# Podobnosti, analogije in posploševanja

FMF seminar

22. 9. 2023

D. Kobal

## Množenje matrik

- Matriki $A_{m\times n}$ in $B_{p\times q}$ lahko zmnožimo, če je $n = p$.
- $A_{m\times n} \cdot B_{n\times q} = C_{m\times q}$. Pri tem je $c_{ij}$ je 'skalarni produkt' $i$-te vrstice $A$ in $j$-tega stolpca $B$:

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

$$\begin{pmatrix} -1 & -1 & 1 & 0 \\ 1 & -1 & 2 & 3 \\ 2 & 3 & 4 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 & -1 \\ 3 & 0 & 1 \\ -1 & -1 & 1 \\ -2 & -2 & 1 \end{pmatrix} = \begin{pmatrix} -6 & -2 & 1 \\ -9 & -7 & 3 \\ 9 & -2 & 5 \end{pmatrix}$$

Če je mogoče izračunajmo:

- $\begin{bmatrix} 1 & 2 & -1 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 2 \\ 0 & -1 & 1 \end{bmatrix}$
- $\begin{bmatrix} 1 & 1 \\ 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$ in $\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & -1 \\ 1 & 0 \end{bmatrix}$
- $\begin{bmatrix} 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 3 & -1 \end{bmatrix}$ in $\begin{bmatrix} 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ -1 \end{bmatrix}$ ter $\begin{bmatrix} 3 \\ -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \end{bmatrix}$

Izračunajmo:

1. $\begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} -1 & 2 \\ 1 & 1 \end{bmatrix}$ in $\begin{bmatrix} -1 & 2 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}$
2. $\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 3 & -2 \end{bmatrix}$
3. $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ in $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$



Izračunajmo:

4. $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -7 & 3 \\ 4 & -5 & 2 \\ -3 & 2 & 0 \end{bmatrix}$ in $\begin{bmatrix} 1 & -7 & 3 \\ 4 & -5 & 2 \\ -3 & 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$
4. $\begin{bmatrix} 1 & 1 & 2 \\ 2 & 3 & 4 \\ 3 & 3 & 7 \end{bmatrix} \cdot \begin{bmatrix} 9 & -1 & -2 \\ -2 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix}$ in $\begin{bmatrix} 9 & -1 & -2 \\ -2 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 2 \\ 2 & 3 & 4 \\ 3 & 3 & 7 \end{bmatrix}$

## Magija ‘več-dimenzionalnih’ števil

Sistem enačb

$$\begin{aligned} x + \phantom{3}y + 2z &= 1 \\ 2x + 3y + 4z &= 0 \\ 3x + 3y + 7z &= 1 \end{aligned} \quad \text{za} \quad A = \begin{bmatrix} 1 & 1 & 2 \\ 2 & 3 & 4 \\ 3 & 3 & 7 \end{bmatrix} \quad X = \begin{bmatrix} x \\ y \\ z \end{bmatrix} \quad B = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

zapišemo $A \cdot X = B$ in kot pri $a \cdot x = b \Longrightarrow x = a^{-1}b$, takoj izračunamo

$$X = A^{-1}B = \begin{bmatrix} 9 & -1 & -2 \\ -2 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 7 \\ -2 \\ -2 \end{bmatrix}$$

## Analogije in posploševanja: števila, polinomi in matrike

- $a = 3$, $p(x) = x^2 - 3x + 2 = (x-1)(x-2)$, $A = \begin{bmatrix} -1 & 3 \\ -2 & 4 \end{bmatrix}$.
- $a^0, a^1, a^2, \ldots, A^0, A^1, A^2, \ldots, p(a) = a^2 - 3a + 2 = (a-1)(a-2)$, $p(A) = A^2 - 3A + 2I = (A - I) \cdot (A - 2I)$, $p(3) = 2$, $p(2) = 0$ in $p(A) = 0$.
- $p(x)$ in matrika $A$ večje stopnje/dimenzije?
- Matrika je 'škatla števil'. Bi lahko imeli 'škatlo polinomov? Konstante so tudi polinomi. 'Aritmetika računanja' je enaka pri 'škatlah števil' kot pri 'škatlah polinomov'.
- Smiselno je zapisati

$$M(x) = \begin{bmatrix} x^2 + x + 1 & x \\ 1 & 2x^2 \end{bmatrix} = x^2 \cdot \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} + x \cdot \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}. \tag{1}$$

