Lineární algebra a geometrie 1, 2

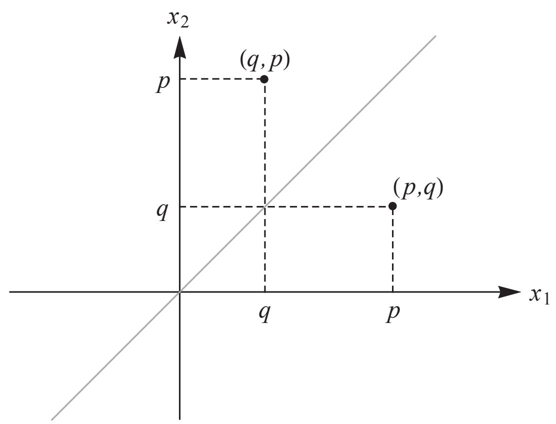
Jiří Tůma

2014/15

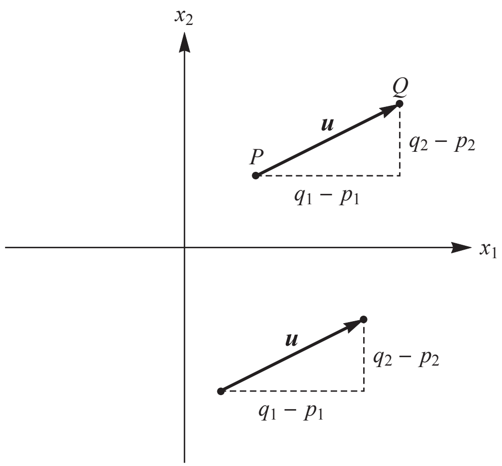
http://www.karlin.mff.cuni.cz/~sir/la/ZS14-15.html

tuma@karlin.mff.cuni.cz

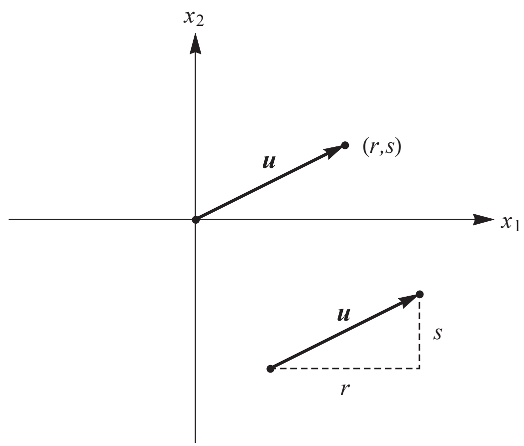
Souřadnice bodu v rovině



Souřadnice vektoru v rovině

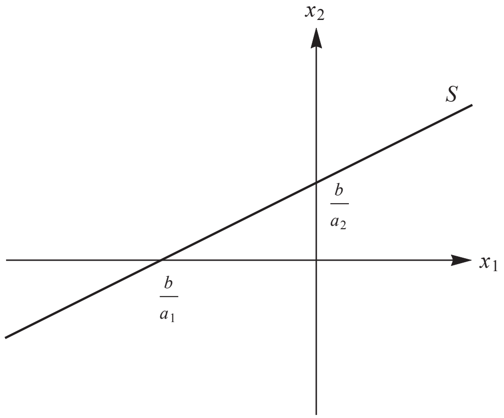


Polohový vektor bodu



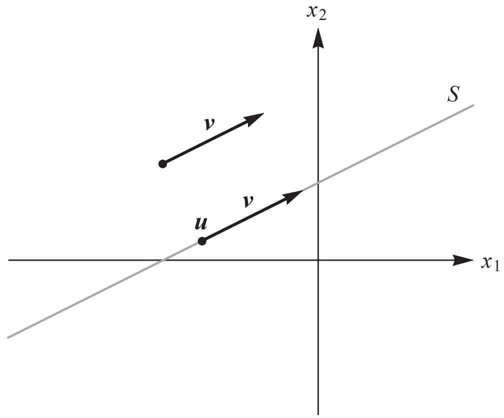
Rovnice přímky v rovině

$$a_1x_1 + a_2x_2 = b \qquad S = \{(x_1, x_2) \in \mathbb{R}^2 : a_1x_1 + a_2x_2 = b\}$$



Parametrické vyjádření přímky v rovině

$$\{\mathbf{u} + t\mathbf{v} : t \in \mathbb{R}\}$$



Příklad

najdeme rovnici a parametrické vyjádření přímky, která prochází body $P = (-1, 3)$ a $Q = (1, 1)$ v rovině

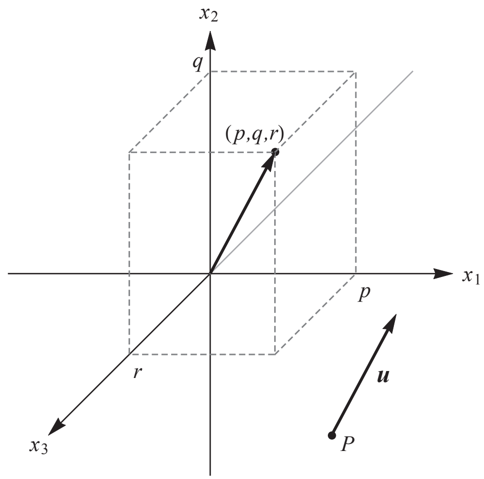
Otázky

- jaké rovnice popisují stejnou přímku jako rovnice $x_1 + x_2 = 2$?
- jaké jsou rovnice přímek rovnoběžných s přímkou $x_1 + x_2 = 2$?
- jaké jsou rovnice přímek různoběžných s přímkou $x_1 + x_2 = 2$?

Další otázka

jak může vypadat řešení libovolné soustavy lineárních rovnic o dvou neznámých ?

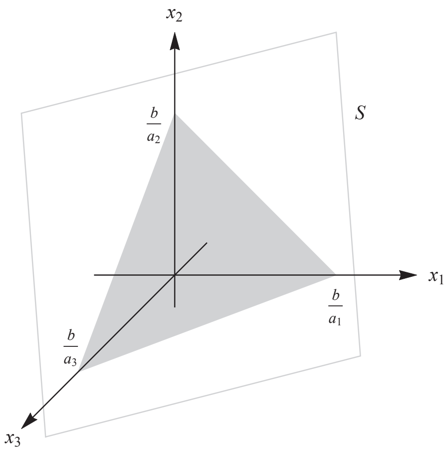
Souřadnice bodu a vektoru v prostoru



Rovnice roviny v prostoru

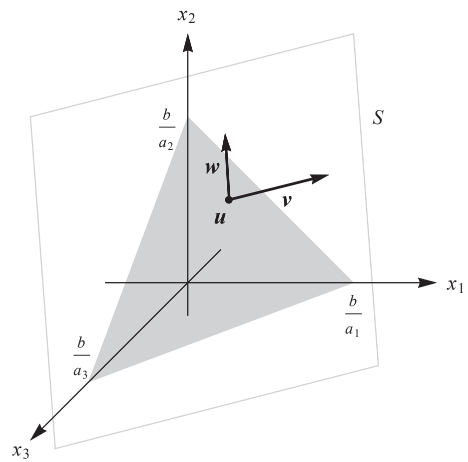
$a_1x_1 + a_2x_2 + a_3x_3 = b$

$S = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : a_1x_1 + a_2x_2 + a_3x_3 = b\}$



Parametrické vyjádření roviny v prostoru

$S = \{\mathbf{u} + s\mathbf{v} + t\mathbf{w} : s, t \in \mathbb{R}\}$



Příklad

najdeme parametrické vyjádření roviny procházející body
$P = (1, 2, 3)$, $Q = (-1, 0, 1)$ a $R = (3, 3, 5)$

Otázky

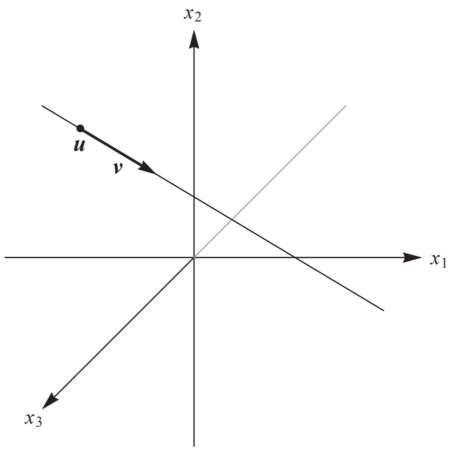
Dvě roviny jsou určené rovnicemi

$$a_1x_1 + a_2x_2 + a_3x_3 = b$$
$$c_1x_1 + c_2x_2 + c_3x_3 = d$$

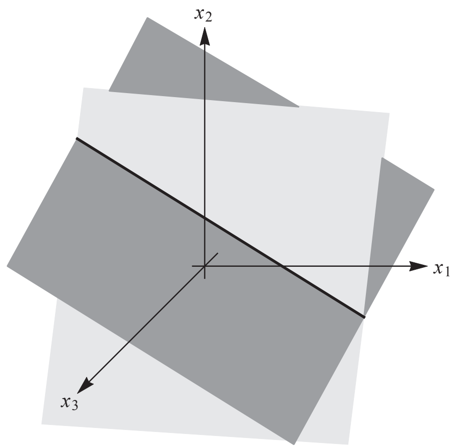
- kdy jsou obě roviny stejné ?
- kdy jsou rovnoběžné ?
- kdy jsou různoběžné ?

Parametrické vyjádření přímky v prostoru

$$\{\mathbf{u} + t\mathbf{v} : t \in \mathbb{R}\}$$



Soustava rovnic pro přímku v prostoru



Otázka

jak může vypadat řešení libovolné soustavy lineárních rovnic o třech neznámých ?

Počítání s komplexními čísly

měli byste umět počítat s komplexními čísly v algebraickém tvaru

$$a + ib$$

včetně počítání s čísly komplexně sdruženými

kdo to neumí nebo si není jistý, tak se to doučí, třeba ze skript

kdo to umí, tak si své pochopení ověří řešením příkladů ze skript

Základní věta algebry

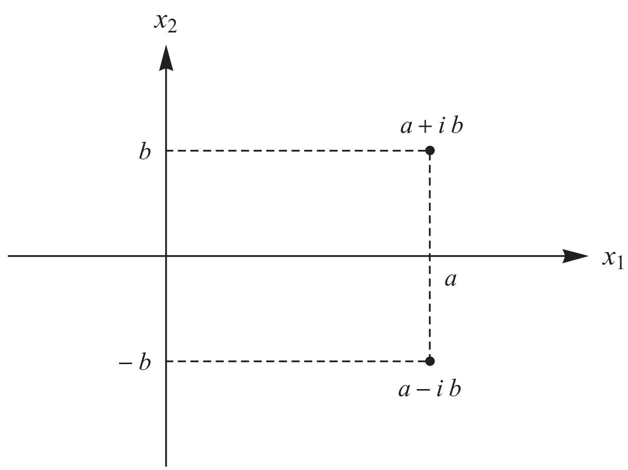
rozšiřování číselných oborů kvůli řešitelnosti rovnic

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

základní věta algebry: každý nekonstantní polynom s komplexními koeficienty má aspoň jeden komplexní kořen

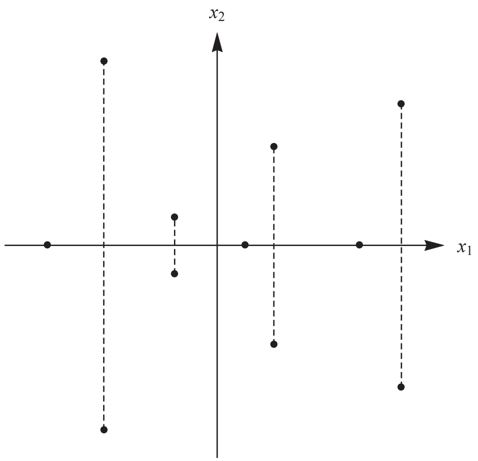
- věta říká, že kořen existuje, neříká jak jej najít
- vzorečky existují pouze pro polynomy stupňů $1, 2, 3, 4$
- pro polynomy stupně $3, 4$ jsou nepraktické
- pro polynomy stupně ≥ 5 žádné vzorečky neexistují

Komplexní rovina

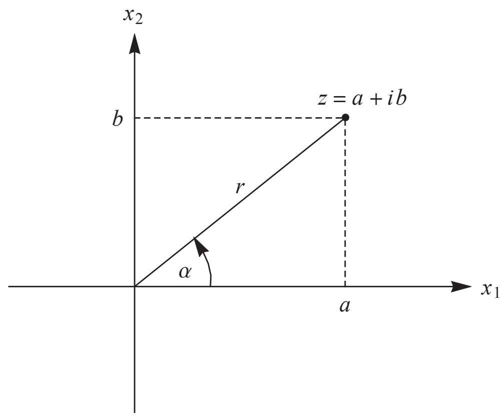


Kořeny polynomů s reálnými koeficienty

věta: je-li $p(x)$ polynom s reálnými koeficienty a z kořen polynomu p, pak také $\overline{z}$ je kořen p



Polární souřadnice



Goniometrický tvar komplexního čísla

měli byste umět počítat s komplexními čísly v goniometrickém tvaru

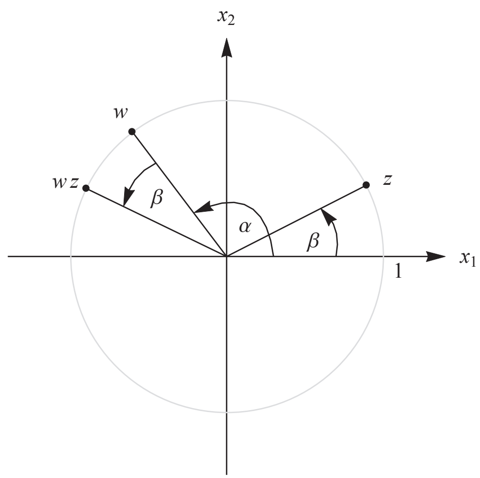
$$r(\cos\alpha + i\sin\alpha)$$

včetně počítání s absolutní hodnotou a argumentem

kdo to neumí nebo si není jistý, tak se to doučí, třeba ze skript

kdo to umí, tak si své pochopení ověří řešením příkladů ze skript

Součin komplexních jednotek



Moivreova věta: $(\cos\alpha + i\sin\alpha)^n = \cos(n\alpha) + i\sin(n\alpha)$

Kapitola 2

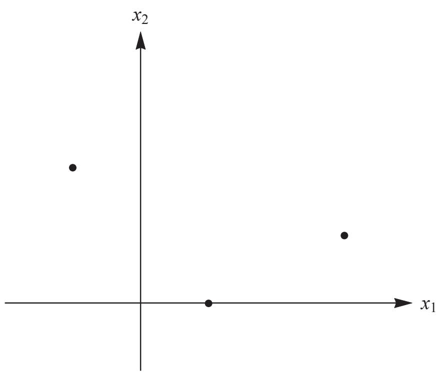
Řešení soustav lineárních rovnic

Příklady - obsah

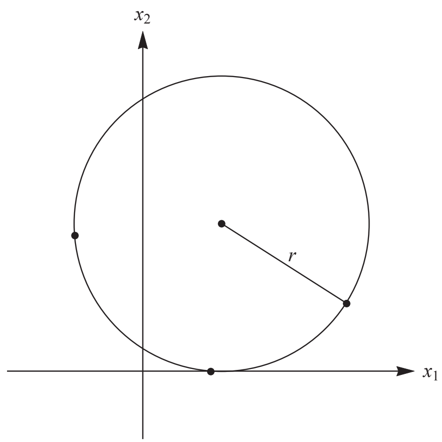
- *Příklady*
  Proložení kružnice danými body
  Vyčíslování chemické rovnice
  Pohyb hlavy disku

Proložení kružnice danými body

najděte střed a poloměr kružnice procházející body $(1, 0)$, $(-1, 2)$, $(3, 1)$



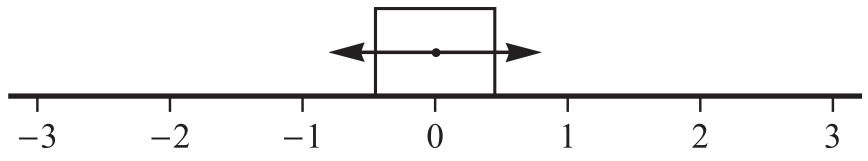
Řešení



Vyčíslování chemické rovnice

$$C_7H_8 + HNO_3 \longrightarrow C_7H_5O_6N_3 + H_2O$$

Pohyb hlavy disku



po dobu 8 vteřin na objekt působí vnější síly $f(t)$

vnější síla je konstantní vždy během jedné vteřiny

Soustavy lineárních rovnic - obsah

Soustavy lineárních rovnic

definice: *lineární rovnice o n neznámých* s reálnými koeficienty je rovnice

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

soustava m lineárních rovnic o n neznámých je soustava

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

a_{ij} je *koeficient* v i-té rovnici u j-té neznámé

každé řešení je nějaká uspořádaná n-tice $(x_1, x_2, \ldots, x_n)$ čísel

Aritmetické vektory

definice: *aritmetickým vektor nad $\mathbb{R}$ s n složkami* rozumíme uspořádanou n-tici reálných čísel $(x_1, x_2, \ldots, x_n)$

množinu všech aritmetických vektorů s n složkami budeme označovat $\mathbb{R}^n$

aritmetické vektory budeme psát sloupcově:

$$\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}$$

kvůli šetření místem také řádkově:

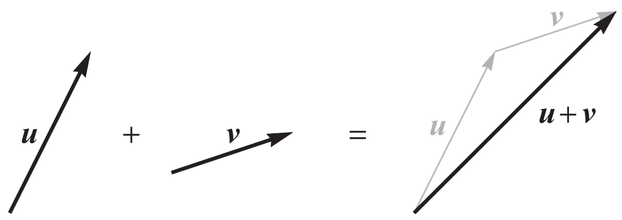
$$(1, 2, 3, 4)^T$$

Součet aritmetických vektorů

definice: jsou-li $\mathbf{u} = (u_1, u_2 \ldots, u_n)^T$ a $\mathbf{v} = (v_1, v_2, \ldots, v_n)^T$ dva n-složkové aritmetické vektory nad $\mathbb{R}$, pak jejich součtem rozumíme aritmetický vektor

$$\mathbf{u} + \mathbf{v} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} + \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 + v_1 \\ u_2 + v_2 \\ \vdots \\ u_n + v_n \end{pmatrix}$$

Geometrický význam součtu aritmetických vektorů



Součin čísla s aritmetickým vektorem

definice: je-li $\mathbf{u} = (u_1, \ldots, u_n)^T$ aritmetický vektor nad $\mathbb{R}$ a $t \in \mathbb{R}$ reálné číslo, pak t-násobkem vektoru $\mathbf{u}$ rozumíme vektor

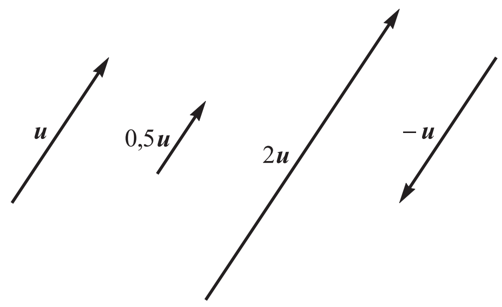
$$t \cdot \mathbf{u} = t\mathbf{u} = t \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} tu_1 \\ tu_2 \\ \vdots \\ tu_n \end{pmatrix}$$

pro dva n-složkové vektory $\mathbf{u}, \mathbf{v}$ definujeme

$$-\mathbf{u} = (-1) \cdot \mathbf{u} \quad \text{a} \quad \mathbf{u} - \mathbf{v} = \mathbf{u} + (-\mathbf{v})$$

vektor $-\mathbf{u}$ nazýváme *opačný vektor* k vektoru $\mathbf{u}$.

