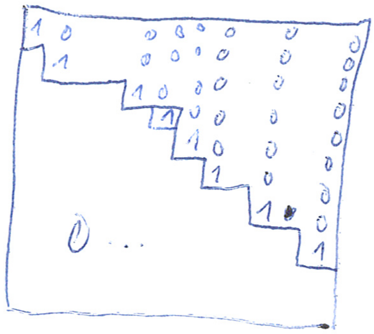
Frobeniova věta: soustava $(A|b)$ má alespoň jedno řešení $\iff$ $\operatorname{rank}(A) = \operatorname{rank}(A|b)$

poslední sloupec nemá pivota

RREF

pivoty můžeme nastavit na 1

můžeme vynulovat hodnoty nad pivotem



def: $a_{1p_1} = a_{2p_2} \dots a_{rp_r} = 1$

$\forall i \in \{2, \dots r\}$ $a_{1p_i} = a_{2p_i} \dots a_{i-1\,p_i} = 0$

RREF je jednoznačný

Gauss-Jordanova eliminace

převedeme soustavu $(A|b)$ na RREF $(A'|b')$

situace

(A) soustava nemá řešení

$\operatorname{rank}(A) < \operatorname{rank}(A|b)$

(B) aspoň 1 řešení

(B1) jediné řešení $\underset{\#\text{pivotů}}{r} = \underset{\#\text{proměnných}}{n}$

$$\left(\begin{array}{ccccc|c} 1 & & 0 & & & b_1 \\ & 1 & & & & b_2 \\ 0 & & 1 & & & b_3 \\ & & & 1 & & b_4 \\ \vdots & & & & 1 & b_5 \\ & & & & 0 & 0 \end{array}\right) \quad \begin{array}{l} x_1 = b'_1 \\ x_2 = b'_2 \\ x_3 = b'_3 \\ x_4 = b'_4 \\ x_5 = b'_5 \end{array}$$

rovnou máme řešení

(B2) nekonečně mnoho řešení $r < n$

$$x_{p_k} + \sum_{j \in N,\ j > p_k} a'_{kj} x_j = b'_k \qquad k = 1 \dots r$$

N nebazické proměnné

porovnání

Gaussova eliminace je $\pm$ o $\frac{1}{3}$ rychlejší

G-J bude třeba pro inverzi matic

Operace s maticemi

Def: rovnost : 2 matice se rovnají $A=B$ pokud mají stejné rozměry $m \times n$ a $A_{ij}=B_{ij}$ pro všechna přípustná ij

Def: součet $A, B \in R^{m \times n}$ $A+B$ je matice $m \times n$ s prvky $(A+B)_{ij} = A_{ij}+B_{ij}$ pro přípustná i, j

Def: násobek αA má prvky $(\alpha A)_{ij} = \alpha A_{ij}$

→ odčítání $A+(-1)B$

nulová matice 0 nebo $0_{m \times n}$

Vlastnosti součtu a násobku matic (tvrzení) dk 1

1. $A+B=B+A$ komutativita
2. $(A+B)+C=A+(B+C)$ asociativita
3. $\alpha(A+B)=\alpha A+\alpha B$ distributivita
4. $(\alpha+\beta)A=\alpha A+\beta A$ — " —
5. $A+0=A$
6. $A+(-1)A=0$
7. $\alpha(\beta A)=(\alpha\beta)A$
8. $1A=A$

ověříme, že mají stejný typ

$(A+B)_{ij}=A_{ij}+B_{ij}$

$(B+A)_{ij}=B_{ij}+A_{ij}$

$A_{ij}+B_{ij}=B_{ij}+A_{ij}$

$(A+B)_{ij}=(B+A)_{ij}$ $\square$

Součin matic

def: $A \in R^{m \times p}$, $B \in R^{p \times n}$ AB je matice typu $m \times n$ s prvky

1. má stejný počet sloupců jako 2. řádků

$$(AB)_{ij}=\sum_{k=1}^{p} A_{ik}B_{kj}$$

Vlastnosti

1. obecně $AB \neq BA$
2. $(AB)C=A(BC)$ asociativita
3. $A(B+C)=AB+AC$ distributivita zleva
4. $(A+B)C=AC+BC$ — " — zprava
5. $\alpha(AB)=(\alpha A)B=A(\alpha B)$

dk: asociativita

$A \in R^{m \times p}$ $B \in R^{p \times r}$ $C \in R^{r \times n}$

obě $(AB)C$ a $A(BC)$ jsou $m \times n$

$((AB)C)_{ij}=\sum_{k=1}^{r}(AB)_{ik}C_{kj}=\sum_{k=1}^{r}\left(\sum_{l=1}^{p}A_{il}B_{lk}\right)C_{kj}$

$(A(BC))_{ij}=\sum_{l=1}^{p}A_{il}(BC)_{lj}=\sum_{l=1}^{p}A_{il}\sum_{k=1}^{r}B_{lk}C_{kj}$

výrazy jsou shodné až na pořadí sčítanců

LA1 P02 S03

Jednotková matice řádu n čtvercová, na diagonále 1 $I_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & & & 0 \\ \vdots & & \ddots & & 0 \\ \vdots & & & 1 & 1 \end{pmatrix}$

Jednotkový vektor e_i ... i-tý sloupec jednotkové matice $e_i = I_{*i}$

Tvrz: pro $A \in R^{m \times n}$ platí $I_m A = A I_n = A$

Def: Transpozice matice

$A \in R^{m \times n}$ $A^T \in R^{n \times m}$ $(A^T)_{ij} := A_{ji}$

překlopení dle hlavní diagonály

Tv: vlastnosti

1. $(A^T)^T = A$
2. $(A+B)^T = A^T + B^T$
3. $(\alpha \cancel{A^*})^T = \alpha A^T$
4. $(AB)^T = B^T A^T$

dk1: ověření stejného typu

$A \in R^{m \times n} \Rightarrow A^T \in R^{n \times m} \Rightarrow (A^T)^T \in R^{m \times n}$

porovnání prvků

$((A^T)^T)_{ij} = (A^T)_{ji} = A_{ij}$ $\square$

Def: Symetrická matice

$A \in R^{n \times n}$ je symetrická $\Leftrightarrow A = A^T$ např. I_n, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix}$

Tvrzení: sym matice jsou uzavřené na součet

nejsou uzavřené na součin

výskyt: matice vzdáleností, kovariační matice, Hessián

Součiny vektorů

$x^T y = \sum_{i=1}^{n} x_i y_i$ skalární součin

$x y^T = \begin{pmatrix} x_1 y_1 & \cdots & x_1 y_n \\ \vdots & & \vdots \\ x_n y_1 & \cdots & x_n y_n \end{pmatrix} = \begin{pmatrix} - x_1 y^T - \\ \vdots \\ - x_n y^T - \end{pmatrix} = \begin{pmatrix} | & & | \\ x y_1 & \cdots & x y_n \\ | & & | \end{pmatrix}$ vnější součin

Tvrz. Matice $A \in R^{m \times n}$ má hodnost 1 $\Leftrightarrow$ $A = x y^T$ pro nějaké nenulové vektory x, y

$e_i^T e_j = 0$ $e_i e_j^T = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & a_{ij} = 1 & \\ 0 & & 0 \end{pmatrix}$

Tvrz.
$A \in R^{m \times n}$ pak platí

1. $Ae_j = A_{*j}$
2. ~~$Ae_i^T = A_{i*}$~~ $e_i^T A = A_{i*}$

Tvrz.