  Matrika polinomov je polinom, katerega koeficienti so matrike.
- $M(x)$ lahko zapišemo tudi

$$M(x) = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \cdot x^2 + \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \cdot x + \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \tag{2}$$

- $p(x), A \longrightarrow p(A)$ toda $M(x), A \not\longrightarrow M(A)$, (zaradi nekomutativnosti množenja matrik) bi v splošnem v (2) in v (1) dobili različni $M(A)$.



**Opozorilo 1.**

Za polinomsko matriko $M(x)$ in za matriko $M$ izraz $M(A)$ **nima smisla**.

## Matrične ničle polinomov

- Za $p(x) = x^2 - 3x + 2 = (x-1)(x-2)$ sta 1 in 2 (edini številski!) ničli.
- Za

$$A = \begin{bmatrix} -1 & 3 \\ -2 & 4 \end{bmatrix} \quad \text{in} \quad B = \begin{bmatrix} 3 & 2 & -2 \\ 1 & 2 & -1 \\ 2 & 2 & -1 \end{bmatrix}$$

  izračunamo $p(A) = 0$ in $p(B) = 0$.
- Smiselno reči: $A$ in $B$ sta matrični ničli polinoma $p(x)$.
- *Število $a$ je ničla polinoma $p(x)$, čee velja $p(a) = 0$.*
- *Matrika $A$ je matrična ničla polinoma $p(x)$, čee velja $p(A) = 0$.*
- Lahko karkoli povemo o matričnih ničlah polinoma?
- Lahko (za začetek) rečemo karkoli o matričnih ničlah tako enostavnega polinoma, kot je $p(x) = x^2 - 3x + 2 = (x-1)(x-2)$?

## Matrične ničle enostavnega polinoma $p(x) = x^2 - 3x + 2 = (x-1)(x-2)$

- $[1]$, $[2]$, $1 \cdot I$, $2 \cdot I$, kjer je $I$ identična matrika. Bolj skrivnostne matrične ničle:

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{3}$$

- Iz razcepa $p(x) = x^2 - 3x + 2 = (x-1)(x-2)$ torej dobimo diagonalne matrične ničle polinoma $p(x)$ z enkami in dvojkami po diagonali. Premislimo, kaj pomeni 'bločno množenje matrik' $p(D) = (D - I)(D - 2I)$.
- Od kje so prišle navidezno poljubne 'matrične ničle', kot sta prejšnji $A$ in $B$? Bi znali poiskati še druge? Ali celo vse?
- Naj bo $D$ diagonalna matrika kot v (3). Izračunajmo $p(M)$ za $M = P \cdot D \cdot P^{-1}$, kjer je $P$ poljubna obrnljiva matrika:

$$p(M) = p(P \cdot D \cdot P^{-1}) = \cdots = P \cdot p(D) \cdot P^{-1} = P \cdot 0 \cdot P^{-1} = 0 \tag{4}$$

- Tako iz razcepa polinoma dobimo ogromno 'zelo naključno izgledajočih' matričnih ničel polinoma.



## Analogije, posploševanja in dokazi

- Za enostavne polinome kot je $p(x) = x^2 - 3x + 2 = (x-1)(x-2)$ vemo vse o njihovih številskih ničlah. V splošnem velja:

**Izrek 1**

Število $m$ je ničla polinoma $p(x)$ čee velja

$$p(x) = r(x) \cdot (x - m)$$

za nek polinom $r(x)$.

Preden se vprašamo, če velja kaj podobnega tudi za matrike, se vprašajmo, ali razumemo, zakaj izrek zares velja. Kako ga dokažemo?

Če je $p(x) = r(x) \cdot (x - m)$, potem je očitno $p(m) = r(m) \cdot (m - m) = 0$. Kaj pa v obratni smeri?