Geometrický význam součinu čísla s vektorem



Příklad

spočítáme

$$3 \cdot \begin{pmatrix} 1 \\ 3 \\ 5 \\ 7 \end{pmatrix} - 2 \begin{pmatrix} 5 \\ 2 \\ -2 \\ 5 \end{pmatrix} =$$

Eliminace neznámých

vyřešíme soustavu

$$\begin{aligned} x_1 + x_2 &= 1 \\ 3x_1 + 7x_2 &= 7 \end{aligned}$$

Elementární úpravy

(i) prohození dvou rovnic

(ii) vynásobení nějaké rovnice **nenulovým** číslem t

(iii) přičtení t-násobku jedné rovnice k **jiné** rovnici

Proč elementární úpravy

tvrzení: elementární úpravy nemění množinu všech řešení soustavy lineárních rovnic

důkaz: sestává ze tří jednoduchých kroků

- každá elementární úprava mění nejvýše jednu rovnici
- každé řešení původní soustavy je řešením změněné rovnice
- elementární úpravy jsou vratné

Příklad

vyřešíme soustavu

$$\begin{aligned} 2x_1 + 6x_2 + 5x_3 &= 0 \\ 3x_1 + 5x_2 + 18x_3 &= 33 \\ 2x_1 + 4x_2 + 10x_3 &= 16 \end{aligned}$$

pomocí elementárních úprav se snažíme dosáhnout toho, aby v každé rovnici bylo na začátku více nulových koeficientů než v rovnici předcházející

Matice

definice: *matice* (nad $\mathbb{R}$) typu $m \times n$ je obdélníkové schéma reálných čísel s m řádky a n sloupci

zápis $A = (a_{ij})_{m\times n}$ znamená, že A je matice typu $m \times n$, která má na pozici (i, j) (tedy v i-tém řádku a j-tém sloupci) číslo a_{ij}

pozor na pořadí indexů – první index označuje řádek, druhý sloupec

Matice soustavy

definice: *matice soustavy*

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\
&\dots \\
a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m
\end{aligned}
$$

je matice koeficientů u neznámých:

$$
A = (a_{ij})_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}
$$

Rozšířená matice soustavy

vektor pravých stran je vektor

$$
\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}
$$

a *rozšířená matice soustavy* je matice typu $m \times (n+1)$

$$
(A \,|\, \mathbf{b}) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array}\right)
$$

Eliminace neznámých pomocí matic

$$
\begin{aligned}
2x_1 + 6x_2 + 5x_3 &= 0 \\
3x_1 + 5x_2 + 18x_3 &= 33 \\
2x_1 + 4x_2 + 10x_3 &= 16
\end{aligned}
$$

Jiný příklad

$$\left(\begin{array}{ccc|c} 1 & 4 & 3 & 11 \\ 1 & 4 & 5 & 15 \\ 2 & 8 & 3 & 16 \end{array}\right)$$

Parametrické vyjádření množiny všech řešení

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 5 - 4t \\ t \\ 2 \end{pmatrix} =$$

Více parametrů

vyřešíme soustavu

$$\left(\begin{array}{ccccc|c} 0 & 0 & 1 & 0 & 2 & -3 \\ 2 & 4 & -1 & 6 & 2 & 1 \\ 1 & 2 & -1 & 3 & 0 & 2 \end{array}\right)$$

pivoty

bázové proměnné

volné proměnné

Parametrické vyjádření množiny všech řešení

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} -1 - 2t_2 - 3t_4 - 2t_5 \\ t_2 \\ -3 - 2t_5 \\ t_4 \\ t_5 \end{pmatrix} =$$

Gaussova eliminace - obsah

- *Gaussova eliminace*
  - Elementární řádkové úpravy
  - Odstupňovaný tvar matice
  - Gaussova eliminace
  - Hodnost matice

Elementární řádkové úpravy

definice: *elementárními řádkovými úpravami* jakékoliv matice $A = (a_{ij})_{m \times n}$ rozumíme následující tři typy úprav:

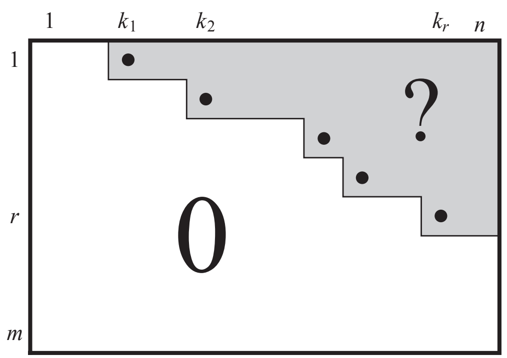
(i) prohození dvou řádků matice

(ii) vynásobení jednoho z řádků matice **nenulovým** číslem

(iii) přičtení libovolného násobku jednoho řádku k **jinému** řádku

Řádkově odstupňovaný tvar

neformálně: v každém nenulovém řádku matice je na počátku (tj. zleva) více nul, než na počátku řádku nad ním



Příklady

které matice jsou v odstupňovaném tvaru?

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 7 & 2 \\ 0 & 3 & 1 \\ 0 & 0 & 7 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 & 3 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 4 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 10 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

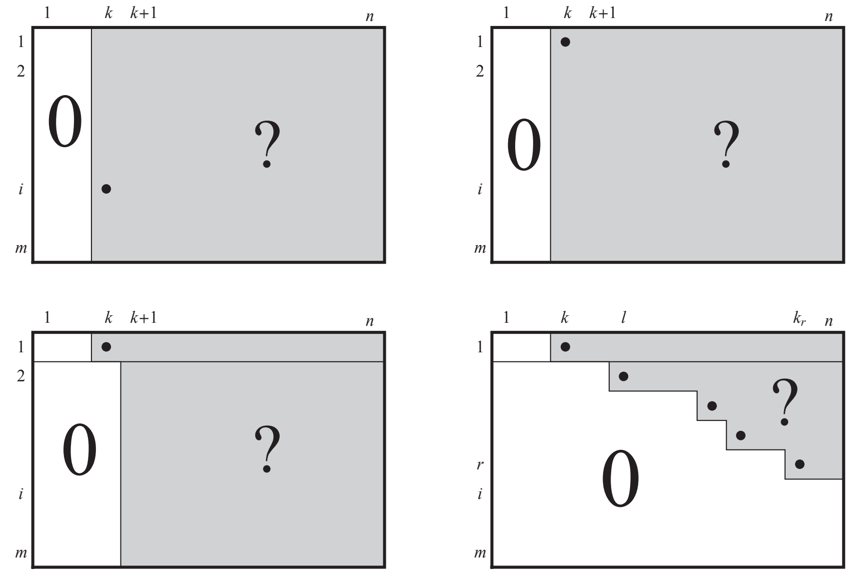
$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 7 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 7 \end{pmatrix} \quad \begin{pmatrix} 2 & 3 & 1 \\ 0 & 3 & 1 \\ 0 & 2 & 0 \end{pmatrix}$$

Gaussova eliminace

převádí každou matici $A = (a_{ij})_{m\times n}$ do odstupňovaného tvaru

1. najdeme první nenulový sloupec, jeho index označíme k_1; pokud takový sloupec neexistuje, je matice A v řádkově odstupňovaném tvaru (neboť je nulová), jsme tedy hotovi
2. pokud je $a_{1k_1} = 0$, prohodíme první řádek s libovolným řádkem i, ve kterém je $a_{ik_1} \neq 0$
3. pro každé $i = 2, 3, \ldots, m$ přičteme $(-a_{ik_1}/a_{1k_1})$-násobek prvního řádku k i-tému řádku
4. postup opakujeme s maticí bez prvního řádku

Gaussova eliminace dělá to, co má



Hodnost matice

věta: Gaussova eliminace převede každou matici $A = (a_{ij})$ typu $m \times n$ do odstupňovaného tvaru

počet r nenulových řádků a indexy $k_1, k_2, \ldots, k_r$ sloupců s pivoty v matici v odstupňovaném tvaru jsou maticí A určené jednoznačně

definice: číslo r, tj. počet nenulových řádků v matici C v odstupňovaném tvaru, kterou dostaneme z matice A Gaussovo eliminací, se nazývá *hodnost matice* A a značí se $r(A)$ nebo $rank(A)$

sloupce v matici A s indexy $k_1, k_2, \ldots, k_r$ z definice odstupňovaného tvaru nazýváme *bázové sloupce* matice A

Příklad

najdeme hodnost a bázové sloupce matice

$$A = \begin{pmatrix} 1 & -1 & 2 & 4 & 5 & 6 \\ 2 & 0 & 4 & 8 & 3 & 4 \\ 0 & 3 & 0 & 0 & 6 & 8 \end{pmatrix}$$

hodnost

bázové sloupce

Eliminační fáze řešení soustavy lineárních rovnic

máme vyřešit soustavu m lineárních rovnic o n neznámých $x_1, \ldots, x_n$ s rozšířenou maticí $(A \,|\, \mathbf{b})$

eliminační fáze řešení spočívá v Gaussově eliminaci matice $(A \,|\, \mathbf{b})$

dostaneme matici $(C \,|\, \mathbf{d})$ v odstupňovaném tvaru

je-li sloupec pravých stran $\mathbf{b}$ bázový, je poslední nenulový řádek

$$(0 \;\; 0 \;\; 0 \;\; \cdots \;\; 0 \,|\, d_r) \quad \text{a} \quad d_r \neq 0$$

soustava $(A \,|\, \mathbf{b})$ je neřešitelná

Volné a bázové proměnné

pokud sloupec pravých stran není bázový, ukážeme že je soustava řešitelná a najdeme všechna řešení

v tom případě pro indexy bázových sloupců platí

$$1 \leq k_1 < k_2 < \cdots < k_r \leq n$$

proměnné $x_{k_1}, x_{k_2}, \ldots, x_{k_r}$ nazýváme *bázové proměnné*

zbylé proměnné x_p pro $p \in P = \{1, 2, \ldots, n\} \setminus \{k_1, k_2, \ldots, k_r\}$ nazýváme *volné proměnné*

hodnoty volných proměnných zvolíme libovolně:

$x_p = t_p$ pro $p \in P$, jsou to parametry

Zpětná substituce

matici $(C \,|\, \mathbf{d})$ po Gaussově eliminaci odpovídá soustava

$$\begin{aligned}
c_{1,k_1}x_{k_1} + c_{1,k_1+1}x_{k_1+1} + c_{1,k_1+2}x_{k_1+2} + \cdots\cdots\cdots\cdots + c_{1,n}x_n &= d_1 \\
&\vdots \\
c_{r-1,k_{r-1}}x_{k_{r-1}} + c_{r-1,k_{r-1}+1}x_{k_{r-1}+1} + \cdots + c_{r-1,n}x_n &= d_{r-1} \\
c_{r,k_r}x_{k_r} + c_{r,k_r+1}x_{k_r+1} + \cdots + c_{r,n}x_n &= d_r
\end{aligned}$$

z ní jednoznačně dopočteme hodnoty bázových proměnných

Výsledek zpětné substituce

tvrzení: pokud sloupec pravých stran rovnice $(A \,|\, \mathbf{b})$ není bázový, pak pro libovolná reálná čísla $x_p \in \mathbb{R}$, $p \in P$, existují jednoznačně určená reálná čísla $x_{k_1}, x_{k_2}, \ldots, x_{k_r} \in \mathbb{R}$ taková, že aritmetický vektor $(x_1, x_2, \ldots, x_n)^T$ je řešením soustavy $(A \,|\, \mathbf{b})$

množinu všech řešení soustavy $(A \,|\, \mathbf{b})$ pak vyjádříme ve tvaru

$$S = \left\{ \mathbf{u} + \sum_{p \in P} t_p \mathbf{v}_p : \; t_p \in \mathbb{R} \;\; \text{pro každé} \;\; p \in P \right\} ,$$

kde $\mathbf{u}$ a $\mathbf{v}_p$ pro $p \in P$ jsou vhodné n-složkové aritmetické vektory

Shrnutí

obecnou soustavu m lineárních rovnic o n neznámých lze vyřešit následujícím postupem

1. Gaussovou eliminací převedeme soustavu na ekvivalentní soustavu v odstupňovaném tvaru
2. pokud existuje rovnice typu $0x_1 + 0x_2 + \cdots + 0x_n = b \neq 0$, skončíme s tím, že soustava je neřešitelná
3. určíme volné proměnné (parametry) x_p pro $p \in P$ a zpětnou substitucí vyjádříme bázové proměnné pomocí volných
4. množinu všech řešení vyjádříme tvaru

$$\left\{ \mathbf{u} + \sum_{p \in P} t_p \mathbf{v}_p : \ t_p \in \mathbb{R} \ \text{ pro každé } \ p \in P \right\}$$

pro vhodné n-složkové aritmetické vektory $\mathbf{u}$ a $\mathbf{v}_p$, $p \in P$

Otázky

- jak rozumět geometrii soustav lineárních rovnic?
- co se může přihodit, budeme-li soustavy lineárních rovnic řešit na počítači?
- jak dlouho to bude trvat?

Geometrie soustav lineárních rovnic - obsah

- *Geometrie soustav lineárních rovnic*
  Řádkový pohled
  Sloupcový pohled
  Lineární kombinace

Nadrovina

množinu všech řešení jedné netriviální rovnice o n neznámých

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

nazýváme *nadrovina* v n-dimenzionálním prostoru $\mathbb{R}^n$

množina všech řešení soustavy m lineárních rovnic o n neznámých se rovná jedné z následujících

- celý prostor $\mathbb{R}^n$
- nebo prázdná
- nebo průnik nadrovin

Sloupcový zápis soustavy

řešíme-li soustavu

$$\begin{aligned} -x_1 + 3x_2 &= 1 \\ 2x_1 - x_2 &= 3 \ , \end{aligned}$$

hledáme hodnoty proměnných x_1, x_2, pro které platí rovnost

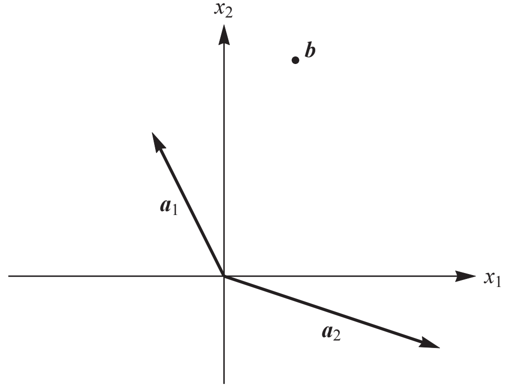
$$\begin{pmatrix} -x_1 + 3x_2 \\ 2x_1 - x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix} ,$$

kterou lze přepsat jako

$$x_1 \begin{pmatrix} -1 \\ 2 \end{pmatrix} + x_2 \begin{pmatrix} 3 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

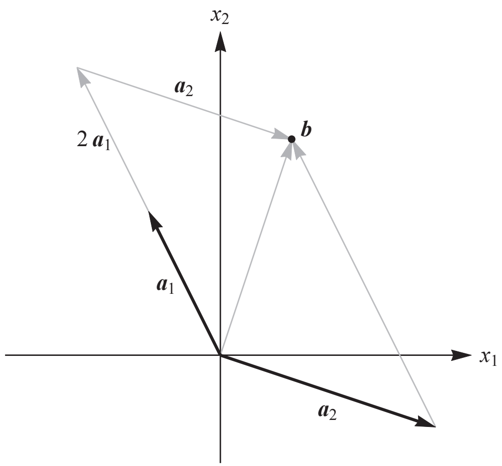
Geometrické znázornění soustavy

$$x_1 \begin{pmatrix} -1 \\ 2 \end{pmatrix} + x_2 \begin{pmatrix} 3 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$



Geometrické řešení soustavy

$$x_1 \begin{pmatrix} -1 \\ 2 \end{pmatrix} + x_2 \begin{pmatrix} 3 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$



Příklad tří rovnic se dvěmi neznámými

soustavu tří rovnic o dvou neznámých

$$\begin{aligned} x_1 + 3x_2 &= -5 \\ 2x_1 + 2x_2 &= -2 \\ 3x_1 + x_2 &= 1 \end{aligned}$$

si přepíšeme do tvaru

$$x_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + x_2 \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} -5 \\ -2 \\ 1 \end{pmatrix}$$

Velmi důležitá definice lineární kombinace

definice: jsou-li $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ m-složkové vektory a $a_1, a_2, \ldots, a_n$ reálná čísla, pak definujeme *lineární kombinaci* vektorů $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ s koeficienty $a_1, a_2, \ldots, a_n$ jako m-složkový vektor

$$a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_n\mathbf{u}_n$$

Podmínka řešitelnosti pomocí lineárních kombinací

je-li $A = (a_{ij})$ matice typu $m \times n$, zapíšeme ji po sloupcích

$$A = (\mathbf{a}_1 \,|\, \mathbf{a}_2 \,|\, \cdots \,|\, \mathbf{a}_n)$$

tvrzení: soustava lineárních rovnic $(A \,|\, \mathbf{b})$ je řešitelná právě když

Numerické záležitosti - obsah

- *Numerické záležitosti*
  Zaokrouhlování
  Podmíněnost
  Počet operací

Plovoucí desetinná čárka

„single precision“, 32-bitový procesor

s	e_7	•	•	•	•	•	e_1	e_0	i_{22}	i_{21}	•	•	•	•	•	•	•	•	•	i_1	i_0

znaménko: $(-1)^s$

exponent: $E = e_7 2^7 + \cdots + e_1 2^1 + e_0 2^0 = \sum_{k=0}^{7} e_k 2^k$

mantisa: $M = 1 + i_{22} 2^{-1} + i_{21} 2^{-2} \cdots + i_1 2^{-22} + i_0 2^{-23}$
$= 1 + \sum_{k=0}^{22} e_k 2^{k-23}$

reprezentovat lze pouze čísla $(-1)^s \cdot M \cdot 2^{E-127}$

těch je konečně mnoho, výsledky aritmetických operací je nutné zaokrouhlovat

Důsledek zaokrouhlování

zaokrouhlování koeficientů není ekvivalentní úprava

vezměme si soustavu s rozšířenou maticí $\left(\begin{array}{cc|c} -10^{-4} & 1 & 2 \\ 1 & 1 & 3 \end{array}\right)$

její přesné řešení je $\left(\dfrac{1}{1{,}0001}, \dfrac{2{,}0003}{1{,}0001}\right)^T$

při zaokrouhlování na tři platná místa Gaussova eliminace vede na

$$\left(\begin{array}{cc|c} -10^{-4} & 1 & 2 \\ 1 & 1 & 3 \end{array}\right) \sim \left(\begin{array}{cc|c} -10^{-4} & 1 & 2 \\ 0 & 10^4 & 2 \cdot 10^4 \end{array}\right)$$

zpětná substituce dá výsledek $(0, 2)^T$, který se od správného řešení liší významně v první složce

Poučení

počítač nám dá **přesné řešení, ale jiné soustavy**

otázka zásadní důležitosti: **jak se liší výsledek na počítači od přesného řešení původní soustavy ?**

to nejlepší, čeho lze dosáhnout, je přesné řešení **blízké soustavy**

pro některé soustavy není Gaussova eliminace ten nejvhodnější postup

Špatně podmíněné soustavy

soustava $\left(\begin{array}{cc|c} 0{,}835 & 0{,}667 & 0{,}168 \\ 0{,}333 & 0{,}266 & 0{,}067 \end{array}\right)$ má řešení $(1, -1)^T$

nepatrná změna druhé složky pravé strany na $0,066$ vede k

$\left(\begin{array}{cc|c} 0{,}835 & 0{,}667 & 0{,}168 \\ 0{,}333 & 0{,}266 & 0{,}066 \end{array}\right)$ s řešením $(-666, 834)^T$

v obou případech jde o přesné řešení, problém není v numerické stabilitě algoritmu

takovým soustavám se říká *špatně podmíněné*

problém je v tom, že obě přímky jsou téměř rovnoběžné

špatně podmíněné soustavy neřešit!

Jak dlouho to bude trvat ?