$A \in R^{m \times n}$ $B \in R^{n \times p}$

1. $(AB)_{*j} = AB_{*j}$
2. $(AB)_{i*} = A_{i*}B$

dk 1:

$(AB)_{*j} = (AB)e_j = A(Be_j) = AB_{*j}$ $\square$

Součin matice a vektoru

Tvrz: $A \in R^{m \times n}$ $x \in R^n$ $y \in R^m$

1. $Ax = \sum_{j=1}^{n} x_j A_{*j}$
2. $y^T A = \sum_{i=1}^{m} y_i A_{i*}$

1. $$\begin{pmatrix} A_{*1} & A_{*2} & \cdots & A_{*n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ y_n \end{pmatrix} = \begin{pmatrix} | \\ A_{*1} \\ | \end{pmatrix} x_1 + \begin{pmatrix} | \\ A_{*2} \\ | \end{pmatrix} y_2 \cdots x_n \begin{pmatrix} | \\ A_{*n} \\ | \end{pmatrix}$$

Matice a lineární zobrazení

$A \in \mathbb{R}^{m \times n}$ → zobrazení z $\mathbb{R}^n$ do $\mathbb{R}^m$ definované $x \mapsto Ax$

př:

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \longmapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -x_1 \\ x_2 \end{pmatrix} \quad \text{překlopení}$$

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \longmapsto \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1\cos\alpha - x_2\sin\alpha \\ x_1\sin\alpha + x_2\cos\alpha \end{pmatrix} \quad \text{otočení o } \alpha$$

$$\ldots \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \ldots \begin{pmatrix} x_1 \\ 0 \end{pmatrix} \quad \text{projekce}$$

→ řešit soustavu lin rovnic $Ax = b$ znamená najít všechny vektory x, které se zobrazí na vektor b.

→ složené zobrazení BA … násobení matic

Regulární matice

$A \in \mathbb{R}^{n \times n}$, A je regulární, pokud $Ax = 0$ má jediné řešení $x = 0$

jinak je singulární

Tvrz: $A \in \mathbb{R}^{n \times n}$ následující jsou ekvivalentní

1. A je regulární
2. $RREF(A) = I_n$
3. $rank(A) = n$
4. $\forall b \in \mathbb{R}^n$ má soustava $Ax = b$ jediné řešení

Tvrz: $A, B \in \mathbb{R}^{n \times n}$ jsou regulární $\Rightarrow$ AB je regulární

Dk: Buď x řešení soustavy $ABx = 0$, ukážeme, že x je nulový vektor

$y = Bx$ … $Ay = 0$

$y = 0$ z regularity matice A $\quad$ $x = 0$ z regularity matice B

Tvrz: Pokud je aspoň 1 z $A, B \in \mathbb{R}^{n \times n}$ singulární, AB je také singulární

Dk: 2 případy $\quad$ 1. B je singulární … $Bx = 0$ pro nějaké $x \neq 0$

$(AB)x = A(Bx) = A0 = 0$ tedy AB je singulární (x nenulové řeší soustavu $ABx = 0$)

2. B je regulární $\Rightarrow$ A je singulární $\exists y \neq 0 : Ay = 0 \Rightarrow$

$\overset{\text{z reg } B}{\Rightarrow} \exists x \neq 0 : Bx = y \Rightarrow (AB)x = A(Bx) = Ay = 0$ tedy AB je singulární

Matice elementárních úprav
– násobení zleva "elementární úpravou"

přičtení α násobku i k j

$$E_{ij} = \begin{array}{c c} & \\ i & \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \\ 0 & \alpha & 1 \end{pmatrix} \\ & \quad j \end{array}$$

Věta: $A \in R^{m \times n}$, $\exists Q \in R^{m \times m}_{(\text{regulární})}$: $RREF(A) = QA$

Dk: RREF je konečně mnoho elementárních kroků

$RREF(A) = E_k \dots E_2 E_1 A = QA$ kde $Q = \underbrace{E_k \dots E_1}_{\text{regulární}} \Rightarrow Q$ regulární

Tvrz: $\forall A \in R^{n \times n}_{\text{regulární}}$ lze vyjádřit jako součin konečně mnoha el. matic

Dk: A dokážu upravit do $I_n \Rightarrow I_n$ mohu upravit na A, protože každá el. úprava má inverzi

Inverzní matice

Def $B B^{-1} = I_n = B^{-1} B$

Věta (o existenci inverzní matice)

Buď $A \in R^{n \times n}$ A je regulární $\Rightarrow \exists A^{-1}$ určená jednoznačně

$\exists A^{-1} \Rightarrow A$ je regulární

Dk: existence

A je regulární $\Rightarrow Ax = e_j$ má řešení x_j $\forall j$

ukážeme $A^{-1} = (x_1 | x_2 | \dots | x_n)$ je hledaná inverze

1. $AA^{-1} = I$ po sloupcích ... $\forall j$ $(AA^{-1})_{*j} = A(A^{-1})_{*j} = Ax_j = e_j = I_{*j}$

2. trik $A(A^{-1}A - I) = AA^{-1}A - A = IA - A = 0$

tedy $\forall j$ platí $A(A^{-1}A - I)_{*j} = 0$ z regularity A $(A^{-1}A - I)_{*j} = 0 \Rightarrow A^{-1}A = I$ □

Dk: jednoznačnost

nechť platí $AB = BA = I$

$B = BI = B(AA^{-1}) = (BA)A^{-1} = IA^{-1} = A^{-1}$

Dk: 2. implikace

Nechť pro A existuje inverzní matice, buď x řešení $Ax = 0$, pak

$x = Ix = (AA^{-1})x = A^{-1}(Ax) = A^{-1}0 = 0$ tedy A je regulární

LA1 P03 S03

Vlastnosti regulárních matic

Tvrz A je reg $\Rightarrow A^T$ je reg

Dk $AA^{-1} = A^{-1}A = I_n$

$(AA^{-1})^T = (A^{-1}A)^T = I_n^T$

$(A^{-1})^T A^T = A^T (A^{-1})^T = I_n$ $\Rightarrow$ matice A^T má inverzi $\Rightarrow$ je regulární

důsledek:

$(A^T)^{-1} = (A^{-1})^T$ ~~značka~~ A^{-T}

Věta jedna rovnost stačí

$A, B \in \mathbb{R}^{n \times n}$ $BA = I_n \Rightarrow$ obě matice jsou regulární a vzájemně inverzní … $B = A^{-1}$ $A = B^{-1}$