$p(m) = 0 \overset{?}{\Longrightarrow} p(x) = r(x) \cdot (x - m)$

Spomnimo se faktorizacije

$$x^i - m^i = (x^{i-1} + x^{i-2}m + \cdots + xm^{i-2} + m^{i-1})(x - m),$$

ki velja za $i \geq 2$. Če je $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, izračunamo

$$\begin{aligned} p(x) - p(m) &= \sum_{i=1}^{n} a_i \cdot (x^i - m^i) \\ &= \sum_{i=2}^{n} a_i \cdot (x^{i-1} + x^{i-2}m + \cdots + xm^{i-2} + m^{i-1})(x - m) + a_1(x - m) \\ &= r(x) \cdot (x - m) \end{aligned}$$

kjer je $r(x)$ polinom stopnje $n - 1$. Torej, če je $p(m) = 0$, dobimo

$$p(x) = p(m) + r(x) \cdot (x - m) = r(x) \cdot (x - m).$$



Kaj bi bila smiselna interpretacija izreka 1 za matrike?

Izrek 1Izrek 2

Število $m$ je ničla polinoma $p(x)$ čee velja

$$p(x) = r(x) \cdot (x - m)$$

za nek polinom $r(x)$. Matrika $M$ je matrična ničla polinoma $p(x)$ čee velja

$$p(x) \cdot I = R(x) \cdot (xI - M)$$

za neko polinomsko matriko $R(x)$, pri čemer je $I$ identična matrika.

Zanimivo, da če je $p(M)$ ničelna matrika, lahko konstruiramo popolnoma analogen dokaz izreku 1, da bi pokazali, da je $p(x) \cdot I = R(x) \cdot (xI - M)$. Dokaz v obratni smeri pa je težji. Namreč, če je $p(x) \cdot I = R(x) \cdot (xI - M)$, ne moremo preprosto izračunati $p(M)I = R(M) \cdot (M \cdot I - M) = 0$. Spomnimo se namreč (Opozorilo 1), da $R(M)$ sploh nima smisla . Da bi dokazali izrek 2, moramo zares razumeti še nekatera zelo elementarna dejstva.

Kako bi natančno dokazali naslednje preprosto dejstvo?

### Dejstvo 1

Če je $p(x)$ tak polinom, da velja $p(x) \cdot (x - a) \equiv c$, kjer sta $a$ in $c$ konstanti, potem mora biti $c = 0$ in $p(x) \equiv 0$.

### Natančen dokaz 'dejstva 1'

Za $p(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$, izračunamo

$$p(x) \cdot (x - a) = b_n x^{n+1} + (b_{n-1} - ab_n) x^n + \cdots + (b_0 - b_1 a) x - b_0 a.$$

Če je to ničelni polinom, potem mora biti $b_n = 0$. Če je $b_n = 0$, sledi, da je $b_{n-1} = 0$. Podobno sklepamo, da so vsi koeficienti polinoma $p(x)$ enaki 0 in $p(x) \equiv 0$ ter $c = 0$.

### Dejstvo 2 (matrike)

Če je $P(x)$ taka polinomska matrika, da velja $P(x) \cdot (xI - A) \equiv C$, kjer sta $A$ in $C$ konstantni matriki, potem mora biti $C = 0$ in $P(x) \equiv 0$.

Dokaz 'dejstva 2' je praktično identičen dokazu 'dejstva 1'



### Dejstvo 2 (matrike)

Če je $P(x)$ taka polinomska matrika, da velja $P(x) \cdot (xI - A) \equiv C$, kjer sta $A$ in $C$ konstantni matriki, potem mora biti $C = 0$ in $P(x) \equiv 0$.

