zamenjamo L z L^*, dobimo $\quad \operatorname{Im} L^* = (\operatorname{Ker} L)^\perp$

Isto formulo dobimo, če na obeh straneh v (3) uporabimo ortogonalni komplement.

Pokažimo sedaj, da formule (1)-(4) veljajo tudi za matrike.

Najprej standardni skalarni produkt zapišemo v matrični obliki

$$\langle v,w\rangle = v_1\bar{w}_1 + \ldots + v_n\bar{w}_n = \begin{bmatrix} \bar{w}_1 & \ldots & \bar{w}_n \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = w^*v. \qquad (5)$$

Naj bo A kompleksna $m \times n$ matrika. Opazimo, da iz (5) sledi

$$\langle Au,v\rangle = v^*Au = v^*A^{**}u = (A^*v)^*u = \langle u,A^*v\rangle \qquad (6)$$

za vsak $u \in \mathbb{C}^n$ in vsak $v \in \mathbb{C}^m$. V $\langle Au,v\rangle$ nastopa standardni skalarni produkt na $\mathbb{C}^m$, v $\langle u,A^*v\rangle$ pa standardni skalarni produkt na $\mathbb{C}^n$. Naj bo L_A linearna preslikava it $\mathbb{C}^n$ v $\mathbb{C}^m$ definirana z $L_Au = Au$. Potem velja

$$(L_A)^* = L_{A^*} \qquad (7)$$

saj po (6) velja $\langle u,(L_A)^*v\rangle = \langle L_Au,v\rangle = \langle Au,v\rangle = \langle u,A^*v\rangle = \langle u,L_{A^*}v\rangle$ za vsak $u \in \mathbb{C}^n$ in vsak $v \in \mathbb{C}^m$. Iz (7) sledi recimo verzija (3) za matrike

$$\operatorname{Ker} A = \operatorname{Ker} L_A = (\operatorname{Im}(L_A)^*)^\perp = (\operatorname{Im} L_{A^*})^\perp = (\operatorname{Im} A^*)^\perp.$$

Če je L slika iz U v V, potem L^*L slika iz U v U, LL^* pa iz V v V. Poleg tega iz lastnosti adjungiranja sledi

$$(L^*L)^* = L^*L \quad \text{in} \quad (LL^*)^* = LL^*. \qquad (5)$$

Sebiadjugirana preslikava:
L : V → V je **sebiadjungirana** če velja **L = L***

če je **A** matrika **sebiadjungirane** preslikave **L : V → V** glede na **ortonormirano** bazo **B** za **V** potem je **A* = ([L]B)* = [L*] B = [L] B = A**

Simetrična in Hermitska matrika:
→ **kompleksna** matrika **A** je hermitska če zadošča **A** = **A***
→ realnim **hermitskim** matrikam pravimo tudi **simetrične** matrik

za vsako matriko **A** sta **A*A** in **AA*** **hermitski** matriki vsaka potenca **hermitske** matrike je spet **hermitska** matrik

TRDITEV: vse **lastne vrednosti** hermitske matrike so **realne**

DOKAZ

Dokaz: Naj bo λ lastna vrednost hermitske matrike in naj bo v pripadajoči lastni vektor. Potem za standardni skalarni produkt velja

$$\lambda\langle v,v\rangle = \langle \lambda v,v\rangle = \langle Av,v\rangle = \langle v,A^*v\rangle = \langle v,Av\rangle = \langle v,\lambda v\rangle = \bar{\lambda}\langle v,v\rangle$$

Ker je $v \neq 0$, lahko pokrajšamo $\langle v,v\rangle$ in dobimo $\lambda = \bar{\lambda}$.

TRDITEV: vsaka **hermitska** matrika je podobna **diagonalni** matriki

DOKAZ

Dokaz. Zadošča dokazati, da se korenski podprostori ujemajo z lastnimi podprostori. Odtod namreč sledi, da so vse Jordanske kletke velikosti 1. Naj bo λ lastna vrednost hermitske matrike A. Radi bi dokazali, da za vsako naravno število m velja $\operatorname{Ker}(A-\lambda I)^m = \operatorname{Ker}(A-\lambda I)$.

Označimo $B = A - \lambda I$ in opazimo, da je tudi matrika B hermitska. Iz formule $\mathrm{Ker}\, B^*B = \mathrm{Ker}\, B$ torej sledi, da je $\mathrm{Ker}\, B^2 = \mathrm{Ker}\, B$. Če namesto B vstavimo B^{2^k} za $k = 1, \dots, m-1$, dobimo

$$\mathrm{Ker}\, B^{2^m} = \mathrm{Ker}\, B^{2^{m-1}} = \mathrm{Ker}\, B^{2^{m-2}} = \dots = \mathrm{Ker}\, B.$$

Ker je $2^m \geq m$ za vsak m, odtod sledi

$$\mathrm{Ker}\, B \subseteq \mathrm{Ker}\, B^m \subseteq \mathrm{Ker}\, B^{2^m} = \mathrm{Ker}\, B$$

$$\mathrm{Ker}\, B^m = \mathrm{Ker}\, B$$

TRDITEV: za vsako **hermitsko** matriko **A** obstaja taka **unitarna** matrika **P** in taka **realna diagonalna** matrika **D** da velja **A = PDP^{-1}**

TRDITEV: za vsako **simetrično** matriko **A** obstaja taka **ortogonalna** matrika **P** in taka **realna diagonalna** matrika **D** da velja **A = PDP^{-1}**

DOKAZ

Dokaz prvega dela: Naj bo A hermitska $n \times n$ matrika. Za vsak lastni podprostor matrike A izberimo ortonormirano bazo. Naj bo $\mathcal{B}$ unija izbranih ortonormiranih baz po vseh lastnih podprostorih matrike A. Ker so lastni podprostori matrike A paroma ortogonalni (po Trditvi 2), je $\mathcal{B}$ ortogonalna množica. Ker je $\mathbb{C}^n$ direktna vsota lastnih podprostorov matrike A (po Trditvi 3), je $\mathcal{B}$ ogrodje za $\mathbb{C}^n$. Torej je $\mathcal{B}$ ortonormirana baza za $\mathbb{C}^n$. Sestavljena je iz lastnih vektorjev matrike A.

Naj bo P matrika, katere stolpci so elementi baze $\mathcal{B}$. Potem je P unitarna matrika, katere stolpci so lastni vektorji matrike A, torej je

$$AP = A\begin{bmatrix} v_1 & \dots & v_n \end{bmatrix} = \begin{bmatrix} Av_1 & \dots & Av_n \end{bmatrix} =$$

$$= \begin{bmatrix} \lambda_1 v_1 & \dots & \lambda_n v_n \end{bmatrix} = \begin{bmatrix} v_1 & \dots & v_n \end{bmatrix} \begin{bmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{bmatrix} = PD$$

Dokaz drugega dela. Naj bo A simetrična matrika. Naj bodo $\lambda_1, \dots, \lambda_k$ vse paroma različne lastne vrednosti matrike A. Ker so matrike $A - \lambda_i I$ realne (po Trditvi 1), lahko za lastni podprostor $\mathrm{Ker}(A - \lambda_i I)$ izberemo ortonormirano bazo $\mathcal{B}_i$ iz realnih vektorjev. (Gram-Schmidtova ortogonalizacija nam realno bazo spremeni v realno ortogonalno bazo.) Ker so lastni podprostori matrike A paroma ortogonalni in ker je njihova vsota enaka $\mathbb{C}^n$ je $\bigcup_{i=1}^k \mathcal{B}_i$ ortonormirana baza za $\mathbb{C}^n$. Elemente te baze vzamemo za stolpce matrike P.

Še en dokaz drugega dela: Dokažimo s popolno indukcijo, da ima $\mathbb{R}^n$ ortonormirano bazo iz lastnih vektorjev matrike A. Recimo, da je $\mathcal{B} = \{v_1, \dots, v_r\}$ ortonormirana množica v $\mathbb{R}^n$ iz lastnih vektorjev A. Trdimo, da za vsak $w \in \mathcal{B}^\perp$ velja $Aw \in \mathcal{B}^\perp$. Za vsak $v \in \mathcal{B}$ je namreč $\langle Aw, v \rangle = \langle w, Av \rangle = \langle w, \lambda v \rangle = \bar{\lambda}\langle w, v \rangle = 0$. Ker je $\mathcal{B}^\perp$ invarianten za A, vsebuje vsaj en realen lastni vektor za A. Če ta lastni vektor normiramo, dobimo tak vektor v_{r+1}, da je $\{v_1, \dots, v_r, v_{r+1}\}$ ortonormirana množica v $\mathbb{R}^n$ iz lastnih vektorjev matrike A.

okej to je pp narjen do 26 predavanja 9 slajd!

Unitarne in ortogonalne matrike:

→ **kompleksna n** × **n** matrika je **unitarna**

→ njeni stolpci tvorijo **ortonormirano** bazo za **C^n** glede na **standardni skalarni produkt**

→ **realni unitarni** matriki pravimo tudi **ortogonalna matrika**

Za unitarno matriko **P** velja **PP*** = **I**. Za **ortogonalno** matriko **P** velja **PP^T** = **I**. V obeh primerih je torej **P^{-1}** = **P***

Normalne matrike:

→ **A A* = A* A**

→ vsaka normalna matrika je **kvadratna**

→ **λ lastna vrednost** matrike **A** je **$\bar{\lambda}$** lastna vrednost matrike **A*** vedno

→ pri normalni matriki velja tudi da če **Av = λv** potem **A*v = $\bar{\lambda}$v**

→ če je A normalna imata **A** in **A*** enake **lastne vektorje**

→ če je **A** normalna potem **A − λI** normalna za vsak **λ**

DOKAZ

Dokaz. Označimo $B = A - \lambda I$. Iz lastnosti adjungiranja sledi, da je $B^* = A^* - \bar{\lambda} I$. Ker je A normalna, velja $A^*A = AA^*$. Odtod sledi $BB^* = AA^* - \lambda A^* - \bar{\lambda} A + \lambda\bar{\lambda} I = A^*A - \lambda A^* - \bar{\lambda} A + \lambda\bar{\lambda} I = B^*B$.

Dokaz: Naj bo λ lastna vrednost normalne matrike A. Po prejšnji trditvi je tudi $B = A - \lambda I$ normalna matrika. Vemo že, da odtod sledi

$$\mathrm{Ker}\, B = \mathrm{Ker}\, B^*B = \mathrm{Ker}\, BB^* = \mathrm{Ker}\, B^*.$$

Torej za normalno matriko A velja

$$\mathrm{Ker}\,(A - \lambda I) = \mathrm{Ker}\,(A^* - \bar{\lambda} I).$$

TRDITEV: vsaka **normalna** matrika je podobna **diagonalni** matriki

DOKAZ

Radi bi dokazali da je vsak **korenski podprostor** normalne matrike **lastni podprostor**. Iz korenskega razcepa sledi, da ima matrika **n linearno neodvisnih lastnih vektorjev** in se da **diagonalizirati**. **A** je normalna matrika in **λ** njena lastna vrednost. Tudi matrika **B = A − λI** je **normalna**. Radi bi dokazali, da velja **Ker B^2** = **Ker B**.

S popolno **indukcijo** dokažemo, da velja Ker **B$^{2^k}$** = **Ker B** za vsak **k**. Ker je **2^k** ≥ **k** sledi da je **Ker B** ⊆ **Ker B^k** ⊆ **Ker B$^{2^k}$** = **Ker B** torej je Ker **B^k** = **Ker B** za vsak **k**. To pomeni, da je **korenski podprostor** za **λ** res enak **lastnemu podprostoru** za **λ**

$\mathrm{Ker}\, B^*B = \mathrm{Ker}\, B$ $\quad$ $\mathrm{Ker}\,(B^*B)^2 = \mathrm{Ker}\, B^*B$ $\quad$ $\mathrm{Ker}\,(B^2)^*B^2 = \mathrm{Ker}\, B^2$

Ker je B **normalna preslikava** velja: $(B^2)^*B^2 = B^*B^*BB = B^*BB^*B = (B^*B)^2$

TRDITEV: lastni podprostori normalne matrike so paroma **ortogonalni**

DOKAZ

Dokaz: Recimo, da je A normalna matrika in da sta λ in μ različni lastni vrednosti za A. Radi bi pokazali, da je vsak vektor $u \in \mathrm{Ker}\,(A - \lambda I)$ pravokoten na vsak vektor $v \in \mathrm{Ker}\,(A - \mu I)$ glede na standardni skalarni produkt na $\mathbb{C}^n$.

Dokazali smo že, da velja $\mathrm{Ker}\,(A - \mu I) = \mathrm{Ker}\,(A^* - \bar{\mu} I)$, torej je

$$\mu\langle u, v \rangle = \langle u, \bar{\mu} v \rangle = \langle u, A^* v \rangle = \langle Au, v \rangle = \langle \lambda u, v \rangle = \lambda\langle u, v \rangle.$$

Ker je $\mu \neq \lambda$, odtod sledi $\langle u, v \rangle = 0$, kar smo želeli dokazati.

PRIMERI

Vektorji

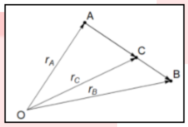
Primer linearne kombinacije

Preverimo, ali je vektor $(0,2,-3)$ linearna kombinacija vektorjev $(1,1,-1)$ in $(2,0,1)$. Če enačbo $(0,2,-3)=\alpha(1,1,-1)+\beta(2,0,1)$ razpišemo po komponentah, dobimo $0=\alpha+2\beta$, $2=\alpha$, $-3=-\alpha+\beta$. Uganemo rešitev $\alpha=2, \beta=-1$, torej je odgovor na vprašanje pozitiven.

Primer: Središče točk

Središče točk $\mathbf{r}_1,\ldots,\mathbf{r}_m$ je točka

$$\frac{1}{m}(\mathbf{r}_1+\ldots+\mathbf{r}_m).$$



Oglejmo si geometrijsko konstrukcijo središča: Naj bo $\mathbf{p}_1=\mathbf{r}_1$. Za vsak $i=2,\ldots,m$ naj bo $\mathbf{p}_i$ taka točka na daljici med $\mathbf{p}_{i-1}$ in $\mathbf{r}_i$, ki to daljico deli v razmerju $1:(i-1)$. Trdimo, da je potem $\mathbf{p}_m$ iskana točka.

Dokaz: S popolno indukcijo bomo dokazali, da za vsak $i=1,\ldots,m$ velja $\mathbf{p}_i=\frac{1}{i}(\mathbf{r}_1+\ldots+\mathbf{r}_i)$. Ker je $\mathbf{p}_1=\mathbf{r}_1$, trditev drži za $i=1$. Po prejšnjem primeru za vsak $i=2,\ldots,m$ velja $\mathbf{p}_i=\frac{i-1}{i}\mathbf{p}_{i-1}+\frac{1}{i}\mathbf{r}_i$. Ko vstavimo indukcijsko predpostavko $\mathbf{p}_{i-1}=\frac{1}{i-1}(\mathbf{r}_1+\ldots+\mathbf{r}_{i-1})$ in uredimo, dobimo $\mathbf{p}_i=\frac{i-1}{i}(\frac{1}{i-1}(\mathbf{r}_1+\ldots+\mathbf{r}_{i-1}))+\frac{1}{i}\mathbf{r}_i=\frac{1}{i}(\mathbf{r}_1+\ldots+\mathbf{r}_i)$, kar smo trdili.

Primer (Paralelogramsko pravilo)

Dokažimo, da za vsak paralelogram $ABCD$ velja

$$\overline{AC}^2+\overline{BD}^2=2(\overline{AB}^2+\overline{AD}^2).$$

Pišimo $\mathbf{a}=\overrightarrow{AB}$ in $\mathbf{b}=\overrightarrow{AD}$. Potem je

$$\overline{AB}=\|\mathbf{a}\|,\quad \overline{AD}=\|\mathbf{b}\|,\quad \overline{AC}=\|\mathbf{a}+\mathbf{b}\|\quad\text{in}\quad \overline{BD}=\|\mathbf{a}-\mathbf{b}\|.$$

Formula sedaj sledi iz računa

$$\begin{aligned}\|\mathbf{a}+\mathbf{b}\|^2+\|\mathbf{a}-\mathbf{b}\|^2&=\langle\mathbf{a}+\mathbf{b},\mathbf{a}+\mathbf{b}\rangle+\langle\mathbf{a}-\mathbf{b},\mathbf{a}-\mathbf{b}\rangle=\\&=(\langle\mathbf{a},\mathbf{a}\rangle+\langle\mathbf{b},\mathbf{b}\rangle+2\langle\mathbf{a},\mathbf{b}\rangle)+(\langle\mathbf{a},\mathbf{a}\rangle+\langle\mathbf{b},\mathbf{b}\rangle-2\langle\mathbf{a},\mathbf{b}\rangle)=\\&=2(\langle\mathbf{a},\mathbf{a}\rangle+\langle\mathbf{b},\mathbf{b}\rangle)=2(\|\mathbf{a}\|^2+\|\mathbf{b}\|^2).\end{aligned}$$

Primer

Poiščimo normalno enačbo premice v $\mathbb{R}^3$, ki gre skozi točki

$$\mathbf{r}_1=(0,-2,1)\quad\text{in}\quad\mathbf{r}_2=(3,-2,-1).$$

Najprej poiščemo točko $\mathbf{r}_0$ na premici in vektor $\mathbf{p}$ v smeri premice. Vzemimo na primer

$$\mathbf{r}_0=\mathbf{r}_1=(0,-2,1)\quad\text{in}\quad\mathbf{p}=\mathbf{r}_2-\mathbf{r}_1=(3,0,-2).$$

Normalna enačba se potem glasi

$$t=\frac{x_1}{3}=\frac{x_2+2}{0}=\frac{x_3-1}{-2}.$$

Primer s parametrično in normalno enačbo ravnine

Poiščimo normalno enačbo ravnine v $\mathbb{R}^3$, ki ima parametrično enačbo

$$\mathbf{r}=(1,2,-1)+s(2,1,3)+t(-1,1,1).$$

Zapišimo enačbo po komponentah:

$$x=1+2s-t,\quad y=2+s+t,\quad z=-1+3s+t.$$

Iz prve enačbe izrazimo s in ga vstavimo v drugo in tretjo enačbo. Dobimo

$$\frac{3}{2}t=-\frac{1}{2}x+y-\frac{3}{2}\quad\text{in}\quad\frac{5}{2}t=-\frac{3}{2}x+z+\frac{5}{2}.$$

Iz prve enačbe izrazimo t in ga vstavimo v drugo enačbo. Dobimo

$$0=-\frac{2}{3}x-\frac{5}{3}y+z+5.$$

To je iskana normalna enačba ravnine.

Primer: Delitev daljice v danem razmerju

Dana je daljica AB. Iščemo tako točko C na tej daljici, ki jo deli v razmerju $3:2$. To pomeni, da velja $\overrightarrow{AC}=\frac{3}{5}\overrightarrow{AB}$. Označimo z $\mathbf{r}_A$, $\mathbf{r}_B$ in $\mathbf{r}_C$ krajevne vektorje, ki ustrezajo točkam A, B in C. Radi bi izrazili $\mathbf{r}_C$ z $\mathbf{r}_A$ in $\mathbf{r}_B$. Ker je $\overrightarrow{AB}=\mathbf{r}_B-\mathbf{r}_A$, dobimo

$$\mathbf{r}_C=\overrightarrow{0A}+\overrightarrow{AC}=\mathbf{r}_A+\frac{3}{5}(\mathbf{r}_B-\mathbf{r}_A)=\frac{2}{5}\mathbf{r}_A+\frac{3}{5}\mathbf{r}_B.$$

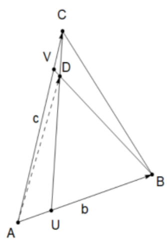
Primer baze

Standardna baza za $\mathbb{R}^n$ je

$$\mathbf{e}_1=(1,0,\ldots,0),\ \mathbf{e}_2=(0,1,\ldots,0),\ \ldots,\ \mathbf{e}_n=(0,0,\ldots,1)$$

Primer uporabe linearne neodvisnosti

Vzemimo trikotnik s oglišči A, B, C. Naj bo U taka točka na daljici AB, da je $\overline{AU}:\overline{UB}=1:3$ in naj bo V taka točka na daljici AC, da velja $\overline{AV}:\overline{VC}=4:1$. Naj bo točka D presečišče daljic CU in BV. (Glej sliko). Izrazimo vektor $\overrightarrow{AD}$ z vektorjema $\mathbf{b}=\overrightarrow{AB}$ in $\mathbf{c}=\overrightarrow{AC}$!



Ker je $\overrightarrow{AU}=\frac{1}{4}\mathbf{b}$, $\overrightarrow{AV}=\frac{4}{5}\mathbf{c}$, $\overrightarrow{UC}=\mathbf{c}-\frac{1}{4}\mathbf{b}$ in $\overrightarrow{VB}=\mathbf{b}-\frac{4}{5}\mathbf{c}$, velja

$$\overrightarrow{AD}=\overrightarrow{AU}+\lambda\overrightarrow{UC}=\frac{1}{4}\mathbf{b}+\lambda(\mathbf{c}-\frac{1}{4}\mathbf{b})=\frac{1-\lambda}{4}\mathbf{b}+\lambda\mathbf{c}$$

in

$$\overrightarrow{AD}=\overrightarrow{AV}+\mu\overrightarrow{VB}=\frac{4}{5}\mathbf{c}+\mu(\mathbf{b}-\frac{4}{5}\mathbf{c})=\mu\mathbf{b}+\frac{4(1-\mu)}{5}\mathbf{c},$$

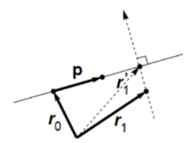
kjer skalarjev λ in μ še ne poznamo. Ker sta $\mathbf{b}$ in $\mathbf{c}$ linearno neodvisna, odtod sledi, da je

Rešitev tega sistema je $\lambda=\frac{3}{4}$ in $\mu=\frac{1}{16}$. Torej je $\overrightarrow{AD}=\frac{1}{16}\mathbf{b}+\frac{3}{4}\mathbf{c}$.

Osnovne naloge z premicami:

Najpogostejše naloge s premicami so:

- pravokotna projekcija točke na premico,
- zrcaljenje točke čez premico in
- razdalja točke od premice.