řešíme soustavu n lineárních rovnic o n neznámých

odhadujeme počet aritmetických operací $+/-/\cdot/:$

Gaussova eliminace vyžaduje nejvýše $\dfrac{2n^3}{3}$ operací

rozdělených zhruba na polovinu mezi $+/-$ a $\cdot/:$

zpětná substituce vyžaduje nejvýše n^2 operací (opět napůl)

pro velká n je časová náročnost zpětné substituce zanedbatelná

Kapitola 3

Tělesa

Babysoustava 1

$x + 2 = 3$

co potřebujeme:

(S1) pro každá čísla $a, b, c \in \mathbb{R}$ platí $(a + b) + c = a + (b + c)$

(S2) existuje číslo $0 \in \mathbb{R}$ takové, že pro každé číslo $a \in \mathbb{R}$ platí $a + 0 = 0 + a = a$

(S3) pro každé číslo $a \in \mathbb{R}$ existuje $-a \in \mathbb{R}$ takové, že $a + (-a) = (-a) + a = 0$

Binární operace

definice: *binární operace* na množině T je zobrazení z $T \times T$ do T

tradiční zápis $u \oplus v$ místo funkčního zápisu $\oplus((u, v))$

příklady operací splňujících podmínky (S1), (S2), (S3):

- běžné sčítání na množině všech celých čísel $\mathbb{Z}$
- běžné sčítání na množině $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$
- sčítání funkcí na množině všech reálných funkcí reálné proměnné

Babysoustava 2

$2 \cdot x = 6$

co potřebujeme:

(N1) pro každá čísla $a, b, c \in \mathbb{R}$ platí $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(N2) existuje číslo $1 \in \mathbb{R}$ takové, že pro každé číslo $a \in \mathbb{R}$ platí $a \cdot 1 = 1 \cdot a = a$

(N3) pro každé číslo $a \in \mathbb{R}$, $a \neq 0$, existuje $a^{-1} \in \mathbb{R}$ takové, že $a \cdot a^{-1} = a^{-1} \cdot a = 1$

Násobení versus sčítání

příklady operací splňujících (N1), (N2) a (N3)

- běžné násobení na množině všech racionálních čísel
- běžné násobení na množině všech reálných čísel
- běžné násobení na množině všech nenulových komplexních čísel

nepříklad

- běžné násobení na množině všech celých čísel $\mathbb{Z}$

porovnání podmínek (S1)-(S3) a (N1)-(N3)

Babysoustava 3

$$\begin{aligned} x + 3y &= 10 \\ (-2)x + 4y &= 15 \end{aligned}$$

přičteme dvojnásobek první rovnice k druhé

Další podmínky

potřebovali jsme ještě

(S4) pro každá čísla $a, b \in \mathbb{R}$ platí $a + b = b + a$

(D) pro každá čísla $a, b, c \in \mathbb{R}$ platí $a(b + c) = ab + ac$, $(a + b)c = ac + bc$

pokud sčítání a násobení nějakých čísel splňuje podmínky (S1)-(S4), (M1)-(M3) a (D), můžeme řešit soustavy lineárních rovnic pomocí eliminace proměnných a zpětné substituce

Definice tělesa

definice: *těleso* **T** je **množina** T **spolu se dvěmi binárními operacemi** $+$ a $\cdot$ na T splňující následující axiomy

(S1) pro každé $a, b, c \in T$ platí $(a + b) + c = a + (b + c)$

(S2) existuje prvek $0 \in T$ takový, že pro každé $a \in T$ platí $a + 0 = a$

(S3) pro každý prvek $a \in T$ existuje $-a \in T$ takový, že $a + (-a) = 0$

(S4) pro každé $a, b \in T$ platí $a + b = b + a$

(N1) pro každé $a, b, c \in T$ platí $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(N2) existuje prvek $1 \in T$ takový, že pro každé $a \in T$ platí $a \cdot 1 = a$

(N3) pro každý prvek $a \in T$, $a \neq 0$, existuje $a^{-1} \in T$ takový, že $a \cdot a^{-1} = 1$

(N4) pro každé $a, b \in T$ platí $a \cdot b = b \cdot a$

(D) pro každé $a, b, c \in \mathbb{R}$ platí $a \cdot (b + c) = a \cdot b + a \cdot c$

(nT) T má aspoň dva prvky

Co je těleso

těleso v algebře není věc, nedá se vzít do ruky

je to soubor pravidel, které používáme při počítání

místo soubor pravidel říkáme **axiomy pro počítání**

není důležité **s čím** počítáme, pouze **jak** počítáme

Jednoduché důsledky axiomů tělesa 1

v každém tělese **T** platí

- nulový prvek je určený jednoznačně
- pro každé $a, b \in T$ má rovnice $a + x = b$ právě jedno řešení
- pro každé $a \in T$ je opačný prvek $-a$ určený jednoznačně

Jednoduché důsledky axiomů tělesa 2

- jednotkový prvek je určený jednoznačně
- pro každé $a \neq 0$ a $b \in T$ má rovnice $ax = b$ právě jedno řešení
- pro každé $a \neq 0$ je inverzní prvek a^{-1} určený jednoznačně

Jednoduché důsledky axiomů tělesa 3

- pro každé $a \in T$ platí $0a = 0$
- je-li $ab = 0$, pak $a = 0$ nebo $b = 0$
- pro každé $a \in T$ platí $-a = (-1)a$

Jednoduché důsledky axiomů tělesa 4

- pro každé $a, b, c \in T$ z rovnosti $a + b = a + c$ plyne $b = c$
- pro každé $b, c \in T$ a $a \neq 0$ z rovnosti $ab = ac$ plyne $b = c$
- $0 \neq 1$

Příklady těles - obsah

Klasická tělesa

klasické číselné obory $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ s obvyklými operacemi sčítání a násobení jsou tělesa

Dělení se zbytkem

tvrzení: pro každé přirozené číslo $n \in \mathbb{N}$ a každé celé číslo $a \in \mathbb{Z}$ existují jednoznačně určená čísla $q \in \mathbb{Z}$ a $r \in \{0, 1, 2, \dots, n-1\}$ taková, že platí

$$a = nq + r$$

příklad:

$$\begin{array}{rlll} 12 : 5 = 2 & \text{zbytek } 2, & \text{neboť} & 12 = 5 \cdot 2 + 2 \\ -32 : 7 = -5 & \text{zbytek } 3, & \text{neboť} & -32 = 7(-5) + 3 \\ 62 : 8 = 7 & \text{zbytek } 6, & \text{neboť} & 62 = 8 \cdot 7 + 6 \end{array}$$

označení zbytku: $a \bmod n$

Počítání modulo n

pro $n \geq 2$ definujeme *modulární operace* s celými čísly a, b:

$a \oplus b = (a + b) \bmod n$ *součet modulo n*

$a \odot b = (a \cdot b) \bmod n$ *součin modulo n*

výsledek vždy leží v množině $\mathbb{Z}_n = \{0, 1, \dots, n-1\} \subset \mathbb{Z}$

příklad: modulo 11 platí:

$10 \oplus 15 =$ $25 \oplus 14 =$ $3 \oplus 4 =$ $(-8) \oplus (-5) =$

$3 \odot 4 =$ $(-2) \odot 8 =$ $12 \odot 6 =$ $8 \odot 7 =$

Pomůcka pro modulární počítání

lemma: pro libovolné přirozené číslo n a celá čísla a, b, d taková, že $a \bmod n = d \bmod n$, platí při počítání modulo n rovnosti

1. $a \oplus b = d \oplus b$
2. $a \odot b = d \odot b$

důkaz 2:

Modulární operace jsou komutativní

protože pro každá dvě celá čísla a, b platí

$$a + b = b + a, \qquad a \cdot b = b \cdot a$$

rovnají se také zbytky

$$(a + b) \bmod n = (b + a) \bmod n$$

$$(ab) \bmod n = (ba) \bmod n$$

příklad: modulo 3 platí

$(324 \odot 16) \oplus (155 \odot 234) =$

totéž modulo 7:

$(324 \odot 16) \oplus (155 \odot 234) =$

Další vlastnosti modulárního počítání

platí $a \oplus b = (a + b) \bmod n \quad (\in \{0, 1, \dots, n-1\})$

proto $(a \oplus b) \bmod n =$

pomocí pomůcky dostaneme

$(a \oplus b) \oplus c = (a + b) \oplus c = ((a + b) + c) \bmod n$

$a \oplus (b \oplus c) = a \oplus (b + c) = (a + (b + c)) \bmod n$

podobně se dokáže asociativita násobení

a distributivita

Význam závorek a přesného vyjadřování

$$(3 \cdot 4) \cdot 5 \bmod 7$$

řidiče traktoru zraněného při nehodě odvezla sanitka

součet trojnásobku neznámého čísla zvětšeného o 2 a dvojnásobku neznámého čísla zmenšeného o 3 se rovná součtu čtyřnásobku neznámého čísla zmenšeného o 5 a dvojnásobku neznámého čísla zvětšeného o 1

Neutrální prvky modulo n

počítáme modulo 7:

$100 \oplus 0 = 100 \bmod 7 = 2$ $\qquad$ $100 \odot 1 = 100 \bmod 7 = 2$

nulový ani jednotkový prvek při počítání modulo n se **všemi** celými čísly neexistují

pokud se omezíme při počítání modulo n na množinu $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$, budou jak $\oplus$ tak $\odot$ binární operace na $\mathbb{Z}_n$

pro každé $a \in \mathbb{Z}_n$ navíc platí $a \oplus 0 = a \bmod n = a$ a $a \odot 1 = a \bmod n = a$

existují proto neutrální prvky při počítání modulo n na množině $\mathbb{Z}_n$

Opačné a inverzní prvky

pro nenulový prvek $a \in \mathbb{Z}_n$ je také $n - a \in \mathbb{Z}_n$ a platí

$a \oplus (n - a) = n \bmod n = 0$

v $\mathbb{Z}_n$ existuje opačný prvek ke každému prvku $a \in \mathbb{Z}_n$

v $\mathbb{Z}_3$ platí

x	0	1	2
$2x$			

v $\mathbb{Z}_4$ platí

x	0	1	2	3
$2x$				

v $\mathbb{Z}_5$ platí

x	0	1	2	3	4
$2x$					

x	0	1	2	3	4
$4x$					

Tělesa $\mathbb{Z}_p$

tvrzení: je-li n složené číslo, pak $\mathbb{Z}_n$ **není** těleso

důkaz:

věta: je-li p prvočíslo, pak $\mathbb{Z}_p$ **je** těleso

důkaz: je založený na tom, že prosté zobrazení mezi dvěma konečnými množinami téže velikosti je také zobrazení na

stačí proto dokázat, že pro každé nenulové $a \in \mathbb{Z}_p$ je prostým zobrazení $f_a : \mathbb{Z}_p \to \mathbb{Z}_p$ definované předpisem

$$f_a(x) = ax$$

Řešení soustavy lineárních rovnic s koeficienty v $\mathbb{Z}_7$

připravíme si tabulku inverzí

x	1	2	3	4	5	6
x^{-1}	1	4	5	2	3	6

$$\left(\begin{array}{ccccc|c} 2 & 4 & 1 & 2 & 3 & 3 \\ 4 & 1 & 3 & 2 & 6 & 3 \\ 1 & 5 & 0 & 2 & 6 & 4 \end{array}\right)$$

Čtyřprvkové těleso

$\mathbb{Z}_4$ **není** těleso

ale **čtyřprvkové těleso existuje**, jen se v něm nepočítá modulo 4

na množině $GF(4) = \{0, 1, \alpha, \alpha + 1\}$ sčítáme a násobíme jako s polynomy v proměnné α

s koeficienty počítáme jako v $\mathbb{Z}_2$: $(\alpha + 1) + \alpha =$

pokud při násobení dostaneme člen α^2, nahradíme jej $\alpha + 1$

$(\alpha + 1)(\alpha + 1) =$

dosáhneme tím toho, že součin dvou prvků z $GF(4)$ bude vždy opět v $GF(4)$

Další konečná tělesa

konečné těleso s n prvky existuje právě když n je mocnina prvočísla

šestiprvkové nebo desetiprvkové těleso tedy **neexistuje**

pro každé prvočíslo p a každé $k \in \mathbb{N}$ existuje „právě jedno“ těleso velikosti p^k

Charakteristika tělesa - obsah

Definice charakteristiky

důležitým číselným parametrem tělesa je jeho *charakteristika*

definice: existuje-li přirozené číslo n takové, že v tělese $\mathbf{T}$ platí

$$\underbrace{1+1+\cdots+1}_{n}=0\ ,$$

pak nejmenší takové kladné číslo nazýváme *charakteristika* tělesa $\mathbf{T}$

pokud žádné takové kladné celé číslo n neexistuje, tak říkáme že těleso $\mathbf{T}$ má *charakteristiku* 0

příklad: charakteristika tělesa $\mathbb{Z}_p$ se rovná

charakteristika tělesa $GF(4)$ je

charakteristika klasických těles $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ je

Věta o charakteristice

věta: charakteristika každého tělesa je buď 0 nebo prvočíslo

důkaz:

Další nekonečná tělesa - obsah

- *Další nekonečná tělesa*
  Tělesa mezi $\mathbb{Q}$ a $\mathbb{C}$
  Těleso kvaternionů

Tělesa mezi $\mathbb{Q}$ a $\mathbb{C}$

mezi tělesem $\mathbb{Q}$ racionálních čísel a tělesem $\mathbb{C}$ komplexních čísel existuje spousta dalších těles:

počítáme v nich stejně jako s komplexními nebo reálnými čísly

$\{a+ib : a, b \in \mathbb{Q}\}$

$\{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$

Těleso kvaternionů

jde o **nekomutativní těleso**

kvaternion je číslo tvaru

$$a + ib + jc + kd$$

$a, b, c, d \in \mathbb{R}$, $\quad i, j, k$ jsou *kvaternionové jednotky*

kvaterniony se sčítají přirozeně

$(a+ib+jc+kd)+(a'+ib'+jc'+kd')=(a+a')+i(b+b')+j(c+c')+k(d+d')$

kvaternionové jednotky komutují s reálnými čísly

mezi sebou se násobí následovně

$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i,\ ik = -j$

Kvaterniony rozšiřují komplexní čísla

příklad: spočteme součin kvaternionů

$(2 + i3 + j2 - k)(3 - i + j + 2k) =$

příklad: spočteme součin dvou kvaternionů

$(a + ib + j0 + k0)(c + id + j0 + k0)$

jejich součet je $(a + ib + j0 + k0) + (c + id + j0 + k0)$

s kvaterniony tvaru $a + ib + j0 + k0$ se tak počítá stejně jako s komplexními čísly

Kvaterniony a rotace v prostoru

kvaternion $a + ib + jc + kd$ je *jednotkový*, pokud $\sqrt{a^2 + b^2 + c^2 + d^2} = 1$

je-li $b^2 + c^2 + d^2 = 1$, pak kvaternion

$$\cos(\alpha/2) + (ia + jb + kc)\sin(\alpha/2)$$

je jednotkový a popisuje rotaci kolem osy procházející počátkem souřadnic a bodem $(b, c, d)^T$ o úhel α v kladném směru

Příklad

příklad: otočení o úhel $\pi/2$ kolem první souřadné osy v kladném směru zapíšeme jako kvaternion

$$\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

otočení kolem třetí souřadné osy o úhel $\pi/2$ v kladném směru zapíšeme pomocí kvaternionu

$$\frac{\sqrt{2}}{2} + k\frac{\sqrt{2}}{2}$$

složení těchto dvou rotací je pak popsáno součinem kvaternionů

$$\left(\frac{\sqrt{2}}{2} + k\frac{\sqrt{2}}{2}\right)\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) =$$

Kapitola 4

Matice

Počítání s maticemi - obsah

Matice nad tělesem

definice: *matice typu $m \times n$ nad tělesem* $\mathbf{T}$ je obdélníkové schéma prvků tělesa $\mathbf{T}$ s m řádky a n sloupci

matice typu $m \times m$ se nazývá *čtvercová matice řádu m*

matice typu $m \times 1$ se nazývá *sloupcový aritmetický vektor*

matice typu $1 \times n$ se nazývá *řádkový aritmetický vektor*

zápis matice $A = (a_{ij})_{m \times n}$ zůstává v platnosti

výraz „nad tělesem $\mathbf{T}$" říká nejenom, z jakého tělesa jsou prvky matice, ale také **jak se s nimi počítá**

množinu všech n-složkových aritmetických vektorů nad $\mathbf{T}$ budeme označovat $\mathbf{T}^n$

Součet matic

definice: *součet matic* $A = (a_{ij}), B = (b_{ij})$ **stejného typu** $m \times n$ **nad stejným tělesem** $\mathbf{T}$ definujeme jako matici $A + B = (a_{ij} + b_{ij})$ typu $m \times n$ nad tělesem $\mathbf{T}$

příklad: spočteme součet matic

$$\begin{pmatrix} 2 & 1 & 3 \\ 4 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 4 & 2 & 2 \\ 1 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2+4 & 1+2 & 3+2 \\ 4+1 & 0+1 & 1+3 \end{pmatrix}$$

matice typu $m \times 1$ se sčítají jako sloupcové aritmetické vektory

Nulová matice a opačná matice, rovnost matic

definice: *opačná matice* k matici $A = (a_{ij})$ typu $m \times n$ je matice $-A = (-a_{ij})$ typu $m \times n$

nulová matice typu $m \times n$ je matice $0_{m\times n} = (0)_{m\times n}$

definice: dvě matice $A = (a_{ij})$ a $B = (b_{ij})$ stejného typu $m \times n$ nad stejným tělesem $\mathbf{T}$ se *rovnají*, pokud mají na stejných místech stejné prvky, tj. pokud $a_{ij} = b_{ij}$ pro každé $i = 1, \dots m$ a každé $j = 1, \dots, n$

ověřit rovnost matic $A = B$ typu $m \times n$ znamená ověřit mn rovností $a_{ij} = b_{ij}$ (pro každé $i \in \{1, 2, \dots, m\}$ a $j \in \{1, 2, \dots, n\}$)

Vlastnosti sčítání matic

součet matic je definovaný „po prvcích“ a prvky sčítáme v tělese $\mathbf{T}$

axiomy (S1)-(S4) pro sčítání prvků v tělese vedou k analogickým vlastnostem sčítání matic

jsou-li A, B, C matice téhož typu $m \times n$ nad tělesem $\mathbf{T}$, pak platí

- $(A + B) + C = A + (B + C)$
- $A + 0_{m\times n} = A$
- $A + (-A) = 0_{m\times n}$
- $A + B = B + A$

k důkazu stačí porovnat prvky na stejných místech v maticích na levé a pravé straně každé rovnosti

Součin čísla s maticí

definice: *součin čísla $s \in \mathbf{T}$ s maticí A* typu $m \times n$ nad tělesem $\mathbf{T}$ je matice $sA = (sa_{ij})$ typu $m \times n$

příklad: spočteme součin

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

Vlastnosti součinu čísla s maticí

z dalších axiomů tělesa plynou další vlastnosti počítání s maticemi

pro každé prvky $s, t \in \mathbf{T}$ a matice A, B téhož typu $m \times n$ nad $\mathbf{T}$ platí

- $s(tA) = (st)A$
- $1A = A$
- $-A = (-1)A$
- $(s + t)A = sA + tA$
- $s(A + B) = sA + sB$

Transponovaná matice

poslední jednoduchou operací je *transponování* – záměna řádků a sloupců matice

příklad: $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ $\quad A^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$

definice: *transponovaná matice* k matici $A = (a_{ij})_{m \times n}$ je matice $A^T = (d_{ji})_{n \times m}$, kde $d_{ji} = a_{ij}$ pro každé $i = 1, \dots, m$ a $j = 1, \dots, n$

Základní vlastnosti transponování matic

následující tři vlastnosti transponování snadno ukážeme z definic

pro každé dvě matice A, B téhož typu $m \times n$ a každé $s \in \mathbf{T}$ platí

- $(A^T)^T = A$,
- $(A + B)^T = A^T + B^T$,
- $(s \cdot A)^T = s \cdot A^T$

Sloupcový pohled na matici

matici $A = (a_{ij})$ typu $m \times n$ nad tělesem $\mathbf{T}$ můžeme také považovat za posloupnost m-složkových vektorů nad tělesem $\mathbf{T}$ délky n

j-tý sloupcový vektor $\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$ matice A budeme označovat $\mathbf{a}_j$

matici A pak zapíšeme jako $A = (\mathbf{a}_1 | \mathbf{a}_2 | \cdots | \mathbf{a}_n)$

$$A = \left(\begin{array}{c|c|c|c} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{array} \right)$$

Řádkový pohled na matici

zapíšeme matici A^T transponovanou k matici A sloupcově

$$A^T = (\tilde{\mathbf{a}}_1 | \tilde{\mathbf{a}}_2 | \cdots | \tilde{\mathbf{a}}_m)$$

po transponování A^T dostaneme zpět původní matici

$$A = \begin{pmatrix} \tilde{\mathbf{a}}_1^T \\ \tilde{\mathbf{a}}_2^T \\ \vdots \\ \tilde{\mathbf{a}}_m^T \end{pmatrix}$$

zapsanou po řádcích

Řádky a sloupce v součtu matic a součinu čísla s maticí

jsou-li $A = (\mathbf{a}_1|\cdots|\mathbf{a}_n)$ a $B = (\mathbf{b}_1|\cdots|\mathbf{b}_n)$ matice typu $m \times n$,

pak platí $A + B = (\mathbf{a}_1 + \mathbf{b}_1|\cdots|\mathbf{a}_n + \mathbf{b}_n)$

zapíšeme-li obě matice řádkově: $A = \begin{pmatrix} \tilde{\mathbf{a}}_1^T \\ \vdots \\ \tilde{\mathbf{a}}_m^T \end{pmatrix}$ a $B = \begin{pmatrix} \tilde{\mathbf{b}}_1^T \\ \vdots \\ \tilde{\mathbf{b}}_m^T \end{pmatrix}$,

pak také $A + B = \begin{pmatrix} \tilde{\mathbf{a}}_1^T + \tilde{\mathbf{b}}_1^T \\ \vdots \\ \tilde{\mathbf{a}}_m^T + \tilde{\mathbf{b}}_m^T \end{pmatrix}$

podobně $sA = (s\mathbf{a}_1|\cdots|s\mathbf{a}_n) = \begin{pmatrix} s\tilde{\mathbf{a}}_1^T \\ \vdots \\ s\tilde{\mathbf{a}}_m^T \end{pmatrix}$