### Dokaz 'dejstva 2'

Spomnimo se, da smo lahko zapisali na primer

$$M(x) = \begin{bmatrix} x^2 + x + 1 & x \\ 1 & 2x^2 \end{bmatrix} = x^2 \cdot \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} + x \cdot \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}.$$

Podobno lahko vsako polinomsko matriko zapišemo v obliki

$$P(x) = P_n x^n + P_{n-1} x^{n-1} + \cdots + P_1 x + P_0,$$

kjer so $P_0, P_1, \ldots, P_n$ konstantne matrike. Povsem analogno kot v številskem primeru izračunamo $C = P(x) \cdot (xI - A)$, in dobimo

$$C = P_n x^{n+1} + (P_{n-1} - P_n \cdot A) x^n + \cdots + (P_0 - P_1 \cdot A) x - P_0 \cdot A.$$

Ker je $C$ konstantna matrika, mora biti $P_n = 0$. In če je $P_n = 0$, sledi tudi $P_{n-1} = 0$. Podobno ugotovimo, da so vsi matrični koeficienti $P(x)$ ničelne matrike in zato $P(x) \equiv 0$ ter $C \equiv 0$.

**Izrek 2**

Matrika $M$ je matrična ničla polinoma $p(x)$ čee velja

$$p(x) \cdot I = R(x) \cdot (xI - M)$$

za neko polinomsko matriko $R(x)$, pri čemer je $I$ identična matrika.

**in njegov dokaz**

Povsem podobno kot pri dokazu izreka 1 zapišemo:

$$x^i I - M^i = (x^{i-1} I + x^{i-2} M + \cdots + x M^{i-2} + M^{i-1}) \cdot (xI - M),$$

za $i \geq 2$. Za $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, lahko zapišemo

$$\begin{aligned} p(x)I - p(M) &= \sum_{i=0}^{n} a_i (x^i I - M^i) \\ &= \sum_{i=2}^{n} a_i (x^{i-1} I + x^{i-2} M + \cdots + M^{i-1}) \cdot (xI - M) + a_1 (xI - M) \\ &= Q(x) \cdot (xI - M) \end{aligned}$$

kjer je $Q(x)$ polinomska matrika. Torej velja

$$p(x)I = p(M) + Q(x) \cdot (xI - M).$$



**Izrek 2**

Matrika $M$ je matrična ničla polinoma $p(x)$ čee velja

$$p(x) \cdot I = R(x) \cdot (xI - M)$$

za neko polinomsko matriko $R(x)$, pri čemer je $I$ identična matrika.

**in njegov dokaz**

... velja

$$p(x)I = p(M) + Q(x) \cdot (xI - M). \tag{5}$$

Če je $p(M) = 0$, torej velja $p(x)I = Q(x) \cdot (xI - M)$.
Za dokaz v obratni smeri privzamemo $p(x)I = R(x) \cdot (xI - M)$, kar skupaj z enakostjo (5) pomeni

$$p(M) + Q(x) \cdot (xI - M) = R(x) \cdot (xI - M).$$

Izrazimo

$$p(M) = (R(x) - Q(x)) \cdot (xI - M).$$

Ker je $p(M)$ konstantna matrika, po 'dejstvu 2' zaključimo, da velja $R(x) \equiv Q(x)$ in $p(M) = 0$.

Izrek 2 smo torej dokazali. Ali ga tudi zares razumemo?

- Izrek “*m je ničla polinoma $p(x)$, čee $p(x) = r(x) \cdot (x - m)$*” smo dobro razumeli. Za dano število npr. 3 smo takoj znali zapisati polinom, npr. $p(x) = (x-3)(x^2+4) = x^3 - 3x^2 + 4x - 12$ za katerega je veljalo $p(3) = 0$.
- Je izrek “*M je matrična ničla polinoma $p(x)$, čee $p(x) \cdot I = R(x) \cdot (xI - M)$*” podoben? Znamo za dano matriko $M$ poiskati polinom $p(x)$, za katerega bo veljalo $p(M) = 0$?
- Precej očitno je, da je za poljubno matriko $M$ precej brezupna naloga poiskati tako polinomsko matriko $R(x)$, da bo $R(x) \cdot (xI - M)$ ravno identična matrika $I$ pomnožena s polinomom $p(x)$. (Mogoče opazimo, da je naloga precej podobna iskanju ‘inverza matrike $(xI - M)$’).
- Zaključimo, da nam izrek 2 ne pove (povsem) kako za poljubno matriko $M$ dobimo polinom $p(x)$ za katerega velja $p(M) = 0$.
- Zamislimo se, da to spoznanje **ne pove**, da je izrek 2 brez veze. Nam pa pomaga bolje razumeti kompleksnost polinomov, matrik in posebej matričnih ničel polinomov.