Recimo torej, da bi radi pravokotno projecirali točko $\mathbf{r}_1$ na premico $\mathbf{r}=\mathbf{r}_0+t\mathbf{p}$. Iskano točko označimo z $\mathbf{r}_1'$.

Ker točka $\mathbf{r}_1'$ leži na premici, obstaja tak skalar t, da velja $\mathbf{r}_1'=\mathbf{r}_0+t\mathbf{p}$

Skalar t moramo določiti tako, da je vektor $\mathbf{r}_1-\mathbf{r}_1'$ pravokoten na vektor $\mathbf{p}$.

Potem je $0=\langle\mathbf{r}_1-\mathbf{r}_1',\mathbf{p}\rangle=\langle\mathbf{r}_1-\mathbf{r}_0,\mathbf{p}\rangle-t\langle\mathbf{p},\mathbf{p}\rangle$. Odtod sledi, da je

$$t=\frac{\langle\mathbf{r}_1-\mathbf{r}_0,\mathbf{p}\rangle}{\langle\mathbf{p},\mathbf{p}\rangle}\qquad \mathbf{r}_1'=\mathbf{r}_0+\frac{\langle\mathbf{r}_1-\mathbf{r}_0,\mathbf{p}\rangle}{\langle\mathbf{p},\mathbf{p}\rangle}\mathbf{p}\qquad d=\|\mathbf{r}_1-\mathbf{r}_1'\|\qquad \mathbf{r}_1''=2\mathbf{r}_1'-\mathbf{r}_1$$

Sedaj lahko izračunamo tudi oddaljenost točke $\mathbf{r}_1$ od premice $\mathbf{r}=\mathbf{r}_0+t\mathbf{p}$ in njeno zrcalno sliko $\mathbf{r}_1''$ glede na to premico. Velja

Zadnja formula sledi iz dejstva, da je $\mathbf{r}_1'$ ravno razpolovišče daljice med $\mathbf{r}_1$ in $\mathbf{r}_1''$, se pravi $\mathbf{r}_1'=\frac{1}{2}(\mathbf{r}_1+\mathbf{r}_1'')$.

Kadar smo v $\mathbb{R}^3$, lahko pri računanju oddaljenosti točke $\mathbf{r}_1$ od premice $\mathbf{r}=\mathbf{r}_0+t\mathbf{p}$ uporabimo vektorski produkt. Velja

$$d=\frac{\|(\mathbf{r}_1-\mathbf{r}_0)\times\mathbf{p}\|}{\|\mathbf{p}\|}$$

Tako leva kot desna stran sta namreč enaki $\|\mathbf{r}_1-\mathbf{r}_0\|\sin\phi$, kjer je ϕ kot med vektorjema $\mathbf{r}_1-\mathbf{r}_0$ in $\mathbf{p}$.

Osnovne naloge z ravninami:

Najprej si poglejmo, kako poiščemo pravokotno projekcijo točke $\mathbf{r}_1$ na parametrično podano ravnino $\mathbf{r}=\mathbf{r}_0+s\mathbf{p}+t\mathbf{q}$. Iskana točka naj bo $\mathbf{r}_1'$

Ker točka $\mathbf{r}_1'$ leži na ravnini, obstajata taka parametra s in t, da velja $\mathbf{r}_1'=\mathbf{r}_0+s\mathbf{p}+t\mathbf{q}$

Ker je vektor $\mathbf{r}_1'-\mathbf{r}_1$ pravokoten na ravnino, je pravokoten tudi na oba smerna vektorja, torej mora veljati: $\langle\mathbf{r}_1'-\mathbf{r}_1,\mathbf{p}\rangle=0$ in $\langle\mathbf{r}_1'-\mathbf{r}_1,\mathbf{q}\rangle=0$

Ko enačbo (1) vstavimo v enačbi (2) in uredimo, dobimo enačbi:

$$s\langle\mathbf{p},\mathbf{p}\rangle+t\langle\mathbf{q},\mathbf{p}\rangle=\langle\mathbf{r}_1-\mathbf{r}_0,\mathbf{p}\rangle\qquad s\langle\mathbf{p},\mathbf{q}\rangle+t\langle\mathbf{q},\mathbf{q}\rangle=\langle\mathbf{r}_1-\mathbf{r}_0,\mathbf{q}\rangle$$

Rešimo sistem (3) po s in t in vstavimo rezultat v (1). Dobimo $\mathbf{r}_1'$

Poglejmo si še, kako poiščemo pravokotno projekcijo točke $\mathbf{r}_1$ na implicitno podano hiperravnino $\langle\mathbf{n},\mathbf{r}-\mathbf{r}_0\rangle=0$. Iskana točka naj bo $\mathbf{r}_1'$

Iskana točka $\mathbf{r}_1'$ leži na preseku hiperravnine in premice, ki gre skozi točko $\mathbf{r}_1$ in je pravokotna na hiperravnino. Velja torej $\langle\mathbf{n},\mathbf{r}_1'-\mathbf{r}_0\rangle=0$

in obstaja tak parameter t, da velja: $\mathbf{r}_1'=\mathbf{r}_1+t\mathbf{n}$

Vstavimo enačbo (5) v enačbo (4) in izrazimo t. $t=-\dfrac{\langle\mathbf{r}_1-\mathbf{r}_0,\mathbf{n}\rangle}{\langle\mathbf{n},\mathbf{n}\rangle}$

skalar (6) vstavimo v enačbo (5)

Sedaj lahko določimo tudi oddajenost točke $\mathbf{r}_1$ od (hiper)ravnine $d=\|\mathbf{r}_1-\mathbf{r}_1'\|$ pa zrcalno sliko točke $\mathbf{r}_1$ glede na (hiper)ravnino $\mathbf{r}_1''=2\mathbf{r}_1'-\mathbf{r}_1$

Sistemi linearnih enačb

Primer projekcije točke na ravnino

Izračunaj pravokotno projekcijo točke $(1,1,1)$ na ravnino $x+2y+3z=4$.

V formulo
$$\mathbf{r}_1' = \mathbf{r}_1 - \frac{\langle \mathbf{r}_1 - \mathbf{r}_0, \mathbf{n}\rangle}{\langle \mathbf{n}, \mathbf{n}\rangle}\mathbf{n}$$
vstavimo $\mathbf{n}=(1,2,3)$, $\mathbf{r}_0=(4,0,0)$, $\mathbf{r}_1=(1,1,1)$ in dobimo
$$\mathbf{r}_1' = \frac{1}{7}(6,5,4).$$

množica rešitev 3 × 2 sistema je **ravnina**, **premica** v ravnini, točka v ravnini ali pa **prazna množica**

Primeri 2×2 sistemov

Množica rešitev 2×2 sistema je lahko

- cela ravnina (samo pri sistemu $0x+0y=0, 0x+0y=0$)
- premica v ravnini (npr. pri sistemu $2x+y=1, 4x+2y=2$ prva enačba določa isto premico kot druga enačba, torej je množica rešitev sistema presek dveh enakih premic.)
- točka v ravnini (npr. pri sistemu $x+y=1, x-y=3$ je množica rešitev presek dveh nevzporednih premic)
- prazna množica (npr. pri sistemu $2x+1=1, 4x+2y=3$) je množica rešitev presek dveh različnih vzporednih premic).

$$\begin{aligned} 2x-y+3u-2v &= 1,\\ x+y+2u-2v &= 0,\\ x+2u-3v &= -2. \end{aligned}$$

Množica rešitev 2 × 3 sistema je cel **prostor** R^3, **ravnina** v prostoru, **premica** v prostoru ali pa **prazna množica**, ne more pa biti točka v prostoru!

Primer reševanja sistema z Gaussovo metodo

$$x = \frac{1+y-3u+2v}{2}$$

Ko formulo za x vstavimo v drugo in tretjo enačbo, dobimo novi enačbi

$$\frac{3}{2}y+\frac{1}{2}u-v = -\frac{1}{2}$$
$$\frac{1}{2}y+\frac{1}{2}u-2v = -\frac{5}{2}$$

Iz prve nove enačbe dobimo

$$y = \frac{-\frac{1}{2}-\frac{1}{2}u+v}{\frac{3}{2}} = \frac{-1-u+2v}{3}$$

Ko izraz za y vstavimo v drugo novo enačbo in uredimo, dobimo

$$\left.\begin{aligned} \frac{1}{3}u-\frac{5}{3}v &= -\frac{7}{3}\\ u = \frac{-\frac{7}{3}+\frac{5}{3}v}{\frac{1}{3}} &= -7+5v \end{aligned}\right\} \qquad \begin{aligned} y &= \frac{6-3v}{3} = 2-v\\ x &= \frac{22+y-13v}{2} \end{aligned}$$

Sedaj še formulo za y vstavimo v formulo za x in dobimo

$$x = \frac{24-14v}{2} = 12-7v$$

Končna rešitev je $x=12-7v$, $y=2-v$ in $u=-7+5v$

$$\mathbf{r} = (x,y,u,v) = (12-7v, 2-v, -7+5v, v) = (12,2,-7,0)+v(-7,-1,5,1)$$

Primer reševanja sistema z izločanjem spremenljivk

Najprej zapišemo razširjeno matriko sistema:

$$\left[\begin{array}{cccc|c} 2 & -1 & 3 & -2 & 1\\ 1 & 1 & 2 & -2 & 0\\ 1 & 0 & 2 & -3 & -2 \end{array}\right] \longrightarrow \left[\begin{array}{cccc|c} 1 & 1 & 2 & -2 & 0\\ 2 & -1 & 3 & -2 & 1\\ 1 & 0 & 2 & -3 & -2 \end{array}\right] \longrightarrow \left[\begin{array}{cccc|c} 1 & 1 & 2 & -2 & 0\\ 0 & -3 & -1 & 2 & 1\\ 0 & -1 & 0 & -1 & -2 \end{array}\right]$$

$$\downarrow$$

$$\left[\begin{array}{cccc|c} 1 & 1 & 2 & -2 & 0\\ 0 & 1 & 0 & 1 & 2\\ 0 & 0 & 1 & -5 & -7 \end{array}\right] \longleftarrow \left[\begin{array}{cccc|c} 1 & 1 & 2 & -2 & 0\\ 0 & 1 & 0 & 1 & 2\\ 0 & 0 & -1 & 5 & 7 \end{array}\right] \longleftarrow \left[\begin{array}{cccc|c} 1 & 1 & 2 & -2 & 0\\ 0 & 1 & 0 & 1 & 2\\ 0 & -3 & -1 & 2 & 1 \end{array}\right]$$

$$\downarrow$$

Na koncu k prvi vrstici prištejemo z -1 pomnoženo drugo vrstico
Dobimo reducirano vrstično stopničasto formo:

$$\left[\begin{array}{cccc|c} 1 & 1 & 0 & 8 & 14\\ 0 & 1 & 0 & 1 & 2\\ 0 & 0 & 1 & -5 & -7 \end{array}\right] \longrightarrow \left[\begin{array}{cccc|c} 1 & 0 & 0 & 7 & 12\\ 0 & 1 & 0 & 1 & 2\\ 0 & 0 & 1 & -5 & -7 \end{array}\right]$$

Če reducirano vrstično formo zapišemo s spremenljivkami, dobimo

$$x+7v = 12 \qquad y+v = 2 \qquad u-5v = -7$$

Odtod izrazimo spremenljivke x,y,u s spremenljivko v:

$$x = 12-7v \qquad y = 2-v \qquad u = -7+5v$$

Primer iskanja najkrajše rešitve poddoločenega sistema

Poišči najkrajšo rešitev sistema

$$\begin{aligned} 2x-y+3u-2v &= 1,\\ x+y+2u-2v &= 0,\\ x+2u-3v &= -2. \end{aligned}$$

Najprej sistem zapišemo v obliki

$$\langle \mathbf{n}_1, \mathbf{r}\rangle = 1, \quad \langle \mathbf{n}_2, \mathbf{r}\rangle = 0, \quad \langle \mathbf{n}_3, \mathbf{r}\rangle = -2,$$

kjer je $\mathbf{r}=(x,y,u,v)$ in

$$\mathbf{n}_1 = (2,-1,3,-2), \quad \mathbf{n}_2 = (1,1,2,-2), \quad \mathbf{n}_3 = (1,0,2,-3).$$

Rešitev iščemo z nastavkom $\mathbf{r} = t_1\mathbf{n}_1 + t_2\mathbf{n}_2 + t_3\mathbf{n}_3$.

Dobimo sistem

$$\begin{aligned} 18t_1+11t_2+14t_3 &= 1,\\ 11t_1+10t_2+11t_3 &= 0,\\ 14t_1+11t_2+14t_3 &= -2, \end{aligned}$$

katerega rešitev je

$$t_1 = \frac{3}{4}, \quad t_2 = \frac{22}{19}, \quad t_3 = -\frac{137}{76}.$$

Ko te vrednosti vstavimo v nastavek, dobimo

$$\mathbf{r} = t_1\mathbf{n}_1 + t_2\mathbf{n}_2 + t_3\mathbf{n}_3 = \left(\frac{65}{76}, \frac{31}{76}, \frac{73}{76}, \frac{121}{76}\right).$$

To je iskana najkrajša rešitev prvotnega sistema.

drug način reševanja je da sistem najprej **rešimo** in nato **projiciramo izhodišče** na **množico** rešitev

Preprost primer predoločenega sistema

Poiščimo posplošeno rešitev 3×2 sistema

$$x=0, \quad y=0, \quad x+y=1.$$

Sistem je očitno nerešljiv. Zapišimo ga v vektorski obliki

$$(0,0,1) = (x,y,x+y) = x(1,0,1)+y(0,1,1)$$

Razliko leve in desne strani skalarno množimo z $(1,0,1)$ in z $(0,1,1)$:

$$\langle x(1,0,1)+y(0,1,1)-(0,0,1),(1,0,1)\rangle = 0$$
$$\langle x(1,0,1)+y(0,1,1)-(0,0,1),(0,1,1)\rangle = 0.$$

Ko uredimo, dobimo sistem enačb

$$2x+y=1, \quad x+2y=1.$$

Običajna rešitev tega sistema je $x=y=\frac{1}{3}$. To je potem tudi posplošena rešitev prvotnega sistema.

Primer

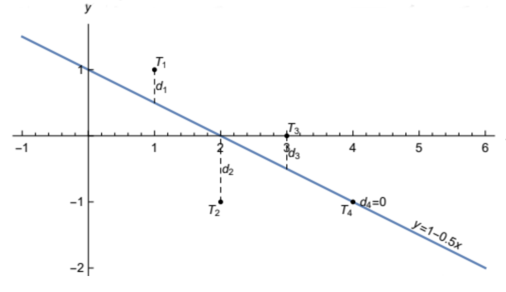
Poišči premico, ki se najbolje prilega točkam $(1,1),(2,-1),(3,0),(4,-1)$.
Najprej izračunamo

$$\sum_{i=1}^{4} x_i^2 = 30, \quad \sum_{i=1}^{4} x_i = 10, \quad \sum_{i=1}^{4} x_iy_i = -5, \quad \sum_{i=1}^{4} y_i = -1$$

in rezultate vstavimo v sistem (8). Dobimo sistem enačb

$$30a+10b=-5, \quad 10a+4b=-1$$

katerega rešitev je $a=-\frac{1}{2}, b=1$. Iskana premica je torej $y=1-0.5x$.



podobno bi poiskali tudi ravnino ki se najbolje prilega točkam v ravnini **z = ax + by + c**

podobno bi poiskali tudi parabolo **y = ax² + bx + c**

$$\begin{aligned} a\sum x_i^2 + b\sum x_iy_i + c\sum x_i &= \sum x_iz_i\\ a\sum x_iy_i + b\sum y_i^2 + c\sum y_i &= \sum y_iz_i\\ a\sum x_i + b\sum y_i + c\sum 1 &= \sum z_i \end{aligned}$$

$$\begin{aligned} a\sum x_i^4 + b\sum x_i^3 + c\sum x_i^2 &= \sum x_i^2y_i\\ a\sum x_i^3 + b\sum x_i^2 + c\sum x_i &= \sum x_iy_i\\ a\sum x_i^2 + b\sum x_i + c\sum 1 &= \sum y_i \end{aligned}$$

Matrike

Primer množenja dveh matrik

Zmnožimo matriki

$$A = \begin{bmatrix} 1 & 2 \\ -2 & 0 \end{bmatrix} \quad \text{in} \quad B = \begin{bmatrix} -1 & 1 \\ 3 & 2 \end{bmatrix}.$$

Velja

$$AB = \begin{bmatrix} 5 & 5 \\ 2 & -2 \end{bmatrix} \quad \text{in} \quad BA = \begin{bmatrix} -3 & -2 \\ -1 & 6 \end{bmatrix}.$$

Torej ni vseeno, v kakšnem vrstnem redu zmnožimo dve matriki.

Primer posplošene rešitve sistema

Posplošena rešitev sistema

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

se ujema z običajno rešitvijo sistema

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

Ko zmnožimo matrike, dobimo sistem

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

ki ima rešitev $x = y = \frac{1}{3}$. To je posplošena rešitev prvotnega sistema.

Primeri matrik, ki nimajo inverza

Če ima matrika A ničelno vrstico, potem nima inverza. Za vsako matriko B ima namreč produkt AB tudi ničelno vrstico, medtem ko matrika I nima ničelne vrstice. Torej je $AB \neq I$ za vsak B.

Če ima matrika A ničeln stolpec, potem nima inverza. Za vsako matriko B ima namreč produkt BA tudi ničeln stolpec, medtem ko matrika I nima ničelnega stolpca. Torej je $BA \neq I$ za vsak B.

Primeri matrik, ki imajo inverz

Elementarne matrike imajo inverze. Velja namreč

$$E_{i,j}(\alpha)^{-1} = E_{i,j}(-\alpha), \quad P_{i,j}^{-1} = P_{i,j} \quad \text{in} \quad E_i(\beta)^{-1} = E_i(\frac{1}{\beta}).$$

Inverze matrik lahko uporabimo pri reševanju kvadratnih linearnih sistemov. Če $A\mathbf{x} = \mathbf{b}$ pomnožimo z leve z A^{-1}, dobimo

$$\mathbf{x} = I\mathbf{x} = (A^{-1}A)\mathbf{x} = A^{-1}(A\mathbf{x}) = A^{-1}\mathbf{b}.$$

Naredimo še preizkus

$$A(A^{-1}\mathbf{b}) = (AA^{-1})\mathbf{b} = I\mathbf{b} = \mathbf{b}.$$

Primer - Regresijska premica v matričnem zapisu

Premico $y = ax + b$, ki se najbolje prilega točkam $(x_i, y_i), i = 1, \dots,$ dobimo kot posplošeno rešitev sistema

$$\begin{bmatrix} x_1 & 1 \\ \vdots & \vdots \\ x_m & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix}$$

se pravi kot običajno rešitev sistema

$$\begin{bmatrix} x_1 & \dots & x_m \\ 1 & \dots & 1 \end{bmatrix} \begin{bmatrix} x_1 & 1 \\ \vdots & \vdots \\ x_m & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} x_1 & \dots & x_m \\ 1 & \dots & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix}$$

Ko zmnožimo matrike, dobimo sistem

$$\begin{bmatrix} \sum_{i=1}^m x_i^2 & \sum_{i=1}^m x_i \\ \sum_{i=1}^m x_i & m \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^m x_i y_i \\ \sum_{i=1}^m y_i \end{bmatrix}$$

Primeri elementarnih 2 × 2 matrik

$$E_{1,2}(7) = \begin{bmatrix} 1 & 7 \\ 0 & 1 \end{bmatrix}$$

$$P_{1,2} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$E_2(5) = \begin{bmatrix} 1 & 0 \\ 0 & 5 \end{bmatrix}$$

Primer najkrajše rešitve sistema

Poiščimo najkrajšo rešitev sistema

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} -2 \\ 0 \end{bmatrix}$$

Pomagamo si z nastavkom

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} u \\ v \end{bmatrix}$$

Ko vstavimo nastavek v sistem in uredimo, dobimo nov sistem

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} -2 \\ 0 \end{bmatrix}$$

katerega rešitev je $u = -\frac{4}{3}$, $v = \frac{2}{3}$.