Součin matice s vektorem

definice: je-li $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ matice typu $m \times n$ nad tělesem $\mathbf{T}$ a $\mathbf{b} = (b_1, b_2, \ldots, b_n)^T$ (sloupcový) aritmetický vektor s n-složkami z tělesa $\mathbf{T}$, pak definujeme *součin matice A s vektorem* $\mathbf{b}$ jako

$$A\mathbf{b} = b_1\mathbf{a}_1 + b_2\mathbf{a}_2 + \cdots + b_n\mathbf{a}_n$$

součin $A\mathbf{b}$ je tedy lineární kombinace posloupnosti sloupcových vektorů $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$ s koeficienty $b_1, b_2, \ldots, b_n$

výsledkem je m-složkový vektor nad $\mathbf{T}$

příklad: $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} =$

Soustava lineárních rovnic pomocí součinu matice s vektorem

řešením soustavy m lineárních rovnic o n neznámých nad $\mathbf{T}$

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

je n-složkový aritmetický vektor $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ nad $\mathbf{T}$, pro který platí

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

kde $A = (a_{ij})$ je matice soustavy a $\mathbf{b}$ vektor pravých stran

Definice součinu matic

definice: je-li A matice typu $m \times n$ a $B = (\mathbf{b}_1|\mathbf{b}_2|\cdots|\mathbf{b}_p)$ matice typu $n \times p$, obě nad stejným tělesem $\mathbf{T}$, pak *součinem matic A a B* (v tomto pořadí) rozumíme matici

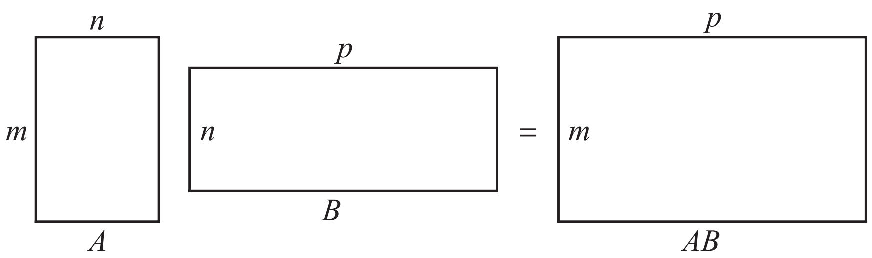
$$AB = (A\mathbf{b}_1|A\mathbf{b}_2|\cdots|A\mathbf{b}_p)$$

j-tý sloupec součinu matic AB se rovná součinu matice A s j-tým sloupcem matice B

součin matice typu $m \times n$ s maticí typu $n \times p$ je matice typu

příklad: $\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{pmatrix} =$

Typy v součinu matic graficky

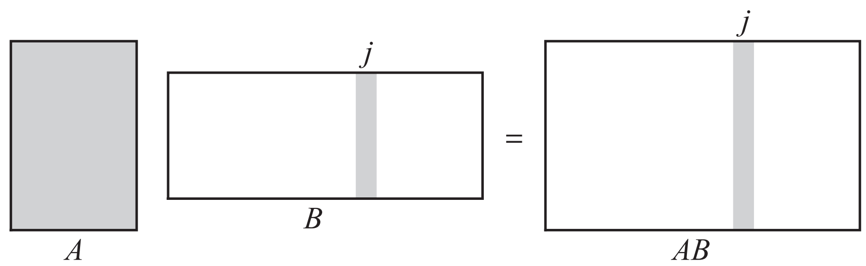


počet sloupců levé matice se musí rovnat počtu řádků pravé matice

počet řádků v součinu se pak rovná počtu řádků levé matice

počet sloupců v součinu se rovná počtu sloupců pravé matice

Sloupce v součinu matic graficky



j-tý sloupce v součinu AB se rovná součinu $A\mathbf{b}_j$ matice A s j-tým sloupcem $\mathbf{b}_j$ matice B

každý sloupec v součinu AB je nějakou lineární kombinací sloupců matice A

Další příklady (nad $\mathbb{R}$)

$$\begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} = \qquad \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} =$$

$$(1,3,5) \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} = \qquad \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} (1,3,5) =$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} = \qquad \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} =$$

násobení matic není komutativní

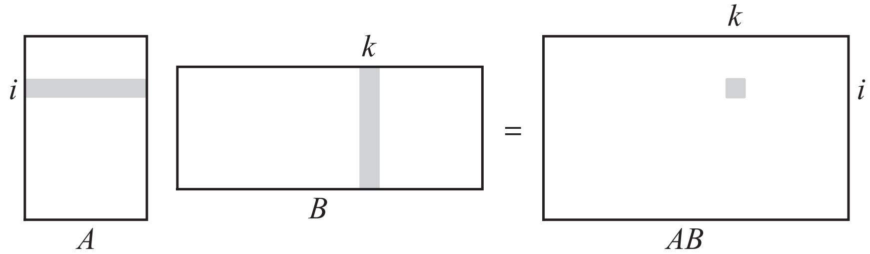
Prvky v součinu matic

čemu se rovná prvek na místě (i,k) v součinu AB matic $A = (a_{ij})_{m\times n}$ a $B = (b_{jk})_{n\times p}$?

tvrzení: jsou-li $A = (a_{ij})_{m\times n}$ a $B = (b_{jk})_{n\times p}$ matice nad tělesem $\mathbf{T}$, pak prvek na místě (i,k) v součinu AB se rovná

$$a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{j=1}^{n} a_{ij}b_{jk} = \tilde{\mathbf{a}}_i^T \mathbf{b}_k$$

Prvky v součinu matic graficky



prvek na místě (i, k) v součinu matic AB se rovná součinu i-tého řádku matice A s k-tým sloupcem matice B

Násobení matic je distributivní vzhledem ke sčítání

tvrzení: jsou-li $A = (a_{ij})$ a $B = (b_{ij})$ matice téhož typu $m \times n$ a $C = (c_{jk})$ matice typu $n \times p$, pak platí

$$(A + B)C = AC + BC$$

důkaz: operace na obou stranách lze provést a výsledkem je matice typu $m \times p$

ověříme rovnost prvků na stejném místě (i, k)

v matici $(A + B)C$:

v matici $AC + BC$:

Platí i druhá distributivita

tvrzení: jsou-li $C = (c_{jk})$ matice typu $n \times p$ a $D = (d_{kl})$, $E = (e_{kl})$ matice téhož typu $p \times q$, pak platí

$$C(D + E) = CD + CE$$

důkaz: tuto a všechny další vlastnosti operací s maticemi lze dokázat podle stejné osnovy

1. přesvědčíme se, že všechny operace na obou stranách jsou definované
2. ověříme, že na obou stranách vyjdou matice stejného typu
3. dokážeme, že každý prvek ve výsledné matici vlevo se rovná prvku na tomtéž místě ve výsledné matici vpravo
4. krok 3. je založený na definici příslušných operací s maticemi a vlastnostech počítání v tělese

Násobení matic je asociativní

tvrzení: jsou-li B matice typu $m \times n$, C matice typu $n \times p$ a D matice typu $p \times q$, pak platí

$$(BC)D = B(CD)$$

důkaz: součiny na obou stranách jsou definované a jsou typu $m \times q$

pro $i \in \{1, 2, \dots, m\}$ a $l \in \{1, 2, \dots, q\}$ je prvek na místě (i, l)

v matici $(BC)D$:

v matici $B(CD)$:

Další vlastnosti operací s maticemi

tvrzení: pro libovolné matice A typu $m \times n$ a B typu $n \times p$ a každý prvek s tělesa $\mathbf{T}$ platí

- $s(AB) = (sA)B = A(sB)$
- $(AB)^T = B^T A^T$

Řádky v součinu matic

jak vypadá i-tý řádek v součinu AB matic $A = (a_{ij})_{m\times n}$ a $B = (b_{jk})_{n\times p}$?

i-tý řádek v součinu AB se rovná i-tému sloupci v matici $(AB)^T$ transponované k AB

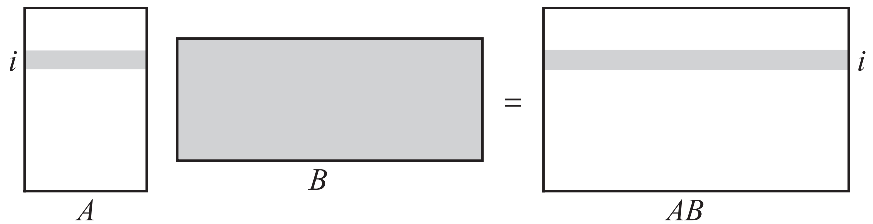
i-tý sloupec v matici $(AB)^T = B^T A^T$ se podle definice součinu matic rovná $B^T \tilde{\mathbf{a}}_i$

$B^T \tilde{\mathbf{a}}_i$ je lineární kombinace sloupců matice $B^T = (\tilde{\mathbf{b}}_1 | \tilde{\mathbf{b}}_2 | \cdots | \tilde{\mathbf{b}}_n)$ s koeficienty v i-tém sloupci $\tilde{\mathbf{a}}_i = (a_{i1}, a_{i2}, \ldots, a_{in})^T$ matice A^T

$B^T \tilde{\mathbf{a}}_i = a_{i1}\tilde{\mathbf{b}}_1 + a_{i2}\tilde{\mathbf{b}}_2 + \cdots + a_{in}\tilde{\mathbf{b}}_n;$ i-tý řádek v AB je tedy

$(B^T \tilde{\mathbf{a}}_i)^T = a_{i1}\tilde{\mathbf{b}}_1^T + a_{i2}\tilde{\mathbf{b}}_2^T + \cdots + a_{in}\tilde{\mathbf{b}}_n^T$

Řádky v součinu matic graficky



i-tý řádek v součinu AB se rovná lineární kombinaci řádků matice B s koeficienty v i-tém řádku matice A

každý řádek v součinu AB je nějakou lineární kombinací řádků matice B

Jednotkové matice

definice: pro každé $n \geq 1$ definujeme *jednotkovou matici* řádu n jako čtvercovou matici $I_n = (a_{ij})_{n\times n}$, pro kterou platí

$$a_{ij} = \begin{cases} 1 & \text{pokud platí } i = j \\ 0 & \text{pokud platí } i \neq j \end{cases}$$

tvrzení: pro každou matici A typu $m \times n$ platí

$$I_m A = A = A I_n$$

důkaz:

Blokové násobení matic

libovolné dvě matice $A = (a_{ij})_{m \times n}$ a $B = (b_{jk})_{n \times p}$ můžeme vynásobit v pořadí AB

obě matice rozdělíme do čtyř bloků

$$A = \left(\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right) , \qquad B = \left(\begin{array}{c|c} B_{11} & B_{12} \\ \hline B_{21} & B_{22} \end{array} \right)$$

mohlo by za nějakých předpokladů platit

$$AB = \left(\begin{array}{c|c} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ \hline A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{array} \right) \quad ?$$

Proč blokové násobení ?

prvek na místě $(1,1)$ v součinu AB je $\sum_{j=1}^{n} a_{1j} b_{j1}$

prvek na místě $(1,1)$ v součtu $A_{11}B_{11} + A_{12}B_{21}$ je

$$\sum_{j=1}^{n_1} a_{1j} b_{j1} + \sum_{j=n_1+1}^{n} a_{1j} b_{j1}$$

počet aritmetických operací je v obou případech stejný

pokud součin matic AB naprogramujete pomocí $\sum_{j=1}^{n} a_{ij} b_{jk}$,

bude váš program v případě velkých matic významně pomalejší než od profesionálů

Software pro lineární algebru

profesionální software je optimalizovaný vzhledem k časové náročnosti přesouvání dat mezi různými typy pamětí

nejkvalitnější knihovna pro lineárně algebraické výpočty je

LAPACK (Linear Algebra PACKage)

využívající knihovnu BLAS (Basic Linear Algebra Software)

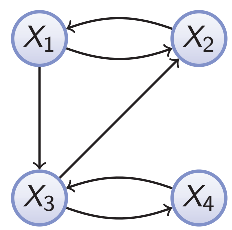
obě knihovny jsou volně ke stažení

využívají je i komerční systémy jako Mathematica, Maple, Matlab

Letecká spojení

mezi čtyřmi městy jsou letecká spojení podle obrázku

kolik je spojení mezi městy X_i a X_k s nejvýše třemi přestupy ?



spojení popíšeme maticí

Mocniny matice spojů

prvek na místě (i,k) v matici A^2 se rovná

$$a_{i1}a_{1k} + a_{i2}a_{2k} + a_{i3}a_{3k} + a_{i4}a_{4k}$$

Fibonacciho posloupnost

v různých matematických i přírodovědných oborech se lze setkat s *Fibonacciho posloupností*

ta je definována rekurentně předpisem

$$a_1 = 1, a_2 = 1, \quad a_{n+2} = a_{n+1} + a_n \quad \text{pro} \quad n \geq 1$$

otázka: čemu se rovná n-tý člen posloupnosti ?

označíme $\quad \mathbf{a}_n = \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix} \quad$ pro každé $n \in \mathbb{N}$

Vzorec pro n-tý člen

rekurentní definici Fibonacciho posloupnosti zapíšeme maticí

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

pro ni platí $\quad B\mathbf{a}_n = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} a_{n+1} \\ a_{n+2} \end{pmatrix} = \mathbf{a}_{n+1}$

takže $\quad \mathbf{a}_2 = B\mathbf{a}_1, \; \mathbf{a}_3 = B\mathbf{a}_2 = BB\mathbf{a}_1 = B^2\mathbf{a}_1, \; \dots \;, \mathbf{a}_{n+1} = B^n\mathbf{a}_1$

vyjde $\quad a_n = \dfrac{(1+\sqrt{5})^n}{2^n\sqrt{5}} - \dfrac{(1-\sqrt{5})^n}{2^n\sqrt{5}}$

metoda, jak rychle umocňovat čtvercové matice, bude na začátku druhého semestru

Speciální typy matic

definice: čtvercovou matici $A = (a_{ij})$ nazýváme

- *diagonální*, pokud $a_{ij} = 0$ kdykoliv $i \neq j$
- *permutační*, má-li v každém řádku a každém sloupci právě jeden prvek 1 a ostatní 0
- *horní trojúhelníková*, pokud $a_{ij} = 0$ kdykoliv $i > j$
- *dolní trojúhelníková*, pokud $a_{ij} = 0$ kdykoliv $i < j$

u libovolné matice říkáme, že prvky a_{ii} tvoří *hlavní diagonálu*.

Součin speciálních typů matic

tvrzení: jsou-li A, B čtvercové matice téhož řádu, pak jejich součin AB je

- diagonální, jsou-li obě matice A, B diagonální
- permutační matice, jsou-li obě matice A, B permutační
- horní trojúhelníková matice, jsou-li obě matice A, B horní trojúhelníkové
- horní trojúhelníková s prvky 1 na hlavní diagonále, jsou-li obě matice A, B horní trojúhelníkové s prvky 1 na hlavní diagonále
- dolní trojúhelníková matice, jsou-li obě matice A, B dolní trojúhelníkové
- dolní trojúhelníková s prvky 1 na hlavní diagonále, jsou-li obě matice A, B dolní trojúhelníkové s prvky 1 na hlavní diagonále

důkaz: ve skriptech nebo jako cvičení

Soustavy lineárních rovnic podruhé - obsah

- *Soustavy lineárních rovnic podruhé*
  Množina všech řešení soustavy lineárních rovnic

Množina všech řešení soustavy lineárních rovnic

množinu všech řešení soustavy

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

m lineárních rovnic o n neznámých nad tělesem $\mathbf{T}$ zapisujeme jako

$$\left\{ \mathbf{u} + \sum_{p \in P} t_p \mathbf{v}_p : \ t_p \in \mathbf{T} \ \text{ pro každé } \ p \in P \right\}$$

- P je množina indexů bázových proměnných
- $\mathbf{u}$, $\mathbf{v}_p$, $p \in P$, jsou „vhodné“ n-složkové aritmetické vektory nad $\mathbf{T}$

co znamená „vhodné“ ?

Partikulární řešení soustavy

hodnotu parametrů $t_p \in \mathbf{T}$ můžeme volit libovolně

zvolíme-li $t_p = 0$ pro každé $p \in P$, dostaneme jedno řešení $\mathbf{x} = \mathbf{u}$

vektor $\mathbf{u}$ je jedno *partikulární* řešení soustavy $A\mathbf{x} = \mathbf{b}$

zvolíme-li jeden parametr $t_p = 1$ a ostatní parametry zvolíme 0, dostaneme jiné řešení $\mathbf{x} = \mathbf{u} + \mathbf{v}_p$ soustavy $A\mathbf{x} = \mathbf{b}$

pozorování: jsou-li $\mathbf{u}, \mathbf{w}$ dvě řešení soustavy $A\mathbf{x} = \mathbf{b}$, pak jejich rozdíl $\mathbf{w} - \mathbf{u}$ je řešením soustavy $A\mathbf{x} = \mathbf{o}$

důkaz: $A(\mathbf{w} - \mathbf{u}) =$

Homogenní soustava lineárních rovnic

$\mathbf{v}_p = (\mathbf{u} + \mathbf{v}_p) - \mathbf{u}$ je rozdíl dvou řešení soustavy $A\mathbf{x} = \mathbf{b}$

vektory $\mathbf{v}_p$, $p \in P$, jsou proto řešením soustavy $A\mathbf{x} = \mathbf{o}$

definice: soustava $A\mathbf{x} = \mathbf{o}$ se nazývá *homogenní soustava lineárních rovnic* (příslušná k soustavě $A\mathbf{x} = \mathbf{b}$)

další pozorování: je-li $\mathbf{u}$ řešení soustavy $A\mathbf{x} = \mathbf{b}$ a $\mathbf{v}$ řešení příslušné homogenní soustavy $A\mathbf{x} = \mathbf{o}$, pak $\mathbf{u} + \mathbf{v}$ je také řešení soustavy $A\mathbf{x} = \mathbf{b}$

důkaz: $A(\mathbf{u} + \mathbf{v}) =$

Jádro matice

definice: množina všech řešení homogenní soustavy lineárních rovnic $A\mathbf{x} = \mathbf{o}$ se nazývá *jádro matice A* nebo také *nulový prostor matice A*

označení: *Ker A*

věta: je-li $\mathbf{u}$ jedno pevně zvolené partikulární řešení soustavy lineárních rovnic $A\mathbf{x} = \mathbf{b}$, pak se množina všech řešení soustavy rovná

$$\{\mathbf{u} + \mathbf{v} : \mathbf{v} \in Ker\ A\} \quad = \quad \mathbf{u} + Ker\ A$$

důkaz: je-li $\mathbf{w}$ řešení soustavy $A\mathbf{x} = \mathbf{b}$, pak $\mathbf{w} - \mathbf{u} \in Ker\ A$

a $\quad \mathbf{w} = \mathbf{u} + (\mathbf{w} - \mathbf{u}) \in \{\mathbf{u} + \mathbf{v} : \mathbf{v} \in Ker\ A\}$

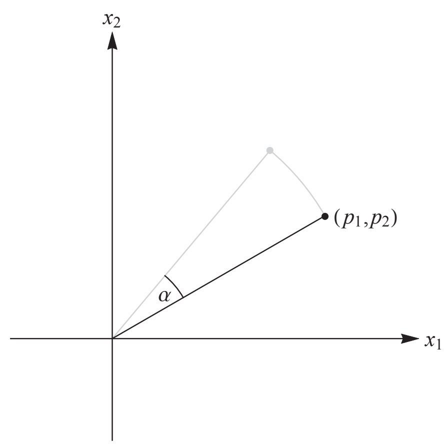
naopak pro libovolné $\mathbf{v} \in Ker\ A$ je $\mathbf{u} + \mathbf{v}$ řešením soustavy $A\mathbf{x} = \mathbf{b}$

Matice jako zobrazení - obsah

- *Matice jako zobrazení*
  Zobrazení v rovině
  Matice určuje zobrazení
  Součin matic podruhé

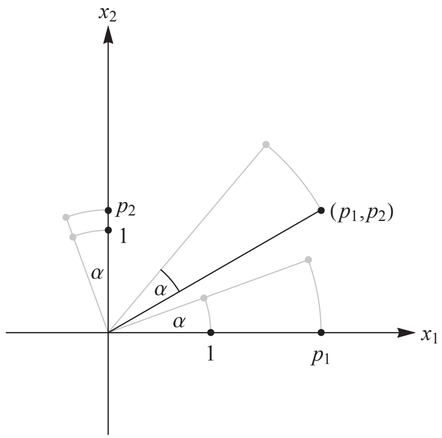
Otočení roviny kolem počátku

rovinu otočíme kolem počátku souřadnic o úhel α

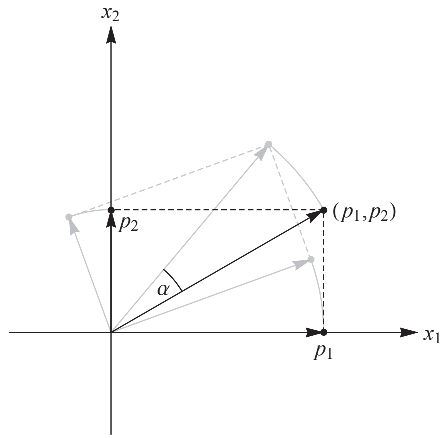


kam se pootočí bod se souřadnicemi (p_1, p_2) ?