Dk: Regularita plyne z věty o ch. inverzní matice tedy existují A^{-1}, B^{-1}

$B = BI_n = B(AA^{-1}) = (BA)A^{-1} = IA^{-1} = A^{-1}$

pro A symetricky □

Výpočet inverzní matice

Věta $A \in \mathbb{R}^{n \times n}$

- $RREF(A|I_n) = (I_n|B) \Rightarrow B = A^{-1}$
- jinak je A singulární

$$(A|I_3) = \left(\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & 2 & -1 & 0 & 1 & 0 \\ 3 & 5 & 7 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -9{,}5 & -4 & 3{,}5 \\ 0 & 1 & 0 & 1{,}5 & 1 & -0{,}5 \\ 0 & 0 & 1 & 3 & 1 & -1 \end{array}\right) = (I_3|A^{-1})$$

Dk: ~~Platí~~ $RREF(A|I_n) = (I_n|B) \Rightarrow \exists$ Q-regulární : $(I_n|B) = Q(A|I_n)$

$I_n = QA$ a $B = QI_n$

$\Downarrow$ $\Downarrow$

$Q = A^{-1}$ $B = Q = A^{-1}$

Když to nefunguje tak RREF nedá I_n

$\Downarrow$

A je singulární □

Vlastnosti inverzní matice

1. $(A^{-1})^{-1} = A$
2. $(A^{-1})^T = (A^T)^{-1}$
3. $(\alpha A)^{-1} = \frac{1}{\alpha} A^{-1}$ pro $\alpha \neq 0$ Dk: plyne z $(\alpha A)(\frac{1}{\alpha}A^{-1}) = \frac{\alpha}{\alpha} AA^{-1} = I_n$
4. $(AB)^{-1} = B^{-1}A^{-1}$ Dk: $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$

vzoreček pro $(A+B)^{-1}$ není

Inverzní matice a SLR

Q regulární $\Rightarrow Ax = b$ je ekvivalentní s $(QA)x = (Qb)$

Dk: žádné řešení neztratíme protože zpět můžeme jít násobením Q^{-1} zleva □

důsledek pro A regulární: $Ax = b$ je ekviv. s $(A^{-1}A)x = (A^{-1}b)$

Věta: soustava rovnic a inverzní matice

$A \in R^{n \times n}$ regulární $\Rightarrow$ řešení $Ax = b$ je dáno $x = A^{-1}b$

Geometrie

$A \in R^{n \times n}$ regulární, zobrazení $x \mapsto Ax$

- $\forall y \in R^n \ \exists! x \in R^n : Ax = y$
- zobrazení je bijekce
- inverzní má předpis $y \mapsto A^{-1}y$

$Ax = b$ řešení znamená hledat vzor b při zobrazení $x \mapsto Ax$

inverzní složené zobrazení $z \mapsto (BA)^{-1}z$

$z \mapsto (A^{-1}B^{-1})z$

Grupy

def: Grupa je dvojice $(G, \circ)$, kde G je množina a $\circ: G^2 \to G$ je binární operací na množině splňující

1. $\forall a, b, c \in G \quad a \circ (b \circ c) = (a \circ b) \circ c$ asociativita
2. $\exists e \in G \, \forall a \in G: e \circ a = a \circ e = a$ neutrální prvek
3. $\forall a \in G \, \exists b \in G: a \circ b = b \circ a = e$ inverzní prvek

abelova grupa

4. $\forall a, b \in G: a \circ b = b \circ a$ komutativita

když je $\circ$ sčítání, neutrální prvek je 0, inverzní $-a$
$\circ$ násobení 1 a^{-1}

- pří:

1. $(\mathbb{Z}, +)$ $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$ $(\mathbb{C}, +)$
2. $(\mathbb{Q} \setminus \{0\}, \cdot)$ $(\mathbb{R} \setminus \{0\}, \cdot)$
3. grupa matic
4. konečná grupa: $(\mathbb{Z}_n, +)$ kde $\mathbb{Z}_n \in \{0 \dots n-1\}$, sčítání se provádí mod n
5. grupa polynomů $(\{p(x): p$ je polynom$\}, +)$

ne nutně Abelova

1. množina všech zobrazení s operací ~~sčítání~~ skládání
2. množina všech regulárních matic řádu n s násobením

negrupy

$(\mathbb{N}, +)$ $(\mathbb{Z}, \cdot)$

LA 1 P09 S02

Vlastnosti grup $(G, \circ)$

1. $a \circ c = b \circ c \Rightarrow b = a$ krácení
2. neutrální prvek je určený jednoznačně
3. $\forall a \in G$ má právě 1 inverzní prvek
4. rovnice $a \circ x = b$ má právě 1 řešení $\forall a, b \in G$
5. $(a^{-1})^{-1} = a$
6. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Dk 1. $a \circ c = b \circ c \Rightarrow a \circ (c \circ c^{-1}) = b \circ (c \circ c^{-1}) \Rightarrow a \circ e = b \circ e \Rightarrow a = b$

nechť máme $e_1\ e_2$

2. $e_1 = e_1 \circ e_2 = e_2 \Rightarrow e_1 = e_2$
3. nechť inverzní prvky a_1, a_2 k $a \Rightarrow a_1 a = e = a_2 a \overset{\text{krácení}}{\Rightarrow} a_1 = a_2$
4. $a \circ x = b$ vynásobíme zleva $a^{-1} \Rightarrow x = a^{-1} \circ b$ - to je jednoznačné
5. hodit e na obě strany
6. ukaž $(a \circ b) \circ (b^{-1} \circ a^{-1}) = e$

Podgrupa

def podgrupa $(G; \circ)$ je $(H; \diamond)$ t.ž. $H \subseteq G$ a $\forall a, b \in H$ $a \diamond b = a \circ b$

značení $(H; \diamond) \leq (G, \circ)$

př: triviální podgrupy $(G, \circ) \leq (G; \circ)$; $(\{e\}, \circ)$

Permutace

- bijekce ... prosté a na
- permutace na X je bijekce $p: X \to X$
- S_n = množina všech permutací

zápisy: tabulka ... nahoře vzory, dole obrazy $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$

graf

rozložení na cykly $(1, 2)(3)(4, 5)$ .. obrazem je následník

$(1, 2)(4, 5)$

identita: id

transpozice: jediný cyklus délky 2, prohození i, j

(i, j)

Operace s permutacemi

1. inverzní permutace p^{-1}

$p^{-1}(i) = j$ pokud $p(j) = i$

2. skládání $p, q \in S_n$ není komutativní

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

$p \circ id = p = id \circ p$ $p \circ p^{-1} = id = p^{-1} \circ p$

Znaménko permutace

$p \in S_n$ se skládá z k cyklů

$sgn(p) = (-1)^{n-k}$

$sgn(id) = 1$ $sgn((i,j)) = -1$

Věta o znaménku složení permutace s transpozicí

$p \in S_n, t = (i,j) \in S_n$ $sgn(p) = -sgn(t \circ p) = -sgn(p \circ t)$

Dk: 1. i, j jsou ve stejném cyklu

velký cyklus se rozloží na 2 $\Rightarrow k += 1$

2. i, j jsou ve stejném cyklu

2 cykly se spojí v 1 $\Rightarrow k -= 1$

přesměrujeme šipky do i a j

Věta: Každou permutaci lze rozložit na složení transpozic.