Najkrajša rešitev prvotnega sistema je torej

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -\frac{4}{3} \\ \frac{2}{3} \end{bmatrix} = \begin{bmatrix} -\frac{4}{3} \\ -\frac{2}{3} \\ \frac{2}{3} \end{bmatrix}$$

Primer

Če imajo matrike $A_1, \dots, A_n$ inverze, potem ima inverz tudi njihov produkt. Velja namreč

$$(A_1 \cdots A_n)^{-1} = A_n^{-1} \cdots A_1^{-1}.$$

iskanje inverza matrike A

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

$$[A|I] = \left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 3 & 4 & 0 & 1 \end{array}\right]$$

$$\left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & -2 & -3 & 1 \end{array}\right]$$

$$\left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 1 & \frac{3}{2} & -\frac{1}{2} \end{array}\right]$$

$$\left[\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & 1 & \frac{3}{2} & -\frac{1}{2} \end{array}\right]$$

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

Determinante

Primer - determinata 2 × 2 matrike

Izpeljimo formulo za determinante matrik velikosti 2×2. Če je

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix},$$

potem je $A_{1,1} = [a_{2,2}]$ in $A_{1,2} = [a_{2,1}]$. Po definiciji determinant matrik velikosti 1×1 je $\det A_{1,1} = a_{2,2}$ in $\det A_{1,2} = a_{2,1}$. Zato velja

$$\det A = a_{1,1} \det A_{1,1} - a_{1,2} \det A_{1,2} = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}.$$

Potem je

$$\det A = a_{1,1} \det A_{1,1} - a_{1,2} \det A_{1,2} + a_{1,3} \det A_{1,3}$$

kjer je

$$A_{1,1} = \begin{bmatrix} a_{2,2} & a_{2,3} \\ a_{3,2} & a_{3,3} \end{bmatrix}, \quad A_{1,2} = \begin{bmatrix} a_{2,1} & a_{2,3} \\ a_{3,1} & a_{3,3} \end{bmatrix} \quad \text{in} \quad A_{1,3} = \begin{bmatrix} a_{2,1} & a_{2,2} \\ a_{3,1} & a_{3,2} \end{bmatrix}$$

Po formuli iz prejšnjega primera je

$$\begin{aligned} \det A_{1,1} &= a_{2,2}a_{3,3} - a_{2,3}a_{3,2}, \\ \det A_{1,2} &= a_{2,1}a_{3,3} - a_{2,3}a_{3,1}, \\ \det A_{1,3} &= a_{2,1}a_{3,2} - a_{2,2}a_{3,1}. \end{aligned}$$

Zato velja

$$\begin{aligned} \det A &= a_{1,1}(a_{2,2}a_{3,3} - a_{2,3}a_{3,2}) - a_{1,2}(a_{2,1}a_{3,3} - a_{2,3}a_{3,1}) + a_{1,3}(a_{2,1}a_{3,2} - a_{2,2}a_{3,1}) \\ &= a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} - a_{1,3}a_{2,2}a_{3,1} - a_{1,2}a_{2,1}a_{3,3} - a_{1,1}a_{2,3}a_{3,2}. \end{aligned}$$

Primer

Izračunajmo determinanto matrike

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

z razvojem po prvem stolpcu. Velja

$$\det A = 2 \cdot \det \begin{bmatrix} 1 & -1 \\ -1 & 3 \end{bmatrix} - 0 \cdot \det \begin{bmatrix} 1 & 1 \\ -1 & 3 \end{bmatrix} + 1 \cdot \det \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= 2 \cdot 2 - 0 \cdot 4 + 1 \cdot (-2) = 2.$$

Primer

Naj bo

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Potem je $\det(A + B) = \det I = 1$ in $\det A + \det B = 0 + 0 = 0$. Torej je

$$\det(A + B) \neq \det A + \det B$$

Naj bo sedaj $C = I$ in $\alpha = 2$. Potem je $\det(\alpha C) = 4$ in $\alpha \det C = 2$, torej

$$\det(\alpha C) \neq \alpha \det C$$

Primer

S pomočjo Gaussove metode izračunaj determinanto matrike

$$A=\begin{bmatrix}1&2&1&2\\2&0&1&-1\\-1&1&1&-1\\0&2&2&1\end{bmatrix}.$$

S transformacijama $E_{2,1}(-2)$ in $E_{3,1}(1)$ dobimo

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

S transformacijama $E_{3,2}(\frac{3}{4})$ in $E_{4,2}(\frac{1}{2})$ dobimo

$$\det A=\det\begin{bmatrix}1&2&1&2\\0&-4&-1&-5\\0&0&\frac{5}{4}&-\frac{11}{4}\\0&0&\frac{3}{2}&-\frac{3}{2}\end{bmatrix}.$$

S transformacijo $E_{4,3}(-\frac{6}{5})$ dobimo

$$\det A=\det\begin{bmatrix}1&2&1&2\\0&-4&-1&-5\\0&0&\frac{5}{4}&-\frac{11}{4}\\0&0&0&\frac{9}{5}\end{bmatrix}.$$

Formula za determinanto zgornje trikotne matrike nam da

$$\det A=1\cdot(-4)\cdot\frac{5}{4}\cdot\frac{9}{5}=-9.$$

Reševanje 3×3 sistema s Cramerovim pravilom

S pomočjo Cramerovega pravila rešimo sistem

$$\begin{aligned}x+y+2z&=1\\2x-y&=1\\3y+z&=-1.\end{aligned}$$

Ker je

$$\det A=\det\begin{bmatrix}a_{1,1}&a_{1,2}&a_{1,3}\\a_{2,1}&a_{2,2}&a_{2,3}\\a_{3,1}&a_{3,2}&a_{3,3}\end{bmatrix}=\det\begin{bmatrix}1&1&2\\2&-1&0\\0&3&1\end{bmatrix}=9,$$

je rešitev sistema

$$x=\frac{\det\begin{bmatrix}b_1&a_{1,2}&a_{1,3}\\b_2&a_{2,2}&a_{2,3}\\b_3&a_{3,2}&a_{3,3}\end{bmatrix}}{\det A}=\frac{\det\begin{bmatrix}1&1&2\\1&-1&0\\-1&3&1\end{bmatrix}}{\det A}=\frac{2}{9},$$

$$y=\frac{\det\begin{bmatrix}a_{1,1}&b_1&a_{1,3}\\a_{2,1}&b_2&a_{2,3}\\a_{3,1}&b_3&a_{3,3}\end{bmatrix}}{\det A}=\frac{\det\begin{bmatrix}1&1&2\\2&1&0\\0&-1&1\end{bmatrix}}{\det A}=\frac{-5}{9},$$

$$z=\frac{\det\begin{bmatrix}a_{1,1}&a_{1,2}&b_1\\a_{2,1}&a_{2,2}&b_2\\a_{3,1}&a_{3,2}&b_3\end{bmatrix}}{\det A}=\frac{\det\begin{bmatrix}1&1&1\\2&-1&1\\0&3&-1\end{bmatrix}}{\det A}=\frac{6}{9}=\frac{2}{3}.$$

Primer

$$\det\begin{bmatrix}a_{1,1}&a_{1,2}&a_{1,3}\\a_{2,1}&a_{2,2}&a_{2,3}\\a_{3,1}&a_{3,2}&a_{3,3}\end{bmatrix}=$$

$$=\operatorname{sgn}\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}a_{1,1}a_{2,2}a_{3,3}+\operatorname{sgn}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}a_{1,2}a_{2,1}a_{3,3}+$$

$$+\operatorname{sgn}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}a_{1,3}a_{2,2}a_{3,1}+\operatorname{sgn}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}a_{1,1}a_{2,3}a_{3,2}+$$

$$+\operatorname{sgn}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}a_{1,2}a_{2,3}a_{3,1}+\operatorname{sgn}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}a_{1,3}a_{2,1}a_{3,2}$$

Polgrupa vseh $n\times n$ matrik

Naj bo $M_n(\mathbb{R})$ množica vseh $n\times n$ matrik in naj bo $\cdot$ množenje matrik. Potem je $(M_n(\mathbb{R}),\cdot)$ polgrupa. Če je $n\geq 2$, ta polgrupa ni komutativna.

Primeri komutativnih polgrup

Naj bo $\mathbb{N}=\{1,2,\ldots\}$ množica vseh naravnih števil. Množenje in seštevanje naravnih števil sta operaciji, ki sta tako komutativni kot asociativni. Torej sta $(\mathbb{N},\cdot)$ in $(\mathbb{N},+)$ komutativni polgrupi.

Primer

$$\det\begin{bmatrix}1&2&3&4&5&6\\7&8&9&10&11&12\\0&0&13&14&15&16\\0&0&17&18&19&20\\0&0&0&0&21&22\\0&0&0&0&23&24\end{bmatrix}=\det\begin{bmatrix}1&2\\7&8\end{bmatrix}\det\begin{bmatrix}13&14&15&16\\17&18&19&20\\0&0&21&22\\0&0&23&24\end{bmatrix}$$

$$=\det\begin{bmatrix}1&2\\7&8\end{bmatrix}\det\begin{bmatrix}13&14\\17&18\end{bmatrix}\det\begin{bmatrix}21&22\\23&24\end{bmatrix}=(-6)(-4)(-2)=-48$$

Primer kofaktorske matrike

$$A=\begin{bmatrix}a&b\\c&d\end{bmatrix}\Rightarrow\qquad \tilde{A}=\begin{bmatrix}d&-c\\-b&a\end{bmatrix}$$

$$A=\begin{bmatrix}a&b&c\\d&e&f\\g&h&i\end{bmatrix}\Rightarrow\qquad \tilde{A}=\begin{bmatrix}ei-fh&fg-di&dh-eg\\ch-bi&ai-cg&bg-ah\\bf-ce&cd-af&ae-bd\end{bmatrix}$$

Reševanje 2×2 sistema s Cramerovim pravilom

Rešimo naslednji sistem s Cramerovim pravilom:

$$\begin{aligned}2x+y&=-1,\\x+3y&=2.\end{aligned}$$

Rešitev se glasi

$$x=\frac{\det\begin{bmatrix}b_1&a_{1,2}\\b_2&a_{2,2}\end{bmatrix}}{\det\begin{bmatrix}a_{1,1}&a_{1,2}\\a_{2,1}&a_{2,2}\end{bmatrix}}=\frac{\det\begin{bmatrix}-1&1\\2&3\end{bmatrix}}{\det\begin{bmatrix}2&1\\1&3\end{bmatrix}}=\frac{-5}{5}=-1,$$

$$y=\frac{\det\begin{bmatrix}a_{1,1}&b_1\\a_{2,1}&b_2\end{bmatrix}}{\det\begin{bmatrix}a_{1,1}&a_{1,2}\\a_{2,1}&a_{2,2}\end{bmatrix}}=\frac{\det\begin{bmatrix}2&-1\\1&2\end{bmatrix}}{\det\begin{bmatrix}2&1\\1&3\end{bmatrix}}=\frac{5}{5}=1.$$

Signature permutacij iz S_3

$$\begin{aligned}
\operatorname{sgn}\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}&=\det I=1\\
\operatorname{sgn}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}&=\det P_{1,2}=-1\\
\operatorname{sgn}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}&=\det P_{1,3}=-1\\
\operatorname{sgn}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}&=\det P_{2,3}=-1\\
\operatorname{sgn}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}&=\det\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}=1\\
\operatorname{sgn}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}&=\det\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}=1
\end{aligned}$$

Primeri permutacij

Vseh preslikav iz $\mathbb{N}_3$ v $\mathbb{N}_3$ je 27. Od teh jih je 6 bijektivnih:

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

Primer - Inverz 3×3 matrike

$$A=\begin{bmatrix}a&b&c\\d&e&f\\g&h&i\end{bmatrix}\Rightarrow A^{-1}=\frac{1}{\det A}\begin{bmatrix}ei-fh&ch-bi&bf-ce\\fg-di&ai-cg&cd-af\\dh-eg&bg-ah&ae-bd\end{bmatrix}$$

kjer $\det A=aei+bfg+cdh-ceg-afh-bdi$.

Primer - Inverz 2×2 matrike

Če je

$$A=\begin{bmatrix}a&b\\c&d\end{bmatrix}$$

potem je

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

Primeri

Če za σ vzamemo identično preslikavo, dobimo $P_\sigma=I$ in $\operatorname{sgn}(\sigma)=1$.

Če za σ vzamemo **transpozicijo** elementov i in j, se pravi permutacijo

$$\sigma(k)=\begin{cases}j & \text{če } k=i\\ i & \text{če } k=j\\ k & \text{če } k\neq i,j\end{cases}$$

dobimo $P_\sigma=P_{i,j}$ in $\operatorname{sgn}(\sigma)=\det P_{i,j}=-1$.

Algebrske strukture

Primer grupoida, ki ni polgrupa

Vektorski produkt je očitno operacija na $\mathbb{R}^3$. Pokažimo, da ta operacija ni niti asociativna niti komutativna. Velja namreč

$$\mathbf{e}_1\times\mathbf{e}_2=\mathbf{e}_3\qquad(\mathbf{e}_1\times\mathbf{e}_1)\times\mathbf{e}_2=\mathbf{0}$$

$$\mathbf{e}_2\times\mathbf{e}_1=-\mathbf{e}_3\qquad\mathbf{e}_1\times(\mathbf{e}_1\times\mathbf{e}_2)=\mathbf{e}_1\times\mathbf{e}_3=-\mathbf{e}_2$$

Grupoid $(\mathbb{R}^3,\times)$ torej ni komutativen in ni polgrupa.

Polgrupa vseh besed s črkami iz A

Naj bo A neprazna množica črk. Naj bo M množica vseh besed, ki jih lahko sestavimo s črkami iz A. Operacija $\circ$ naj bo stikanje besed.

Recimo aba in bab sta dve besedi s črkami iz $A=\{a,b\}$. Če ju staknemo, dobimo besedo $aba\circ bab=ababab$. To ni isto kot $bab\circ aba=bababa$.

Očitno je stikanje besed asociativna operacija, torej je $(M,\circ)$ polgrupa.

Če množica A vsebuje vsaj dve črki, potem je ta polgrupa nekomutativna.

Polgrupa vseh preslikav iz S v S

2) Naj bo S poljubna množica in naj bo F_S množica vseh funkcij iz S v S. Operacija $\circ$ naj bo kompozitum dveh funkcij. Potem je $(F_S, \circ)$ polgrupa. Za vse funkcije $f, g, h \in F_S$ in vse elemente $s \in S$ namreč velja

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

Če ima S vsaj tri različne elemente potem polgrupa $(F_S, \circ)$ ni komutativna. Recimo, da so $a, b, c \in S$ paroma različni elementi. Naj bo f transpozicija elementov a in b, g pa transpozicija elementov a in c. Potem velja, da $f(g(a)) = f(c) = c$ ni enak $g(f(a)) = g(b) = b$. Torej $f \circ g \neq g \circ f$.

Primeri enot

- Polgrupa $(\mathbb{N}, \cdot)$ ima enoto 1. Polgrupa $(\mathbb{N}, +)$ nima enote, ker $0 \notin \mathbb{N}$.
- Polgrupa $(M_n(\mathbb{R}), \cdot)$ ima za enoto identično $n \times n$ matriko I_n.
- Polgrupa $(F_S, \circ)$ ima za enoto **identično preslikavo** iz S v S. To je preslikava definirana z $\mathrm{id}_S(x) = x$ za vsak $x \in S$.
- Polgrupa vseh besed s črkami iz A ima za enoto prazno besedo.
- Grupoid $(\mathbb{R}^3, \times)$ nima niti leve niti desne enote.

Primer: Inverzi števil

- Množica vseh celih števil $\mathbb{Z}$ je grupa za operacijo seštevanja $+$. Očitno je namreč $(\mathbb{Z}, +)$ monoid z enoto 0 in vsak $x \in \mathbb{Z}$ ima inverz $-x \in \mathbb{Z}$.
- Tudi $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ so grupe.
- $(\mathbb{Q}, \cdot)$ je monoid z enoto 1, ampak ni grupa, ker element 0 ni obrnljiv. Vsak neničeln element $x \in \mathbb{Q}$ ima inverz $\frac{1}{x}$. Množica obrnljivih elementov v $\mathbb{Q}$ je torej $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$. Vemo, da je $(\mathbb{Q}^\times, \cdot)$ grupa.
- Tudi $(\mathbb{R}^\times, \cdot)$ in $(\mathbb{C}^\times, \cdot)$ sta grupi.

Primer: Aditivna grupa matrik

Naj bo $M_{m,n}(\mathbb{R})$ množica vseh $m \times n$ matrik in naj bo operacija $+$ seštevanje matrik. Potem je $(M_{m,n}(\mathbb{R}), +)$ Abelova grupa z enoto $0_{m,n}$. Inverz matrike A v tej Abelovi grupi je matrika $-A$.

Primer: Inverzi matrik

Naj bo $M_n(\mathbb{R})$ množica vseh $n \times n$ matrik in naj bo $\cdot$ operacija množenja matrik. Pokazali smo, da je $(M_n(\mathbb{R}), \cdot)$ polgrupa z enoto I_n, torej monoid.

Vemo, da je matrika $A \in M_n(\mathbb{R})$ obrnljiva natanko tedaj, ko je $\det A \neq 0$. V tem primeru je $A^{-1} = \frac{1}{\det A} \tilde{A}^T$. Vemo tudi, da iz $AB = I$ sledi $BA = I$, torej pojmi levega inverza, desnega inverza in inverza sovpadejo.

Grupo vseh obrnljivih $n \times n$ matrik označimo z $\mathrm{GL}_n(\mathbb{R})$. Pravimo ji n-ta **glavna linearna grupa**.

Primeri

- Množica sodih naravnih števil je podpolgrupa v $(\mathbb{N}, +)$ in v $(\mathbb{N}, \cdot)$.
- Množica lihih naravnih števil je podmonoid v $(\mathbb{N}, \cdot)$.
- Množica vseh matrik oblike $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ je podpolgrupa v $(M_2(\mathbb{R}), \cdot)$.
- Množica 2×2 matrik s elementi ≥ 0 je podmonoid v $(M_2(\mathbb{R}), +)$.
- Množica vseh besed, ki se začnejo z črko a je podpolgrupa v monoidu vseh besed. (Operacija je stikanje besed.)
- Množica vseh funkcij oblike $kx + n$ je podmonoid v monoidu vseh funkcij iz $\mathbb{R}$ v $\mathbb{R}$. (Operacija je kompozitum funkcij.)
- Množica vseh polinomov s pozitivnim vodilnim koeficientom je podpolgrupa v $(\mathbb{R}[x], +)$ ter podmonoid v $(\mathbb{R}[x], \cdot)$ in v $(\mathbb{R}[x], \circ)$.

Primer podpolgrupe z različno enoto

Množica $M = \mathbb{N} \times \mathbb{N}$ je monoid za operacijo $(a, b) \circ (c, d) = (ac, bd)$. Monoid $(M, \circ)$ ima enoto $e = (1, 1)$. Podmnožica $N = \mathbb{N} \times \{0\}$ je zaprta za $\circ$ in ne vsebuje e. Torej je N podpolgrupa, ki ni podmonoid. Polgrupa $(N, \circ_N)$ ima enoto $f = (1, 0)$. Očitno f ni enaka enoti monoida $(M, \circ)$.

Primer podgrupoida

Vemo, da je $(\mathbb{R}^3, \times)$ grupoid, ki ni polgrupa. Naj bo $N \subseteq \mathbb{R}^3$ premica skozi izhodišče, se pravi linearna ogrinjača nekega vektorja. Za vsaka elementa $\mathbf{a}, \mathbf{b} \in N$ velja $\mathbf{a} \times \mathbf{b} = \mathbf{0}$, kar je element N.

Primeri podgrup v $\mathrm{GL}_n(\mathbb{R})$

Spomnimo se, da je $\mathrm{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$. Definirajmo:

- $\mathrm{SL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A = 1\}$.
- $\mathrm{UT}_n(\mathbb{R}) =$ vse zgornje trikotne $n \times n$ matrike z enkami po diagonali.
- $\mathrm{O}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid A^T A = I\}$.

Te množice so podgrupe v $\mathrm{GL}_n(\mathbb{R})$.

Primer komutativnega grupoida, ki ni polgrupa

Označimo z $M_2(\mathbb{R})$ množico vseh 2×2 matrik. Jordanski produkt na $M_2(\mathbb{R})$ je definiran z

$$A \circ B = \frac{1}{2}(AB + BA)$$

Očitno je ta operacija komutativna. Pokažimo, da ni asociativna. Vzemimo

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

Očitno je $A \circ B = \frac{1}{2} I$ in $A \circ A = 0$. Torej je

$$(A \circ A) \circ B = 0, \qquad A \circ (A \circ B) = A \circ \frac{1}{2} I = \frac{1}{2} A$$

Torej je $(M_2(\mathbb{R}), \circ)$ komutativen grupoid, ki ni polgrupa.

Primer polgrupe, ki ima več levih enot in nobene desne enote

Naj bo

$$M = \{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a, b \in \mathbb{R} \}$$

in naj bo $\circ$ običajno množenje matrik. Ker velja

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix}$$

je produkt dveh matrik iz M spet matrika iz M. Torej je $(M, \circ)$ grupoid. Ker je matrično množenje asociativno, je tudi operacija $\circ$ asociativna. Torej je $(M, \circ)$ polgrupa. Opazimo, da je vsak element oblike

$$\begin{bmatrix} 1 & x \\ 0 & 0 \end{bmatrix}$$

leva enota polgrupe $(M, \circ)$. Imamo torej neskončno levih enot. Odtod in iz prve opombe sledi, da nimamo nobene desne enote.

Primer: Inverzi besed

Naj bo M množica vseh besed nad neko abecedo in naj bo $\circ$ stikanje besed. Potem je $(M, \circ)$ monoid, katerega enota je prazna beseda. Če staknemo neprazno besedo s poljubno besedo, dobimo neprazno besedo. Neprazne besede torej niso obrnljive, saj nimajo niti levega niti desnega inverza. Prazna beseda je seveda obrnljiva in njen inverz je spet prazna beseda.

Primer: Inverzi funkcij

Naj bo S neprazna množica in naj bo F_S množica vseh funkcij iz S v S. Vemo, da je F_S monoid za operacijo kompozitum funkcij. Pokazali bomo, da je funkcija $f: S \to S$ obrnljiva natanko tedaj, ko je bijektivna. Bijektivni funkciji iz S v S pravimo tudi **permutacija** množice S. Grupo vseh permutacij množice S bomo označili z $\mathcal{P}(S)$. Primer je $S_n := \mathcal{P}(\mathbb{N}_n)$.

Ekvivalentnost obrnljivosti in bijektivnosti sledi iz naslednjih dveh trditev:

- Funkcija $f: S \to S$ ima levi inverz natanko tedaj, ko je injektivna.
- Funkcija $f: S \to S$ ima desni inverz natanko tedaj, ko je surjektivna.

Dokaz: Če ima funkcija f levi inverz g, potem iz $f(x) = f(y)$ sledi $x = g(f(x)) = g(f(y)) = y$. Torej je f injektivna.

Če je funkcija f injektivna, potem definirajmo funkcijo $g: S \to S$ takole: Elemente, ki so v zalogi vrednosti funkcije f, preslikamo v njihove originale (ti so zaradi injektivnosti f enolično določeni). Elemente, ki niso v zalogi vrednosti funkcije f, preslikajmo v poljubne elemente. Po definiciji g velja $g(f(x)) = x$ za vsak $x \in S$, torej je g levi inverz f.

Če ima funkcija f desni inverz g, potem iz $y = f(g(y))$ sledi, da je f surjektivna, saj je vsak element $y \in S$ slika nekega elementa $g(y) \in S$.

Če je funkcija f surjektivna, potem definirajmo funkcijo $g: S \to S$ takole: $g(x) =$ poljuben tak $y \in S$, da velja $f(y) = x$. Obstoj y sledi iz definicije surjektivnosti. Iz definicije g sledi, da velja $f(g(x)) = x$ za vsak $x \in S$, torej je g desni inverz f. $\square$

Za konec si oglejmo še konkreten primer. Naj bo $S = \mathbb{N}$ in naj bo funkcija $f: \mathbb{N} \to \mathbb{N}$ definirana z $f(x) = x + 1$. Očitno je f injektivna, ni pa surjektivna. Torej ima f levi inverz, nima pa desnega. Za vsak $a \in \mathbb{N}$ je

$$g(x) = \begin{cases} x - 1 & \text{če } x \geq 2 \\ a & \text{če } x = 1 \end{cases}$$

levi inverz funkcije f. Torej ima f neskončno levih inverzov.