Otočení roviny podruhé

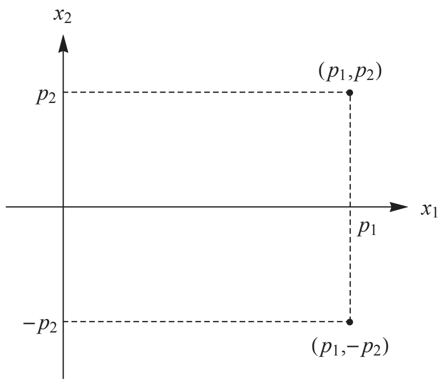


Otočení roviny potřetí



Symetrie v rovině vzhledem k souřadné ose

také symetrii vzhledem k první souřadné ose v rovině lze popsat pomocí matice



Zobrazení určené maticí

definice: je-li $A = (a_{ij})$ matice typu $m \times n$ nad tělesem $\mathbf{T}$, pak definujeme *zobrazení* $f_A : \mathbf{T}^n \to \mathbf{T}^m$ *určené maticí* A předpisem

$$f_A(\mathbf{x}) = A\mathbf{x}$$

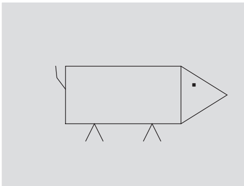
pro každý aritmetický vektor $\mathbf{x} \in \mathbf{T}^n$

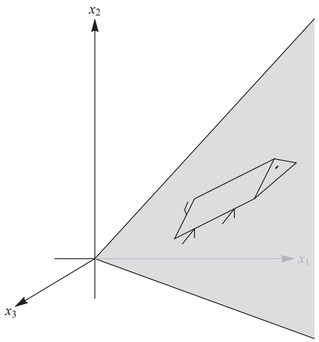
příklad: otočení v rovině kolem počátku o úhel α v kladném směru je určené reálnou maticí

symetrie v rovině vzhledem k první souřadné ose je určená reálnou maticí

Z roviny do prostoru

zobrazení $f_A : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ určené maticí $\begin{pmatrix} 5 & 1 \\ 2 & 3 \\ 1 & -1 \end{pmatrix}$



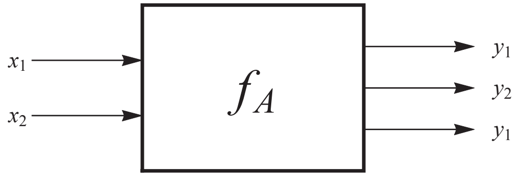


Jak si f_A představit?

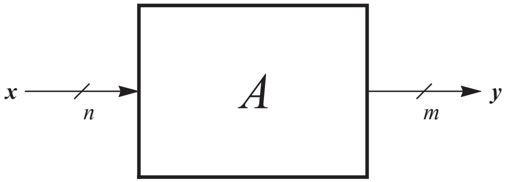
geometricky to nejde, pouze v případě „malých“ matic

známe předpis, jak spočítat $f_A(\mathbf{x})$ pro každé $\mathbf{x} \in \mathbf{T}^n$

je to „černá skříňka“



Dotazy pro černou skříňku



$A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ typu $m \times n$

jaká je tvoje hodnota v bodě $\mathbf{x}$?

je-li $\mathbf{x} = (1, 0, \dots, 0)^T$, zrcadlo odpoví:

Prvky kanonické báze v $\mathbf{T}^n$

definice: vektory $\mathbf{e}_j = (0, \dots, 0, 1, 0, \dots, 0)^T \in \mathbf{T}^n$ pro $j = 1, \dots, n$ nazýváme *prvky kanonické báze* v $\mathbf{T}^n$

pro každý prvek kanonické báze platí $f_A(\mathbf{e}_j) = \mathbf{a}_j$

vhodnými dotazy ke krabičce f_A zjistíme, jak vypadá matice A

matice A je zobrazením f_A určená jednoznačně

nebo jinak: různé matice téhož typu $m \times n$ určují různá zobrazení z $\mathbf{T}^n$ do $\mathbf{T}^m$

Důležité vlastnosti zobrazení f_A

tvrzení: je-li A matice typu $m \times n$ nad tělesem $\mathbf{T}$, pak pro každé dva aritmetické vektory $\mathbf{x}, \mathbf{y} \in \mathbf{T}^n$ a každý prvek $s \in \mathbf{T}$ platí

- $f_A(s\mathbf{x}) = s\, f_A(\mathbf{x})$
- $f_A(\mathbf{x} + \mathbf{y}) = f_A(\mathbf{x}) + f_A(\mathbf{y})$

důkaz: $f_A(s\mathbf{x}) =$

$f_A(\mathbf{x} + \mathbf{y}) =$

otázka: zobrazení $f : \mathbb{R}^2 \to \mathbb{R}^2$ je definované předpisem

$$f\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1^2 \\ x_1 x_2 \end{pmatrix}$$

může být $f = f_A$ pro nějakou matici A ?

Zobrazení určená maticemi a součin matic

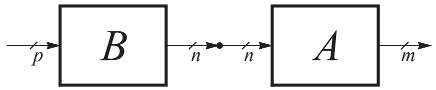
tvrzení: je-li A matice typu $m \times n$ a B matice typu $n \times p$ nad stejným tělesem $\mathbf{T}$, pak zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ a $f_B : \mathbf{T}^p \to \mathbf{T}^n$ můžeme složit v pořadí $f_A f_B$ a pro složené zobrazení $f_A f_B : \mathbf{T}^p \to \mathbf{T}^m$ platí

$$f_A f_B = f_{AB}$$

důkaz: pro každý vektor $\mathbf{x} \in \mathbf{T}_p$ platí

$f_A f_B(\mathbf{x}) =$

krabičkově:



Součtové vzorce pro *sinus* a *cosinus*

příklad: rovinu otočíme kolem počátku o úhel β a poté o úhel α

otočení o $\alpha + \beta$ má matici:

coby složení dvou rotací má také matici

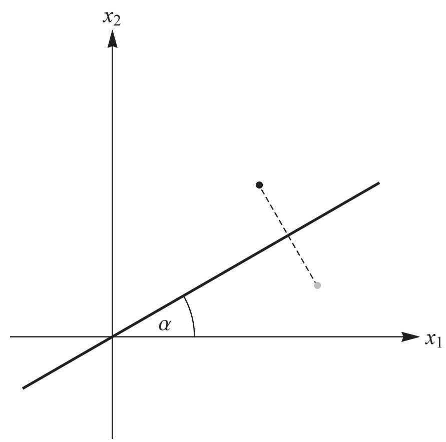
$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} =$$

obě matice určují tutéž rotaci o úhel $\alpha + \beta$, musí se rovnat

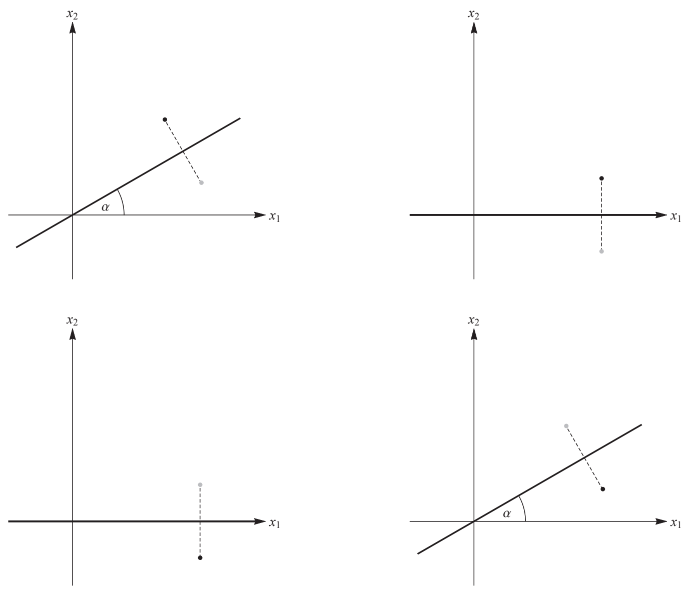
proto platí

Symetrie vzhledem k přímce procházející počátkem

najdeme matici symetrie určené přímkou procházející počátkem



Rozklad symetrie na jednodušší zobrazení

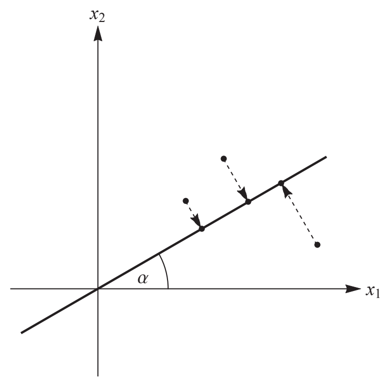


Výpočet matice symetrie

Složení rotace se symetrií

co vyjde složením rotace o úhel $-\alpha$ se symetrií vzhledem k ose x_1 ?

Ortogonální projekce na přímku procházající počátkem



Regulární matice - obsah

- *Regulární matice*
  - Elementární matice
  - Invertovatelné matice
  - Regulární matice
  - Výpočet inverzní matice
  - Ekvivalentní podmínky s regularitou

Elementární matice

definice: *elementární matice* řádu n je libovolná matice, kterou dostaneme z matice I_n jednou elementární řádkovou úpravou

příklady elementárních matic řádu 3:

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & t \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ t & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}$$

elementárních matic řádu 4:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Efekt násobení elementární maticí zleva

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \tilde{\mathbf{b}}_1^T \\ \tilde{\mathbf{b}}_2^T \\ \tilde{\mathbf{b}}_3^T \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & t \end{pmatrix} \begin{pmatrix} \tilde{\mathbf{b}}_1^T \\ \tilde{\mathbf{b}}_2^T \\ \tilde{\mathbf{b}}_3^T \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ t & 0 & 1 \end{pmatrix} \begin{pmatrix} \tilde{\mathbf{b}}_1^T \\ \tilde{\mathbf{b}}_2^T \\ \tilde{\mathbf{b}}_3^T \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \tilde{\mathbf{b}}_1^T \\ \tilde{\mathbf{b}}_2^T \\ \tilde{\mathbf{b}}_3^T \end{pmatrix} =$$

Obecné elementární matice 1

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & \dots & 1 & & \\ & & \vdots & \ddots & \vdots & & \\ & & 1 & \dots & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & t & & & \\ & & & & \ddots & & \\ & & & & & 1 & \\ & & & & & & 1 \end{pmatrix}$$

přehození řádků — násobení řádku nenulovým číslem

všechny nevyznačené prvky na hlavní diagonále jsou 1,
všechny nevyznačené prvky mimo hlavní diagonálu jsou 0

Obecné elementární matice 2

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & \vdots & \ddots & & & \\ & & t & \dots & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & \dots & t & & \\ & & & \ddots & \vdots & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

přičtení t-násobku jednoho řádku k jinému řádku

všechny ostatní prvky mimo hlavní diagonálu jsou 0,
všechny prvky na hlavní diagonále jsou 1

???

co se stane, vynásobíme-li matici elementární maticí **zprava** ?

Invertovatelné matice

definice: čtvercová matice A řádu n se nazývá *invertovatelná*, pokud existuje čtvercová matice X řádu n, pro kterou platí $AX = I_n = XA$, matice X se pak nazývá *inverzní matice* k matici A; **označení** inverzní matice: A^{-1}

pozorování: jsou-li A, X, Y čtvercové matice téhož řádu n, pro které platí $YA = I_n = AX$, pak platí $Y = X$

důkaz:

důsledek: je-li A invertovatelná, pak je A^{-1} určená jednoznačně

příklad matice, která není invertovatelná: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

Regulární matice

definice: čtvercová matice A řádu n nad tělesem $\mathbf{T}$ se nazývá *regulární*, pokud určuje vzájemně jednoznačné zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^n$

pozorování 1: je-li A regulární, pak má soustava lineárních rovnic $A\mathbf{x} = \mathbf{b}$ právě jedno řešení pro každou pravou stranu $\mathbf{b}$

důkaz:

pozorování 2: každá invertovatelná matice je regulární

důkaz:

Které matice jsou regulární?

$$A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

$$B = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$$

$$C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$D = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Výpočet inverzní matice k regulární matici

sloupcový zápis jednotkové matice $I_n = (\mathbf{e}_1|\mathbf{e}_2|\cdots|\mathbf{e}_n)$

platí-li $AX = I_n$ pro nějakou matici $X = (\mathbf{x}_1|\mathbf{x}_2|\cdots|\mathbf{x}_n)$ řádu n, je

$$AX = A(\mathbf{x}_1|\mathbf{x}_2|\cdots|\mathbf{x}_n) = (A\mathbf{x}_1|A\mathbf{x}_2|\cdots|A\mathbf{x}_n) = (\mathbf{e}_1|\mathbf{e}_2|\cdots|\mathbf{e}_n)$$

tj. $A\mathbf{x}_j = \mathbf{e}_j$ pro každé $j = 1, 2, \dots, n$

je-li A regulární, má každá taková soustava jednoznačné řešení

ke každé regulární matici existuje matice inverzní zprava

Příklad

$$A = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix},$$ zkusíme najít matici inverzní zprava

Uděláme to lépe

$$\left(\begin{array}{ccc|ccc} 2 & -1 & 0 & 1 & 0 & 0 \\ -1 & 2 & -1 & 0 & 1 & 0 \\ 0 & -1 & 2 & 0 & 0 & 1 \end{array}\right) \sim$$

Proč to vyjde vždy

každou elementární řádkovou úpravu matice $(A|I_n)$ uděláme pomocí nějaké elementární matice E:

$$E(A|I_n) = (EA|EI_n)$$

posloupností elementárních řádkových úprav dosteneme

$$E_k \cdots E_3 E_2 E_1 (A|I_n) = E_k \cdots E_3 E_2 (E_1 A|E_1)$$
$$= E_k \cdots E_3 (E_2 E_1 A|E_2 E_1) = (E_k \cdots E_3 E_2 E_1 A|E_k \cdots E_3 E_2 E_1)$$

je-li výsledkem elementárních úprav matice $(I_n|X)$, platí

$$(E_k \cdots E_3 E_2 E_1 A|E_k \cdots E_3 E_2 E_1) = (I_n|X),$$

tj. $\quad E_k \cdots E_3 E_2 E_1 = X \quad$ a $\quad XA = E_k \cdots E_3 E_2 E_1 A = I_n$

Příklad

zkusíme najít matici inverzní k matici A nad tělesem $\mathbb{Z}_5$

$$A = \begin{pmatrix} 0 & 2 & 4 \\ 3 & 1 & 4 \\ 4 & 2 & 1 \end{pmatrix}$$

Když inverzní matice neexistuje

zkusíme najít matici inverzní k matici A nad tělesem $\mathbb{Z}_2$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Někdy to lze uhádnout

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}^{-1}$$

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}^{-1}$$

$$\begin{pmatrix} \cos^2\alpha & \sin\alpha\cos\alpha \\ \sin\alpha\cos\alpha & \sin^2\alpha \end{pmatrix}^{-1}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix}^{-1}$$

Shrnutí - 1. část

věta: pro čtvercovou matici A řádu n nad $\mathbf{T}$ je ekvivalentní

1. A je regulární
2. zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^n$ je na množinu $\mathbf{T}^n$
3. zobrazení f_A je prosté
4. soustava $A\mathbf{x} = \mathbf{o}$ má jediné řešení $\mathbf{x} = \mathbf{o}$
5. Gaussova eliminace převede A do horní trojúhelníkové matice s nenulovými prvky na hlavní diagonále (tj. bez nulových řádků)
6. A lze převést pomocí *eřú* do matice I_n
7. A je invertovatelná

důkaz:

Dokončení důkazu

Elementární matice jsou regulární

stačí najít ke každé elementární matici inverzní matici

inverzní matice k elementární matici je opět elementární

Vztah inverze a dalších operací

tvrzení: jsou-li A, B regulární/invertovatelné matice stejného řádu n nad $\mathbf{T}$ a $t \in \mathbf{T}$ nenulový prvek, pak platí

- A^{-1} je regulární a $(A^{-1})^{-1} = A$
- A^T je regulární a $(A^T)^{-1} = (A^{-1})^T$
- tA je regulární a $(tA)^{-1} = t^{-1}A^{-1}$
- AB je regulární a $(AB)^{-1} = B^{-1}A^{-1}$

důkaz: stačí vždy ověřit, že matice vpravo je inverzní k té vlevo

Shrnutí - druhá část

pokračování důležité věty: pro čtvercovou matici A řádu n nad $\mathbf{T}$ jsou následující podmínky ekvivalentní

7. A je invertovatelná
8. existuje matice X taková, že $AX = I_n$
9. existuje matice Y taková, že $YA = I_n$
10. A lze vyjádřit jako součin elementárních matic

důkaz: víme už, že podmínka 7. je ekvivalentní jakékoliv z podmínek 1.-6.

Příklad nad $\mathbb{Z}_5$

zkusíme najít inverzní matici k matici $A = \begin{pmatrix} 0 & 2 & 4 \\ 3 & 1 & 4 \\ 4 & 2 & 1 \end{pmatrix}$

Příklad nad $\mathbb{Z}_2$

zkusíme najít inverzní matici k matici $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$

Vzorec

je-li A regulární, pak $A\mathbf{x} = \mathbf{b}$ má řešení $\mathbf{x} = A^{-1}\mathbf{b}$

soustava $\begin{pmatrix} 0 & 2 & 4 \\ 3 & 1 & 4 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ má nad $\mathbb{Z}_5$ řešení

Desátá charakterizace regularity

tvrzení: čtvercová matice A je regulární právě tehdy, když jde napsat jako součin elementárních matic

důkaz:

Posloupnost elementárních řádkových úprav

tvrzení: jsou-li A, B jsou matice typu $m \times n$ nad tělesem $\mathbf{T}$, pak B lze z A získat posloupností elementárních řádkových úprav právě tehdy, když existuje regulární matice R řádu m nad $\mathbf{T}$ taková, že $B = RA$

důkaz:

LU-rozklad - obsah

- *LU-rozklad*
  Příklad
  LU-rozklad
  Když je nutné prohazovat řádky

Příklad

řešíme soustavu $\left(\begin{array}{ccc|c} 2 & 2 & 2 & 1 \\ 4 & 7 & 7 & 2 \\ 6 & 18 & 22 & 7 \end{array}\right)$

a soustavu $\left(\begin{array}{ccc|c} 2 & 2 & 2 & 7 \\ 4 & 7 & 7 & 2 \\ 6 & 18 & 22 & 1 \end{array}\right)$

pokračování

a teď $\left(\begin{array}{ccc|c} 2 & 2 & 2 & 6 \\ 4 & 7 & 7 & 24 \\ 6 & 18 & 22 & 70 \end{array}\right)$

$A\mathbf{x} = \mathbf{b}$ $\quad RA\mathbf{x} = R\mathbf{b}$ $\quad U\mathbf{x} = R\mathbf{b}$ $\quad R^{-1}U\mathbf{x} = \mathbf{b}$

Záznamy jednotlivých cyklů Gaussovy eliminace

$R = E_3(E_2E_1)$ $\qquad R^{-1} = (E_2E_1)^{-1}E_3^{-1}$

$E_2E_1 =$ $\qquad (E_2E_1)^{-1} =$

$E_3 =$ $\qquad E_3^{-1} =$

$R^{-1} = (E_2E_1)^{-1}E_3^{-1} =$

Přímá a zpětná substituce

řešíme soustavu $\quad R^{-1}U\mathbf{x} = \mathbf{b}$, $\quad$ kde

$$R^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 4 & 1 \end{pmatrix}, \quad U = \left(\begin{array}{ccc|c} 2 & 2 & 2 & 6 \\ 0 & 3 & 3 & 12 \\ 0 & 0 & 4 & 4 \end{array}\right), \quad \mathbf{b} = \begin{pmatrix} 6 \\ 24 \\ 70 \end{pmatrix}$$

Inverzní matice k trojúhelníkovým

tvrzení: pro regulární dolní (horní) trojúhelníkovou matici R řádu n platí, že inverzní matice R^{-1} je také dolní (horní)trojúhelníková

má-li navíc matice R na hlavní diagonále všechny prvky rovné 1, pak i matice R^{-1} má samé jednotky na hlavní diagonále

důkaz:

Dokončení důkazu

LU-rozklad obecně

předpoklady: při řešení soustavy $A\mathbf{x} = \mathbf{b}$ nepřehazujeme řádky, matice A je regulární

výsledkem Gaussovy eliminace matice A je horní trojúhelníková matice U s nenulovými prvky na hlavní diagonále

všechny řádkové úpravy odpovídají dolním trojúhelníkovým maticím $E_1, E_2, \ldots, E_k$ s jednotkami na hlavní diagonále

jejich součin $R = E_k \cdots E_2 E_1$ je dolní trojúhelníková matice s jednotkami na hlavní diagonále

$R^{-1} = L$ je dolní trojúhelníková s jednotkami na hlavní diagonále

$RA = U$, proto $A = R^{-1}U = LU$

Věta o LU-rozkladu

věta: je-li A je regulární matice řádu n, u které při Gaussově eliminaci nemusíme prohazovat řádky, pak existují regulární matice L, U řádu n, pro které platí

- $A = LU$
- L je dolní trojúhelníková s jednotkami na hlavní diagonále
- U je horní trojúhelníková s nenulovými prvky na hlavní diagonále

matice L, U jsou těmito podmínkami určeny jednoznačně

důkaz jednoznačnosti

Matice $L = R^{-1}$

záznam prvního cyklu Gaussovy eliminace

záznam druhého cyklu Gaussovy eliminace

Záznam j-tého cyklu Gaussovy eliminace

Součin matic F_j^{-1}

Dokončení popisu matice $L = R^{-1}$

Příklad

spočteme LU-rozklad matice $A = \begin{pmatrix} 2 & 1 & 1 \\ 4 & -6 & 0 \\ -2 & 7 & 2 \end{pmatrix}$

Využití LU-rozkladu

při opakovaném řešení soustavy $A\mathbf{x} = \mathbf{b}$ pro různá $\mathbf{b}$

Někdy to bez prohazování řádků nejde

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Gaussova eliminace s *částečnou pivotací* je numericky stabilnější

věta: je-li A regulární matice řádu n, pak existuje permutační matice P a regulární matice matice L, U, všechny řádu n, pro které platí

- $PA = LU$
- L je dolní trojúhelníková matice s jednotkami na hlavní diagonále
- U je horní trojúhelníková matice s nenulovými prvky na hlavní diagonále

Příklad

permutační matice P není určena jednoznačně

pokud LU-rozklad matice PA existuje, je jednoznačný

příklad použijeme Gaussovu eliminaci s částečnou pivotací na matici

$$A = \begin{pmatrix} 1 & 2 & -3 & 4 \\ 4 & 8 & 12 & -8 \\ 2 & 3 & 2 & 1 \\ -3 & -1 & 1 & -4 \end{pmatrix}$$

najdeme permutační matici P a LU-rozklad $PA = LU$

Počítadlo permutace P

k A přidáme sloupec $(1, 2, 3, 4)^T$, do kterého budeme zaznamenávat prohazování řádků

$$\left(\begin{array}{cccc||c} 1 & 2 & -3 & 4 & 1 \\ 4 & 8 & 12 & -8 & 2 \\ 2 & 3 & 2 & 1 & 3 \\ -3 & -1 & 1 & -4 & 4 \end{array}\right)$$

Dokončení příkladu

použití LU-rozkladu s částečnou pivotací

máme řešit soustavu $A\mathbf{x} = \mathbf{b}$ s regulární maticí A

známe rozklad $PA = LU$

soustava je ekvivalentní soustavě $PA\mathbf{x} = P\mathbf{b}$

vektor $P\mathbf{b}$ snadno spočteme

soustavu $LU\mathbf{x} = P\mathbf{b}$ vyřešíme přímou a zpětnou substitucí

Použití matic - obsah

Úložiště dat

mnohá data jsou přirozeně uspořádaná do matic

ceny akcií:

řádky $\approx$ akcie sloupce $\approx$ dny

a_{ij} závěrečná cena i-té akcie v j-tém dni

přijímací řízení: část je formou pohovoru

skupina tří porotců hodnotí uchazeče ve 12 kritériích

hodnocení můžeme uložit do tří matic A, B, C podle porotců

$A = (a_{ij})$, kde a_{ij} je hodnocení i-tého posluchače v j-tém kritériu

Vstupy do výroby

nějaká korporace vyrábí řadu produktů

k jejich výrobě používá mnoho vstupů (materiál, součástky, pracovní síly, energie, vodu, atd.)

materiálovou náročnost výroby lze zapsat do matice $A = (a_{ij})$

- a_{ij} je počet jednotek vstupu j potřebných k výrobě produktu i

může být někdy $a_{ij} < 0$?

- vektor vstupů $\mathbf{x}$: x_j označuje cenu jednotky vstupu j

co znamená součin $A\mathbf{x}$?

který produkt má výrobní cenu nejcitlivější na cenu vody ?

Digitální foto

digitální fotoaparát zaznamenává pro každý pixel jeho barvu

každou barvu lze složit ze tří barev - R,G,B

intenzita každé ze tří barev v daném pixelu je zaznamenána pomocí 1 bytu, čili posloupností 8 nul a jedniček

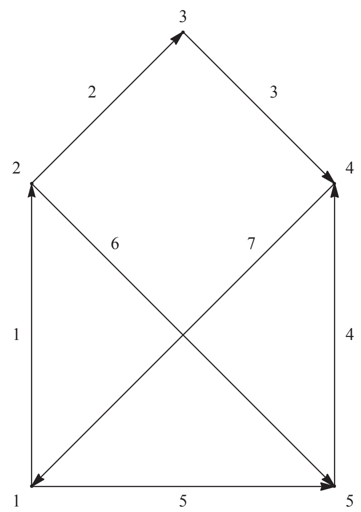
ty jsou ukládány pro každou ze tří barev do samostatné matice jako celá čísla mezi -127 a $+128$

jedna fotka vyrobená fotoaparátem, který má 8 Mpixelů, by tak vyžadovala paměť velikosti 24 MB

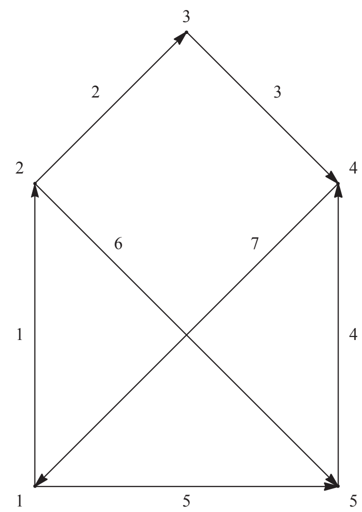
na disk velikosti 1 GB bychom mohli uložit 40 fotek

fotky se proto *komprimují*, nejznámější komprimační formát je *jpeg*

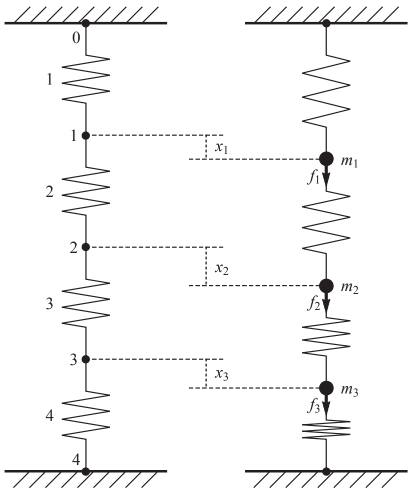
Matice grafu



Jiná matice grafu



Pružiny



Matice A

Hookeův zákon

vnitřní síly v pružinách

vektor vnitřních sil působících na spoje

Rovnovážný stav

Kapitola 5

Lineární prostory

Pojem lineárního prostoru - obsah

Operace s vektory

těleso je abstrakce počítání s reálnými čísly

lineární prostor je abstrakce počítání s aritmetickými vektory

operace s aritmetickými vektory

počítání s reálnými funkcemi jedné reálné proměnné

Definice lineárního prostoru

definice: *Lineární prostor nad tělesem nad tělesem* $\mathbf{T}$ je množina V spolu s binární operací $+$ na V a operací $\cdot$ násobení prvků množiny V prvky tělesa $\mathbf{T}$, které splňují následující axiomy

(vS1) pro libovolné $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ platí $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$

(vS2) existuje $\mathbf{o} \in V$ takový, že pro libovolné $\mathbf{v} \in V$ platí $\mathbf{v} + \mathbf{o} = \mathbf{v}$

(vS3) pro každé $\mathbf{v} \in V$ existuje $-\mathbf{v} \in V$ takové, že $\mathbf{v} + (-\mathbf{v}) = \mathbf{o}$

(vS4) pro libovolné $\mathbf{u}, \mathbf{v} \in V$ platí $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$

(vN1) pro libovolné $\mathbf{v} \in V$ a $a, b \in T$ platí $a \cdot (b \cdot \mathbf{v}) = (a \cdot b) \cdot \mathbf{v}$

(vN2) pro libovolné $\mathbf{v} \in V$ platí $1 \cdot \mathbf{v} = \mathbf{v}$

(vD1) pro libovolné $\mathbf{v} \in V$ a $a, b \in T$ platí $(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$

(vD2) pro libovolné $\mathbf{u}, \mathbf{v} \in V$ a $a \in T$ platí $a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$

Poznámky k definici lineárního prostoru

- lineární prostor $\mathbf{V}$ je množina V **spolu s operacemi**
- prvkům tělesa $\mathbf{T}$ budeme říkat *skaláry*
- prvkům množiny V budeme říkat *prvky prostoru* $\mathbf{V}$
- místo $a \cdot \mathbf{v}$ budeme psát $a\,\mathbf{v}$
- $\mathbf{v} \cdot a$ ani $\mathbf{v}a$ **není definované**
- lineární prostor má vždy aspoň jeden prvek $\mathbf{o}$
- v definici vystupují dvě nuly – nulový skalár $0 \in \mathbf{T}$ a nulový prvek $\mathbf{o} \in \mathbf{V}$
- v lineárním prostoru lze definovat lineární kombinace:

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k$$

- součet lineárních kombinací a skalární násobek lineární kombinace jsou opět lineární kombinace

Příklady lineárních prostorů

- *aritmetický vektorový prostor* $\mathbf{T}^n$
- prostor $\mathbf{T}^{m\times n}$ matic typu $m \times n$ nad $\mathbf{T}$
- prostor $\mathbf{P}$ polynomů s reálnými koeficienty
- prostor $\mathbf{P}_{10}$ polynomů stupně nejvýše 10 s reálnými koeficienty
- prostor $\mathbf{F}$ reálných funkcí jedné reálné proměnné
- prostor $\mathbf{C}\langle 0,1\rangle$ spojitých reálných funkcí na intervalu $\langle 0,1\rangle$
- prostor $\mathbf{C}(0,1)$ diferencovatelných funkcí na intervalu $(0,1)$

Jednoduché důsledky axiomů lineárního prostoru

tvrzení: v každém lineárním prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ platí

1. nulový prvek $\mathbf{o}$ je určený jednoznačně
2. rovnice $\mathbf{u} + \mathbf{x} = \mathbf{v}$ má pro pevná $\mathbf{u}, \mathbf{v} \in V$ právě jedno řešení, speciálně, opačný prvek $-\mathbf{v}$ je prvkem $\mathbf{v}$ určen jednoznačně
3. $0\mathbf{v} = \mathbf{o}$ pro libovolný prvek $\mathbf{v} \in V$
4. $a\mathbf{o} = \mathbf{o}$ pro libovolný skalár $a \in T$
5. je-li $a\mathbf{v} = \mathbf{o}$, pak buď $a = 0$ nebo $\mathbf{v} = \mathbf{o}$
6. $-\mathbf{v} = (-1)\mathbf{v}$ pro libovolný prvek $\mathbf{v} \in V$, speciálně $-(-\mathbf{v}) = \mathbf{v}$

Podprostory - obsah

Definice podprostoru

definice: je-li **V** lineární prostor nad **T**, pak lineární prostor **U** nad tělesem **T** je *podprostorem* **V**, pokud $U \subseteq V$ a operace $+$ a $\cdot$ v **U** se shodují s příslušnými operacemi ve **V**; **zápis**: $\mathbf{U} \leq \mathbf{V}$

budeme také říkat, že *podmnožina* $U \subseteq V$ je podprostor **V**

tvrzení: je-li **V** vektorový prostor nad tělesem **T**, pak neprázdná podmnožina U množiny V je podprostorem **V** právě tehdy, když

- („uzavřenost na sčítání“) pro libovolné $\mathbf{u}, \mathbf{v} \in U$ platí $\mathbf{u} + \mathbf{v} \in U$
- („uzavřenost na násobení skalárem“) pro libovolné $\mathbf{v} \in U$ a $a \in T$ platí $a\mathbf{v} \in U$.

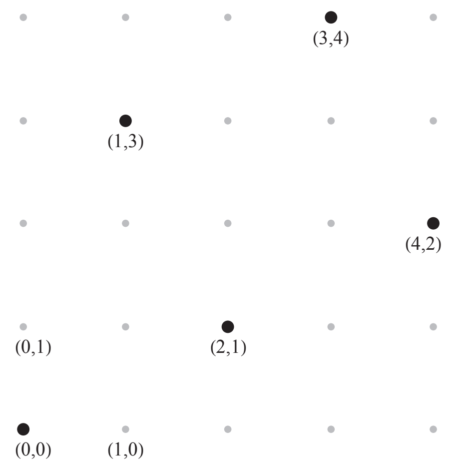
Důkaz

triviální podprostory prostoru V

Podprostory $\mathbb{R}^2$

Podprostory $\mathbb{R}^3$

Přímka v $\mathbb{Z}_5^2$



Jádro matice je podprostor

tvrzení: pro libovolnou matici A typu $m \times n$ nad $\mathbf{T}$ je jádro $Ker\ A$ podprostor $\mathbf{T}^n$

důkaz:

otázka: umíme popsat $Ker\ A$ pomocí zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$?

Lineární kombinace a lineární obal

definice: jsou-li $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ prvky lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$ a $t_1, t_2, \ldots, t_k \in \mathbf{T}$ skaláry, pak prvek

$$t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_k\mathbf{v}_k$$

se nazývá *lineární kombinace prvků* $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in \mathbf{V}$ s koeficienty $t_1, t_2, \ldots, t_k$

Lineární kombinaci prázdného systému vektorů definujeme jako nulový vektor.

definice: je-li $\mathbf{V}$ lineární prostor nad $\mathbf{T}$ a $X \subseteq V$, pak *lineárním obalem množiny* X rozumíme množinu $\langle X \rangle$ všech možných lineárních kombinací prvků X, tj.

$$\langle X \rangle = \{t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_k\mathbf{v}_k : k \in \mathbb{N}_0,\ \mathbf{v}_1, \ldots, \mathbf{v}_k \in X,\ t_1, \ldots, t_k \in T\}$$

Lineární obal je podprostor

tvrzení: pro každou podmnožinu X lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$ je lineární obal $\langle X \rangle$ podprostor $\mathbf{V}$

důkaz:

Co je lineární obal

tvrzení: je-li $\mathbf{V}$ lineární prostor nad $\mathbf{T}$ a $X \subseteq U \leq \mathbf{V}$, pak $\langle X \rangle \subseteq \mathbf{U}$

důkaz:

důsledek: lineární obal $\langle X \rangle$ je nejmenší podprostor $\mathbf{V}$ obsahující množinu X

Rovnost lineárních obalů

tvrzení: jsou-li X, Y dvě podmnožiny lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$, pak platí

$$\langle X \rangle \subseteq \langle Y \rangle \quad \text{právě když pro každé} \quad x \in X \quad \text{platí} \quad x \in \langle Y \rangle$$

důkaz:

příklad: $\left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}, \begin{pmatrix} 9 \\ 12 \\ 15 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \right\rangle$

Generátory

definice: říkáme, že množina X *generuje* lineární prostor $\mathbf{V}$ nad tělesem $\mathbf{T}$, pokud $\langle X \rangle = V$

také říkáme, že X je *množina generátorů prostoru* $\mathbf{V}$

vždy X generuje $\langle X \rangle$

příklady: co generují následující množiny ?

- prázdná množina $\emptyset \subseteq \mathbf{V}$
- $\{\mathbf{e}_1, \mathbf{e}_2\} = \{(0,1)^T, (1,0)^T\} \subseteq \mathbf{T}^2$
- $\{(1,2,3)^T\} \subseteq \mathbb{R}^3$
- $\{1, x, x^2\} \subseteq \mathbf{P}$

Prostor posloupností reálných čísel

symbolem $\mathbb{R}^\infty$ označujeme lineární prostor všech posloupností reálných čísel s přirozenými operacemi

příklad: množina všech posloupností konvergujících k 0 je

příklad: co generuje množina

$$\{(1,0,0,0,\dots),(0,1,0,0,\dots),(0,0,1,0,\dots),\ \dots\} \subseteq \mathbb{R}^\infty \ ?$$

Lineární obal konečného souboru

tvrzení: je-li $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ posloupnost prvků lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$, pak

$$\langle \mathbf{v}_1, \ldots, \mathbf{v}_k \rangle = \{t_1\mathbf{v}_1 + \cdots + t_k\mathbf{v}_k : t_1, \ldots, t_k \in T\}$$

důkaz:

Sloupcový a řádkový prostor

definice: je-li $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ matice typu $m \times n$ nad $\mathbf{T}$, pak

- *sloupcový prostor matice A* je lineární obal $\langle \mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_n \rangle \subseteq \mathbf{T}^m$; **označení**: $Im\, A$
- *řádkový prostor matice A* je prostor $Im\, A^T = \langle \tilde{\mathbf{a}}_1, \tilde{\mathbf{a}}_2, \cdots, \tilde{\mathbf{a}}_m \rangle \subseteq \mathbf{T}^n$

příklad: pro reálnou matici $A = \begin{pmatrix} 1 & 3 & 4 \\ 2 & 7 & -1 \end{pmatrix}$ je

- $Im\, A =$
- $Im\, A^T =$

Ekvivalentní definice $Im\, A$

pro matici $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ typu $m \times n$ nad $\mathbf{T}$ a $\mathbf{b} \in \mathbf{T}^m$ platí

$\mathbf{b} \in Im\, A$ právě když

tvrzení: soustava lineárních rovnic $A\mathbf{x} = \mathbf{b}$ je řešitelná právě když

Příklad

platí $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in Im\, A$ pro matici $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$?

platí $(7, 8, 9)^T \in Im\, A^T$?