## * Vektorski prostori in Cayley-Hamiltonov izrek

- Matrike dimenzij $n \times n$ tvorijo vektorski prostor $n^2$.
- Determinante.
- *Laplaceov razvoj po vrsticah in stolpcih* je zaobsežen je v enakosti:

$$\det(M) \cdot I = \mathrm{adj}(M) \cdot M. \tag{6}$$

$$M = \begin{bmatrix} 3 & 2 & -2 \\ 1 & 2 & -1 \\ 2 & 2 & -1 \end{bmatrix} \longrightarrow \mathrm{adj}(M) = \begin{bmatrix} \begin{vmatrix} 2 & -1 \\ 2 & -1 \end{vmatrix} & -\begin{vmatrix} 2 & -2 \\ 2 & -1 \end{vmatrix} & \begin{vmatrix} 2 & -2 \\ 2 & -1 \end{vmatrix} \\ -\begin{vmatrix} 1 & -1 \\ 2 & -1 \end{vmatrix} & \begin{vmatrix} 3 & -2 \\ 2 & -1 \end{vmatrix} & -\begin{vmatrix} 3 & -2 \\ 1 & -1 \end{vmatrix} \\ \begin{vmatrix} 1 & 2 \\ 2 & 2 \end{vmatrix} & -\begin{vmatrix} 3 & 2 \\ 2 & 2 \end{vmatrix} & \begin{vmatrix} 3 & 2 \\ 1 & 2 \end{vmatrix} \end{bmatrix}$$

- V primeru obstoja inverza matrike iz enakosti (6) dobimo znano formulo za inverz $M^{-1} = \frac{1}{\det(M)} \mathrm{adj}(M)$.
- V primeru

$$M = \begin{bmatrix} 3 & 2 & -2 \\ 1 & 2 & -1 \\ 2 & 2 & -1 \end{bmatrix} \quad \text{je} \quad \det(M) = 2 \quad \text{in} \quad M^{-1} = \frac{1}{2}\mathrm{adj}(M) = \frac{1}{2} \begin{bmatrix} 0 & -2 & 2 \\ -1 & 1 & 1 \\ -2 & -2 & 4 \end{bmatrix}$$

## * Vektorski prostori in Cayley-Hamiltonov izrek

- Ponovimo koncept matrične ničle polinoma. Za preprost razcepen polinom smo znali poiskati (nekatere) njegove matrične ničle. Poznamo tudi izrek:
  *$M$ je matrična ničla polinoma $p(x)$, čee $p(x) \cdot I = R(x) \cdot (xI - M)$*
  A za dano splošno matriko $M$ ne vemo, če in kako bi lahko dobili polinom $p(x)$, da bi veljalo $p(M) = 0$.
- Spomnimo se, da matrike dimenzij $n \times n$ tvorijo vektorski prostor dimenzije $n^2$. Razmislimo o vektorjih $I = M^0, M^1, M^2, \ldots, M^{n^2}$ znotraj tega prostora. Ker je teh matrik/vektorjev $n^2 + 1$, morajo biti med seboj linearno odvisni. To pomeni, da obstajajo konstante $a_0, a_1, a_2, \ldots, a_{n^2}$, da velja

$$a_0 I + a_1 M + a_2 M^2 + \cdots + a_{n^2} M^{n^2} = 0.$$

  Torej bo za polinom $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n^2} x^{n^2}$, veljalo $p(M) = 0$. Poudarimo, da je to 'eksistencialni (in ne konstrukcijski) dokaz'. Torej vemo, da za matriko $M$ obstaja polinom $p(x)$, da velja $p(M) = 0$. A še vedno ne vemo, kako bi v konkretnem primeru tak polinom dobili.