Lahko poiščemo tudi funkcijo iz $\mathbb{N}$ v $\mathbb{N}$, ki ima neskončno desnih inverzov in nobenega levega. Primer je funkcija $f(2x) = x$ in $f(2x - 1) = 1$.

Primer: Ciklične podgrupe

Če je $(G, \circ)$ grupa, potem je za vsak element $a \in G$ množica $\langle a \rangle := \{a^m \mid m \in \mathbb{Z}\}$ podgrupa v $(G, \circ)$. Izraz a^m definiramo z $a^0 = e$, $a^n = \underbrace{a \circ \ldots \circ a}_{\text{n-krat}}$ in $a^{-n} = \underbrace{a^{-1} \circ \ldots \circ a^{-1}}_{\text{n-krat}}$ za vsak $n \in \mathbb{N}$.

Primer: Red cikla

Oglejmo si najprej poseben primer permutacije, ki mu pravimo **cikel**. Naj bodo $a_1, \ldots, a_k$ paroma različni elementi množice $\mathbb{N}_n$. Označimo z

$$(a_1\ a_2\ \ldots\ a_k)$$

permutacijo, ki preslika $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, $\ldots$, $a_{k-1} \mapsto a_k$, $a_k \mapsto a_1$, elemente iz $\mathbb{N}_n \setminus \{a_1, \ldots, a_k\}$ pa preslika same vase.

Pokažimo, da je red elementa $\sigma := (a_1\ a_2\ \ldots\ a_k)$ enak k. Velja

$$\sigma^l(a_i) = \begin{cases} a_{i+l} & \text{če } i + l \leq k \\ a_{i+l-k} & \text{če } i + l > k \end{cases}$$

za vsak $i, l = 1, \ldots, k$. Torej je $\sigma^k = \mathrm{id}$ in $\sigma \neq \mathrm{id}, \ldots, \sigma^{k-1} \neq \mathrm{id}$.

Primeri homomorfizmov

Preslikava $f(x) = 2x$ je homomorfizem polgrup iz $(\mathbb{N}, +)$ v $(\mathbb{N}, +)$, ker velja $f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$ za vsaka $x, y \in \mathbb{N}$.

Preslikava $f(x) = x^2$ je homomorfizem monoidov iz $(\mathbb{N}, \cdot)$ v $(\mathbb{N}, \cdot)$, ker velja $f(xy) = (xy)^2 = x^2y^2 = f(x)f(y)$ za vsaka $x, y \in \mathbb{N}$ in $f(1) = 1$.

Primer: Homomorfizem polgrup, ki ne slika enote v enoto

Vemo, da je $(\mathbb{Z}, \cdot)$ polgrupa z enoto 1 in da je $(\mathbb{Z} \times \mathbb{Z}, \circ)$, kjer $(a, b) \circ (c, d) = (ac, bd)$, polgrupa z enoto $(1, 1)$. Preslikava

$$f \colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}, \quad f(x) = (x, 0)$$

je homomorfizem polgrup, ker $f(xy) = (xy, 0) = (x, 0) \circ (y, 0) = f(x) \circ f(y)$, ampak ne slika enote v enoto, ker $f(1) = (1, 0) \neq (1, 1)$.

Primer

Determinanta $\det\colon M_n(\mathbb{R}) \to \mathbb{R}$ zadošča $\det AB = \det A \det B$ in $\det I_n = 1$. Torej je $\det$ homomorfizem monoidov iz $(M_n(\mathbb{R}), \cdot)$ v $(\mathbb{R}, \cdot)$. Po zgornji trditvi $\det$ slika obrnljive matrike v neničelna realna števila in velja $\det A^{-1} = \frac{1}{\det A}$.

Primer: Homomorfizmi monoidov

Naj bo M množica vseh funkcij iz $\mathbb{R}$ v $\mathbb{R}$ oblike $\phi_{k,l}(x) = kx + l$ in naj bo operacija $\circ$ kompozitum funkcij. Iz $k(k'x + l') + l = kk'x + kl' + l$ sledi $\phi_{k,l} \circ \phi_{k',l'} = \phi_{kk',kl'+l}$. Enota te polgrupe je $\phi_{1,0} = \mathrm{id}$. Preslikava

$$f(\phi_{k,l}) = \begin{bmatrix} k & l \\ 0 & 1 \end{bmatrix}$$

je homomorfizem monoidov iz $(M, \circ)$ v $(M_2(\mathbb{R}), \cdot)$, ker je

$$f(\mathrm{id}) = f(\phi_{1,0}) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$

$$f(\phi_{k,l} \circ \phi_{k',l'}) = f(\phi_{kk',kl'+l}) = \begin{bmatrix} kk' & kl' + l \\ 0 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} k & l \\ 0 & 1 \end{bmatrix} \begin{bmatrix} k' & l' \\ 0 & 1 \end{bmatrix} = f(\phi_{k,l}) f(\phi_{k',l'})$$

Primer: Kolobar funkcij

Naj bo S neprazna množica. Označimo z $\mathbb{R}^S$ množico vseh funkcij iz S v $\mathbb{R}$. Za dve funkciji $f, g \in \mathbb{R}^S$ definiramo funkciji $f + g$ in $f \cdot g$ takole:

$$(f + g)(x) := f(x) + g(x) \quad \text{in} \quad (f \cdot g)(x) := f(x) \cdot g(x)$$

za vsak $x \in S$. $(\mathbb{R}^S, +, \cdot)$ je komutativen in asociativen kolobar z enoto.

Za vajo dokažimo asociativnost seštevanja funkcij. Ostale lastnosti kolobarja se dokaže podobno. Za vse $f, g, h \in \mathbb{R}^S$ in vse $x \in S$ velja

$$(f + (g + h))(x) = f(x) + (g + h)(x) = f(x) + (g(x) + h(x)) =$$
$$= (f(x) + g(x)) + h(x) = (f + g)(x) + h(x) = ((f + g) + h)(x)$$

Primeri kolobarjev

- $(\mathbb{R}^3, +, \times)$ je kolobar, ki ni asociativen, ni komutativen in nima enote.
- $(M_n(\mathbb{R}), +, \cdot)$ je asociativen kolobar z enoto, ki ni komutativen.
- $(\mathbb{Z}, +, \cdot)$ je komutativen in asociativen kolobar z enoto.
- $(\mathbb{R}[x], +, \cdot)$ je komutativen in asociativen kolobar z enoto.

Primeri podgrup v S_n

Spomnimo se, da je S_n grupa vseh permutacij množice $\mathbb{N}_n = \{1, \ldots, n\}$.

- Podmnožica $A_n = \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1\}$ je podgrupa v S_n.
- Naj bo $\sigma = \left(\begin{smallmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{smallmatrix} \right)$. Potem je $Z_n := \langle \sigma \rangle$ podgrupa v S_n.
- Naj bo R neka relacija na množici $\mathbb{N}_n$. Permutacija $\sigma \in S_n$ je **avtomorfizem** relacije R, če iz iRj vedno sledi $\sigma(i)R\sigma(j)$. Množica vseh avtomorfizmov relacije R je podgrupa v S_n.
- Označimo z R relacijo sosednosti oglišč v n-kotniku. Podgrupi vseh avtomorfizmov R pravimo n-ta **diedrska** grupa in jo označimo z D_n.

Primer: Red permutacije

Če cikla σ in τ nimata skupnih elementov, potem velja $\sigma \circ \tau = \tau \circ \sigma$. Potem za vsako naravno število k velja $(\sigma \circ \tau)^k = \sigma^k \circ \tau^k$. Ker σ^k in τ^k nimata skupnih elementov, je $\sigma^k \circ \tau^k = \mathrm{id}$ natanko tedaj, ko je $\sigma^k = \mathrm{id}$ in $\tau^k = \mathrm{id}$. Torej je $(\sigma \circ \tau)^k = \mathrm{id}$ natanko tedaj, ko red σ deli k in red τ deli k. Dokazali smo, da je red $\sigma \circ \tau$ enak najmanjšemu skupnemu večkratniku redov σ in τ. To trditev lahko posplošimo tudi na več ciklov.

Kratek premislek pokaže, da lahko vsako permutacijo zapišemo kot kompozitum disjunktnih ciklov. Torej je njen red enak najmanjšemu skupnemu večkratniku redov teh disjunktnih ciklov.

Izračunajmo red permutacije

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

Najprej izrazimo permutacijo kot kompozitum disjunktnih ciklov. Dobimo $\rho = (1\ 4\ 3) \circ (2\ 5)$. Red cikla $(1\ 4\ 3)$ je enak 3, red cikla $(2\ 5)$ pa je 2. Najmanjši skupni večkratnik 3 in 2 je 6. Torej je red permutacije ρ enak 6.

Primer: Homomorfizem grupoidov

Naj bo $A = [\mathbf{a}_1\ \mathbf{a}_2\ \mathbf{a}_3]$ taka 3×3 matrika, katere stolpci zadoščajo $\mathbf{a}_1 \times \mathbf{a}_2 = \mathbf{a}_3$, $\mathbf{a}_2 \times \mathbf{a}_3 = \mathbf{a}_1$ in $\mathbf{a}_3 \times \mathbf{a}_1 = \mathbf{a}_2$. Potem je preslikava $\mathbf{x} \mapsto A\mathbf{x}$ homomorfizem grupoidov iz $(\mathbb{R}^3, \times)$ v $(\mathbb{R}^3, \times)$. Velja namreč

$$A\mathbf{x} \times A\mathbf{y} = (x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + x_3\mathbf{a}_3) \times (y_1\mathbf{a}_1 + y_2\mathbf{a}_2 + y_3\mathbf{a}_3)$$
$$= (x_1y_2 - x_2y_1)\mathbf{a}_1 \times \mathbf{a}_2 + (x_3y_1 - x_1y_3)\mathbf{a}_3 \times \mathbf{a}_1 + (x_2y_3 - x_3y_2)\mathbf{a}_2 \times \mathbf{a}_3$$
$$= (x_1y_2 - x_2y_1)\mathbf{a}_3 + (x_3y_1 - x_1y_3)\mathbf{a}_2 + (x_2y_3 - x_3y_2)\mathbf{a}_1 = A(\mathbf{x} \times \mathbf{y})$$

Primeri homomorfizmov grup

- Determinanta je homomorfizem grup iz $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ v $(\mathbb{R}^\times, \cdot)$, ker velja $\det AB = \det A \det B$.
- Preslikava $\sigma \mapsto P_\sigma := [\mathbf{e}_{\sigma(1)} \ldots \mathbf{e}_{\sigma(n)}]$ je homomorfizem grup iz $(S_n, \circ)$ v $(\mathrm{GL}_n(\mathbb{R}), \cdot)$, ker velja $P_{\sigma \circ \tau} = P_\sigma P_\tau$.
- Signatura permutacije je homomorfizem grup iz $(S_n, \circ)$ v $(\mathbb{R}^\times, \cdot)$, ker velja $\mathrm{sgn}(\sigma \circ \tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)$.

Primer izomorfizma grup

Naj bo $G_1 = \{0, 1, 2\}$ in $G_2 = \{e, a, b\}$. Operaciji naj bosta definirani z

$$\begin{array}{c|ccc} \circ_1 & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array} \qquad \text{in} \qquad \begin{array}{c|ccc} \circ_2 & e & a & b \\ \hline e & e & a & b \\ a & a & b & e \\ b & b & e & a \end{array}$$

Potem sta $(G_1, \circ_1)$ in $(G_2, \circ_2)$ grupi. Izomorfizem je $0 \mapsto e, 1 \mapsto a, 2 \mapsto b$. S preimenovanjem elementov v tabeli za $\circ_1$ smo dobili ravno tabelo za $\circ_2$.

Primeri polkolobarjev, ki niso kolobarji

- $(\mathbb{N}, +, \cdot)$ je polkolobar, ki ni kolobar. $(\mathbb{Z}, +, \cdot)$ je kolobar.
- Naj bo M_S množica vseh podmnožic dane množice S. Potem je M_S polkolobar za operaciji unija in presek množic.
- $(\mathbb{R}^{>0}, +, \cdot)$ je polkolobar, ki ni kolobar. $(\mathbb{R}, +, \cdot)$ je kolobar
- Na $\mathbb{R}$ vzemimo za $a + b$ maksimum a in b in za $a \cdot b$ običajno vsoto a in b. Potem dobimo polkolobar.

Primer: Boolov kolobar

Naj bo M_S množica vseh podmnožic dane množice S. Potem je M_S kolobar za operaciji

$$A + B := (A \setminus B) \cup (B \setminus A)$$
$$A \cdot B := A \cap B$$

Primeri podkolobarjev v $M_n(\mathbb{R})$

- Zgornje trikotne $n \times n$ matrike so podkolobar v $(M_n(\mathbb{R}), +, \cdot)$.
- Matrike z ničelno zadnjo vrstico so podkolobar v $(M_n(\mathbb{R}), +, \cdot)$.
- Matrike z elementi iz $\mathbb{Z}$ so podkolobar v $(M_n(\mathbb{R}), +, \cdot)$.
- oblike $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$, kjer $a, b \in \mathbb{R}$, so podkolobar v $(M_2(\mathbb{R}), +, \cdot)$.

Primeri podkolobarjev in podpolkolobarjev

- $\mathbb{N}$ je podpolkolobar v $(\mathbb{Z}, +, \cdot)$.
- Števila deljiva s 3 so podkolobar v $(\mathbb{Z}, +, \cdot)$.
- $\mathbb{Z}$ je podkolobar v $(\mathbb{Q}, +, \cdot)$.

Primer: Kolobar endomorfizmov Abelove grupe

Naj bo $(G,+)$ Abelova grupa. **Endomorfizem** $(G,+)$ je homomorfizem iz $(G,+)$ v $(G,+)$. Naj bo $\mathrm{End}(G,+)$ množica vseh endomorfizmov $(G,+)$. Vsota in produkt dveh endomorfizmov $\phi,\psi\in\mathrm{End}(G,+)$ definirajmo z

$$(\phi+\psi)(x):=\phi(x)+\psi(x) \quad \text{in} \quad (\phi\cdot\psi)(x):=\phi(\psi(x)).$$

Ker je kompozitum homomorfizmov homomorfizem, je $\phi\cdot\psi\in\mathrm{End}(G,+)$. Pokažimo, da je tudi $\phi+\psi\in\mathrm{End}(G,+)$. Ker je $(G,+)$ Abelova grupa, je

$$\begin{aligned}(\phi+\psi)(x+y)&=\phi(x+y)+\psi(x+y)=\phi(x)+\phi(y)+\psi(x)+\psi(y)=\\&=\phi(x)+\psi(x)+\phi(y)+\psi(y)=(\phi+\psi)(x)+(\phi+\psi)(y).\end{aligned}$$

Radi bi pokazali, da je $(\mathrm{End}(G,+),+,\cdot)$ asociativen kolobar z enoto.

Očitno je $\mathrm{End}(G,+)$ Abelova grupa za seštevanje endomorfizmov in očitno je množenje endomorfizmov asociativno. Dokažimo sedaj distributivnost.

Velja

$$\begin{aligned}((\phi+\psi)\cdot\rho)(x)&=(\phi+\psi)(\rho(x))=\phi(\rho(x))+\psi(\rho(x))=\\&=(\phi\cdot\rho)(x)+(\psi\cdot\rho)(x)=(\phi\cdot\rho+\psi\cdot\rho)(x)\end{aligned}$$

in

$$\begin{aligned}(\rho\cdot(\phi+\psi))(x)&=\rho((\phi+\psi)(x))=\rho(\phi(x)+\psi(x))=\\=\rho(\phi(x))+\rho(\psi(x))&=(\rho\cdot\phi)(x)+(\rho\cdot\psi)(x)=(\rho\cdot\phi+\rho\cdot\psi)(x)\end{aligned}$$

Enota za množenje je identični endomorfizem.

Primeri polj

Kolobarji $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ in $(\mathbb{C},+,\cdot)$ so polja. Za vsako polje F naj bo $F(x)$ množica vseh racionalnih funkcij v spremenljivki x s koeficienti iz F. Ta množica je polje za običajno seštevanje in množenje racionalnih funkcij. Torej so $(\mathbb{Q}(x),+,\cdot)$, $(\mathbb{R}(x),+,\cdot)$ in $(\mathbb{C}(x),+,\cdot)$ polja.

Primer obsega, ki ni polje

Množica vseh matrik oblike

$$\begin{bmatrix}\alpha & \beta\\ -\bar\beta & \bar\alpha\end{bmatrix}$$

kjer $\alpha,\beta\in\mathbb{C}$, je obseg za običajno seštevanje in množenje matrik. Pravimo mu **obseg kvaternionov**.

Če vstavimo $\alpha=a+bi$ in $\beta=c+di$, velja

$$\begin{bmatrix}\alpha & \beta\\ -\bar\beta & \bar\alpha\end{bmatrix}=a\begin{bmatrix}1&0\\0&1\end{bmatrix}+b\begin{bmatrix}i&0\\0&-i\end{bmatrix}+c\begin{bmatrix}0&1\\-1&0\end{bmatrix}+d\begin{bmatrix}0&i\\i&0\end{bmatrix}$$

Ta izraz lahko na kratko zapišemo kot $a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$. Matrika $\mathbf{1}$ je identična matrika, za matrike $\mathbf{i},\mathbf{j},\mathbf{k}$ pa velja

$$\mathbf{i}^2=\mathbf{j}^2=\mathbf{k}^2=-\mathbf{1},\quad \mathbf{ij}=-\mathbf{ji}=\mathbf{k},\quad \mathbf{jk}=-\mathbf{kj}=\mathbf{i},\quad \mathbf{ki}=-\mathbf{ik}=\mathbf{j}.$$

Odtod med drugim sledi, da obseg kvaternionov ni komutativen.

Primeri podpolj

Očitno je $\mathbb{Q}$ podpolje polja $\mathbb{R}$ in $\mathbb{R}$ je podpolje polja $\mathbb{C}$.

Primer podpolja

Označimo s $\mathbb{Q}(\sqrt[3]{2})$ množico vseh realnih števil oblike $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, kjer $a,b,c\in\mathbb{Q}$. Pokažimo, da je $\mathbb{Q}(\sqrt[3]{2})$ podpolje v $\mathbb{R}$.

Očitno je $\mathbb{Q}(\sqrt[3]{2})$ zaprta za odštevanje in množenje, torej je podkolobar. Pokazati je treba še, da za vsake $a,b,c\in\mathbb{Q}$, ki niso vsi nič, obstajajo taki $x,y,z\in\mathbb{Q}$, da je $(a+b\sqrt[3]{2}+c\sqrt[3]{4})^{-1}=x+y\sqrt[3]{2}+z\sqrt[3]{4}$. Treba je rešiti sistem $ax+2cy+2bz=1$, $bx+ay+2cz=0$, $cx+by+az=0$ z $\det\neq 0$.

Kolobar $F[x]/(p)$

Naj bo F polje. Označimo s $F[x]$ množico vseh polinomov v spremenljivki x s koeficienti iz F. Običajno seštevanje in množenje polinomov označimo s $+$ in $\cdot$. Potem je $(F[x],+,\cdot)$ komutativen in asociativen kolobar z enoto.

Vzemimo nek nekonstanten polinom $p\in F[x]$ in označimo z $F[x]/(p)$ množico vseh polinomov iz $F[x]$, ki so nižje stopnje kot p. Za vsaka polinoma $r,s\in F[x]/(p)$ definirajmo polinoma

$$r\oplus s:=r+s \quad \text{in} \quad r\odot s:=(r\cdot s) \bmod p$$

kjer je $q \bmod p$ ostanek pri deljenju polinoma q s polinomom p.

Podobno kot v prejšnjem primeru pokažemo, da je $(F[x]/(p),\oplus,\odot)$ komutativen in asociativen kolobar z enoto.

Primer

Polinom x^2-3 leži tako v $\mathbb{Q}[x]$ kot v $\mathbb{R}[x]$. V $\mathbb{Q}[x]$ je nerazcepen, ker nima racionalne ničle. V $\mathbb{R}[x]$ je razcepen, ker velja $x^2-3=(x+\sqrt{3})(x-\sqrt{3})$.

Primeri podkolobarjev v $\mathbb{R}^S$

Množico vseh funkcij iz intervala $[a,b]$ v množico $\mathbb{R}$ označimo z $\mathbb{R}^{[a,b]}$.

- Podmnožica vseh zveznih funkcij je podkolobar v $(\mathbb{R}^{[a,b]},+,\cdot)$.
- Podmnožica vseh odvedljivih funkcij je podkolobar v $(\mathbb{R}^{[a,b]},+,\cdot)$.
- Podmnožica vseh omejenih funkcij je podkolobar v $(\mathbb{R}^{[a,b]},+,\cdot)$.
- Množica vseh funkcij $f\colon[a,b]\to\mathbb{R}$, ki zadoščajo $f(b)=0$ je podkolobar v $(\mathbb{R}^{[a,b]},+,\cdot)$.

Primer homomorfizma kolobarjev, ki ne slika enote v enoto

Preslikava

$$f\colon M_n(\mathbb{R})\to M_{n+k}(\mathbb{R}),\quad f(A):=\begin{bmatrix}A&0\\0&0\end{bmatrix}$$

je homomorfizem kolobarjev, ki ne slika enote v enoto.

Primer

Množica $\mathbb{Z}\times\mathbb{Z}$ je kolobar za operaciji $(a,b)+(c,d):=(a+c,b+d)$ in $(a,b)\cdot(c,d):=(ac,bd)$. Preslikava

$$f\colon\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad f((a,b))=a$$

je homomorfizem kolobarjev z enoto.

Primer

Preslikava

$$f\colon\mathbb{C}\to M_2(\mathbb{R}),\quad f(a+bi):=\begin{bmatrix}a&b\\-b&a\end{bmatrix}$$

je homomorfizem kolobarjev z enoto.

Primer

Naj bo a neko realno število. Preslikava

$$f_a\colon\mathbb{R}[x]\to\mathbb{R},\quad f_a(p):=p(a)$$

je homomorfizem kolobarjev z enoto. Pravimo ji **evalvacija** v točki a.

Primer izomorfizma kolobarjev

Naj bo $B\in M_n(\mathbb{R})$ obrnljiva matrika. Preslikava

$$f\colon M_n(\mathbb{R})\to M_n(\mathbb{R}),\quad f(A):=BAB^{-1}$$

je izomorfizem kolobarjev z enoto.