Dk: Postupně na transpozice rozložíme všechny cykly

rozložení cyklu $(u_1 \dots u_n) = (u_1, u_2) \circ (u_2, u_3) \circ \dots \circ (u_{n-1}, u_n)$ $\square$

důsledek:

$sgn(p) = (-1)^r$, kde $r = \#(i,j)$ v rozkladu p

důsledek 2

$\forall p, q \in S_n$ platí $sgn(p \circ q) = sgn(p) \cdot sgn(q)$

důsledek 3

$\forall p \in S_n$ platí $sgn(p) = sgn(p^{-1})$

Symetrická grupa $(S_n, \circ)$

množina permutací, skládání

- Každá grupa je isomorfní nějaké podgrupě symetrické grupy S_{48} - rubikova kostka

Tělesa

- zobecnění číselných oborů

Def: Těleso je množina T spolu se dvěma binárními komutativními operacemi $+$ a $\circ$

1. $(T, +)$ je abelova grupa (neut. prvek 0, inverzní k a $-a$)
2. $(T \setminus \{0\}; \circ)$ je abelova grupa (1, a^{-1})
3. $\forall a, b, c \in T$: $a \cdot (b+c) = a \cdot b + a \cdot c$ (distributivita

Každé těleso má aspoň 2 prvky, $0 \neq 1$

inverzní operace $-$ a $/$ $a - b = a + (-b)$

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

podtěleso

příklady: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

$\{0; 1\}$ sčítání násobení mod 2

((kvaternion)) - nekomutativní tělesa

Základní vlastnosti těles

1. $0a = 0$
2. $ab = 0 \Rightarrow a = 0 \vee b = 0$
3. $-a = (-1)a$

Konečná tělesa

- $\mathbb{Z}_n = \{0, \dots n-1\}$ + a · mod n
- $\mathbb{Z}_2$, $\mathbb{Z}_3$ $\qquad$ $\mathbb{Z}_4$ ne protože neex 2^{-1}

Lemma
pro prvočíslo n a nenulové $a \in \mathbb{Z}_n$ při násobení mod n
platí $\{0, 1 \dots n-1\} = \{0a, 1a \dots (n-1)a\}$ (žádný prvek se neztratí)

Dk: sporem $ka \equiv la \pmod n$ pro $\boxed{\text{nerovné}}$ $k, l \in \mathbb{Z}_n$
pak $(k-l)a \equiv 0$, protože n je prvočíslo n dělí $k-l$
protože $n > a$, $k-l$ tak $\underline{a \neq 0}$ nebo $k-l \underline{= 0}$ ↯

Věta
$\mathbb{Z}_n$ tvoří těleso $\Leftrightarrow$ n je prvočíslo

Dk: $\Rightarrow$ sporem $n = pq$ pro $1 < \underline{p, q} < n$
je-li $\mathbb{Z}_n$ těleso $pq \equiv 0 \pmod n \Rightarrow p \equiv 0 \vee q \equiv 0 \pmod n$ ↯

$\Leftarrow$ ověříme axiomy tělesa, existence inverze a^{-1} plyne z lemmatu
(na dlouho, triviální) $\qquad$ (mezi násobky a musí být 1) □

- předchozí výsledky (Gaussova eliminace) platí nad libovolným tělesem
$\mathbb{T}^{m \times n}$ matice nad tělesem $\mathbb{T}$

Věta o velikosti konečných těles
Konečná tělesa existují o velikostech právě p^n kde p je prvočíslo a $n \geq 1$

$GF(p^n)$ .. polynomy stupně nejvýš $n-1$ s koeficienty $\in \mathbb{Z}_p$
sčítání jako pro reálné polynomy
násobení — " " — mod ireducibilní polynom stupně n

- Galois field - každé konečné těleso je isomorfní

Charakteristika tělesa
def: $\underline{\text{nejmenší}}$ n takové, že $\overbrace{1+1 \dots +1}^{n} = 0$
pokud neex. tak 0 $\qquad$ př: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ mají char 0 $\qquad$ $\mathbb{Z}_p$ .. p

Tvrz: Charakteristika každého tělesa je 0 nebo prvočíslo

Dk: 1. $0 \neq 1$ $\Rightarrow$ char nemůže být 1
sporem: $n = p \cdot q$ $\qquad$ $0 = \underbrace{1+1 \dots +1}_{n = pq} \overset{\text{dist axiom}}{=} \underbrace{(1+1 \dots +1)}_{p} \underbrace{(1+1 \dots +1)}_{q}$
podle $ab = 0 \Rightarrow a = 0 \vee b = 0$, $\underline{p \text{ or } q = 0}$ ↯

Malá Fermatova věta
pro každé prvočíslo p a nenulové $a \in \mathbb{Z}_p$ platí $a^{p-1} \equiv 1 \pmod p$
$= 1$ v tělese $\mathbb{Z}_p$

Dk: z prvočíselnosti $\{0, 1, 2 \ldots p-1\} = \{0a, 1a \ldots (p-1)a\}$
protože $0a = 0$ $\{1 \ldots p-1\} = \{1a \ldots (p-1)a\}$
$1 \cdot 2 \cdot \ldots (p-1) = (1a) \cdot (2a) \ldots ((p-1)a)$
vykrátíme $1 \ldots p-1$
$1 = a \cdot a \ldots a = a^{p-1}$ □

Samoopravné kódy
- zdvojení bitů - detekce 1 chyby ; ztrojení - oprava 1 chyby
- Hammingův kód $(7,4,3)$ ... generující matice, detekční matice

Vektorové prostory
- zobecnění $\mathbb{R}^n$
def: Buď $\mathbb{T}$ těleso s neutr. prvky $0, 1$ pro sčít. a násob.
Vektorový prostor nad $\mathbb{T}$ je množina V s operacemi sčítání vektorů
$+ : V^2 \to V$ a násobení vektoru skalárem $\cdot : \mathbb{T} \times V \to V$: $\forall \alpha, \beta \in \mathbb{T}$ a $\forall u, v \in V$: splňující
1. $(V, +)$ je abelova grupa
2. $(\alpha\beta)v = \alpha(\beta v)$ asociativita
3. $1v = v$
4. $(\alpha + \beta)u = \alpha u + \beta u$ distributivita
5. $\alpha(u + v) = \alpha u + \alpha v$ — " —

prvky V .. vektory
T .. skaláry

př: $\mathbb{T}^n$, prostor matic $T^{m \times n}$, P - polynomy proměnné x, P^n stupně $\leq n$
F všechny reálné funkce, C spojité funkce, $C_{a,b}$ v intervalu

Tvrzení - základní vlastnosti
Dk: analogicky k tělesu
1 $0v = o$
2 $\alpha o = o$
3 $\alpha v = o \Rightarrow \alpha = 0 \vee v = o$
4 $-v = (-1)v$

Vektorový podprostor $U \subseteq V$ je podprostorem pokud tvoří VP nad T se stejnými operacemi. zn. $U \Subset V$. Ekviv: U musí mít o a být uzavřené na obě operace
1. $o \in U$ 2. $\forall u, v \in U : u + v \in U$
3. $\forall \alpha \in T \; \forall u \in U : \alpha u \in U$

př: triv $V \Subset V$, $\{o\} \Subset V$
přímka procházející počátkem $\Subset \mathbb{R}^2$
$P^n \Subset P \Subset C \Subset F$
symetrické mat. řádu n $\Subset \mathbb{R}^{n \times n}$
$\mathbb{Q}^n$ nad $\mathbb{Q} \Subset \mathbb{R}^n$ nad $\mathbb{Q}$ $\not\Subset \mathbb{R}^n$ nad $\mathbb{R}$

Dk: $\Rightarrow$ pokud $U \Subset V$, tak tyto tři vlastnosti splňuje
$\Leftarrow$ Když máme tyto tři vlastnosti tak ostatní plynou z $U \subseteq V$
uzavřenost U na opačné vektory plyne z uzavřenosti na násobky
a z $(-1)u = -u$

Lineární obal

Tvrz: Nechť V je VP nad T. Pak $\bigcap$ libovolného systému $(V_i)_{i\in I}$ VPP prostoru V je VPP V.