- Začnimo s poljubno matriko $M$ in razmislimo o *polinomski matriki* $xI - M$. Za (prejšnja) primera matrik

$$A = \begin{bmatrix} -1 & 3 \\ -2 & 4 \end{bmatrix} \quad \text{in} \quad B = \begin{bmatrix} 3 & 2 & -2 \\ 1 & 2 & -1 \\ 2 & 2 & -1 \end{bmatrix}$$

  bi dobili

$$xI - A = \begin{bmatrix} x+1 & -3 \\ 2 & x-4 \end{bmatrix} \quad \text{in} \quad xI - B = \begin{bmatrix} x-3 & -2 & 2 \\ -1 & x-2 & 1 \\ -2 & -2 & x+1 \end{bmatrix}$$

- Če za tako polinomsko matriko izračunamo $\det(xI - M)$, dobimo polinom ustrezne stopnje. Za naša primera bi dobili $\det(xI - A) = x^2 - 3x + 2$ in $\det(xI - B) = x^3 - 4x^2 + 5x - 2$.
- V primerih npr. $3 \times 3$, $4 \times 4$ in $n \times n$ matrike $M$ bi dobili polinome $\det(xI - M)$ stopenj 3, 4 in $n$.

### Karakteristični polinom matrike

- Za matriko $M$ definiramo njen *karakteristični polinom*

$$\chi_M(x) = \det(xI - M).$$

  Karakterističen polinom matrike $M$ je skrivnosten polinom, ki je seveda odvisen od matrike. O karakterističnem polinomu ne vemo skoraj ničesar razen njegove stopnje $n$, ki ustreza dimenziji $n \times n$ matrike $M$.
- Velja pa slavni:

### Cayley-Hamiltonov izrek

$$\chi_M(M) = 0$$



### Primera

Za matriki

$$A = \begin{bmatrix} -1 & 3 \\ -2 & 4 \end{bmatrix} \quad \text{in} \quad B = \begin{bmatrix} 3 & 2 & -2 \\ 1 & 2 & -1 \\ 2 & 2 & -1 \end{bmatrix}$$

smo izračunali njuna karakteristična polinoma

$$\begin{aligned} \chi_A(x) &= x^2 - 3x + 2 &&= (x-1)(x-2) \quad \text{in} \\ \chi_B(x) &= x^3 - 4x^2 + 5x - 2 &&= (x-1)^2(x-2), \end{aligned}$$

in tudi $\chi_A(A) = 0$ in $\chi_B(B) = 0$.

Dobili smo tudi $\chi_A(B) = 0$.

Kako pa bi dokazali Cayley-Hamiltonov izrek?

### Cayley-Hamiltonov izrek

$$\chi_M(M) = 0.$$

### Dokaz Cayley-Hamiltonovega izreka

- Je to dokaz: za $\chi_M(x) = \det(x \cdot I - M)$ izračunamo

$$\chi_M(M) = \det(M \cdot I - M) = \det(0) = 0$$

- Zakaj je razmislek napačen? Enakosti nimajo smisla: Na levi imamo matriko, na desni število.
- Pravi in zelo eleganten dokaz: Spomnimo se enakosti (6)

$$\det(M) \cdot I = \mathrm{adj}(M) \cdot M.$$

  Če v enačbo (6) namesto $M$ vstavimo $xI - M$ dobimo

$$\det(xI - M) \cdot I = \mathrm{adj}(xI - M) \cdot (xI - M).$$

  oziroma

$$\chi_M(x) \cdot I = \mathrm{adj}(xI - M) \cdot (xI - M).$$

  Izrek 2 nam pove, da je $M$ matrična ničla polinoma $\chi_M(x)$.



### Ponovno o izreku 2

Da bi še bolje razumeli izrek

*$M$ je matrična ničla polinoma $p(x)$, čee $p(x) \cdot I = R(x) \cdot (xI - M)$*

se vrnimo k primeroma

$$A = \begin{bmatrix} -1 & 3 \\ -2 & 4 \end{bmatrix} \quad \text{in} \quad B = \begin{bmatrix} 3 & 2 & -2 \\ 1 & 2 & -1 \\ 2 & 2 & -1 \end{bmatrix}$$

ter k njunima karakterističnima polinomoma

$$\begin{aligned} \chi_A(x) = &\quad x^2 - 3x + 2 &&= (x-1)(x-2) \quad \text{in} \\ \chi_B(x) = &\quad x^3 - 4x^2 + 5x - 2 &&= (x-1)^2(x-2). \end{aligned}$$