Primer homomorfizma obsegov

Preslikava iz realnih števil v kvaternione, ki je definirana z

$$f(a):=\begin{bmatrix}a&0\\0&a\end{bmatrix}$$

je homomorfizem obsegov.

Primer podpolja

Označimo s $\mathbb{Q}(\sqrt{3})$ množico vseh realnih števil oblike $a+b\sqrt{3}$, kjer $a,b\in\mathbb{Q}$. Pokažimo, da je $\mathbb{Q}(\sqrt{3})$ podpolje v $\mathbb{R}$.

Ker je

$$(a+b\sqrt{3})-(c+d\sqrt{3})=(a-c)+(b-d)\sqrt{3},$$

je množica $\mathbb{Q}(\sqrt{3})$ zaprta za odštevanje. Ker je

$$\frac{a+b\sqrt{3}}{c+d\sqrt{3}}=\frac{(a+b\sqrt{3})(c-d\sqrt{3})}{(c+d\sqrt{3})(c-d\sqrt{3})}=\frac{ac-3bd}{c^2-3d^2}+\frac{bc-ad}{c^2-3d^2}\sqrt{3},$$

je množica $\mathbb{Q}(\sqrt{3})\setminus\{0\}$ zaprta za deljenje. Pri tem smo upoštevali, da je $c+d\sqrt{3}\neq 0$ in $c^2-3d^2\neq 0$, če $c\neq 0$ ali $d\neq 0$. V nasprotnem primeru bi namreč bilo $\sqrt{3}$ racionalno število.

Kolobar $\mathbb{Z}_n$

Vzemimo neko naravno število n in označimo $\mathbb{Z}_n=\{0,1,\ldots,n-1\}$. Za vsaka $x,y\in\mathbb{Z}_n$ naj bo

$$x\oplus y:=(x+y) \bmod n \quad \text{in} \quad x\odot y:=(x\cdot y) \bmod n$$

kjer sta $+$ in $\cdot$ operaciji na $\mathbb{Z}$ in je $z \bmod n$ ostanek pri deljenju z z n. Trdimo, da je $(\mathbb{Z}_n,\oplus,\odot)$ komutativen in asociativen kolobar z enoto.

Komutativnost $\oplus$ in $\odot$ sledi direktno iz komutativnosti $+$ in $\cdot$. Pokažimo asociativnost $\oplus$. Vzemimo $x,y,z\in\mathbb{Z}_n$ in označimo $u=x\oplus y$ in $v=y\oplus z$. Vzemimo take $i,j,k,l\in\mathbb{N}$, da je

$$\begin{aligned}x+y&=in+u & u+z&=kn+(u\oplus z)\\ y+z&=jn+v & x+v&=ln+(x\oplus v)\end{aligned}$$

Odtod sledi

$$\begin{aligned}(x\oplus y)\oplus z&=u\oplus z=u+z-kn=(x+y-in)+z-kn\\ x\oplus(y\oplus z)&=x\oplus v=x+v-ln=x+(y+z-jn)-ln\end{aligned}$$

torej je $(x\oplus y)\oplus z-x\oplus(y\oplus z)=(j+l-i-k)n$. Ker sta $(x\oplus y)\oplus z$ in $x\oplus(y\oplus z)$ med 0 in $n-1$ in ker je njuna razlika deljiva z n, sta enaka.

Podobno dokažemo tudi asociativnost $\odot$ in distributivnost. Aditivna enota je 0, multiplikativna enota pa 1. Aditivni inverz elementa $x\neq 0$ je $n-x$.

Primer
Poiščimo inverz elementa 12 v polju $\mathbb{Z}_{41}$.

Iščemo tak $x \in \mathbb{Z}$, da je $12x \bmod 41 = 1$. To velja natanko tedaj, ko obstaja tak $y \in \mathbb{Z}$, da velja $12x + 41y = 1$. Evklidov algoritem nam da

$$\begin{aligned} 41 &= 3 \cdot 12 + 5 &\Rightarrow\quad 5 &= 41 - 3 \cdot 12 \\ 12 &= 2 \cdot 5 + 2 &\Rightarrow\quad 2 &= 12 - 2 \cdot 5 \\ 5 &= 2 \cdot 2 + 1 &\Rightarrow\quad 1 &= 5 - 2 \cdot 2 \end{aligned}$$

Ko vstavimo prvo enačbo v drugo, dobimo

$$2 = 12 - 2 \cdot (41 - 3 \cdot 12) = -2 \cdot 41 + 7 \cdot 12$$

Ko to in prvo enačbo vstavimo v tretjo enačbo, dobimo

$$1 = (41 - 3 \cdot 12) - 2 \cdot (-2 \cdot 41 + 7 \cdot 12) = 5 \cdot 41 + (-17) \cdot 12$$

Torej je $x = -17$, kar pa ni v $\mathbb{Z}_{41}$. Sledi $12^{-1} = x \bmod 41 = 24$.

Polje s štirimi elementi
Iščemo polje, ki ima štiri elemente. Kolobar $\mathbb{Z}_4$ sicer ima štiri elemente, ampak ni polje. Iskano polje je $\mathbb{Z}_2[x]/(x^2 + x + 1)$.

Množica $\mathbb{Z}_2[x]/(x^2 + x + 1)$ se sestoji iz vseh polinomov v $\mathbb{Z}_2[x]$, ki so nižje stopnje kot $x^2 + x + 1$. To so polinomi $0, 1, x, x + 1$.

Operaciji na množici $\mathbb{Z}_2[x]/(x^2 + x + 1)$ sta seštevanje in množenje modulo $x^2 + x + 1$. Njuni tabeli sta:

$\oplus$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\odot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Pokazali smo že, da je $(\mathbb{Z}_2[x]/(x^2 + x + 1), \oplus, \odot)$ komutativen in asociativen kolobar z enoto. Iz tabele za $\odot$ se vidi, da ima vsak neničeln element inverz. Torej je ta kolobar polje.

Primer: Vektorski prostor $M_{m,n}(F)$
Naj bo F polje in naj bosta m in n naravni števili. Označimo z $M_{m,n}(F)$ množico vseh $m \times n$ matrik z elementi iz F. Definirajmo vsoto dveh matrik in produkt matrike s skalarjem na običajen način, se pravi po komponentah. Potem je $M_{m,n}(F)$ vektorski prostor nad F.

Primer: Trivialni vektorski prostor nad F
Množica $V = \{0\}$ je vektorski prostor nad poljem F. Vsota vektorjev je definirana z $0 + 0 = 0$. Produkt vektorja s skalarjem je definiran z $\alpha 0 = 0$.

Primer: Vektorski prostor polinomov
Naj bo F polje in naj bo $F[x]$ množica vseh polinomov v spremenljivki x s koeficienti iz F. Vsoto dveh polinomov in produkt polinoma s skalarjem definiramo na običajen način. Potem je $F[x]$ vektorski prostor nad F.

Primer: Razširitev polj
Če je F podpolje polja K, potem je K vektorski prostor nad F za običajno vsoto na K in običajen produkt na K. (Funkcija iz $F \times K$ v K je skrčitev operacije množenja, ki je funkcija iz $K \times K$ v K.)

Definicija vektorskega podprostora
Naj bo V vektorski prostor nad poljem F. Neprazna podmnožica $U \subseteq V$ je **vektorski podprostor** v V, če velja:

- Za vsaka $u_1, u_2 \in U$ velja $u_1 + u_2 \in U$.
- Za vsak $u \in U$ in vsak $\alpha \in F$ velja $\alpha u \in U$.

Ker je polje F **podpolje** polja racionalnih funkcij **F(x)** je **F(x)** **vektorski prostor** nad **F**

Primer: Vektorski podprostori v F^2
Naj bo F polje in $u \in F^2$. Množica $U := \{\alpha u \mid \alpha \in F\}$ je očitno zaprta za seštevanje in množenje s skalarjem, torej je vektorski podprostor v F^2.

Pokažimo, da je U pravi vektorski podprostor. Če $U = F^2$, bi obstajala taka $\alpha_1, \alpha_2 \in F$, da bi veljalo $(1, 0) = \alpha_1 u$ in $(0, 1) = \alpha_2 u$. Odtod bi sledilo, da je $\alpha_2(1, 0) = \alpha_1(0, 1)$, se pravi $\alpha_1 = \alpha_2 = 0$, kar da protislovje.

Primer
Izračunajmo inverz polinoma $x^3 - 2x + 2$ v polju $\mathbb{Q}[x]/(x^4 + 1)$.

Najprej uporabimo Evklidov algoritem

$$\begin{aligned} x^4 + 1 &= x(x^3 - 2x + 2) + 2x^2 - 2x + 1 \\ x^3 - 2x + 2 &= \frac{x+1}{2}(2x^2 - 2x + 1) + \frac{3 - 3x}{2} \\ 2x^2 - 2x + 1 &= -\frac{4x}{3}\left(\frac{3 - 3x}{2}\right) + 1 \end{aligned}$$

Iz prve enačbe dobimo

$$2x^2 - 2x + 1 = (x^4 + 1) - x(x^3 - 2x + 2)$$

Iz druge enačbe potem dobimo

$$\begin{aligned} \frac{3 - 3x}{2} &= (x^3 - 2x + 2) - \frac{x+1}{2}(2x^2 - 2x + 1) \\ &= (x^3 - 2x + 2) - \frac{x+1}{2}((x^4 + 1) - x(x^3 - 2x + 2)) \\ &= -\frac{x+1}{2}(x^4 + 1) + \frac{x^2 + x + 2}{2}(x^3 - 2x + 2) \end{aligned}$$

Upoštevajmo sedaj oba izraza v tretji enačbi. Dobimo

$$\begin{aligned} 1 &= (2x^2 - 2x + 1) + \frac{4x}{3}\left(\frac{3 - 3x}{2}\right) \\ &= ((x^4 + 1) - x(x^3 - 2x + 2)) \\ &\quad + \frac{4x}{3}\left(-\frac{x+1}{2}(x^4 + 1) + \frac{x^2 + x + 2}{2}(x^3 - 2x + 2)\right) \\ &= \frac{3 - 2x(x+1)}{3}(x^4 + 1) + \frac{-3x + 2x(x^2 + x + 2)}{3}(x^3 - 2x + 2) \end{aligned}$$

Inverz polinoma $x^3 - 2x + 2$ v $\mathbb{Q}[x]/(x^4 + 1)$ je torej

$$\frac{-3x + 2x(x^2 + x + 2)}{3} = \frac{2x^3 + 2x^2 + x}{3}.$$

Produkt polinoma in njegovega inverza je res enak 1 v $\mathbb{Q}[x]/(x^4 + 1)$, ker

$$\frac{2x^3 + 2x^2 + x}{3}(x^3 - 2x + 2) = \frac{2x^2 + 2x - 3}{3}(x^4 + 1) + 1.$$

Vektorski prostori

Primer: Vektorski prostor F^n
Naj bo F polje in n naravno število. Označimo z F^n množico vseh n-teric elementov iz F. Vsota dveh vektorjev in produkt vektorja s skalarjem naj bosta definirana po komponentah.

$$(\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) := (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$$
$$\gamma(\alpha_1, \ldots, \alpha_n) := (\gamma\alpha_1, \ldots, \gamma\alpha_n)$$

Potem je F^n vektorski prostor nad F.

Pri **n** je **1** dobimo da **F** vektorski prostor **nad F**

Primer: Vektorski prostor F^S
Naj bo F polje in naj bo S neprazna množica. Množico vseh funkcij iz S v F označimo z F^S. Vsota funkcij je definirana po elementih:

$$(f + g)(s) := f(s) + g(s)$$

Tudi produkt funkcije s skalarjem je definiran po elementih

$$(\gamma f)(s) := \gamma f(s)$$

Potem je F^S vektorski prostor.

Če je **S** = {**1**,…,**n**} potem je $\mathbf{F^S}$ lahko kar $\mathbf{F^n}$ in če **S** = {**1**,..,**m**} × {**1**,..,**n**} potem je $\mathbf{F^S}$ lahko $\mathbf{M_{m,n}}$**(F)**

Primer: Direktna vsota vektorskih prostorov
Naj bo F polje in naj bodo $V_1, \ldots, V_k$ vektorski prostori nad F. Označimo z $V_1 \oplus \ldots \oplus V_k$ množico vseh k-teric $(v_1, \ldots, v_k)$, kjer $v_i \in V_i$ za vse i. Vsota dveh k-teric in produkt k-terice s skalarjem sta definirana po komponentah. Potem je $V_1 \oplus \ldots \oplus V_k$ vektorski prostor nad F.

Primer: Trivialni in nepravi vektorski podprostor
Če je V vektorski prostor nad F, potem sta $\{0\}$ in V vedno vektorska podprostora v V. Prvemu pravimo **trivialni vektorski podprostor**, drugemu pa **nepravi vektorski podprostor**.

Če je $V = F$ sta to edina vektorska podprostora v V. Vsak netrivialen vektorski podprostor U v F namreč vsebuje neničeln element $\alpha \in F$. Potem za vsak $\beta \in F$ velja $\beta = (\beta\alpha^{-1})\alpha \in U$. Torej je $U = F$.

Primer: Množica rešitev homogenega sistema linearnih enačb

Naj bo A $m \times n$ matrika z elementi iz F. Množico vseh n-teric $\mathbf{x} \in F^n$, ki rešijo homogeni sistem linearnih enačb $A\mathbf{x} = 0$ označimo z $\operatorname{Ker} A$ in ji pravimo **jedro** matrike A. Vemo, da je $\operatorname{Ker} A$ vektorski podprostor v F^n.

Primer: Prostori polinomov in racionalnih funkcij

Naj bo F polje. Množica vseh polinomov $F[x]$ je vektorski podprostor v vektorskem prostoru $F(x)$ vseh racionalnih funkcij. Množica $F[x]_{\leq n}$ vseh polinomov stopnje $\leq n$ je vektorski podprostor v vektorskem prostoru $F[x]$.

Primer: Matrični prostori

Naj bo $V = M_n(F)$ vektorski prostor $n \times n$ matrik. Naslednje podmnožice v V so vektorski podprostori v V.

- Vse simetrične matrike. (Matrika A je **simetrična**, če je $A^T = A$.)
- Vse antisimetrične matrike. (A je **antisimetrična**, če je $A^T = -A$.)
- Vse matrike X, ki zadoščajo enačbi $A_1XB_1 + \ldots + A_kXB_k = 0$.
- Vse matrike, ki imajo sled enako nič.
- Vse matrike, ki imajo ničle na predpisanih mestih $(i_1, j_1), \ldots, (i_k, j_k)$. (Npr. vse diagonalne matrike, vse zgornje trikotne matrike, vse matrike z ničelnim prvim stolpcem, vse matrike z $a_{1,n} = 0$, itd.)

Primer: Funkcijski prostori

Naj bo $V = \mathbb{R}^{[a,b]}$ vektorski prostor vseh funkcij iz intervala $[a, b]$ v $\mathbb{R}$. Naslednje podmnožice v V so vektorski podprostori v V:

- Vse omejene funkcije.
- Vse integrabilne funkcije.
- Vse zvezne funkcije.
- Vse odvedljive funkcije.
- Vse dvakrat odvedljive funkcije $y(x)$, ki rešijo dano homogeno linearno diferencialno enačbo 2. reda $p(x)y''(x) + q(x)y'(x) + r(x)y(x) = 0$.
- Vse funkcije, ki zadoščajo $f(a) = 0$.
- Vse funkcije, ki zadoščajo $f(a) = f(b)$.

Opomba: Standardna baza v $M_{m,n}(F)$ so koordinatne matrike $E_{i,j}$. Matrika $E_{i,j}$ ima na (i, j)-tem mestu enko, drugod pa same ničle

Primer - Baze v F^n

Stolpčni vektorji $v_1, \ldots, v_n \in F^n$ so baza natanko tedaj, ko je

$$\det \begin{bmatrix} v_1 & \ldots & v_n \end{bmatrix} \neq 0.$$

To sledi iz karakterizacij obrnljivih matrik. Posebna primera sta:

- Standardna baza $e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, e_2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \ldots, e_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$.
- Vektorji $\begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$ so baza za F^n.

Primer - Lagrangeov interpolacijski polinom

Naj bo $n \geq 2$ naravno število, F polje z vsaj n elementi in $x_1, \ldots, x_n$ paroma različni elementi polja F. Naj bo $V = F[x]_{n-1}$ vektorski prostor vseh polinomov stopnje $\leq n-1$ s koeficienti iz F. Trdimo, da so polinomi

$$p_i(x) = \frac{(x - x_1) \cdots (x - x_n)}{x - x_i} = \prod_{j \in \mathbb{N}_n, j \neq i} (x - x_j), \qquad \text{za } i = 1, \ldots, n$$

baza vektorskega prostora V. Začnimo z linearno neodvisnostjo. Če je

$$\sum_{i=1}^{n} \alpha_i p_i(x) = 0,$$

potem za vsak j vstavimo x_j. Ker je $p_i(x_j) = 0$ za vsak $i \neq j$, ostane $\alpha_j p_j(x_j) = 0$. Ker so x_k paroma različni, je $p_j(x_j) \neq 0$. Sledi $\alpha_j = 0$.
Dokažimo, da za vsak polinom $f(x) \in V$ velja formula

$$f(x) = \frac{f(x_1)}{p_1(x_1)} p_1(x) + \ldots + \frac{f(x_n)}{p_n(x_n)} p_n(x)$$

Odtod sledi, da so polinomi $p_i(x)$ ogrodje. Obe strani formule imata namreč stopnjo $\leq n-1$ in se ujemata v n različnih točkah $x_1, \ldots, x_n$.

Primer te metode

Pokažimo, da so stolpci matrike

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

ogrodje za F^4 in poiščimo take štiri stolpce, ki so baza za F^4.
Z Gaussovo metodo izračunamo njeno reducirano vrstično kanonično formo

$$R = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

Ker matrika R nima ničelne vrstice, so stolci matrike A ogrodje za F^4. Zaporedne številke pivotnih stolpcev v R so $1, 2, 3, 5$. Stolpci v A z istimi zaporednimi številkami so potem baza za F^4. Iz R lahko odčitamo tudi, kako se s temi stolpci izražata preostala stolpca matrike A.

Primer: $F[x]$ ni končno-razsežen

Spomnimo se, da je $F[x]$ vektorski prostor vseh polinomov v x s koeficienti iz F. Množica $\{1, x, x^2, \ldots\}$ je ogrodje $F[x]$. Če bi imeli končno ogrodje $\{p_1, \ldots, p_n\}$, potem bi vsak polinom p iz $F[x]$ lahko izrazili kot $p = \alpha_1 p_1 + \ldots \alpha_n p_n$, odkoder bi sledilo $\deg p \leq \max\{\deg p_1, \ldots, \deg p_n\}$, kar je protislovje, saj imajo lahko polinomi poljubno visoko stopnjo.

Primer iz enoličnosti moči baze

Naj bo F polje in S neskončna množica. Pokažimo, da vektorski prostor F^S vseh funkcij iz S v F ni končno-razsežen. Recimo, da ima F^S ogrodje iz n elementov. Konstruirali bomo linearno neodvisno množico v F^S, ki ima $n+1$ elementov, kar je v nasprotju z Izrekom 3.

Za vsak $s \in S$ označimo z δ_s funkcijo, ki pošlje element s v 1, elemente iz $S \setminus \{s\}$ pa v nič. Ker je S neskončna množica, lahko izberemo $n+1$ paroma različnih elementov $s_1, \ldots, s_{n+1} \in S$. Pokažimo, da so funkcije $\delta_{s_1}, \ldots, \delta_{s_{n+1}}$ linearno neodvisne. Recimo, da velja

$$\alpha_1 \delta_{s_1} + \ldots + \alpha_{n+1} \delta_{s_{n+1}} = 0 \quad \alpha_1 \delta_{s_1}(x) + \ldots + \alpha_{n+1} \delta_{s_{n+1}}(x) = 0$$

za neke skalarje $\alpha_1, \ldots, \alpha_{n+1} \in F$. Potem ze vsak $x \in S$ velja

Ko vstavimo $x = s_i$ za $i = 1, \ldots, n+1$, in upoštevamo $\delta_j(s_i) = 0$ za vsak $j \neq i$, dobimo $\alpha_i \delta_{s_i}(s_i) = 0$. Ker je $\delta_{s_i}(s_i) = 1$, sledi $\alpha_i = 0$.

Primer iz dopolnjevanja linearno neodvisnih množic

Zanima nas, kako za dano množico $\{v_1, \ldots, v_m\}$ v F^n ugotovimo ali je linearno neodvisna in kako jo dopolnimo do baze. Tvorimo matriko

$$A = \begin{bmatrix} v_1 & \ldots & v_m & e_1 & \ldots & e_n \end{bmatrix}$$

kjer je $e_1, \ldots, e_n$ standardna baza za F^n. Z Gaussovo metodo prevedemo matriko A na reducirano vrstično stopničasto formo R.

Zaporedne številke pivotnih stolpcev matrike R naj bodo $i_1, \ldots, i_n$. Vektorji $v_1, \ldots, v_m$ so linearno neodvisni natanko tedaj, ko velja $i_1 = 1$ in $\ldots$ in $i_m = m$. Stolpci v A z zaporednimi številkami $i_{m+1}, \ldots, i_n$ so potem dopolnitev množice $\{v_1, \ldots, v_m\}$ do baze.

Primer

Dopolni vektorja $\begin{bmatrix} 1 \\ -1 \\ 0 \\ 2 \end{bmatrix}$ in $\begin{bmatrix} 2 \\ 2 \\ 0 \\ 1 \end{bmatrix}$ do baze za $\mathbb{R}^4$.

$$A = \begin{bmatrix} 1 & 2 & 1 & 0 & 0 & 0 \\ -1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad R = \begin{bmatrix} 1 & 0 & 0 & -\frac{1}{5} & 0 & \frac{2}{5} \\ 0 & 1 & 0 & \frac{2}{5} & 0 & \frac{1}{5} \\ 0 & 0 & 1 & -\frac{3}{5} & 0 & -\frac{4}{5} \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Njeni pivotni stolpci imajo zaporedne številke $1, 2, 3$ in 5. Torej sta $\begin{bmatrix} 1 \\ -1 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 0 \\ 1 \end{bmatrix}$ linearno neodvisna in $\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$ ju dopolnita do baze.