Dk: Podle alt. def VPP ověříme $\sigma \in \bigcap_{i\in I} V_i$ a uzavřenost na sčítání vektorů a násobení sk.

$\forall i$ • V_i je podprostor $\Rightarrow V_i \ni \sigma$

• pro $u,v \in \bigcap_{i\in I} V_i \Rightarrow u,v \in V_i\ \forall i\in I \Rightarrow u+v \in V_i\ \forall i\in I \Rightarrow u+v \in \bigcap_{i\in I} V_i$

• násobek skalárem analogicky □

Def: Pro VP V nad T a $W \subseteq$ je lineárním obalem množiny W $\bigcap_{U: W\subseteq U \Subset V} U$

průnik všech podprostorů které obsahují W

Značíme $span(W)$

Def Generátory: Nechť $U = span(W)$ pro nějaké $W \subseteq V$. Pak W generuje prostor U, prvky množiny W jsou generátory prostoru U.

- U je konečně generovaný pokud je W konečná

Def: Buď V VP nad T a $v_1, \dots, v_n \in V$, pak lineární kombinace $v_1 \dots v_n$ je výraz $\sum_{i=1}^{n} \alpha_i v_i$, kde $\alpha_i \in T$

Věta: Nechť V je VP n T a $v_1 \dots v_n \in V$. Pak $span(v_1 \dots v_n) = \overbrace{\left\{\sum_{i=1}^{n} \alpha_i v_i : \alpha_i \in T\right\}}^{M}$

Dk: Inkluze $\supseteq$: Lin obal je PP V obsahující $v_1 \dots v_n \Rightarrow$ je uzavřený na součty a nás. sk. $\Rightarrow$ obsahuje všechny lin. komb $\sum_{i=1}^{n} \alpha_i v_i$

Inkluze $\subseteq$: Ukážeme, že M je PP V obsahujícím $v_1 \dots v_n$; M je jeden z PP jejichž průnikem vznikl $span\{v_1 \dots v_n\}$

• $\sigma \in M$? ano zvolíme $\alpha_i = 0\ \forall i$

• $v_1 \dots v_n \in M$? ano zvolíme $\alpha_i = 1$ pro v_i a ostatní $\alpha = 0$

• Uzavřenost na součty: u je lin komb $= \sum_{i=1}^{n} \beta_i v_i$ a v taky $= \sum_{i=0}^{n} \gamma_i v_i \Rightarrow u+v \overset{distr}{=} \sum_{i=1}^{n} (\beta_i + \gamma_i) v_i \in M$

násobky $\alpha \in T$ a $u = \sum_{i=1}^{n} \beta_i v_i \overset{distr}{\Rightarrow} \alpha u = \sum_{i=1}^{n} (\alpha \beta_i) v_i \in M$ □

Def: Nechť V je VP n T a $v_1 \dots v_n \in V$, pak $v_1 \dots v_n$ jsou lineárně nezávislé pokud $\sum_{i=1}^{n} \alpha_i v_i = \sigma$ nastane pouze pro $\alpha_i = 0\ \forall i$

V opačném případě jsou lineárně závislé

- pro nekonečnou množinu M: M je lineárně nezávislá pokud každá konečná podmn. M je lineárně nezávislá.

Souvislost s maticemi: sloupce i řádky reg matice jsou lineárně nezávislé

Věta: Nechť V je VP n T a $v_1 \dots v_n \in V$, pak $v_1 \dots v_n$ jsou lin závislé $\iff \exists k \in \{1 \dots n\}$ a $\alpha_1 \dots \alpha_n \in T$ t.ž. $v_k = \sum_{i \neq k} \alpha_i v_i$ neboli $v_k \in span\{v_1 \dots v_{k-1}, v_{k+1} \dots v_n\}$

Dk: $\Rightarrow$: $\sum_{i=1}^{n} \beta_i v_i = \sigma$, nějaké $\beta_k \neq 0 \Rightarrow \beta_k v_k + \sum_{i\neq k} \beta_i v_i = \sigma \Rightarrow v_k = -\sum_{i \neq k} \beta_i \beta_k^{-1} v_i$

$\Leftarrow$: $v_k = \sum_{i \neq k} \beta_i v_i \Rightarrow \underbrace{v_k - \sum_{i \neq k} \beta_i v_i}_{\text{to je lin. kombinace a } \beta_k = 1} = \sigma$ □

Důsledek: ... $v_1 \dots v_n$ jsou lin závislé $\Leftrightarrow$ ~~span~~ $\exists k \in \{1 \dots n\}$:

$\mathrm{span}\{v_1 \dots v_n\} = \{v_1 \dots v_{k-1}, v_{k+1} \dots v_n\}$

neboli $v_1 \dots v_n$ jsou LZ, když je mezi nimi nadbytečný pro generování

Dk $\Rightarrow$: $\supseteq$: minimální - přidali jsme generátor

$\subseteq$: libovolný $w = \beta_k v_k + \sum_{i \neq k} \beta_i v_i \Rightarrow w = \beta_k \left(\sum_{i \neq k} \alpha_i v_i\right) + \sum_{i \neq k} \beta_i v_i \Rightarrow w = \sum_{i \neq k}^{n} (\beta_k \alpha_i + \beta_i) v_i$ $\in \mathrm{span}\{v_1 \dots v_{k-1}, v_{k+1} \dots v_n\}$

$\Leftarrow$ z věty $v_k \in \{v_1 \dots v_{k-1}, v_{k+1}, \dots, v_n\} = \{v_1 \dots v_n\}$

□

Def: nechť V je VP nad T, báze je jakýkoliv lin nezávislý systém generátorů prostoru V.