Vemo, da je $\chi_A(A) = 0$ in $\chi_B(B) = 0$, izračunali smo pa tudi $\chi_A(B) = 0$. Po izreku 2 obstajajo polinomske matrike $R(x)$, $Q(x)$ and $T(x)$ da bo veljalo

$$\begin{aligned} \chi_A(x) \cdot I = &\quad R(x) \cdot (xI - A) \\ \chi_A(x) \cdot I = &\quad Q(x) \cdot (xI - B) \quad \text{in} \\ \chi_B(x) \cdot I = &\quad T(x) \cdot (xI - B) \end{aligned}$$

Take polinomske matrike obstajajo in so naslednje

$$R(x) = \begin{bmatrix} x-4 & 3 \\ -2 & x+1 \end{bmatrix}, \quad Q(x) = \begin{bmatrix} x & 2 & -2 \\ 1 & -1+x & -1 \\ 2 & 2 & -4+x \end{bmatrix} \text{ in}$$

$$T(x) = \begin{bmatrix} x^2-x & 2x-2 & 2-2x \\ x-1 & x^2-2x+1 & 1-x \\ 2x-2 & 2x-2 & x^2-5x+4 \end{bmatrix}.$$

Že prej smo opazili, da je $\chi_B(x) = (x-1)\cdot\chi_A(x)$. $R(x)$, $Q(x)$ in $T(x)$ lahko razumemo kot:

$$\begin{array}{llcll} \chi_A(x)\cdot I = & R(x)\cdot(xI-A) & & R(x) = & \chi_A(x)\cdot(xI-A)^{-1} \\ \chi_A(x)\cdot I = & Q(x)\cdot(xI-B) & \longrightarrow & Q(x) = & \chi_A(x)\cdot(xI-B)^{-1} \\ \chi_B(x)\cdot I = & T(x)\cdot(xI-B) & & T(x) = & \chi_B(x)\cdot(xI-B)^{-1} \end{array}$$



- Cayley-Hamiltonov izrek je prvič in v zelo posebnem primeru obravnaval irski matematik, fizik in astronom William Rowan Hamilton (1805 - 1865) in sicer leta 1853 v knjigi:
  Hamilton W. R., Lectures on Quaternions, *Doblin, Americana collection, 1853*, 884 strani.
- Cayley-Hamiltonov izrek je prvič v celoti 'bolj omenil kot dokazal' angleški matematik Arthur Cayley (1821 - 1895) in sicer leta 1858 v članku:
  Cayley A., A Memoir on the Theory of Matrices, *Philosophical Transactions of the Royal Society of London, 1858*, 148: 17–37.
  Cayley je namreč za poljubno $2\times 2$ matriko

  $$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

  eksplicitno izračunal $M^2 - (a+d)M^1 + (ad-bc)M^0 = 0$. V modernem jeziku to ustreza izračunu, da izrek velja za matrike dimenzije $2\times 2$. Izračun za matrike dimenzij $3\times 3$ je zgolj nakazal, za še večje dimenzije pa napisal: "*Za primere matrik splošnih dimenzij se mi zahtevni izračuni ne zdijo niti potrebni niti vredni napornega dela.*" [na strani str. 24]
- Izrek je v celoti prvi dokazal 38 let pozneje nemški matematik Ferdinand Georg Frobenius (1849 - 1917) v članku:
  Frobenius F. G., Über vertauschbare Matrizen, *Sitz. Preuß. Akad. Wiss. Berlin, 1896*. 601–614.

## Podobnosti, analogije in posploševanja

- Naravni in matematični jezik nista in ne smeta biti v protislovju, ampak je matematični jezik le ’rafiniranje naravnega izražanja’.
- Lep primer je pojem podobnosti.
- Matematični jezik je lahko ‘nerazumljiv’, nikoli pa v naravnem jeziku ne sporoča ‘neresnice’. Primer: ’Matematični jezik je enoumen.’ (!)
- Matematični in naravni jezik si ne nasprotujeta, ampak se dopolnjujeta.
- Primer iz logike: ‘Pomil boš avto ali pa ne dobiš nagrade’.