Osnovni primer

Za vse vektorje $v_1, \ldots, v_n$ v V velja

$$\operatorname{Lin}\{v_1\} + \ldots + \operatorname{Lin}\{v_n\} = \operatorname{Lin}\{v_1, \ldots, v_n\}$$

Torej so vektorji $v_1, \ldots, v_n$ ogrodje za V natanko tedaj, ko velja $\operatorname{Lin}\{v_1\} + \ldots + \operatorname{Lin}\{v_n\} = V$ ($\Leftrightarrow \operatorname{Lin}\{v_1\}, \ldots, \operatorname{Lin}\{v_n\}$ so "ogrodje").
Neničelni vektorji $v_1, \ldots, v_n$ v V so LN natanko tedaj, ko je vsota $\operatorname{Lin}\{v_1\} + \ldots + \operatorname{Lin}\{v_n\}$ direktna ($\Leftrightarrow \operatorname{Lin}\{v_1\}, \ldots, \operatorname{Lin}\{v_n\}$ so "LN").
D: Vsota $\operatorname{Lin}\{v_1\} + \ldots + \operatorname{Lin}\{v_n\}$ je direktna natanko tedaj, ko za vsake skalarje α_i, β_j velja, da iz $\alpha_1 v_1 + \ldots + \alpha_n v_n = \beta_1 v_1 + \ldots + \beta_n v_n$ sledi $\alpha_1 v_1 = \beta_1 v_1, \ldots, \alpha_n v_n = \beta_n v_n$. Ker so vektorji $v_1, \ldots, v_n$ neničelni je to ekvivalentno lastnosti, da iz $\alpha_1 v_1 + \ldots + \alpha_n v_n = \beta_1 v_1 + \ldots + \beta_n v_n$ sledi $\alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n$. To pa je ravno linearna neodvisnost $v_1, \ldots, v_n$.

Opomba: Vektorske podprostore $U_1, \ldots, U_n$ lahko smatramo za "bazo" vektorskega prostora V, če lahko vsak vektor $v \in V$ na **natanko en** način izrazimo kot $v = u_1 + \ldots + u_n$, kjer $u_1 \in U_1, \ldots, u_n \in U_n$. To velja natanko tedaj, ko je $V = U_1 \oplus \ldots \oplus U_n$.

Primeri prehodnih matrik

Vzemimo dve bazi v $\mathbb{R}^3$

$$\mathcal{B}=\left\{\begin{bmatrix}1\\0\\0\end{bmatrix},\begin{bmatrix}0\\1\\0\end{bmatrix},\begin{bmatrix}0\\0\\1\end{bmatrix}\right\} \quad \text{in} \quad \mathcal{C}=\left\{\begin{bmatrix}1\\0\\0\end{bmatrix},\begin{bmatrix}1\\1\\0\end{bmatrix},\begin{bmatrix}1\\1\\1\end{bmatrix}\right\}$$

Izračunajmo prehodni matriki $P_{\mathcal{C}\leftarrow\mathcal{B}}$ in $P_{\mathcal{B}\leftarrow\mathcal{C}}$. Ker je

$$\begin{bmatrix}1\\0\\0\end{bmatrix}=1\cdot\begin{bmatrix}1\\0\\0\end{bmatrix}+0\cdot\begin{bmatrix}1\\1\\0\end{bmatrix}+0\cdot\begin{bmatrix}1\\1\\1\end{bmatrix}$$

$$\begin{bmatrix}0\\1\\0\end{bmatrix}=(-1)\cdot\begin{bmatrix}1\\0\\0\end{bmatrix}+1\cdot\begin{bmatrix}1\\1\\0\end{bmatrix}+0\cdot\begin{bmatrix}1\\1\\1\end{bmatrix}$$

$$\begin{bmatrix}0\\0\\1\end{bmatrix}=0\cdot\begin{bmatrix}1\\0\\0\end{bmatrix}+(-1)\cdot\begin{bmatrix}1\\1\\0\end{bmatrix}+1\cdot\begin{bmatrix}1\\1\\1\end{bmatrix}$$

velja $P_{\mathcal{C}\leftarrow\mathcal{B}}=\begin{bmatrix}1&-1&0\\0&1&-1\\0&0&1\end{bmatrix}$. Izračun $P_{\mathcal{B}\leftarrow\mathcal{C}}$ je preprostejši. Iz

$$\begin{bmatrix}1\\0\\0\end{bmatrix}=1\cdot\begin{bmatrix}1\\0\\0\end{bmatrix}+0\cdot\begin{bmatrix}0\\1\\0\end{bmatrix}+0\cdot\begin{bmatrix}0\\0\\1\end{bmatrix}$$

$$\begin{bmatrix}1\\1\\0\end{bmatrix}=1\cdot\begin{bmatrix}1\\0\\0\end{bmatrix}+1\cdot\begin{bmatrix}0\\1\\0\end{bmatrix}+0\cdot\begin{bmatrix}0\\0\\1\end{bmatrix}$$

$$\begin{bmatrix}1\\1\\1\end{bmatrix}=1\cdot\begin{bmatrix}1\\0\\0\end{bmatrix}+1\cdot\begin{bmatrix}0\\1\\0\end{bmatrix}+1\cdot\begin{bmatrix}0\\0\\1\end{bmatrix}$$

sledi, da je $P_{\mathcal{B}\leftarrow\mathcal{C}}=\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix}$. Opazimo, da je produkt obeh prehodnih matrik identična matrika. To velja tudi v splošnem.

Linearne preslikave

Primer: Če je $F=K=\mathbb{C}$ in $\phi(z)=\bar{z}$ (se pravi $\phi(a+bi)=a-bi$), potem ϕ-linearni preslikavi iz U v V pravimo **konjugirano linearna** preslikava.

Primer: Konjugiranje je $\mathbb{R}$-linearna preslikava iz $\mathbb{C}$ v $\mathbb{C}$, ni pa $\mathbb{C}$-linearna.

Primer - Odvajanje

Vemo, da za odvod velja

$$(f+g)'=f'+g' \quad \text{in} \quad (cf)'=cf'$$

kjer je c konstanta. Odvod je torej linearna preslikava iz vektorskega podprostora vseh odvedljivih funkcij v $\mathbb{R}^{[a,b]}$ v vektorski prostor $\mathbb{R}^{[a,b]}$

Primer - Projekcija na x os

Če točko (x,y) v ravnini projeciramo na x os, dobimo točko $(x,0)$. Dokažimo, da je $L(x,y)=(x,0)$ linearna preslikava. To sledi iz

$$L(\alpha_1(x_1,y_1)+\alpha_2(x_2,y_2))=L(\alpha_1x_1+\alpha_2x_2,\alpha_1y_1+\alpha_2y_2)=$$
$$=(\alpha_1x_1+\alpha_2x_2,0)=\alpha_1(x_1,0)+\alpha_2(x_2,0)=\alpha_1L(x_1,y_1)+\alpha_2L(x_2,y_2)$$

Primer - Integriranje

Vemo, da je določeni integral definiran za zvezne funkcije in da velja

$$\int_a^b(f(x)+g(x))\,dx=\int_a^b f(x)\,dx+\int_a^b g(x)\,dx$$

$$\text{in} \quad \int_a^b cf(x)\,dx=c\int_a^b f(x)\,dx$$

Torej je $\int_a^b$ linearna preslikava iz vektorskega podprostora vseh zveznih funkcij v $\mathbb{R}^{[a,b]}$ v vektorski prostor $\mathbb{R}$.

Primer

Če smatramo $\mathbb{C}$ za vektorski prostor nad $\mathbb{R}$, potem je konjugiranje linearna preslikava iz $\mathbb{C}$ v $\mathbb{C}$. Za bazi vzemimo $\mathcal{B}=\mathcal{C}=\{1,i\}$. Velja

$$\bar{1}=1=1\cdot1+0\cdot i$$
$$\bar{i}=-i=0\cdot1+(-1)\cdot i$$

Potem je $[L]_{\mathcal{C}\leftarrow\mathcal{B}}=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$

Primer - Vrtež okrog izhodišča

Če točko $(x,y)=(r\cos\phi,r\sin\phi)$ v ravnini zavrtimo okrog izhodišča za kot τ v nasprotni smeri od urinega kazalca, potem dobimo točko $(r\cos(\phi+\tau),r\sin(\phi+\tau))=(x\cos\tau-y\sin\tau,x\sin\tau+y\cos\tau)$, kjer smo uporabili adicijska izreka za cos in sin. Dokažimo, da je $L(x,y)=(x\cos\tau-y\sin\tau,x\sin\tau+y\cos\tau)$ linearna preslikava:

$$L(\alpha_1(x_1,y_1)+\alpha_2(x_2,y_2))=L(\alpha_1x_1+\alpha_2x_2,\alpha_1y_1+\alpha_2y_2)=$$
$$=((\alpha_1x_1+\alpha_2x_2)\cos\tau-(\alpha_1y_1+\alpha_2y_2)\sin\tau,(\alpha_1x_1+\alpha_2x_2)\sin\tau+(\alpha_1y_1+\alpha_2y_2)\cos\tau)=$$
$$=\alpha_1(x_1\cos\tau-y_1\sin\tau,x_1\sin\tau+y_1\cos\tau)+\alpha_2(x_2\cos\tau-y_2\sin\tau,x_2\sin\tau+y_2\cos\tau)=$$
$$=\alpha_1L(x_1,y_1)+\alpha_2L(x_2,y_2).$$

Primer - Linearni izomorfizem iz $M_{m,n}(F)$ v $\mathcal{L}(F^n,F^m)$

Naj bo F polje in naj bosta m in n naravni števili. Naj bo $\mathcal{L}(F^n,F^m)$ vektorski prostor vseh linearnih preslikav iz F^n v F^m. Seštevanje je definirano z $(L_1+L_2)u:=L_1u+L_2u$, množenje s skalarjem pa z $(\alpha L)u:=\alpha Lu$. Naj bo $M_{m,n}(F)$ vektorski prostor vseh $m\times n$ matrik nad F. Konstruirali bomo linearni izomorfizem iz $M_{m,n}(F)$ v $\mathcal{L}(F^n,F^m)$.

Za vsako $m\times n$ matriko $A=[a_{i,j}]$ definirajmo preslikavo L_A iz F^n v F^m

$$L_A(x_1,\ldots,x_n)=(a_{1,1}x_1+\ldots+a_{1,n}x_n,\ldots,a_{m,1}x_1+\ldots+a_{m,n}x_n)$$

To lahko zapišemo kot $L_Ax=Ax$, kjer x smatramo za stolpčni vektor. Iz lastnosti matričnega množenja sledi, da je L_A linearna preslikava.

Radi bi pokazali, da je preslikava $A\to L_A$ iz $M_{m,n}(F)$ v $\mathcal{L}(F^n,F^m)$ linearni izomorfizem. Linearnost sledi iz

$$L_{\alpha A+\beta B}x=(\alpha A+\beta B)x=\alpha Ax+\beta Bx=\alpha L_Ax+\beta L_Bx=(\alpha L_A+\beta L_B)x$$

Bijektivnost dokažemo tako, da konstruiramo inverzno preslikavo.

Vsaki linearni preslikavi $L\colon F^n\to F^m$ lahko priredimo $m\times n$ matriko $\begin{bmatrix}Le_1&\ldots&Le_n\end{bmatrix}$, kjer je $e_1,\ldots,e_n$ standardna baza za F^n. Pokažimo, da je $L\mapsto\begin{bmatrix}Le_1&\ldots&Le_n\end{bmatrix}$ inverzna preslikava od preslikave $A\mapsto L_A$.

Najprej preverimo, da je kompozitum $A\mapsto L_A\mapsto\begin{bmatrix}L_Ae_1&\ldots&L_Ae_n\end{bmatrix}$ identična preslikava. Če upoštevamo, da je $\begin{bmatrix}e_1&\ldots&e_n\end{bmatrix}=I$, dobimo

$$\begin{bmatrix}L_Ae_1&\ldots&L_Ae_n\end{bmatrix}=\begin{bmatrix}Ae_1&\ldots&Ae_n\end{bmatrix}=A\begin{bmatrix}e_1&\ldots&e_n\end{bmatrix}=A$$

Preverimo še, da je kompozitum $L\mapsto\begin{bmatrix}Le_1&\ldots&Le_n\end{bmatrix}\mapsto L_{[Le_1\ldots Le_n]}$ identična preslikava. Za vsak $x\in F^n$ velja

$$L_{[Le_1\ldots Le_n]}x=\begin{bmatrix}Le_1&\ldots&Le_n\end{bmatrix}\begin{bmatrix}x_1\\\vdots\\x_n\end{bmatrix}=$$

$$=x_1Le_1+\ldots+x_nLe_n=L(x_1e_1+\ldots+x_ne_n)=Lx$$

kjer smo pri prvem enačaju upoštevali definicijo L_A, pri drugem bločno množenje matrik in pri tretjem linearnost preslikave L. □

Primer

Naj bo A $m\times n$ matrika nad F in naj bo L_A linearna preslikava iz F^n v F^m, ki je definirana z $L_Ax=Ax$. Naj bo $\mathcal{B}=\{e_1,\ldots,e_n\}$ standardna baza za F^n in $\mathcal{C}=\{f_1,\ldots,f_m\}$ standardna baza za F^m. Velja

$$L_Ae_1=Ae_1=a_1=a_{1,1}f_1+\ldots+a_{m,1}f_m$$
$$\vdots$$
$$L_Ae_n=Ae_n=a_m=a_{1,n}f_1+\ldots+a_{m,n}f_m$$

Torej je

$$[L_A]_{\mathcal{C}\leftarrow\mathcal{B}}=\begin{bmatrix}a_{1,1}&\ldots&a_{1,n}\\\vdots&&\vdots\\a_{m,1}&\ldots&a_{m,n}\end{bmatrix}=A$$

Primer - Linearni izomorfizem iz F^n v n-razsežen vektorski prostor

Radi bi dokazali, da je vsak n-razsežen vektorski prostor nad F linearno izomorfen F^n.

Naj bo V n-razsežen vektorski prostor nad F in naj bo $\mathcal{B}=\{v_1,\ldots,v_n\}$ baza za V. Definirajmo preslikavo $\phi_{\mathcal{B}}\colon F^n\to V$ s predpisom

$$\phi_{\mathcal{B}}(x_1,\ldots,x_n)=x_1v_1+\ldots+x_nv_n$$

Ker je $\mathcal{B}$ ogrodje, je $\phi_{\mathcal{B}}$ surjektivna. Ker je $\mathcal{B}$ linearno neodvisna, je $\phi_{\mathcal{B}}$ injektivna. Pokažimo še, da je $\phi_{\mathcal{B}}$ linearna preslikava. To sledi iz

$$\phi_{\mathcal{B}}(\alpha(x_1,\ldots,x_n)+\beta(y_1,\ldots,y_n))=\phi_{\mathcal{B}}(\alpha x_1+\beta y_1,\ldots,\alpha x_n+\beta y_n)=$$
$$=(\alpha x_1+\beta y_1)v_1+\ldots+(\alpha x_n+\beta y_n)v_n=\alpha(x_1v_1+\ldots+x_nv_n)+$$
$$+\beta(y_1v_1+\ldots+y_nv_n)=\alpha\phi_{\mathcal{B}}(x_1,\ldots,x_n)+\beta\phi_{\mathcal{B}}(y_1,\ldots,y_n)$$

Torej je $\phi_{\mathcal{B}}$ linearni izomorfizem. Njegova inverzna preslikava je $v\mapsto[v]_{\mathcal{B}}$. Po trditvi je tudi inverzna preslikava linearni izomorfizem.

Primer

Naj bo U vektorski prostor vseh realnih polinomov stopnje ≤3 in V vektorski prostor vseh realnih polinomov stopnje ≤2. Za bazo prostora U vzemimo $\mathcal{B}=\{1,x,x^2,x^3\}$, za bazo prostora V pa $\mathcal{C}=\{1,x,x^2\}$. Naj bo $D\colon U\to V$ odvajanje polinomov. Iščemo matriko $[D]_{\mathcal{C}\leftarrow\mathcal{B}}$.

Razvijmo vektorje $D1,Dx,Dx^2,Dx^3$ po bazi $1,x,x^2$. Velja

$$\begin{aligned}D1&=0&&=0\cdot1+0\cdot x+0\cdot x^2\\Dx&=1&&=1\cdot1+0\cdot x+0\cdot x^2\\Dx^2&=2x&&=0\cdot1+2\cdot x+0\cdot x^2\\Dx^3&=3x^2&&=0\cdot1+0\cdot x+3\cdot x^2\end{aligned}$$

Torej je

$$[D]_{\mathcal{C}\leftarrow\mathcal{B}}=\begin{bmatrix}0&1&0&0\\0&0&2&0\\0&0&0&3\end{bmatrix}$$

Primer

Naj bo V vektorski prostor in naj bo id_V identična preslikava iz V v V. Naj bosta $\mathcal{B}=\{u_1,\ldots,u_n\}$ in $\mathcal{C}=\{v_1,\ldots,v_n\}$ bazi za V. Razvijmo

$$\mathrm{id}_V(u_1)=u_1=\alpha_{1,1}v_1+\ldots+\alpha_{1,n}v_n$$
$$\vdots$$
$$\mathrm{id}_V(u_n)=u_n=\alpha_{n,1}v_1+\ldots+\alpha_{n,n}v_n$$

Dobimo enake razvoje kot pri definiciji prehodne matrike. Torej je

$$[idV]_{\mathcal{C}\leftarrow\mathcal{B}}=\begin{bmatrix}\alpha_{1,1}&\ldots&\alpha_{n,1}\\\vdots&&\vdots\\\alpha_{1,n}&\ldots&\alpha_{n,n}\end{bmatrix}=P_{\mathcal{C}\leftarrow\mathcal{B}}$$

Primer

Izračunaj sliko in rang matrike

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

Najprej izračunamo reducirano vrstično stopničasto formo

$$R = \begin{bmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Ker elementarne vrstične transformacije ohranjajo linearne relacije med stolpci, odtod sledi, da je $\mathrm{r}(A) = 2$ in

$$\mathrm{Im}\, A = \mathrm{Lin}\{\begin{bmatrix} 1 \\ 5 \\ 9 \end{bmatrix}, \begin{bmatrix} 2 \\ 6 \\ 10 \end{bmatrix}\}$$

Primer: Podobnost ni ekvivalentnost

Matriki $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ in $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ sta ekvivalentni, ker imata enako velikost in enak rang. Če bi bili matriki A in B podobni, potem bi obstajala taka obrnljiva matrika P, da bi veljalo $B = PAP^{-1}$. Odtod bi sledilo

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ u & v \end{bmatrix} = \begin{bmatrix} x & y \\ u & v \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{kjer} \quad P = \begin{bmatrix} x & y \\ u & v \end{bmatrix}$$

Z množenjem matrik bi dobili

$$\begin{bmatrix} u & v \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} x & 0 \\ u & 0 \end{bmatrix}$$

Odtod pa bi sledilo $u = v = 0$. To bi bilo protislovje s predpostavko, da je matrika P obrnljiva.

Primeri invariantnih podprostorov

Naj bo $A \in M_n(F)$ in naj bo $\mathbf{e}_1, \ldots, \mathbf{e}_n$ standardna baza za F^n.
Če je A zgornje trikotna, potem so naslednji podprostori invariantni za A:

$$\mathrm{Lin}\{\mathbf{e}_1\}, \mathrm{Lin}\{\mathbf{e}_1, \mathbf{e}_2\}, \ldots, \mathrm{Lin}\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$$

Če je A diagonalna, potem so naslednji podprostori invariantni za A:

$$\mathrm{Lin}\{\mathbf{e}_1\}, \mathrm{Lin}\{\mathbf{e}_2\}, \ldots, \mathrm{Lin}\{\mathbf{e}_n\}$$

Primer invariantnega podprostora

Naj bo $V = F[x]$ vektorski prostor vseh polinomov s koeficienti v F in naj bo $D \colon V \to V$ odvajanje polinomov. Za vsako naravno število n je $F[x]_{\leq n}$ (se pravi vektorski podprostor vseh polinomov v $F[x]$, ki so stopnje $\leq n$) invarianten podprostor za D.

Primer

Naj bo $L \colon U \to V$ linearna preslikava, $\mathcal{B}, \mathcal{B}'$ bazi za U in $\mathcal{C}, \mathcal{C}'$ bazi za V. Potem sta matriki $[L]_{\mathcal{C} \leftarrow \mathcal{B}}$ in $[L]_{\mathcal{C}' \leftarrow \mathcal{B}'}$ ekvivalentni. Velja namreč

$$[L]_{\mathcal{C}' \leftarrow \mathcal{B}'} = P_{\mathcal{C}' \leftarrow \mathcal{C}} [L]_{\mathcal{C} \leftarrow \mathcal{B}} P_{\mathcal{B} \leftarrow \mathcal{B}'}$$

in matriki $P_{\mathcal{C}' \leftarrow \mathcal{C}}$ ter $P_{\mathcal{B} \leftarrow \mathcal{B}'}$ sta obrnljivi.

Opomba: Velja tudi obratno. Če sta matriki A in A' ekvivalentni, potem obstaja taka linearna preslikava $L \colon U \to V$ in take baze $\mathcal{B}, \mathcal{B}'$ za U in $\mathcal{C}, \mathcal{C}'$ za V, da je $[L]_{\mathcal{C} \leftarrow \mathcal{B}} = A$ in $[L]_{\mathcal{C}' \leftarrow \mathcal{B}'} = A'$.

Dokaz: Recimo, da je $A' = PAQ$, kjer sta P in Q obrnljivi matriki. Naj bo $U = F^n$ in $V = F^m$ in naj bo $L = L_A$, se pravi linearna preslikava, ki vektor množi z matriko A. Naj bo $\mathcal{B}$ standardna baza za F^n in $\mathcal{C}$ standardna baza za F^m. Potem velja $[L]_{\mathcal{C} \leftarrow \mathcal{B}} = A$. Naj bodo $\mathcal{B}'$ stolpci matrike P^{-1} in naj bodo $\mathcal{C}'$ stolpci matrike Q. Potem velja $P_{\mathcal{C} \leftarrow \mathcal{C}'} = P^{-1}$ in $P_{\mathcal{B} \leftarrow \mathcal{B}'} = Q$. Torej je $[L]_{\mathcal{C}' \leftarrow \mathcal{B}'} = P_{\mathcal{C}' \leftarrow \mathcal{C}} [L]_{\mathcal{C} \leftarrow \mathcal{B}} P_{\mathcal{B} \leftarrow \mathcal{B}'} = PAQ = A'$.