... systém generátorů V minimální co do inkluze

uspořádaná množina

Kanonická báze T^n kan $= \{e_1 \dots e_n\}$, kde e_i má 1 na pozici i, jinde 0

P^n má bázi $1, x, x^2 \dots x^n$

Věta: nechť $B = \{v_1 \dots v_n\}$ je bází VP V, pak $\forall w \in V \; \exists \alpha_1 \dots \alpha_n \in T$ jednoznačně: $w = \sum_{i=1}^{n} \alpha_i v_i$

Dk: existence: z definice báze $\exists \alpha_1 \dots \alpha_n$ t.ž. $\sum_{i=1}^{n} \alpha_i v_i$

jednoznačnost: sporem $\alpha_1 \dots \alpha_n$, $\beta_1 \dots \beta_n$, pro nějaké k je $\alpha_k \neq \beta_k \Rightarrow$

$\Rightarrow w - w = 0 \Rightarrow \sum_{i=1}^{n} \alpha_i v_i - \sum_{i=1}^{n} \beta_i v_i = 0 \Rightarrow \sum_{i=1}^{n} (\alpha_i - \beta_i) v_i = 0$, jelikož pro $\alpha_k - \beta_k \neq 0$ spor s lin. nezávislostí □

Koeficienty $\alpha_1 \dots \alpha_n$ nazýváme souřadnicemi $[w]_B$

Tvrz: $[u+v]_B = [u]_B + [v]_B$ a $[\alpha v]_B = \alpha [v]_B$

Věta o existenci báze: Každý VP má bázi

Dk pro konečně generované VP:

nechť $v_1 \dots v_n$ je systém generátorů VP

pokud jsou $v_1 \dots v_n$ lin nezávislé $\Rightarrow$ tvoří bázi

jinak podle důsledku vyhazujeme v_k takové: $\mathrm{span}\{v_1 \dots v_n\} = \mathrm{span}\{v_1 \dots v_{k-1}, v_{k+1} \dots v_n\}$

dokud nezbyde báze

někdy však skončíme protože $v_1 \dots v_n$ je konečný

□

Lemma o výměně

Nechť $y_1 \dots y_n$ je systém generátorů VP V a $\forall x \in V$ má vyjádření $x = \sum_{i=1}^{n} \alpha_i y_i$, pak pro libovolné k t.ž. $\alpha_k \neq 0$ je $y_1 \dots y_{k-1}, x, y_{k+1} \dots y_n$ systémem generátorů V.

Dk: $x = \sum_{i=1}^{n} \alpha_i y_i \Rightarrow x - \sum_{i \neq k} \alpha_i y_i = \alpha_k y_k \overset{\alpha_k \neq 0}{\Rightarrow} y_k = \frac{1}{\alpha_k}\left(x - \sum_{i \neq k} \alpha_i y_i\right)$

z je libovolný vektor $z = \sum_{i=1}^{n} \beta_i y_i \Rightarrow \beta_k y_k + \sum_{i \neq k} \beta_i y_i \Rightarrow \frac{\beta_k}{\alpha_k}\left(x - \sum_{i \neq k} \alpha_i y_i\right) + \sum_{i \neq k} \beta_i y_i$ □

Steinitzova věta o výměně

Nechť $x_1 \dots x_m$ je lineárně nezávislý systém ve VP V, nechť $y_1 \dots y_n$ jsou generátory ~~..~~ V.

1. $m \leq n$
2. existují vzájemně různé indexy $k_1 \dots k_{n-m}$ t.ž. $x_1 \dots x_m, y_{k_1} \dots y_{k_{n-m}}$ jsou generátory V

Dk: indukcí podle m

m = 0 .. triviální

m − 1 ⇒ m

podle IP jsou $x_1 \dots x_{m-1}$ lin nezávislé a $m-1 \leq n$ a existují navzájem různé indexy $l_1 \dots l_{n-m+1}$ t.ž. $x_1 \dots x_{m-1}, y_{l_1} \dots y_{l_{n-m+1}}$ generují V.

Kdyby $m-1 = n$ tak $x_1 \dots x_{m-1}$ generují $V \Rightarrow x_m \in span\{x_1 \dots x_{m-1}\}$ ↯ lineární nezávislost

takže $m-1 < n \Rightarrow m \leq n$, takže 1. část dokázaná

x_m lze vyjádřit jako $x_m = \sum_{i=1}^{m-1} \alpha_i x_i + \sum_{j=1}^{n-m+1} \beta_j y_{l_j}$ $\exists \beta_k \neq 0$ aby nebyl spor s lin nezáv.

podle lemma o výměně můžeme vyměnit x_m za ~~y~~ l_k a $x_1 \dots x_m, y_{l_1} \dots y_{k-1}, y_{k+1} \dots y_{n-m+1}$ pak generují V □

Důsledek: Všechny báze konečně generovaného prostoru V jsou stejně velké

Dk: 2 báze $x_1 \dots x_m$; $y_1 \dots y_n$

$x_1 \dots x_m$ je nezávislý systém ⇒ podle S věty $m \leq n$

$y_1 \dots y_n$ je . . . . . . ⇒ . . . . . . $n \leq m$

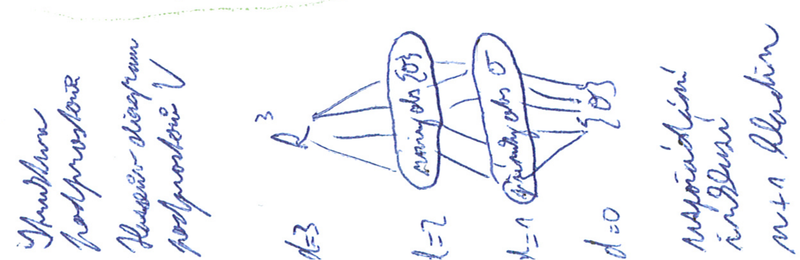
$\} n = m$ □

víme že báze existují a jsou stejně velké

Def: Dimenze konečně generovaného prostoru je velikost nějaké ~~jeho~~ báze.

když ~~je~~ není KG ⇒ ∞   zn: dim V

$\dim R^{m \times n} = mn$



LA P07 S02

Tvrz: pro VP V platí: 1. jsou-li $x_1 \dots x_m \in V$ lin nezáv., pak $m \leq \dim V$. Pokud $m = \dim V$, pak je $x_1 \dots x_m$ báze V

2. Jsou-li $y_1 \dots y_n$ generátory V, pak $n \geq \dim V$. Pokud $n = \dim V$ pak $y_1 \dots y_n$ je bází V

Dk: $d = \dim V$, $z_1 \dots z_d$ je báze V

1. $x_1 \dots x_m$ jsou lin nezávislé a $z_1 \dots z_d$ jsou generátory $\overset{\text{3 věta}}{\Rightarrow} m \leq d$; při $m = d$ lze $x_1 \dots x_m$ doplnit $d - m = 0$ vektory na systém generátorů $V \Rightarrow x_1 \dots x_m$ tvoří bázi

2. $z_1 \dots z_d$ jsou nezávislé a $y_1 \dots y_n$ jsou generátory $\overset{\text{3 věta}}{\Rightarrow} d \leq n$; pokud $n = d$ pak jsou $y_1 \dots y_n$ lin nezávislé a tvoří tedy bázi

Věta: Každý lin nez systém VP V lze doplnit na bázi V.

Dk: máme $x_1 \dots x_m \in V$ nezávislé a bázi $z_1 \dots z_d$, $d = \dim V$
podle 3 věty můžeme k $x_1 \dots x_m$ přidat $z_{k_1} \dots z_{k_{d-m}}$, taktéž máme d generátorů $V \Rightarrow$ tvoří bázi podle Tvrz 2.