Prostory určené maticí

každá matice A typu $m \times n$ nad tělesem $\mathbf{T}$ určuje čtyři prostory

$Im\, A\,,\ Ker\, A^T \ \leq\ \mathbf{T}^m$

$Im\, A^T,\ Ker\, A\ \leq\ \mathbf{T}^n$

tyto prostory obsahují mnoho důležitých informací o matici A

abychom tyto informace z matice A dostali, budeme zkoumat jak se prostory určené maticí A změní pod vlivem řádkových a sloupcových úprav

Vliv řádkových úprav

tvrzení je-li R regulární matice řádu m a $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ matice typu $m \times n$, obě nad stejným $\mathbf{T}$, pak

- $Ker\,(RA) = Ker\, A$
- $Im\,(RA)^T = Im\, A^T$

důkaz:

Příklad

řádkové úpravy mohou změnit sloupcový prostor $Im\, A$

jednoduchý příklad je reálná matice $A = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$

platí $Im\, A = \left\langle (0,1)^T \right\rangle = \{t(0,1)^T : t \in \mathbb{R}\}$

prohodíme-li v A řádky, dostaneme matici $B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$

$Im\, B = \left\langle (1,0)^T \right\rangle = \{s(1,0)^T : s \in \mathbb{R}\} \neq Im\, A$

podobně jednoduchý výpočet také ukáže $Ker\, A^T \neq Ker\, B^T$

Vliv sloupcových úprav

tvrzení je-li Q regulární matice řádu n a $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ matice typu $m \times n$, obě nad stejným $\mathbf{T}$, pak

- $Im\,(AQ) = Im\, A$
- $Ker\,(AQ)^T = Ker\, A^T$

důkaz:

Lineární (ne)závislost - obsah

Definice lineární (ne)závislosti

definice: je-li $\mathbf{V}$ lineární prostor nad tělesem $\mathbf{T}$, pak posloupnost prvků $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ prostoru $\mathbf{V}$ nazýváme *lineárně závislá*, pokud je některý z prvků $\mathbf{v}_i$ lineární kombinací zbývajících prvků

$$\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \dots, \mathbf{v}_k$$

v opačném případě říkáme, že posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ je *lineárně nezávislá*

příklad: posloupnost aritmetických vektorů

$$\left((1,0,0,0)^T, (0,1,0,0)^T, (0,0,1,0)^T, (0,0,0,1)^T\right)$$

z aritmetického prostoru $\mathbb{Z}_3^4$ je lineárně

Lineární (ne)závislost pomocí lineárního obalu

příklad:

- v libovolném lineárním prostoru $\mathbf{V}$ je posloupnost $(\mathbf{u}, \mathbf{v}, \mathbf{u}+\mathbf{v})$
- v prostoru $\mathbf{F}$ reálných funkcí reálné proměnné je posloupnost

  $(\cos x \sin x + 5, 1, \sin(2x) + 3)$

pozorování: posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ je LN právě když v ní existuje prvek $\mathbf{v}_i$ takový, že

$$\mathbf{v}_i \in \langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \dots, \mathbf{v}_k \rangle$$

což nastane právě když

$$\langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k \rangle = \langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \dots, \mathbf{v}_k \rangle$$

Jednoduché vlastnosti lineární (nezávislosti)

neformálně: posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ je LN právě když každý její prvek zvětší lineární obal ostatních prvků

další jednoduchá pozorování:

- obsahuje-li posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ nulový prvek $\mathbf{o}$, je
- obsahuje-li dva stejné prvky, je
- jsou-li všechny její prvky navzájem různé, je
- jednoprvková posloupnost $\mathbf{v}$ je lineárně nezávislá právě když
- podposloupnost lineárně nezávislé posloupnosti je
- nadposloupnost lineárně závislé posloupnosti je
- lineární (ne)závislost nezávisí na pořadí prvků v posloupnosti

Ekvivalentní podmínky s lineární nezávislostí

věta: pro posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ prvků lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ jsou následující tvrzení ekvivalentní

1. posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ je lineárně nezávislá
2. žádný z prvků $\mathbf{v}_i$ $(1 \le i \le k)$ nelze vyjádřit jako lineární kombinaci předchozích prvků $\mathbf{v}_1, \dots, \mathbf{v}_{i-1}$
3. nulový prvek $\mathbf{o}$ lze vyjádřit jako lineární kombinaci prvků $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k$ pouze triviálním způsobem $\mathbf{o} = 0\mathbf{v}_1 + 0\mathbf{v}_2 + \cdots + 0\mathbf{v}_k$
4. každý prvek $\mathbf{b} \in V$ lze vyjádřit jako lineární kombinaci prvků $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ nejvýše jedním způsobem

Formulaci 3. lze také vyjádřit tak, že pro každé $a_1, a_2, \dots, a_k \in T$ z rovnosti

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k = \mathbf{o} \ ,$$

plyne $a_1 = a_2 = \cdots = a_k = 0$

Důkaz

Příklad

v aritmetickém vektorovém prostoru $\mathbb{Z}_3^4$ zjistíme, je-li posloupnost

$$((1,1,1,1)^T, (1,2,1,1)^T, (0,1,0,1)^T)$$

lineárně nezávislá

Lineární nezávislost posloupnosti aritmetických vektorů

tvrzení: posloupnost sloupcových vektorů matice $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ typu $m \times n$ nad tělesem $\mathbf{T}$ je lineárně nezávislá právě tehdy, když $Ker\, A = \{\mathbf{o}\}$, tj. právě když má soustava $A\mathbf{x} = \mathbf{o}$ pouze triviální řešení $\mathbf{x} = \mathbf{o}$

důkaz:

Elementární úpravy a lineární (ne)závislost

tvrzení: jsou-li $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ matice typu $m \times n$, R regulární matice řádu m a Q regulární matice řádu n, všechny nad stejným tělesem $\mathbf{T}$, pak platí

1. posloupnost $(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n)$ sloupcových vektorů matice A je lineárně nezávislá právě tehdy, když je lineárně nezávislá posloupnost sloupcových vektorů matice AQ
2. posloupnost $(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n)$ sloupcových vektorů matice A je lineárně nezávislá právě tehdy, když je lineárně nezávislá posloupnost sloupcových vektorů matice RA

Důkaz

Důsledek

elementární řádkové úpravy nemění lineární (ne)závislost posloupnosti sloupcových vektorů ani posloupnosti řádkových vektorů matice

elementární sloupcové úpravy nemění lineární (ne)závislost posloupnosti sloupcových vektorů ani posloupnosti řádkových vektorů matice

důkaz:

Znovu Gaussova eliminace a zpětná substituce

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 7 & 9 & 12 \\ 2 & 4 & 8 & 11 & 14 \end{pmatrix}$$

Co ještě plyne z rovnosti $Ker\, A = Ker\,(RA)$

pro každý aritmetický vektor $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T \in \mathbf{T}^n$ platí

$$x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + \cdots + x_n\mathbf{a}_n = \mathbf{o}$$

právě když $(x_1, x_2, \ldots, x_n)^T \in Ker\, A = Ker\,(RA)$, což je právě když

$$x_1(R\mathbf{a}_1) + x_2(R\mathbf{a}_2) + \cdots + x_n(R\mathbf{a}_n) = \mathbf{o}$$

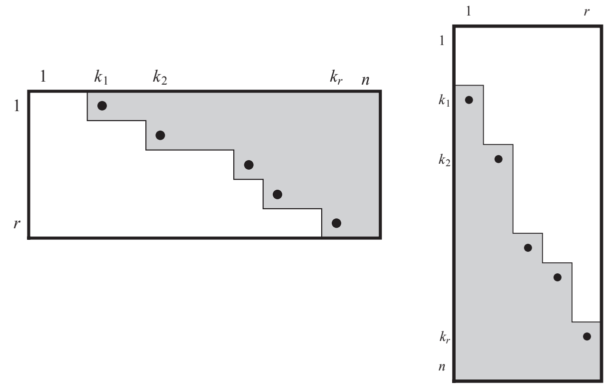
neformálně to lze vyjádřit: „mezi sloupci matice A platí tytéž lineární vztahy jako mezi sloupci matice RA“

například:

Lineární (ne)závislost posloupnosti řádkových vektorů

tvrzení: posloupnost řádkových vektorů matice v odstupňovaném tvaru je lineárně nezávislá právě tehdy, když matice neobsahuje nulový řádek

důkaz:



Příklad

chceme zjistit, je-li posloupnost aritmetických vektorů

$$((1, 37, 3, 45, 1)^T, (0, -e, 1, \pi^e, 4)^T, (0, -12, 0, 33, 2)^T)$$

v prostoru $\mathbb{R}^5$ lineárně závislá nebo nezávislá

Další příklad

zjistíme jiným způsobem, je-li posloupnost vektorů

$$((1, 1, 1, 1)^T, (1, 2, 1, 1)^T, (0, 1, 0, 1)^T)$$

v aritmetickém vektorvém prostoru $\mathbb{Z}_3^4$ lineárně nezávislá

Báze a dimenze - obsah

- *Báze a dimenze*
  - Pojem báze
  - Konečně generované prostory
  - Steinitzova věta o výměně
  - Báze jako systém souřadnic
  - Změna báze
  - Dimenze podprostorů určených maticemi

Definice báze

definice: posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ prvků lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$ se nazývá *báze*, pokud je lineárně nezávislá a současně $\langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \rangle = \mathbf{V}$

ekvivalentní definice: posloupnost prvků $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ tvoří bázi lineárního prostoru $\mathbf{V}$ právě tehdy, když lze každý prvek $\mathbf{b} \in \mathbf{V}$ vyjádřit právě jedním způsobem jako lineární kombinaci prvků $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_n$

Kanonická báze v aritmetickém prostoru $\mathbf{T}^n$

posloupnost sloupcových vektorů jednotkové matice I_n nad $\mathbf{T}$ je báze v aritmetickém prostoru $\mathbf{T}^n$

každý aritmetický vektor $(x_1, x_2, \dots, x_n)^T \in \mathbf{T}^n$ lze vyjádřit

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + x_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

je to báze protože toto vyjádření je jednoznačné

tato báze se nazývá *kanonická báze* v aritmetickém prostoru $\mathbf{T}^n$

budeme ji zapisovat $(\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$

Posloupnost sloupcových vektorů regulární matice nad $\mathbf{T}$

tvrzení: posloupnost $(\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n)$ sloupcových vektorů čtvercové matice $A = (\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_n)$ řádu n nad tělesem $\mathbf{T}$ je báze v aritmetickém prostoru $\mathbf{T}^n$ právě když je matice A regulární

důkaz:

Jsou to báze ?

- posloupnost $((3,3,3)^T)$ v prostoru $\langle (1,1,1)^T \rangle \leq \mathbb{R}^3$
- posloupnost $(1, x, x^2, x^3)$ v prostoru $\mathbf{P}_3$ reálných polynomů stupně ≤ 3
- prázdná posloupnost v triviálním prostoru $\{\mathbf{o}\}$
- posloupnost $((1,2,3)^T, (9,12,15)^T, (4,5,6)^T)$ v prostoru $\mathbf{V} = \langle (1,2,3)^T, (9,12,15)^T, (4,5,6)^T \rangle \leq \mathbb{R}^3$
- posloupnost $((1,2,3)^T, (9,12,15)^T, (4,5,6)^T)$ v prostoru $\mathbf{V}$

Jak najít bázi

najdeme nějakou bázi v prostoru

$$\mathbf{V} = \left\langle \begin{pmatrix} 2 \\ 1 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 5 \\ 0 \end{pmatrix}, \begin{pmatrix} 6 \\ 3 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 6 \\ 6 \end{pmatrix} \begin{pmatrix} 3 \\ 5 \\ 2 \\ 3 \end{pmatrix} \right\rangle \leq \mathbb{Z}_7^4$$

Fibonacci ještě jednou

množina všech posloupností $(a_1, a_2, a_3, \dots)$ reálných čísel splňujících pro každé $n \geq 3$ rovnost

$$a_n = a_{n-1} + a_{n-2}$$

tvoří lineární prostor $\mathbf{V}$ nad $\mathbb{R}$

Fibonacciho posloupnost leží ve $\mathbf{V}$

najdeme nějakou bázi ve $\mathbf{V}$

Záblesk geniality

je ve $\mathbf{V}$ nějaká geometrická posloupnost $(q, q^2, q^3, \dots)$?

číslo q musí splňovat $q^n = q^{n-1} + q^{n-2}$ pro každé $n \geq 3$, tj.

$$q^2 - q - 1 = 0$$

tato kvadratická rovnice má kořeny

$$\varphi = \frac{1+\sqrt{5}}{2} \quad \text{a} \quad \frac{1-\sqrt{5}}{2} = 1 - \varphi$$

v prostoru $\mathbf{V}$ jsou tedy dvě geometrické posloupnosti

$p_1 = (\varphi, \varphi^2, \varphi^3, \dots)$

$p_2 = (1-\varphi, (1-\varphi)^2, (1-\varphi)^3, \dots)$

Posloupnost (p_1, p_2) je báze ve $\mathbf{V}$

(p_1, p_2) je lineárně nezávislá ve $\mathbf{V}$:

$\langle p_1, p_2 \rangle = \mathbf{V}$:

Fibonacciho posloupnost jako lineární kombinace prvků (p_1, p_2)

vyjádříme Fibonacciho posloupnost $a = (1, 1, 2, 3, 5, \dots)$ ve tvaru

$$a = sp_1 + tp_2$$

pro první dva členy musí platit

$$s\varphi + t(1 - \varphi) = 1$$
$$s\varphi^2 + (1 - \varphi)^2 = 1$$

Konečně generované prostory

definice: lineární prostor $\mathbf{V}$ (nad $\mathbf{T}$) se nazývá *konečně generovaný*, pokud má nějakou konečnou množinu generátorů

tvrzení: minimální posloupnost generátorů $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ lineárního prostoru $\mathbf{V}$ je báze $\mathbf{V}$

důkaz:

důsledek 1: z každé konečné množiny generátorů lineárního prostoru lze vybrat bázi

důsledek 2: každý konečně generovaný lineární prostor má bázi

Příklad

najdeme nějakou bázi prostoru

$\mathbf{V} = \langle (1, 2, 3)^T, (9, 12, 15)^T, (4, 5, 6)^T \rangle \leq \mathbb{R}^3$

Steinitzova věta o výměně

věta: je-li $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ lineárně nezávislá posloupnost prvků lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$ a pokud prvky posloupnosti $(\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_l)$ generují $\mathbf{V}$, pak $k \leq l$ a existují prvky $\mathbf{w}_{i_1}, \mathbf{w}_{i_2}, \ldots, \mathbf{w}_{i_{l-k}}$ takové, že posloupnost

$$(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k, \mathbf{w}_{i_1}, \mathbf{w}_{i_2}, \ldots, \mathbf{w}_{i_{l-k}})$$

také generuje $\mathbf{V}$

důkaz:

Dimenze

důsledek: libovolné dvě báze konečně generovaného lineárního prostoru mají stejný počet prvků

důkaz:

definice: *dimenze* konečně generovaného lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$ je počet prvků libovolné báze $\mathbf{V}$; **označení**: $\dim(V)$

příklad: aritmetický vektorový prostor $\mathbf{T}^n$ má dimenzi n

Další příklady

- triviální prostor $\{\mathbf{o}\}$ má dimenzi
- podprostor $\langle (3,3,3)^T \rangle \leq \mathbb{R}^3$ má dimenzi
- $\left\langle \begin{pmatrix} 2 \\ 1 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 5 \\ 0 \end{pmatrix}, \begin{pmatrix} 6 \\ 3 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 4 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 5 \\ 2 \\ 3 \end{pmatrix} \right\rangle \leq \mathbb{Z}_7^4$ má
- prostor $\mathbf{T}^{m \times n}$ matic typu $m \times n$ nad $\mathbf{T}$ má dimenzi
- prostor $\mathbf{P}$ všech polynomů s reálnými koeficienty má dimenzi
- prostor posloupností reálných čísel konvergentních k 0 má dimenzi
- prostor konvergentních posloupností reálných čísel má dimenzi
- prostor reálných funkcí reálné proměnné má dimenzi

Další důsledky

důsledek: je-li X konečná množina generátorů lineárního prostoru $\mathbf{V}$, pak každou lineárně nezávislou posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ prvků $\mathbf{V}$ lze doplnit nějakými prvky X na bázi $\mathbf{V}$

důkaz:

důsledek: maximální (co do počtu prvků) lineárně nezávislá posloupnost v konečně generovaném lineárním prostoru je báze

obecněji, maximální lineárně nezávislá podposloupnost konečné posloupnosti generátorů lineárního prostoru je báze

Příklad

z posloupnosti vektorů generujících podprostor

$$\left\langle \begin{pmatrix} 2 \\ 1 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 5 \\ 0 \end{pmatrix}, \begin{pmatrix} 6 \\ 3 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 6 \\ 6 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \\ 2 \\ 3 \end{pmatrix} \right\rangle \leq \mathbb{Z}_7^4$$

vybereme bázi tohoto podprostoru

Další důsledky Steinitzovy věty

pozorování: v každém lineárním prostoru **V** dimenze n platí

1. každá množina generátorů **V** obsahuje alespoň n prvků
2. každá n-prvková posloupnost generátorů je bází **V**
3. každá lineárně nezávislá posloupnost ve **V** obsahuje nejvýše n prvků
4. každá n-prvková lineárně nezávislá posloupnost ve **V** je bází **V**

důkaz:

Dimenze podprostoru

příklad: v $\mathbb{C}^3$ je posloupnost aritmetických vektorů
$((3i+5,2,3)^T,(5,2+i,1)^T,(4,2,12)^T,(\pi,e^\pi,4)^T)$ lineárně

je $\{(1,3,i+e^\pi,-10)^T,(i,2i,3+2i,-311)^T,(2,\pi,\pi,-4)^T\}$
množinou generátorů aritmetického prostoru $\mathbb{C}^4$?

tvrzení: každý podprostor **W** konečně generovaného lineárního prostoru **V** je také konečně generovaný a platí $\dim \mathbf{W} \leq \dim \mathbf{V}$, přičemž rovnost nastane právě tehdy, když $\mathbf{W} = \mathbf{V}$

Důkaz

Báze jako systém souřadnic

definice: je-li $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ báze lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ a $\mathbf{w} \in \mathbf{V}$, pak *souřadnicemi* (též *vyjádřením*) *prvku* $\mathbf{w}$ *vzhledem k* B rozumíme jednoznačně určený aritmetický vektor $(a_1, a_2, \ldots, a_n)^T \in \mathbf{T}^n$ takový, že

$$\mathbf{w} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n$$

souřadnice $\mathbf{w}$ vzhledem k B označujeme $[\mathbf{w}]_B$, tj.

$$[\mathbf{w}]_B = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = (a_1, a_2, \ldots, a_n)^T$$

souřadnice vektoru vzhledem k bázi závisí na pořadí prvků báze

Příklady

- pro kanonickou bázi $K = (\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)$ v prostoru $\mathbf{T}^n$ a libovolný vektor $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in T^n$ platí
$$\mathbf{v} = v_1\mathbf{e}_1 + v_2\mathbf{e}_2 + \cdots + v_n\mathbf{e}_n \ ,$$
což znamená že $[\mathbf{v}]_K = \mathbf{v}$
- jednou z bází prostoru $\mathbf{V} = \langle (1,2,3)^T, (4,5,6)^T \rangle \leq \mathbb{R}^3$ je posloupnost $B = ((1,2,3)^T, (4,5,6)^T)$, vektor $(9,12,15)^T$ leží ve $\mathbf{V}$, neboť $(9,12,15)^T = (1,2,3)^T + 2 \cdot (4,5,6))^T$; proto
$$[(9,12,15)^T]_B = (1,2)^T$$
- posloupnost $B = (x, x^2, 1)$ je báze v prostoru reálných polynomů stupně nejvýše dva, souřadnice polynomu $a + bx + cx^2$ vzhledem k této bázi je aritmetický vektor
$$[a + bx + cx^2]_B = (b, c, a)^T$$

Jak spočítat souřadnice aritmetického vektoru vzhledem k bázi

příklad: ověříme, že posloupnost

$$B = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) = \left(\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} \right)$$

je báze v prostoru $\mathbb{Z}_5^3$, a najdeme souřadnice vektoru $\mathbf{w} = (4,0,1)^T$ vzhledem k bázi B

Souřadnice součtu a skalárního násobku

tvrzení: je-li $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ báze lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ a $\mathbf{u}, \mathbf{w} \in V$, $t \in T$, pak platí

1. $[\mathbf{u} + \mathbf{w}]_B = [\mathbf{u}]_B + [\mathbf{w}]_B$
2. $[t\mathbf{u}]_B = t[\mathbf{u}]_B$

důkaz:

Konečně generované prostory jsou „v podstatě“ aritmetické

volbou báze v konečně generovaném lineárním prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ se z obecného lineárního prostoru nad $\mathbf{T}$ stává „v podstatě“ aritmetický vektorový prostor $\mathbf{T}^n$

do aritmetického prostoru můžeme „překládat“ i množiny $X \subseteq V$:

$$[X]_B = \{[\mathbf{v}]_B : \mathbf{v} \in X\} \subseteq T^n$$

Několik jednoduchých pozorování

je-li B báze lineárního prostoru $\mathbf{V}$ dimenze n nad tělesem $\mathbf{T}$, pak

1. posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ je lineárně nezávislá ve $\mathbf{V}$ právě tehdy, když je posloupnost $([\mathbf{v}_1]_B, [\mathbf{v}_2]_B, \dots, [\mathbf{v}_k]_B)$ lineárně nezávislá v $\mathbf{T}^n$
2. množina X generuje $\mathbf{V}$ právě tehdy, když $[X]_B$ generuje $\mathbf{T}^n$
3. posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ je báze $\mathbf{V}$ právě tehdy, když je posloupnost $([\mathbf{v}_1]_B, [\mathbf{v}_2]_B, \dots, [\mathbf{v}_k]_B)$ báze $\mathbf{T}^n$