Primer podobnih matrik

Naj bo $L \colon V \to V$ linearna preslikava in naj bosta $\mathcal{B}$ in $\mathcal{B}'$ bazi vektorskega prostora V. Potem sta matriki $[L]_{\mathcal{B} \leftarrow \mathcal{B}}$ in $[L]_{\mathcal{B}' \leftarrow \mathcal{B}'}$ podobni, ker velja

$$[L]_{\mathcal{B}' \leftarrow \mathcal{B}'} = P_{\mathcal{B}' \leftarrow \mathcal{B}} [L]_{\mathcal{B} \leftarrow \mathcal{B}} P_{\mathcal{B} \leftarrow \mathcal{B}'} = P_{\mathcal{B}' \leftarrow \mathcal{B}} [L]_{\mathcal{B} \leftarrow \mathcal{B}} (P_{\mathcal{B}' \leftarrow \mathcal{B}})^{-1}$$

kjer je $P_{\mathcal{B}' \leftarrow \mathcal{B}}$ obrnljiva matrika.

$\mathrm{Ker}\, L$ in $\mathrm{Im}\, L$ sta invariantna podprostora za L

Naj bo $L \colon V \to V$ linearna preslikava. Očitno L pošlje elemente $\mathrm{Ker}\, L$ v 0. Ker je $0 \in \mathrm{Ker}\, L$, torej L pošlje vse elemente $\mathrm{Ker}\, L$ v elemente $\mathrm{Ker}\, L$. Torej je $\mathrm{Ker}\, L$ invarianten podprostor za L.

Očitno L pošlje vse elemente V v elemente $\mathrm{Im}\, L$. Torej pošlje tudi vse elemente $\mathrm{Im}\, L$ v elemente $\mathrm{Im}\, L$. To pomeni, da je $\mathrm{Im}\, L$ invarianten podprostor za L.

Primer

Naj bo A kvadratna $n \times n$ matrika nad F. Recimo, da obstaja tak vektor $v \in F^n$, da so vektorji $v, Av, \ldots, A^{n-1}v$ linearno neodvisni (=baza).
Razvijmo vektor $A^n v$ po tej bazi: $A^n v = \alpha_0 v + \alpha_1 Av + \ldots + \alpha_{n-1} A^{n-1} v$.
Trdimo, da je $A = PBP^{-1}$, kjer je

$$B = \begin{bmatrix} 0 & 0 & \ldots & 0 & \alpha_0 \\ 1 & 0 & \ldots & 0 & \alpha_1 \\ 0 & 1 & \ldots & 0 & \alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & \alpha_{n-1} \end{bmatrix}$$

in je $P = \begin{bmatrix} v & Av & \ldots & A^{n-2}v & A^{n-1}v \end{bmatrix}$ obrnljiva matrika. To sledi iz

$$AP = \begin{bmatrix} Av & A^2 v & \ldots & A^{n-1}v & A^n v \end{bmatrix} =$$

$$= \begin{bmatrix} Av & A^2 v & \ldots & A^{n-1}v & \alpha_0 v + \alpha_1 Av + \ldots + \alpha_{n-1} A^{n-1} v \end{bmatrix} = PB$$

Lastne vrednosti

Oglejmo si zdaj posplošitev zadnjega primera na polinome v L.
Naj bo V vektorski prostor nad F. Za vsak polinom

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k \in F[x].$$

in vsako linearno preslikavo $L \colon V \to V$ definirajmo

$$p(L) = a_0 \mathrm{id}_V + a_1 L + a_2 L^2 + \ldots + a_k L^k$$

kjer je $L^2 = L \circ L$, $L^3 = L \circ L \circ L$, itd. Očitno je $p(L)$ linearna preslikava iz V v V, ki pošlje vektor $v \in V$ v $p(L)v = a_0 v + a_1 Lv + \ldots + a_k L^k v$.

Opomba: Podobno za vsako matriko $A \in M_n(F)$ definiramo

$$p(A) = a_0 I_n + a_1 A + a_2 A^2 + \ldots + a_k A^k$$

Primer

Določi vse lastne vrednosti in lastne podprostore matrike $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

Rešitev: Karakteristični polinom je $p_A(x) = \det(A - xI) = x^2 + 1$.
Ima dve kompleksni ničli $\lambda_1 = i$ in $\lambda_2 = -i$. Lastna podprostora sta

$$\mathrm{Ker}(A - \lambda_1 I) = \mathrm{Ker} \begin{bmatrix} -i & 1 \\ -1 & -i \end{bmatrix} = \mathrm{Lin}\{\begin{bmatrix} 1 \\ i \end{bmatrix}\}$$

$$\mathrm{Ker}(A - \lambda_2 I) = \mathrm{Ker} \begin{bmatrix} i & 1 \\ -1 & i \end{bmatrix} = \mathrm{Lin}\{\begin{bmatrix} 1 \\ -i \end{bmatrix}\}$$

Opomba: Ker sta oba lastna podprostora enorazsežna, imata tako λ_1 kot λ_2 geometrijsko večkratnost 1. Poleg tega imata tako λ_1 kot λ_2 algebraično večkratnost enako 1 saj sta obe enostavni ničli $p_A(x)$.

Opomba: Podobno izpeljemo, da je karakteristični polinom $n \times n$ matrike $A = [a_{i,j}]$ oblike $p_A(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0$ kjer je

$$c_n = (-1)^n, \quad c_{n-1} = (-1)^{n-1} \sum_i a_{i,i} \quad \text{in} \quad c_0 = \det A$$

Ostali koeficienti so bolj komplicirani, npr.

$$c_{n-2} = (-1)^{n-2} \sum_{i<j} \det \begin{bmatrix} a_{i,i} & a_{i,j} \\ a_{j,i} & a_{j,j} \end{bmatrix}$$

Karakteristični polinom 2×2 matrike

Karakteristični polinom matrike $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ je

$$p_A(x) = \det \begin{bmatrix} a - x & b \\ c & d - x \end{bmatrix} = (a - x)(d - x) - bc =$$

$$= x^2 - (a + d)x + ad - bc = x^2 - (\mathrm{sled}\, A)x + \det A$$

Karakteristični polinom zgornje trikotne matrike

Če je

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ 0 & a_{2,2} & \ldots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_{n,n} \end{bmatrix}$$

potem je $\det(A - xI) = (-1)^n (x - a_{1,1})(x - a_{2,2}) \ldots (x - a_{n,n})$

Primer

Določi vse lastne vrednosti in lastne podprostore matrik

$$A_1 = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}$$

Rešitev: Vse tri matrike imajo enak karakteristični polinom

$$(2 - x)^3 = -(x - 2)^3.$$

Torej je pri vseh 2 edina lastna vrednost in ima algebraično večkratnost 3.
V prvem primeru je lastni podprostor lastne vrednosti 2 enak

$$\mathrm{Ker}\,(A_1 - 2I) = \mathrm{Lin}\{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}\} = \mathbb{C}^3$$

torej je geometrijska večkratnost lastne vrednosti 2 enaka 3.

V drugem primeru je lastni podprostor lastne vrednosti 2 enak

$$\mathrm{Ker}\,(A_2 - 2I) = \mathrm{Lin}\{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}\}$$

torej je geometrijska večkratnost lastne vrednosti 2 enaka 2.
V tretjem primeru je lastni podprostor lastne vrednosti 2 enak

$$\mathrm{Ker}\,(A_3 - 2I) = \mathrm{Lin}\{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}\}$$

torej je geometrijska večkratnost lastne vrednosti 2 enaka 1.

Primer

Poišči diagonalno matriko, ki je podobna matriki $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

$v_1 = \begin{bmatrix} 1 \\ i \end{bmatrix}$ in $v_2 = \begin{bmatrix} 1 \\ -i \end{bmatrix}$ lastna vektorja matrike A linearno neodvisna

$$P = \begin{bmatrix} v_1 & v_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}$$

Ker sta njuni lastni vrednosti $\lambda_1 = i$ in $\lambda_2 = -i$, vzamemo

$$D = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

Po gornjem računu je $A = PDP^{-1}$

Primer

Poišči kako zgornje trikotno matriko, ki je podobna matriki

$$A = \begin{bmatrix} 3 & 4 \\ -1 & -1 \end{bmatrix}$$

Karakteristični polinom matrike A je

$$\det(A - xI) = (3-x)(-1-x) + 4 = 1 - 2x + x^2 = (1-x)^2$$

torej je 1 lastna vrednost matrike A. Pripadajoči lastni vektor je v jedru matrike $A - I$. Vzemimo recimo

$$v_1 = \begin{bmatrix} 2 \\ -1 \end{bmatrix}$$

Dopolnimo ta vektor do baze za $\mathbb{C}^2$ z vektorjem

$$v_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Označimo

$$P = \begin{bmatrix} v_1 & v_2 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ -1 & 1 \end{bmatrix}$$

Potem velja

$$P^{-1}AP = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 3 & 4 \\ -1 & -1 \end{bmatrix}\begin{bmatrix} 2 & 0 \\ -1 & 1 \end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 2 & 4 \\ -1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

Torej je matrika A podobna zgornje trikotni matriki

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

Primer matrike, ki nima diagonalizacije

Pokažimo, da matrika $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ nima diagonalizacije.

Prvi način: Poskusimo najti tako obrnljivo matriko $P = \begin{bmatrix} x & y \\ u & v \end{bmatrix}$ in tako diagonalno matriko $D = \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$, da velja $AP = PD$. Primerjava istoležnih elementov nam da $u = d_1 x$, $v = d_2 y$, $0 = d_1 u$, $0 = d_2 u$. Če prvo enačbo pomnožimo z u in upoštevamo tretjo, dobimo $u^2 = 0$. Če drugo enačbo pomnožimo z v in upoštevamo četrto, dobimo $v^2 = 0$. Matrika P torej ima ničelno vrstico, kar je v nasprotju z obrnljivostjo.

Drugi način: Izračunajmo lastne vrednosti in lastne vektorje. Karakteristični polinom je x^2, torej je 0 edina lastna vrednost. Pripadajoči lastni podprostor $\mathrm{Ker} A = \mathrm{Lin}\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}\}$ je enodimenzionalen, torej matrika A nima dveh linearno neodvisnih lastnih vektorjev.

Primer

Matriki $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ in $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ imata enak karakteristični polinom toda različna minimalna polinoma $m_A(x) = x - 1$ in $m_B(x) = (x-1)^2$.

Primeri invariantnih podprostorov matrike A

- Trivialni podprostor $\{0\}$.
- Lastni podprostori matrike A.
- Korenski podprostori matrike A.
- Presek invariantnih podprostorov za A je invarianten podprostor za A.

Primer sistema linearnih rekurzivnih enačb

$$x_{n+1} = -4x_n + 4y_n, \quad x_0 = 0$$
$$y_{n+1} = -x_n, \quad y_0 = 1.$$

Najprej sistem zapišemo v matrični obliki

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A\begin{bmatrix} x_n \\ y_n \end{bmatrix}, \quad A = \begin{bmatrix} -4 & 4 \\ -1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = A^n\begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = \begin{bmatrix} -4 & 4 \\ -1 & 0 \end{bmatrix}^n\begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Kot v prejšnjem razdelku izračunamo jordansko kanonično formo za A

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

$$J^n = \begin{bmatrix} -2 & 1 \\ 0 & -2 \end{bmatrix}^n = \begin{bmatrix} (-2)^n & n(-2)^{n-1} \\ 0 & (-2)^n \end{bmatrix}$$

Primer matrike, ki ima diagonalizacijo

Poiščimo diagonalizacijo matrike

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

Najprej izračunamo karakteristični polinom

$$p_A(x) = \det(A - xI) = 2 - 5x + 4x^2 - x^3 = -(x-1)^2(x-2)$$

Lastni podprostor, ki pripada lastni vrednosti 1 je

$$\mathrm{Ker}\,(A - I) = \mathrm{Ker}\begin{bmatrix} -1 & 2 & 2 \\ 1 & -2 & -2 \\ -2 & 4 & 4 \end{bmatrix} = \mathrm{Lin}\{\begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}\}$$

$$P = \begin{bmatrix} 2 & 2 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 2 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

torej velja

$$AP = A\begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix} = \begin{bmatrix} Av_1 & Av_2 & Av_3 \end{bmatrix} = \begin{bmatrix} v_1 & v_2 & 2v_3 \end{bmatrix} = PD$$

odkoder sledi

$$A = PDP^{-1}$$

Primer uporabe: S pomočjo diagonalizacije je preprosto izračunati potenco matrike, kar pride prav pri reševanju sistemov diferenčnih enačb. Velja

$$A^n = AA \cdots A = PDP^{-1}PDP^{-1} \cdots PDP^{-1} = PDD \cdots DP^{-1} = PD^nP^{-1}$$

kjer D^n izračunamo tako, da potenciramo vse diagonalne elemente.

Odtod sledi, da za vsak polinom (ali konvergentno potenčno vrsto) $f(x) = \sum_i c_i x^i$ velja

$$f(A) = \sum_i c_i A^i = \sum_i c_i PD^iP^{-1} = P(\sum_i c_i D^i)P^{-1} = Pf(D)P^{-1}$$

kjer $f(D)$ izračunamo tako, da uporabimo f na vseh diagonalnih elementih. To nam pride prav reševanju sistemov linearnih diferencialnih enačb s konstantnimi koeficienti, kjer moramo izračunati $e^A = \sum_{n=0}^{\infty} \frac{1}{n!}A^n$.

Primer

Poiščimo diagonalizacijo $n \times n$ matrike

$$A = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix}$$

Rešitev: Naj bo $\varepsilon = e^{2\pi i/n}$ in $v_k = \sum_{j=1}^{n} \varepsilon^{jk}\mathbf{e}_j$

$$Av_k = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix}\begin{bmatrix} \varepsilon^k \\ \varepsilon^{2k} \\ \varepsilon^{3k} \\ \vdots \\ \varepsilon^{nk} \end{bmatrix}$$

$$= \begin{bmatrix} \varepsilon^{2k} \\ \varepsilon^{3k} \\ \varepsilon^{4k} \\ \vdots \\ \varepsilon^{k} \end{bmatrix} = \varepsilon^k\begin{bmatrix} \varepsilon^k \\ \varepsilon^{2k} \\ \varepsilon^{3k} \\ \vdots \\ \varepsilon^{nk} \end{bmatrix} = \varepsilon^k v_k$$

Ker so lastne vrednosti ε^k, $k = 1, \ldots, n$, paroma različne, so lastni vektorji v_k, $k = 1, \ldots, n$, linearno neodvisni. Torej ima A diagonalizacijo

$$P = \begin{bmatrix} v_1 & v_2 & \ldots & v_n \end{bmatrix}$$

$$D = \begin{bmatrix} \varepsilon & 0 & \ldots & 0 \\ 0 & \varepsilon^2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \varepsilon^n \end{bmatrix}$$

Potem je $AP = PD$, torej je iskana diagonalizacija

$$A = PDP^{-1}$$

Primer

Poiščimo diagonalizacijo $n \times n$ matrike

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \ldots & c_{n-2} & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \ldots & c_{n-3} & c_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ c_3 & c_4 & c_5 & \ldots & c_1 & c_2 \\ c_2 & c_3 & c_4 & \ldots & c_0 & c_1 \\ c_1 & c_2 & c_3 & \ldots & c_{n-1} & c_0 \end{bmatrix}$$

Naj bo A matrika iz prejšnjega primera. Podobno dobimo $A^3, A^4, \ldots$.

$$C = c_0 I + c_1 A + \ldots + c_{n-1}A^{n-1}$$

$$A^2 = \begin{bmatrix} 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & 0 & \ldots & 0 \end{bmatrix}$$

Označimo $p(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$.

$$C = p(A) = p(PDP^{-1}) = Pp(D)P^{-1}$$

kjer sta P in D kot v prejšnjem primeru.

Opomba: Matrike z večkratnimi lastnimi vrednostmi včasih imajo diagonalizacijo (npr. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$) včasih pa ne (npr. $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$). Izkaže se, da je to povezano z algebraično in geometrijsko večkratnostjo lastnih vrednosti. V prvem primeru sta obe večkratnosti enaki ($a(1) = g(1) = 2$), v drugem pa sta različni ($a(0) = 2$ in $g(0) = 1$).

Primer

Poišči jordansko kanonično formo matrike

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

Rešitev: Najprej izračunamo karakteristični polinom

$$\det(A - xI) = x(x-2)^3.$$

Potem izračunamo lastne in korenske podprostore za lastno vrednost 0

$$\mathrm{Ker} A = \mathrm{Lin}\{\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}\} = \mathrm{Ker} A^2$$

in nato še za lastno vrednost 2

$$\mathrm{Ker}(A - 2I) = \mathrm{Lin}\{\begin{bmatrix} 3 \\ 0 \\ -2 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 0 \\ 0 \end{bmatrix}\} \quad \mathrm{Ker}(A - 2I)^2 = \mathrm{Lin}\{\begin{bmatrix} 1 \\ 0 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 0 \\ 0 \end{bmatrix}\} = \mathrm{Ker}(A - 2I)^3$$

Opazimo, da je $\begin{bmatrix} 1 \\ 0 \\ 0 \\ 2 \end{bmatrix}$ dopolnitev baze $\mathrm{Ker}(A - 2I)$ do baze $\mathrm{Ker}(A - 2I)^2$

n da je $(A - 2I)\begin{bmatrix} 1 \\ 0 \\ 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 2 \\ 4 \\ 0 \\ 0 \end{bmatrix}$ linearno neodvisen od $\begin{bmatrix} 3 \\ 0 \\ -2 \\ 2 \end{bmatrix}$

Torej imamo naslednjo situacijo.

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad \begin{matrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 2 \end{bmatrix} \\ \downarrow \\ \begin{bmatrix} 2 \\ 4 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 3 \\ 0 \\ -2 \\ 2 \end{bmatrix} \end{matrix}$$

Jordanske verige zložimo v matriko

$$P = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & -2 \\ 0 & 0 & 2 & 2 \end{bmatrix} \quad J = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

Vsaki jordanski verigi dolžine k pripada ena jordanska kletka velikosti $k \times k$. Torej je jordanska kanonična forma matrike A enaka

Matriko A torej lahko izrazimo kot $A = PJP^{-1}$

Odtod sledi, da je

$$A^n = PJ^nP^{-1} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} (-2)^n & n(-2)^{n-1} \\ 0 & (-2)^n \end{bmatrix} \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} (-2)^n - 2n(-2)^{n-1} & 4n(-2)^{n-1} \\ -n(-2)^{n-1} & (-2)^n + 2n(-2)^{n-1} \end{bmatrix}$$

kar lahko še naprej poenostavimo. Če A^n pomnožimo z $\begin{bmatrix} x_0 \\ y_0 \end{bmatrix}$, dobimo

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 4n(-2)^{n-1} \\ (-2)^n + 2n(-2)^{n-1} \end{bmatrix} = (-2)^n \begin{bmatrix} -2n \\ 1-n \end{bmatrix}$$

Vektorski prostori z skalarnim produktom

Primer: Standardni skalarni produkt na $\mathbb{R}^n$

Običajnemu skalarnemu produktu iz prvega semestra bomo tu pravili **standardni skalarni produkt** na $\mathbb{R}^n$. Definiran je z

$$\langle(\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)\rangle = \alpha_1\beta_1 + \ldots + \alpha_n\beta_n$$

Pokazali smo že, da zadošča lastnostim (1),(2),(3).

Seveda standardni skalarni produkt ni edini skalarni produkt na $\mathbb{R}^n$. Klasifikacijo vseh skalarnih produktov na $\mathbb{R}^n$ bomo obdelali v naslednjem poglavju. Tu pokažimo samo, da jih je neskončno.

Na **funkcijskih prostorih** je **skalarni produkt** običajno definiran z **integralom**

Dodatni primeri skalarnih produktov na $\mathbb{R}^n$

Za vsako n-terico $\delta = (\delta_1, \ldots, \delta_n)$ strogo pozitivnih realnih števil je s

$$\langle(\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)\rangle = \delta_1\alpha_1\beta_1 + \ldots + \delta_n\alpha_n\beta_n$$

definiran skalarni produkt na $\mathbb{R}^n$. (Preveri lastnosti (1),(2),(3)!)

Konstruirajmo še neskončno mnogo drugih skalarnih produktov na $\mathcal{C}[a,b]$.

Dodatni primeri skalarnih produktov na $\mathcal{C}[a,b]$

Naj bo $w \in \mathcal{C}[a,b]$ taka funkcija, ki zadošča $w(x) > 0$ za vsak $x \in [a,b]$. S

$$\langle f, g\rangle = \int_a^b w(x)f(x)g(x)\,dx.$$

je definiran skalarni produkt na $\mathbb{R}^n$. (Preveri lastnosti (1),(2),(3)!)

Standardni skalarni produkt na $\mathcal{C}([a,b],\mathbb{C})$

Za dve zvezni funkciji f, g iz intervala $[a,b]$ v $\mathbb{C}$ definirajmo.

$$\langle f, g\rangle = \int_a^b f(x)\overline{g(x)}\,dx.$$

Pozor, za razliko od realnega primera imamo tu $\overline{g(x)}$ namesto $g(x)$.

Primer

Vektorja $(1,2)$ in $(2,-3)$ iz $\mathbb{R}^2$ sta pravokotna glede na skalarni produkt

$$\langle(\alpha_1, \alpha_2), (\beta_1, \beta_2)\rangle = 3\alpha_1\beta_1 + \alpha_2\beta_2,$$

nista pa pravokotna glede na standardni skalarni produkt.

Primer

Standardna baza v $\mathbb{R}^n$ je ortogonalna baza glede na standardni skalarni produkt.

Primer

Naj bo V vektorski prostor vseh realnih polinomov stopnje ≤ 3 in naj bo skalarni produkt na V definiran z $\langle p, q\rangle = \int_{-1}^1 p(x)q(x)\,dx$. Konstruirajmo ortonormirano bazo za V.