Dimenze podprostorů: Věta: Je-li $W \Subset V \Rightarrow \dim W \leq \dim V$ a po $\dim W = \dim V \Rightarrow W = V$

Dk: Definujeme $M = \emptyset$, pokud $\operatorname{span}(M) = W$ jsme hotovi. Jinak $\exists v \in W \setminus \operatorname{span}(M)$. Přidáme v do M a opakujeme. M je lin nez $\overset{\text{tvrzení}}{\Rightarrow} |M| \leq \dim V$, po konečně mnoha krocích $W = \operatorname{span}(M)$ a M bude báze W přičemž $\dim W = |M| \leq \dim V$. pokud $\dim W = \dim V \Rightarrow M$ je báze V podle tvrzení

Spojení podprostorů U a V VP W := $\{u + v : u \in U, v \in V\}$

Tvrz: Pro podprostory U a V VP W platí $U + V = \operatorname{span}\{U \cup V\}$

Dk: $\subseteq$: triviální z uzavřenosti na součty prostoru $\operatorname{span}\{U \cup V\}$ $u + v \in U + V$, $w \in V + V$

$\supseteq$: Víme $U + V \supseteq U \cup V$ a $U + V \Subset W$, první část plyne z $o \in U, V$

$U + V \Subset W$ ověříme uzavřenost na součty a násobky

Mějme $x_1, x_2 \in U + V$ a skalár $\lambda \Rightarrow x_1 = u_1 + v_1$ $x_2 = u_2 + v_2$ $u_1 u_2 \in U$ $v_1 v_2 \in V$

součty: $x_1 + x_2 = u_1 + v_1 + u_2 + v_2 = (u_1 + u_2) + (v_1 + v_2) \in U + V$

násobky: $\lambda x_1 = \lambda u_1 + \lambda v_1 \in U + V$

Dimenze spojení: Věta: Pro podprostory U, V VP W platí: $\dim(U + V) + \dim(U \cap V) = \dim U + \dim V$

Dk: Z uzavřenosti podprostorů na průniky $\Rightarrow U \cap V \Subset W$ a má bázi $z_1 \dots z_d \Rightarrow$ z věty o rozšíření na bázi rozšíříme na $z_1 \dots z_d\, x_1 \dots x_m$ podprostoru U a $z_1 \dots z_d\, y_1 \dots y_n$ podprostoru V

Ukážeme, že $z_1 \dots z_d\, y_1 \dots y_n\, x_1 \dots x_m$ je báze $U + V$ (ukážeme, že jsou to generátory a pak lin. nezáv.)

Generujícnost: máme-li $x \in U + V$ pak $x = u + v$ pro $u \in U$ $v \in V$

vyjádříme $u = \sum_{i=1}^{d} \alpha_i z_i + \sum_{j=1}^{m} \beta_j x_j$ a $v = \sum_{i=1}^{d} \gamma_i z_i + \sum_{k=1}^{n} \delta_k y_k$

pak $x = u + v = \sum_{i=1}^{d} (\alpha_i + \gamma_i) z_i + \sum_{j=1}^{m} \beta_j x_j + \sum_{k=1}^{n} \delta_k y_k$

je lin komb $z_1 \dots z_d\, x_1 \dots x_m\, y_1 \dots y_n$

Lineární nezávislost: chceme ukázat, že všechny koeficienty $\alpha, \beta, \gamma = 0$ když $o = \sum \alpha z + \sum \beta x + \sum \gamma y$

označíme $z = \sum \alpha_i z_i + \sum \beta_j x_j = -\sum \gamma_k y_k \Rightarrow z \in U \cap V$ lze zapsat $z = \sum_{i}^{d} \delta_i z_i \Rightarrow \sum_{i}^{d} \delta_i z_i + \sum_{k}^{n} \gamma_k y_k = o$

$z_1 \dots z_d, y_1 \dots y_n$ jsou lin nezávislé $\Rightarrow \delta_1 = \dots = \delta_d = \gamma_1 = \dots = \gamma_n = 0$ po dosazení $\sum_{i}^{d} \alpha_i z_i + \sum_{j}^{m} \beta_j x_j = o$

$z_1 \dots z_d, x_1 \dots x_m$ — " — $\Rightarrow \alpha_1 = \alpha_d = \dots = \beta_1 = \dots = \beta_m = 0$ □

Pokud $U \cap V = \{o\}$ pak $U + V$ nazveme direktním součtem podprostorů a značíme $U \oplus V$

Podle věty platí $\dim(U \oplus V) = \dim U + \dim V$

Každé $w \in W$ lze zapsat jako jediným způsobem $w = u + v$ $u \in U$ $v \in V$

př: $\mathbb{R}^2 = \operatorname{span}\{e_1\} \oplus \operatorname{span}\{e_2\}$

Maticové prostory

pro matici $\mathbb{T}^{m \times n}$ zavedeme prostory:

- sloupcový p. $S(A) = \text{span}\{A_{*1}, A_{*2} \dots A_{*n}\}$
- řádkový p. $R(A) = \text{span}\{A_{1*}, A_{2*}, A_{m*}\} = S(A^T)$
- jádro $\text{Ker}(A) = \{x \in \mathbb{T}^n : Ax = 0\}$

z definice je $S(A) \subseteq \mathbb{T}^m$ a $R(A) \subseteq \mathbb{T}^n$

ukážeme, že $\text{Ker}(A) \subseteq \mathbb{T}^n$:

- $0 \in \text{Ker}(A)$, protože $A0 = 0$

uzavřenost na součty: pro $x, y \in \text{Ker}(A)$ platí $Ax = Ay = 0 \Rightarrow A(x+y) = Ax + Ay = 0 + 0 = 0$

— // — násobky: pro $x \in \text{Ker}(A)$ platí $Ax = 0 \Rightarrow \forall \alpha \in \mathbb{T}\ A(\alpha x) = \alpha(Ax) = \alpha 0 = 0$

Tvrzení: pro $A \in \mathbb{T}^{m \times n}$ platí

$S(A) = \{Ax : x \in \mathbb{T}^n\}$ $\qquad$ $R(A) = \{A^T y : y \in \mathbb{T}^m\}$

množina všech x vynásobených A

Dk: z $Ax = \sum_{j=1}^{n} x_j A_{*j}$ ... to je lin. komb. sloupců A, což jsme chtěli

a $A^T y = \sum_{i=1}^{m} y_i A_{i*}$ ... to je lin. kombinace řádků — // — $\square$

Tvrzení: Pro $V \subseteq \mathbb{T}^n$ $\exists A \in \mathbb{T}^{m \times n}$ a $B, C \in \mathbb{T}^{m \times n}$ t. ž.