  V naravnem jeziku razumemo poved kot izključujočo disjunkcijo, ali bomo avto pomili ali pa ne bomo dobili nagrade. Izjava je resnična, če se uresniči natanko eden od obeh stavkov v povedi. Ta pomen se ne sklada s pomenom logične disjunkcije, kjer je izjava resnična, če je resničen vsaj en od obeh stavkov v povedi. Matematična logika dopušča resničnost obeh stavkov, zato je izjava resnična tudi, če pomijemo avto in ne dobimo nagrade.

  Gre tu sploh za izjave?



## Podobnosti, analogije in posploševanja

- Ali primeri iz učbenikov:

GEOMETRIJSKA TELESA
razdelimo na
OGLATA IN OKROGLA

  - OGLATA TELESA:
    Vse ploskve oglatega telesa so ravne.
  - OKROGLA TELESA:
    Vsaj ena ploskev okroglega telesa je kriva.

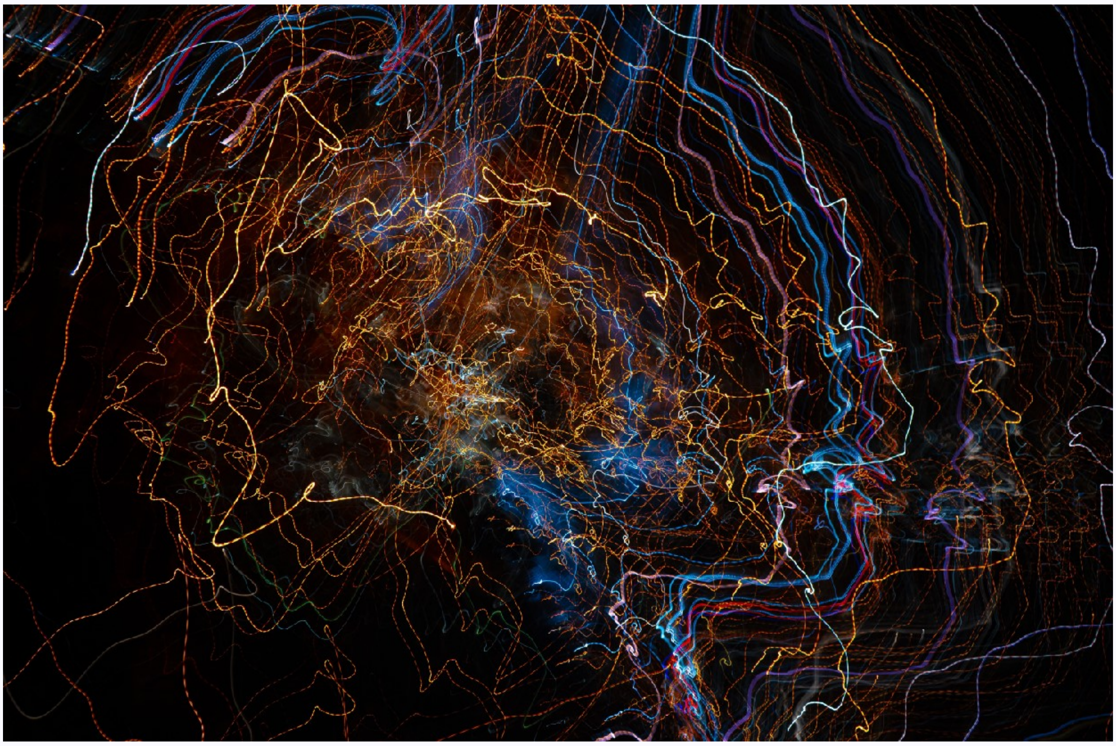
## Definicija vektorja

Vektor je določen s

- smerjo,
- usmerjenostjo in
- dolžino.

## Naravni in matematični jezik

- Naravni jezik je pogled na fraktal/resnico od ... daleč.





## Naravni in matematični jezik

- Matematični jezik je pogled na fraktal/resnico od ... nekoliko bliže.