Vzemimo standardno bazo $u_1 = 1, \quad u_2 = x, \quad u_3 = x^2, \quad u_4 = x^3$

$$v_1 = 1$$

$$v_2 = x - \frac{\langle x, v_1\rangle}{\langle v_1, v_1\rangle}v_1 = x - 0v_1 = x$$

$$v_3 = x^2 - \frac{\langle x^2, v_1\rangle}{\langle v_1, v_1\rangle}v_1 - \frac{\langle x^2, v_2\rangle}{\langle v_2, v_2\rangle}v_2 = x^2 - \frac{1}{3}$$

$$v_4 = x^3 - \frac{\langle x^3, v_1\rangle}{\langle v_1, v_1\rangle}v_1 - \frac{\langle x^3, v_2\rangle}{\langle v_2, v_2\rangle}v_2 - \frac{\langle x^3, v_3\rangle}{\langle v_3, v_3\rangle}v_3 = x^3 - \frac{3}{5}x$$

Oglejmo si primer uporabe funkcij matrik. Iz Analize vemo, da je funkcija $y(t) = ce^{at}$ rešitev diferencialne enačbe $y'(t) = ay(t)$. To nam da idejo za reševanje naslednjega sistema diferencialnih enačb:

$$\begin{aligned} y_1'(t) &= a_{1,1}y_1(t) + \ldots + a_{1,d}y_d(t) \\ &\vdots \\ y_d'(t) &= a_{d,1}y_1(t) + \ldots + a_{d,d}y_d(t) \end{aligned}$$

Ta sistem najprej zapišemo v matrični obliki kot

$$\mathbf{y}'(t) = A\,\mathbf{y}(t).$$

Izkaže se, da je njegova rešitev vektorska funkcija

$$\mathbf{y}(t) = e^{At}\mathbf{c},$$

kjer je $\mathbf{c}$ konstanten vektor.

Matrično funkcijo e^{At} izračunamo tako, da v funkcijo $f(x) = e^{tx}$ vstavimo A namesto x. Kot zgoraj to prevedemo na primer e^{Jt}, kjer je J jordanska kletka. V tem primeru iz formule za funkcijo jordanske kletke dobimo

$$e^{Jt} = \begin{bmatrix} e^{\lambda t} & te^{\lambda t} & \frac{t^2}{2}e^{\lambda t} & \ldots & \frac{t^{k-1}}{(k-1)!}e^{\lambda t} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \frac{t^2}{2}e^{\lambda t} \\ \vdots & & & \ddots & te^{\lambda t} \\ 0 & \ldots & \ldots & \ldots & e^{\lambda t} \end{bmatrix}$$

Primer: Standardni skalarni produkt na $\mathcal{C}[a,b]$

Za dve zvezni funkciji f, g iz intervala $[a,b]$ v $\mathbb{R}$ definirajmo.

$$\langle f, g\rangle = \int_a^b f(x)g(x)\,dx.$$

Preverimo lastnosti (1),(2),(3), torej je to skalarni produkt.

Primer: Standardni skalarni produkt na $\mathbb{C}^n$.

Za dve kompleksni n-terici definirajmo njun **standardni skalarni produkt**

$$\langle(\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)\rangle = \alpha_1\bar{\beta}_1 + \ldots + \alpha_n\bar{\beta}_n.$$

Pozor, za razliko od realnega primera imamo tu $\bar{\beta}_i$ namesto β_i.

Opomba: Če $\sum_i \alpha_i\bar{\beta}_i$ zamenjamo z $\sum_i \delta_i\alpha_i\bar{\beta}_i$, kjer so $\delta_i > 0$ fiksni, dobimo drug skalarni produkt na $\mathbb{C}^n$.

Opomba: Če vzamemo $\int_a^b w(x)f(x)\overline{g(x)}\,dx$, kjer je $w(x)$ zvezna in za vsak x realna in strogo pozitivna, potem dobimo drug skalarni produkt.

Primer

Vektorji $(1,1,1,1,1,1,1,1)$, $(-1,-1,-1,-1,1,1,1,1)$, $(-1,-1,1,1,-1,-1,1,1)$ in $(-1,1,-1,1,-1,1,-1,1)$ tvorijo ortogonalno množico v $\mathbb{R}^8$ za standardni skalarni produkt.

Primer

Funkcije $f_k(x) = \sin\frac{k\pi x}{a}$, kjer $k = 1,2,3,\ldots$, tvorijo neskončno ortogonalno množico v $\mathcal{C}[0,a]$ za standardni skalarni produkt.

Primer normiranja ortogonalne baze

Vektorji $(-\frac{1}{2},1,1), (1,-\frac{1}{2},1), (1,1,-\frac{1}{2})$ tvorijo ortogonalno bazo za $\mathbb{R}^3$, ki ni normirana. Če te vektorje normiramo (delimo s $\frac{3}{2}$), dobimo vektorje $(-\frac{1}{3},\frac{2}{3},\frac{2}{3}), (\frac{2}{3},-\frac{1}{3},\frac{2}{3}), (\frac{2}{3},\frac{2}{3},-\frac{1}{3})$, ki tvorijo ortonormirano bazo za $\mathbb{R}^3$.

Vektorji v_1, v_2, v_3, v_4 so (po dokazu izreka) ortogonalna baza za V. Izračunajmo sedaj njihove norme in njihove normalizacije:

$$\|v_1\|^2 = \int_{-1}^1 1\,dx = 2, \qquad \frac{v_1}{\|v_1\|} = \frac{1}{\sqrt{2}},$$

$$\|v_2\|^2 = \int_{-1}^1 x^2\,dx = \frac{2}{3}, \qquad \frac{v_2}{\|v_2\|} = \sqrt{\frac{3}{2}}\,x,$$

$$\|v_3\|^2 = \int_{-1}^1 (x^2 - \tfrac{1}{3})^2\,dx = \frac{8}{45}, \qquad \frac{v_3}{\|v_3\|} = \sqrt{\frac{45}{8}}(x^2 - \tfrac{1}{3}),$$

$$\|v_4\|^2 = \int_{-1}^1 (x^3 - \tfrac{3}{5}x)^2\,dx = \frac{8}{175}, \qquad \frac{v_4}{\|v_4\|} = \sqrt{\frac{175}{8}}(x^3 - \tfrac{3}{5}x)$$

Normalizirani vektorji tvorijo ortonormirano bazo za V.

Opomba: Iz tega primera vidimo, da je ortonormirana baza običajno vključuje komplicirane korene. Za računske namene so zato pogosto boljše ortogonalne baze. Za teoretične namene pa so boljše ortonormirane baze.

Primer ortogonalnega komplementa

Naj bo V končnorazsežen vektorski prostor s skalarnim produktom, $\{u_1, \dots, u_k\}$ ortogonalna množica v V in $\{v_1, \dots, v_l\}$ njena dopolnitev do ortogonalne baze za V. Potem je $(\mathrm{Lin}\{u_1, \dots, u_k\})^\perp = \mathrm{Lin}\{v_1, \dots, v_l\}$.

Dokaz: Vzemimo poljuben element $v \in V$ in ga razvijmo po bazi za V. Dobimo $v = \sum_{i=1}^k \alpha_i u_i + \sum_{j=1}^l \beta_j v_j$. Ker je $\langle v, u_i\rangle = \alpha_i \langle u_i, u_i\rangle$, je v ortogonalen na vse u_i natanko tedaj, ko so vsi α_i enaki nič. To pa velja natanko tedaj, ko je $v \in \mathrm{Lin}\{v_1, \dots, v_l\}$.

Primera linearnih funkcionalov

Naj bo V vektorski prostor vseh realnih polinomov stopnje $\le n$. Potem sta

$$\phi(p) = \int_0^1 p(x)\, dx \quad \text{in} \quad \psi(p) = p(1)$$

dva primera linearnih funkcionalov na V.

Naj bo $\mathcal{B} = \{1, x, \dots, x^n\}$ in naj bosta ϕ ter ψ kot zgoraj. Potem je

$$[\phi]_{\mathcal{S}\leftarrow\mathcal{B}} = \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \dots & \frac{1}{n} \end{bmatrix} \qquad [\psi]_{\mathcal{S}\leftarrow\mathcal{B}} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \end{bmatrix}$$

Primer

Naj bo V vektorski prostor s skalarnim produktom in $w \in V$. Potem je

$$\phi_w(v) := \langle v, w\rangle$$

linearen funkcional na V.

Adjungirana preslikava

Primer

Naj bo V vektorski prostor vseh realnih polinomov stopnje ≤ 3 in naj bo $\langle p, q\rangle = \int_{-1}^1 p(x)q(x)\, dx$ skalarni produkt na V. Za linearni funkcional $\phi(p) = p(1)$ na V določi tak $r \in V$, da bo $\phi(p) = \langle p, r\rangle$ za vsak $p \in V$.

Prva rešitev: Najprej poiščemo ortonormirano bazo za V. Recimo

$$v_1 = \frac{1}{\sqrt{2}},\ v_2 = \sqrt{\frac{3}{2}}x,\ v_3 = \sqrt{\frac{45}{8}}(x^2 - \frac{1}{3}),\ v_4 = \sqrt{\frac{175}{8}}(x^3 - \frac{3}{5}x)$$

Vstavimo to bazo v formulo $w = \sum_{i=1}^n \overline{\phi(v_i)} v_i$ in dobimo

$$\begin{aligned} w &= v_1(1)v_1 + v_2(1)v_2 + v_3(1)v_3 + v_4(1)v_4 \\ &= \Big(\frac{1}{\sqrt{2}}\Big)^2 + \Big(\sqrt{\frac{3}{2}}\Big)^2 x + \frac{2}{3}\Big(\sqrt{\frac{45}{8}}\Big)^2 (x^2 - \frac{1}{3}) + \frac{2}{5}\Big(\sqrt{\frac{175}{8}}\Big)^2 (x^3 - \frac{3}{5}x) \\ &= -\frac{3}{4} - \frac{15}{4}x + \frac{15}{4}x^2 + \frac{35}{4}x^3. \end{aligned}$$

Druga rešitev: Recimo, da je $r(x) = e + fx + gx^2 + hx^3$. Potem je

$$\begin{aligned} 1 = \phi(1) = \langle 1, r\rangle &= \int_{-1}^1 (e + fx + gx^2 + hx^3)\, dx = 2e + \frac{2}{3}g \\ 1 = \phi(x) = \langle x, r\rangle &= \int_{-1}^1 x(e + fx + gx^2 + hx^3)\, dx = \frac{2}{3}f + \frac{2}{5}h \\ 1 = \phi(x^2) = \langle x^2, r\rangle &= \int_{-1}^1 x^2(e + fx + gx^2 + hx^3)\, dx = \frac{2}{3}e + \frac{2}{5}g \\ 1 = \phi(x^3) = \langle x^3, r\rangle &= \int_{-1}^1 x^3(e + fx + gx^2 + hx^3)\, dx = \frac{2}{5}f + \frac{2}{7}h \end{aligned}$$

Odtod dobimo $e = -\frac{3}{4}, g = \frac{15}{4}$ in $f = -\frac{15}{4}, h = \frac{35}{4}$.

Opomba: Prednost druge metode je, da nam ni treba računati ortonormirane baze, slabost pa je, da moramo rešiti sistem linearnih enačb. To metodo lahko spremenimo v alternativen dokaz Rieszovega izreka.

Primer računanja adjungirane preslikave

Naj bo $U = V$ vektorski prostor $\mathbb{C}^2$ z nestandardnim skalarnim produktom $\langle(\alpha_1, \alpha_2), (\beta_1, \beta_2)\rangle = 2\alpha_1\bar\beta_1 + 3\alpha_2\bar\beta_2$. Izračunaj adjungirano linearno preslikavo linearne preslikave $L(x, y) = (ax + by, cx + dy)$.

Ker je L^* linearna preslikava iz $\mathbb{C}^2$ v $\mathbb{C}^2$, je oblike

$$L^*(x, y) = (ex + fy, gx + hy).$$

Poleg tega mora veljati

$$\langle L(x_1, y_1), (x_2, y_2)\rangle = \langle (x_1, y_1), L^*(x_2, y_2)\rangle$$

za vse $x_1, x_2, y_1, y_2 \in \mathbb{C}$. Ko upoštevamo definiciji L in L^* dobimo

$$\langle (ax_1 + by_1, cx_1 + dy_1), (x_2, y_2)\rangle = \langle (x_1, y_1), (ex_2 + fy_2, gx_2 + hy_2)\rangle$$

za vse $x_1, x_2, y_1, y_2 \in \mathbb{C}$.

Ko upoštevamo še definicijo skalarnega produkta dobimo

$$2(ax_1 + by_1)\bar x_2 + 3(cx_1 + dy_1)\bar y_2 = 2x_1\overline{(ex_2 + fy_2)} + 3y_1\overline{(gx_2 + hy_2)}$$

za vse $x_1, x_2, y_1, y_2 \in \mathbb{C}$. Primerjajmo istoležne koeficiente:

koeficienti pri $x_1\bar x_2$: $2a = 2\bar e$

koeficienti pri $y_1\bar x_2$: $2b = 3\bar g$

koeficienti pri $x_1\bar y_2$: $3c = 2\bar f$

koeficienti pri $y_1\bar y_2$: $3d = 3\bar h$

Odtod izrazimo e, f, g, h z a, b, c, d in vstavimo v definicijo L^*. Dobimo

$$L^*(x, y) = (\bar a x + \frac{3}{2}\bar c y, \frac{2}{3}\bar b x + \bar d y)$$

Primer

Naj bo $U = V$ vektorski prostor $\mathbb{C}^2$ z nestandardnim skalarnim produktom $\langle(\alpha_1, \alpha_2), (\beta_1, \beta_2)\rangle = 2\alpha_1\bar\beta_1 + 3\alpha_2\bar\beta_2$. Izračunajmo še enkrat adjungirano linearno preslikavo linearne preslikave $L(x, y) = (ax + by, cx + dy)$.

$$u_1 = \frac{1}{\sqrt{2}}(1, 0), \quad u_2 = \frac{1}{\sqrt{3}}(0, 1)$$

ortonormirana baza glede na dani skalarni produkt. Označimo jo z $\mathcal{B}$. Določimo sedaj matriko preslikave L glede na to bazo. Velja

$$Lu_1 = \frac{1}{\sqrt{2}}(a, c) = au_1 + c\sqrt{\frac{3}{2}}u_2$$

$$Lu_2 = \frac{1}{\sqrt{3}}(b, d) = b\sqrt{\frac{2}{3}}u_1 + du_2$$

$$[L]_{\mathcal{B}\leftarrow\mathcal{B}} = \begin{bmatrix} a & b\sqrt{\frac{2}{3}} \\ c\sqrt{\frac{3}{2}} & d \end{bmatrix}$$

$$[L^*]_{\mathcal{B}\leftarrow\mathcal{B}} = ([L]_{\mathcal{B}\leftarrow\mathcal{B}})^* = \begin{bmatrix} a & b\sqrt{\frac{2}{3}} \\ c\sqrt{\frac{3}{2}} & d \end{bmatrix}^* = \begin{bmatrix} \bar a & \bar c\sqrt{\frac{3}{2}} \\ \bar b\sqrt{\frac{2}{3}} & \bar d \end{bmatrix}$$

$$\begin{aligned} L^*(x, y) &= L^*(\sqrt{2}xu_1 + \sqrt{3}yu_2) = \sqrt{2}xL^*(u_1) + \sqrt{3}yL^*(u_2) = \\ &= \sqrt{2}x(\bar a u_1 + \bar b\sqrt{\frac{2}{3}}u_2) + \sqrt{3}y(\bar c\sqrt{\frac{3}{2}}u_1 + \bar d u_2) = \\ &= (\bar a x + \frac{3}{2}\bar c y, \frac{2}{3}\bar b x + \bar d y) \end{aligned}$$

Primer

Določi lastne vrednosti in lastne vektorje matrike

$$A = \begin{bmatrix} 1 & 2 \\ i & 1 \end{bmatrix}$$

in njene adjungirane matrike A^*.

Rešitev: Karakteristični polinom matrike A je

$$\det(A - \lambda I) = (1 - \lambda)^2 - 2i = (1 - \lambda)^2 - (1 + i)^2 = (\lambda + i)(\lambda - 2 - i)$$

torej sta $-i$ in $2 + i$ lastni vrednosti matrike A. Podobno je

$$\det(A^* - \lambda I) = (1 - \lambda)^2 + 2i = (1 - \lambda)^2 - (1 - i)^2 = (\lambda - i)(\lambda - 2 + i)$$

karakteristični polinom matrike A^*. Torej sta i in $2 - i$ lastni vrednosti matrike A^*. Torej so lastne vrednosti za A^* res konjugirane lastnim vrednostim za A.

Lastna podprostora za A sta

$$\mathrm{Ker}\,(A + iI) = \mathrm{Lin}\begin{bmatrix} 1 - i \\ -1 \end{bmatrix}, \quad \mathrm{Ker}\,(A - (2 + i)I) = \mathrm{Lin}\begin{bmatrix} 1 - i \\ 1 \end{bmatrix}.$$

Lastna podprostora za A^* pa sta

$$\mathrm{Ker}\,(A^* - iI) = \mathrm{Lin}\begin{bmatrix} 1 - i \\ -2 \end{bmatrix}, \quad \mathrm{Ker}\,(A^* - (2 - i)I) = \mathrm{Lin}\begin{bmatrix} 1 - i \\ 2 \end{bmatrix}.$$

Odtod je razvidno, da $\mathrm{Ker}\,(A - \lambda I)$ in $\mathrm{Ker}\,(A^* - \bar\lambda I)$ nista nujno enaka.

Opomba: Pokazali bomo, da za normalne matrike vedno velja $\mathrm{Ker}\,(A - \lambda I) = \mathrm{Ker}\,(A^* - \bar\lambda I)$. Gornji primer kaže, da to v splošnem ni res. Vemo pa, da vedno velja $\dim \mathrm{Ker}\,(A - \lambda I) = \dim \mathrm{Ker}\,(A^* - \bar\lambda I)$.

Primer: Ortogonalni projektorji

Naj bo V vektorski prostor s skalarnim produktom, W podprostor v V in $L\colon V \to V$ taka linearna preslikava, ki vsakemu vektorju iz V priredi njegovo ortogonalno projekcijo na W. Pokažimo, da je $L = L^*$ in $L = L^2$.

Dokaz: Naj bo $w_1, \ldots, w_k$ ortonormirana baza za W. Potem za vsak $v \in V$ velja $Lv = \sum_{i=1}^{k} \langle v, w_i \rangle w_i$. Za vsak $v' \in V$ velja

$$\langle Lv, v' \rangle = \langle \sum_{i=1}^{k} \langle v, w_i \rangle w_i, v' \rangle = \sum_{i=1}^{k} \langle v, w_i \rangle \langle w_i, v' \rangle,$$

$$\langle v, Lv' \rangle = \langle v, \sum_{i=1}^{k} \langle v', w_i \rangle w_i \rangle = \sum_{i=1}^{k} \overline{\langle v', w_i \rangle} \langle v, w_i \rangle.$$

Torej je za vsaka $v, v' \in V$ velja $\langle Lv, v' \rangle = \langle v, Lv' \rangle$ kar pomeni $L = L^*$.
Ker je $Lw_i = w_i$ za vsak i, je

$$L^2 v = \sum_{i=1}^{k} \langle v, w_i \rangle L w_i = \sum_{i=1}^{k} \langle v, w_i \rangle w_i = Lv.$$

Primer 1: Hermitske matrike so normalne

Če je A hermitska, potem velja $A^* = A$. Odtod sledi $A^*A = A^2 = AA^*$. Torej je A normalna matrika.

Primer 2: Unitarne matrike so normalne

Če je A unitarna, potem je $A^* = A^{-1}$. Odtod sledi $A^*A = I = AA^*$. Torej je A normalna matrika.

Primer 3: Diagonalne matrike so normalne

Če je A diagonalna, potem je tudi A^* diagonalna. Dve diagonalni matriki vedno komutirata, zato je $A^*A = AA^*$. Torej je A normalna matrika.

Primer 4: Iz $A = A^T$ ne sledi nujno, da je A normalna

Matrika $A = \begin{bmatrix} 1 & i \\ i & 0 \end{bmatrix}$ zadošča $A = A^T$, vendar ni normalna.

Primer 5: Normalne 2×2 matrike

Matrika $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ je normalna $\iff |b| = |c|$ in $\bar{c}(a-d) = b(\bar{a} - \bar{d})$.

2×2 matrika je normalna natanko tedaj, ko velja

$$\begin{bmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{bmatrix}$$

$$\bar{a}a + \bar{c}c = a\bar{a} + b\bar{b} \qquad \bar{a}b + \bar{c}d = a\bar{c} + b\bar{d}$$

$$\bar{b}a + \bar{d}c = c\bar{a} + d\bar{b} \qquad \bar{b}b + \bar{d}d = c\bar{c} + d\bar{d} \qquad \bar{c}(a-d) = b(\bar{a} - \bar{d})$$

Prva in četrta enakost sta ekvivalentni z $b\bar{b} = c\bar{c}$, se pravi z $|b| = |c|$

Primer

Naj bo

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

Poišči tako ortogonalno matriko P in tako diagonalno matriko D, da je

$$A = PDP^{-1}.$$

Karakteristični polinom matrike A je

$$\det(A - xI) = -x^3 + 7x^2 - 12x = -x(x-3)(x-4)$$

Lastni vektorji, ki pripadajo lastnim vrednostim 4, 3, 0 so

$$\begin{bmatrix} 0 \\ -1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} -2 \\ 1 \\ 1 \end{bmatrix}$$

Očitno so to vektorji paroma ortogonalni. Če jih normiramo, dobimo

$$\begin{bmatrix} 0 \\ -1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}, \begin{bmatrix} 1/\sqrt{3} \\ 1/\sqrt{3} \\ 1/\sqrt{3} \end{bmatrix}, \begin{bmatrix} -2/\sqrt{6} \\ 1/\sqrt{6} \\ 1/\sqrt{6} \end{bmatrix}$$

Iskana matrika P je torej

$$P = \begin{bmatrix} 0 & 1/\sqrt{3} & -2/\sqrt{6} \\ -1/\sqrt{2} & 1/\sqrt{3} & 1/\sqrt{6} \\ 1/\sqrt{2} & 1/\sqrt{3} & 1/\sqrt{6} \end{bmatrix}$$

iskana matrika D pa je

$$D = \begin{bmatrix} 4 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$