1. $V = S(A)$ $\qquad$ 2. $V = R(B)$ $\qquad$ 3. $V = \text{Ker}(C)$

Dk 17 generátory $v_1 \dots v_m$ tvoří sloupce A a řádky B $\square$

Pozn: Buď f zobrazení $\mathbb{T}^n \to \mathbb{T}^m$ $\quad f(x) = Ax$

pak $\text{Ker}(A)$ je z definice tvořeno všemi $x : f(x) = 0$

$S(A)$ pak tvoří množinu všech obrazů přes f neboli $f(\mathbb{T}^n)$

Tvrzení: Pro matice $A \in \mathbb{T}^{m \times n}$ a $Q \in \mathbb{T}^{p \times m}$ platí

1) $R(QA) \subseteq R(A)$ $\qquad$ 2) platí-li $A_{*k} = \sum_{j \neq k} \alpha_j A_{*j}$ pro nějaké k a nějaká $\alpha_j \in \mathbb{T} \Rightarrow (QA)_{*k} = \sum_{j \neq k} \alpha_j (QA)_{*j}$

Dk: 1) víme $R(QA) \subseteq \mathbb{T}^n$, ukážeme $R(QA) \subseteq R(A)$; $\forall x \in R(QA)\ \exists y \in \mathbb{T}^p$ t. ž. $x = (QA)^T y =$
$= A^T Q^T y = A^T (Q^T y) \in R(A)$

2) $(QA)_{*k} = QA_{*k} = Q\left(\sum_{j \neq k} \alpha_j A_{*j}\right) = \sum_{j \neq k} \alpha_j QA_{*j} = \sum_{j \neq k} \alpha_j (QA)_{*j}$ $\square$

pro sloupce 1 nemá smysl, 2 funguje taky

náhled ... zobrazování sloupců

Tvrzení 2: Pro matici $A \in T^{m \times n}$ a reg. matici $Q \in T^{m \times m}$

① $R(QA) = R(A)$

② $A_{*k} = \sum_{j \neq k} \alpha_j A_{*j}$ pro nějaká $k \in N^{\{1, \dots, n\}}$ a $\alpha_j \in T \iff (QA)_{*k} = \sum_{k \neq j} \alpha_j (QA)_{*j}$

Dk: ① $R(QA) \subseteq R(A)$ z Tvrzení 1, aplikujeme Tvr 1 ještě jednou na QA vynásobenou Q^{-1} zleva

$R(A) = R(Q^{-1}QA) \subseteq R(QA)$

② $\Rightarrow$ zleva vyplývá z Tvr 1

$\Leftarrow$: použijeme Tvr 1 na QA vynásobenou Q^{-1} zleva $(Q^{-1}QA)_{*k} = \sum_{j \neq k} \alpha_j (Q^{-1}QA)_{*j}$ □

Věta 1: Pro matici $A \in T^{m \times n}$ a její RREF tvar A^R s pivoty na pozicích $(1, p_1) \dots (r, p_r)$, kde $r = \operatorname{rank}(A)$ platí:

1. nenulové řádky A^R $(A^R_{1*} \dots A^R_{r*})$ tvoří bázi $R(A)$
2. sloupce $A_{*p_1} \dots A_{*p_r}$ tvoří bázi $S(A)$
3. $\dim(S(A)) = \dim(R(A)) = r$

Dk: Víme, že $\exists Q$ t. ž. $QA = RREF(A) = A^R$ (Q je reg $\in T^{m \times m}$)

① podle tvrzení 2 $R(A) = R(QA) = R(A^R)$; nenulové řádky A^R jsou lin. nezávislé a tvoří tak bázi $R(A^R) \Rightarrow$ tedy i $R(A)$

② Sloupce $A^R_{*p_1} \dots A^R_{*p_r}$ jsou lin. nezávislé a generují $S(A^R)$

$A^R_{*j} = \sum_{i=1}^{m} a^R_{ij} e_i = \sum_{i=1}^{r} a^R_{ij} e_i = \sum_{i=1}^{r} a^R_{ij} A^R_{*p_i}$ $\Rightarrow$ každý sloupec dokážu zapsat jako LK $\Rightarrow$

$\Rightarrow$ generuje $S(A) \Rightarrow$ jsou lin. nezávislé tedy jsou ~~generátory~~ báze $S(A^R) \Rightarrow$

$\Rightarrow$ z tvrzení 2 jsou báze $S(A)$

③ $\dim R(A) = r$ podle 1

$\dim S(A) = r$ podle 2 ∵ je tam báze velikosti r □

Důsledek: Pro každou matici $A \in T^{m \times n}$ platí $\operatorname{rank}(A) = \operatorname{rank}(A^T)$

$\operatorname{rank}(A) = \dim(R(A)) = \dim S(A) = \dim S(A^T) = \dim R(A^T) = \operatorname{rank}(A^T)$

Vztah k SLR: Soustava $Ax = b$ je řešitelná $\iff$ b je LK sloupců mat A – – – $b \in S(A)$, což nastane $\iff S(A) = S(A|b)$

Což nám dává Frobeniovu větu: Soustava $(A|b)$ má aspoň 1 řešení $\iff \operatorname{rank}(A) = \operatorname{rank}(A|b)$

Věta 2: $\forall A \in T^{m \times n}$ platí $\dim Ker(A) + rank(A) = n$

Dk: Pro $k = \dim Ker(A)$ uvažíme bázi $v_1 \dots v_k$ jádra $Ker(A)$

Podle věty o rozšíření na bázi získáme $v_1 \dots v_k \dots v_n$ bázi prostoru T^n

Chceme dokázat, že $Av_{k+1} \dots Av_n$ je bází $S(A)$, protože podle ~~Věty~~ věty 1 je $rank(A) = \dim(S(A)) = n - k$

Generujícnost: $\forall y \in S(A)\ \exists x \in T^n : y = Ax$; takové x můžeme zapsat: $x = \sum_{i=1}^{n} \alpha_i v_i$

dosadíme $y = A\left(\sum_{i=1}^{n} \alpha_i v_i\right) = \sum_{i=1}^{n} \alpha_i A v_i = \sum_{i=k+1}^{n} \alpha_i (A v_i)$ takže jsem vyjádřil lib. vektor pomocí $v_{k+1} \dots v_n$, takže je to systém generátorů ~~báze~~

z def. Ker jsou $Av_1 \dots v_k = 0$

Lin nezávislost: Chceme $\sum_{i=k+1}^{n} \alpha_i (A v_i) = 0 \Rightarrow A\left(\sum_{i=k+1}^{n} \alpha_i v_i\right) = 0 \in Ker(A)$ takže jej lze vyjádřit jako LK jádra $\Rightarrow$
$\alpha_i = 0$

$\Rightarrow \sum_{i=k+1}^{n} \alpha_i v_i = \sum_{i=1}^{k} \beta_i v_i \Rightarrow \sum_{i=1}^{k} (-\beta_i) v_i + \sum_{i=k+1}^{n} \alpha_i v_i = 0$ ... to je vyjádření v bázi $v_1 \dots v_k \dots v_n$, která je lin nezávislá $\Rightarrow$

$\Rightarrow \beta_i = 0 = \alpha_i$ □

Geometrie V2: máme $f: T^n \to T^m$ dané $f(x) = Ax$ ... pak f zobrazuje n-dimenzionální prostor T^n na r-dimenzionální ~~prostor~~ $S(A)$, kde $r = rank(A)$

$n - r \geq 0$ je $\dim Ker A$, takže čím větší jádro, tím menší obraz

Ker určuje míru "degenerace" zobrazení, máme i popis protože v Ker máme právě ty vektory, které se zobrazí na počátek

Aplikace: Samoopravné kódy

Detekce obličejů

Lagrangeův interpolační polynom