Jak se změní souřadnice prvku, změníme-li bázi

aritmetický vektor $\mathbf{x} = (x_1, x_2, x_3)^T = [\mathbf{x}]_K \in \mathbb{R}^3$ máme zadaný pomocí jeho souřadnic vzhledem ke kanonické bázi $K = (\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$

v prostoru $\mathbb{R}^3$ zvolíme nějakou jinou bázi $B = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$

vzhledem k bázi B má vektor $\mathbf{x}$ souřadnice $[\mathbf{x}]_B = (a_1, a_2, a_3)^T$

to znamená, že $\mathbf{x} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + a_3\mathbf{v}_3$

poslední rovnost přepíšeme pomocí souřadnic vzhledem k bázi K

$$[\mathbf{x}]_K = a_1[\mathbf{v}_1]_K + a_2[\mathbf{v}_2]_K + a_3[\mathbf{v}_3]_K$$

označíme-li $[id]^B_K$ matici $([\mathbf{v}_1]_K \,|\, [\mathbf{v}_2]_K \,|\, [\mathbf{v}_3]_K)$, můžeme poslední rovnost zapsat jako

$$[\mathbf{x}]_K = [id]^B_K \, [\mathbf{x}]_B$$

Matice přechodu a přepočet souřadnic

definice: jsou-li $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ a C dvě báze lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$, pak *matice přechodu od báze B k bázi C* je matice

$$[id]^B_C = ([\mathbf{v}_1]_C \,|\, [\mathbf{v}_2]_C \,|\, \dots \,|\, [\mathbf{v}_n]_C)$$

tvrzení: je-li $\mathbf{V}$ lineární prostor dimenze n nad tělesem $\mathbf{T}$ a B, C dvě báze ve $\mathbf{V}$, pak pro libovolný prvek $\mathbf{x} \in \mathbf{V}$ platí

$$[\mathbf{x}]_C = [id]^B_C [\mathbf{x}]_B$$

navíc je matice $[id]^B_C$ tímto vztahem určena jednoznačně

Důkaz

Příklad

matice přechodu od báze $B = ((1,2)^T, (5,6)^T)$ ke kanonické bázi K prostoru $\mathbb{R}^2$ je

$$[id]_K^B = \begin{pmatrix} 1 & 5 \\ 2 & 6 \end{pmatrix}$$

pro libovolný prvek $\mathbf{x} \in \mathbb{R}^2$ platí

Další příklad

najdeme matici přechodu od báze B k bázi C prostoru $\mathbf{V} \leq \mathbb{R}^3$, kde

$$\mathbf{V} = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\rangle$$

$$B = \left(\begin{pmatrix} 2 \\ 4 \\ 4 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix} \right), \ C = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right)$$

Dokončení příkladu

Bázové sloupce matice

každá matice A typu $m \times n$ nad tělesem $\mathbf{T}$ určuje

- sloupcový prostor $Im\, A \leq \mathbf{T}^m$
- řádkový prostor $Im\, A^T \leq \mathbf{T}^n$

ukážeme, že oba prostory mají stejnou dimenzi

definice: je-li $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ matice nad $\mathbf{T}$, pak říkáme, že i-tý sloupec matice A je *bázový*, pokud není lineární kombinací předchozích sloupců, tj. pokud platí

$$\mathbf{a}_i \notin \langle \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{i-1} \rangle$$

pozorování: pro libovolnou matici A tvoří bázové sloupce bázi sloupcového prostoru $Im\, A$; speciálně, dimenze $Im\, A$ je rovna počtu bázových sloupců matice A

Bázové sloupce a řádkové úpravy

matici $B = (\mathbf{b}_1|\mathbf{b}_2|\cdots|\mathbf{b}_n)$ dostaneme z matice $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ řádkovými úpravami právě když $B = RA$ pro nějakou regulární matici R

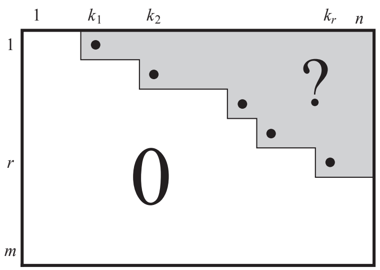
víme už, že v tom případě „mezi sloupci matice A platí tytéž lineární vztahy jako mezi sloupci matice $RA = B$“

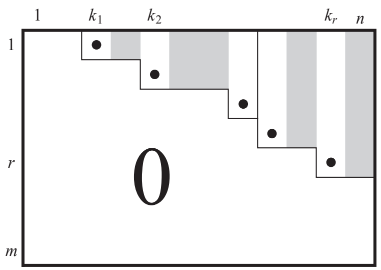
tvrzení: pokud platí $B = RA$ pro nějakou regulární matici R, pak pro každé $i = 1, 2, \ldots, n$ je $\mathbf{a}_i$ bázový sloupec matice A právě když je $\mathbf{b}_i$ bázový sloupec matice B

důkaz:

Bázové sloupce matice v odstupňovaném tvaru

tvrzení: je-li matice $B = (\mathbf{b}_1|\mathbf{b}_2|\cdots|\mathbf{b}_n)$ v odstupňovaném tvaru, pak $\mathbf{b}_i$ je bázový sloupec právě když obsahuje pivot





důkaz:

Příklad

příklad: $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 3 & 6 & 3 & 6 \\ 0 & -2 & -4 & 4 & 2 \end{pmatrix}$

Dimenze sloupcového a řádkového prostoru matice

věta: pro každou matici A nad tělesem $\mathbf{T}$ platí

$$\dim(Im\,A) = \dim(Im\,A^T)$$

myšlenka důkazu: je-li matice v odstupňovaném tvaru, pak rovnost platí, a řádkové úpravy na tom nic nezmění

důkaz: je-li matice B v řádkově odstupňovaném tvaru, pak

- $\dim(Im\,B)$ se rovná počtu bázových sloupců B
- počet bázových sloupců B se rovná počtu pivotů
- počet pivotů se rovná počtu nenulových řádků v B
- nenulové řádky tvoří bázi $Im\,B^T$
- jejich počet se tedy rovná $\dim(Im\,B^T)$

Hodnost matice

dokončení důkazu: matici A převedeme do odstupňovaného tvaru B pomocí řádkových úprav; pak

- $B = RA$ pro nějakou regulární matici R
- bázové sloupce v B mají tytéž indexy jako bázové sloupce v A
- proto $\dim(Im\,A) = \dim(Im\,B)$
- platí $Im\,A^T = Im\,(RA)^T = Im\,B^T$ (bylo dříve)
- takže $\dim(Im\,A) = \dim(Im\,B) = \dim(Im\,B^T) = \dim Im\,(RA)^T = \dim(Im\,A^T)$

definice: *hodnost* matice A definujeme jako dimenzi řádkového (sloupcového) prostoru matice A **označení**: $rank(A)$

Důsledky

1. pro libovolnou matici $A \in \mathbf{T}^{m\times n}$ platí $rank(A) \leq m, n$
2. pro libovolnou matici $A \in \mathbf{T}^{m\times n}$ platí $rank(A) = rank(A^T)$
3. pokud je součin AB matic A, B definován, pak

$$rank(AB) \leq rank(A), \quad rank(AB) \leq rank(B)$$

4. pro regulární matici R řádu n platí $rank(RA) = rank(A)$

Příklad

v závislosti na $a, b \in \mathbb{Z}_3$ určíme dimenzi prostoru

$$\mathbf{V}_{a,b} = \left\langle \begin{pmatrix} a \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ b \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} \right\rangle \leq \mathbb{Z}_3^3$$

Dokkončení příkladu

Dimenze jádra matice

věta o dimenzi jádra a obrazu: pro každou matici A typu $m \times n$ nad $\mathbf{T}$ platí

$$\dim(\mathit{Ker}\, A) = n - \mathit{rank}(A) = n - \dim(\mathit{Im}\, A)$$

důkaz:

Frobeniova věta: soustava lineárních rovnic $A\mathbf{x} = \mathbf{b}$ nad $\mathbf{T}$ je řešitelná právě když $\mathit{rank}(A) = \mathit{rank}(A \mid \mathbf{b})$

Další podmínky ekvivalentní s regularitou

věta pro čtvercovou matici $A \in \mathbf{T}^{n \times n}$ je ekvivalenentní

1. A je regulární
11. $\mathit{rank}(A) = n$
12. posloupnost sloupcových (řádkových) vektorů matice A je lineárně nezávislá
13. sloupce (řádky) matice A generují $\mathbf{T}^n$
14. sloupce (řádky) matice A tvoří bázi $\mathbf{T}^n$

důkaz:

Bezztrátová komprimace dat pomocí skeletního rozkladu

k uložení matice A řádu 10^3 potřebujeme uložit 10^6 prvků

má-li A hodnost 999, stačí uložit

má-li hodnost 998, stačí uložit

má-li hodnost 100, stačí uložit

Skeletní rozklad

tvrzení: každou matici A typu $m \times n$ nad $\mathbf{T}$ s hodností r lze zapsat jako součin součinu $A = CD$, kde C je matice typu $m \times r$ a D je matice typu $r \times n$

důkaz:

Průnik a součet podprostorů - obsah

- *Průnik a součet podprostorů*
  Definice
  Věta o dimenzi součtu a průniku podprostorů
  Direktní součet podprostorů

Součet dvou podprostorů

definice: jsou-li $\mathbf{U}$ a $\mathbf{W}$ dva podprostory lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$, pak definujeme *součet podprostorů* $\mathbf{U} + \mathbf{W}$ jako podprostor $\mathbf{V}$ rovný lineárnímu obalu $\langle U \cup W \rangle$

tvrzení: pro podprostory $\mathbf{U}$, $\mathbf{W}$ lineárního prostoru $\mathbf{V}$ platí

$$\mathbf{U} + \mathbf{W} = \{\mathbf{u} + \mathbf{w} : \mathbf{u} \in U, \mathbf{w} \in W\}$$

důkaz:

Součet libovolného souboru podprostorů

definice: jsou-li $\mathbf{V}_i, i \in I$, podprostory lineárního prostoru $\mathbf{V}$, pak *součtem* (též *spojením*) podprostorů $\mathbf{V}_i, i \in I$, rozumíme lineární obal jejich sjednocení, tj.

$$\sum_{i \in I} \mathbf{V}_i = \left\langle \bigcup_{i \in I} V_i \right\rangle$$

označení: $\sum_{i \in I} \mathbf{V}_i$, součet podprostorů $\mathbf{V}_1, \mathbf{V}_2, \dots, \mathbf{V}_k$ také značíme $\mathbf{V}_1 + \mathbf{V}_2 + \cdots + \mathbf{V}_k$

tvrzení: jsou-li $\mathbf{V}_1, \mathbf{V}_2, \dots, \mathbf{V}_k$ podprostory lin. prostoru $\mathbf{V}$, pak

$$\mathbf{V}_1 + \mathbf{V}_2 + \cdots + \mathbf{V}_k = \{\mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_k : \mathbf{v}_i \in \mathbf{V}_i\}$$

Věta o dimenzi součtu a průniku podprostorů

tvrzení: jsou-li $\mathbf{V}_i, i \in I$, podprostory lineárního prostoru $\mathbf{V}$, pak jejich průnik $\bigcap_{i\in I} V_i$ je také podprostor $\mathbf{V}$

důkaz:

věta o dimenzi součtu a průniku podprostorů: pro libovolné dva konečně generované podprostory $\mathbf{U}, \mathbf{V}$ lineárního prostoru $\mathbf{W}$ platí

$$\dim(\mathbf{U}) + \dim(\mathbf{V}) = \dim(\mathbf{U} \cap \mathbf{V}) + \dim(\mathbf{U} + \mathbf{V})$$

Důkaz

Příklad

určíme dimenzi průniku podprostorů $\mathbf{U}, \mathbf{V} \leq \mathbb{Z}_5^4$:

$$\mathbf{U} = \left\langle \begin{pmatrix} 2 \\ 1 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 3 \\ 3 \end{pmatrix} \right\rangle, \quad \mathbf{V} = \left\langle \begin{pmatrix} 2 \\ 3 \\ 4 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 4 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

napřed zjistíme dimenzi obou podprostorů $\mathbf{U}, \mathbf{V}$

Dokončení příkladu

poté spočítáme dimenzi součtu $\mathbf{U} + \mathbf{V}$

Direktní součet dvou podprostorů

tvrzení: pro podprostory $\mathbf{U}$ a $\mathbf{W}$ konečně generovaného lineárního prostoru $\mathbf{V}$ jsou následující podmínky ekvivalentní

1. $\mathbf{U} + \mathbf{W} = \mathbf{V}$ a $\mathbf{U} \cap \mathbf{W} = \{\mathbf{o}\}$
2. jsou-li $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k)$ báze v $\mathbf{U}$ a $(\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_l)$ báze ve $\mathbf{W}$, pak $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k, \mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_l)$ je báze ve $\mathbf{V}$
3. $\mathbf{V} = \mathbf{U} + \mathbf{W}$ a $\dim \mathbf{V} = \dim \mathbf{U} + \dim \mathbf{W}$
4. $\mathbf{V} = \mathbf{U} + \mathbf{W}$ a pro každé $\mathbf{u} \in \mathbf{U}$ a $\mathbf{w} \in \mathbf{W}$ z rovnosti $\mathbf{u} + \mathbf{w} = \mathbf{o}$ plyne $\mathbf{u} = \mathbf{w} = \mathbf{o}$

důkaz:

Definice direktního součtu

definice: říkáme, že lineární prostor $\mathbf{V}$ je *direktním součtem* podprostorů $\mathbf{W}_1, \mathbf{W}_2, \ldots, \mathbf{W}_k$, pokud platí

1. $\mathbf{V} = \mathbf{W}_1 + \mathbf{W}_2 + \cdots + \mathbf{W}_k$
2. pro každé prvky $\mathbf{w}_i \in \mathbf{W}_i$, $i = 1, 2, \ldots, k$, z rovnosti $\mathbf{w}_1 + \mathbf{w}_2 + \cdots + \mathbf{w}_k = \mathbf{o}$ plyne $\mathbf{w}_1 = \mathbf{w}_2 = \cdots = \mathbf{w}_k = \mathbf{o}$

označení: $\mathbf{V} = \mathbf{W}_1 \oplus \mathbf{W}_2 \oplus \cdots \oplus \mathbf{W}_k$

příklad: posloupnost $(\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k)$ prvků lineárního prostoru $\mathbf{V}$ je báze ve $\mathbf{V}$ právě když

$$\mathbf{V} = \langle \mathbf{w}_1 \rangle \oplus \langle \mathbf{w}_2 \rangle \oplus \cdots \oplus \langle \mathbf{w}_k \rangle$$

Ekvivalentní podmínky s direktním součtem

tvrzení: pro podprostory $\mathbf{W}_1, \mathbf{W}_2, \ldots, \mathbf{W}_k$ konečně generovaného lineárního prostoru $\mathbf{V}$ jsou následující podmínky ekvivalentní

1. $\mathbf{V} = \mathbf{W}_1 + \mathbf{W}_2 + \cdots + \mathbf{W}_k$
2. je-li pro každé $i = 1, 2, \ldots, k$ posloupnost $(\mathbf{w}_1^{(i)}, \mathbf{w}_2^{(i)}, \ldots, \mathbf{w}_{r_i}^{(i)})$ báze podprostoru $\mathbf{W}_i$, pak
$$(\mathbf{w}_1^{(1)}, \mathbf{w}_2^{(1)}, \ldots, \mathbf{w}_{r_1}^{(1)}, \ldots, \mathbf{w}_1^{(k)}, \mathbf{w}_2^{(k)}, \ldots, \mathbf{w}_{r_k}^{(k)})$$
báze ve $\mathbf{W}$
3. $\mathbf{V} = \mathbf{W}_1 + \mathbf{W}_2 + \cdots + \mathbf{W}_k$ a současně $\dim \mathbf{V} = \dim \mathbf{W}_1 + \dim \mathbf{W}_2 + \cdots + \dim \mathbf{W}_k$

Důkaz

Kapitola 6

Lineární zobrazení

Zobrazení - obsah

Zobrazení, jak ho zadat

jsou-li X, Y nějaké množiny, pak *zobrazení* $f : X \to Y$ je „předpis“, který každému prvku $x \in X$ přiřazuje jednoznačně určený prvek $f(x) \in Y$

„předpis“ může mít různou podobu:

- vzorec (formule) – např. $f(x) = |x|$ definuje zobrazení $f : \mathbb{R} \to \mathbb{R}$
- algoritmus – např. hašovací funkce MD5 je složitý algoritmus, který každému vstupu, posloupnosti nejvýše $2^{64} - 1$ bitů, přiřadí výstup délky 128 bitů
- geometrická konstrukce – např. otočení v rovině kolem nějakého bodu o úhel α proti směru hodinových ručiček

Různé předpisy mohou definovat stejné zobrazení

předpisy $f(x) = |x|$ a $g(x) = \sqrt{x^2}$ definují totéž zobrazení z $\mathbb{R}$ do $\mathbb{R}$

stejně tak otočení v rovině kolem daného bodu o úhel α nebo o úhel $\alpha + 2\pi$ definují stejné zobrazení

někdy můžeme nakreslit graf zobrazení, např. pro zobrazení $f : \mathbb{R} \to \mathbb{R}$ definované předpisem $f(x) = x^2$

jindy to nejde, např. pro zobrazení $f : \mathbb{R}^3 \to \mathbb{R}^2$ definované

$$f(x_1, x_2, x_3) = (x_1 x_2 + x_3^3, 5x_1 - x_2^2 x_3)$$

Bramborový pohled na zobrazení

$f : X \to Y$

naše zobrazení jsou vždy definovaná na **celé** množině X

Složené zobrazení

definice: jsou-li $f : X \to Y$ a $g : Y \to Z$ zobrazení, pak definujeme složení $gf : X \to Z$ jako zobrazení, které každému $x \in X$ přiřazuje

$$(gf)(x) = g(f(x)) \in Z$$

Skládání zobrazení je asociativní

tvrzení jsou-li $f : X \to Y$, $g : Y \to Z$ a $h : Z \to W$ zobrazení, pak platí

$$h(gf) = (hg)f$$

důkaz:

Typy zobrazení

definice: zobrazení $f : X \to Y$ je

- *prosté*, pokud z rovnosti $f(u) = f(v)$ plyne $u = v$ pro jakékoliv $u, v \in X$
- *na* Y, pokud pro každé $y \in Y$ existuje $x \in X$ takové, že $f(x) = y$
- *vzájemně jednoznačné*, je-li současně prosté a na Y, tj. pokud pro každé $y \in Y$ existuje právě jedno $x \in X$ takové, že $f(x) = y$

Prosté zobrazení

pozorování: zobrazení $f : X \to Y$ je prosté právě když existuje zobrazení $g : Y \to X$ takové, že $gf = id_X$

důkaz $\Rightarrow$:

$\Leftarrow$:

Zobrazení na

pozorování: zobrazení $f : X \to Y$ je na množinu Y právě když existuje $h : Y \to X$ takové, že $fh = id_Y$

důkaz $\Rightarrow$:

$\Leftarrow$:

Vzájemně jednoznačné zobrazení

pozorování: zobrazení $f : X \to Y$ je vzájemně jednoznačné právě když existuje zobrazení $g : Y \to X$ takové, že $gf = id_X$ a $fg = id_Y$

důkaz: téměř stejný

definice: zobrazení g nazýváme *inverzní zobrazení k f* a označujeme jej f^{-1}

Lineární zobrazení - obsah

Zobrazení určené maticí

už jsme viděli, že matice A typu $m \times n$ nad $\mathbf{T}$ určuje zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ předpisem

$$f_A(\mathbf{x}) = A\,\mathbf{x}$$

mnohé pojmy o maticích mají vysvětlení pomocí zobrazení f_A

součin matic:

inverzní matice:

jádro matice:

sloupcový prostor matice:

hodnost matice:

Definice lineárního zobrazení

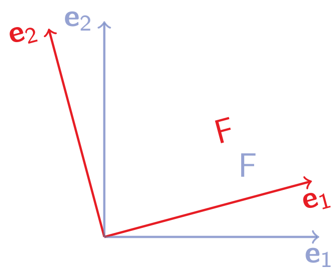
definice: jsou-li $\mathbf{V}, \mathbf{W}$ lineární prostory nad stejným tělesem $\mathbf{T}$, pak zobrazení $f : V \to W$ nazýváme *lineární zobrazení* (nebo *homomorfismus*) z $\mathbf{V}$ do $\mathbf{W}$, pokud

1. $f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v})$ pro libovolné $\mathbf{u}, \mathbf{v} \in V$ a
2. $f(t\mathbf{u}) = tf(\mathbf{u})$ pro libovolné $\mathbf{u} \in V$ a $t \in T$

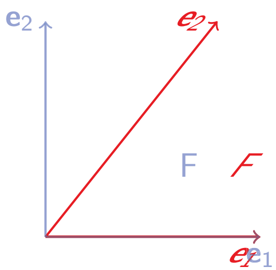
skutečnost, že f je lineární zobrazení z $\mathbf{V}$ do $\mathbf{W}$ zapisujeme $f : \mathbf{V} \to \mathbf{W}$

pozorování: zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ je lineární

Příklady lineárních zobrazení v $\mathbb{R}^2$

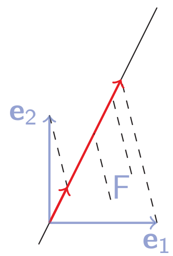


Otočení

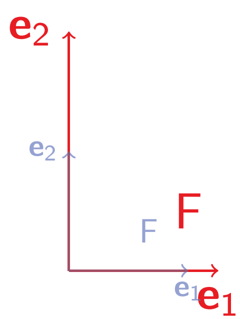


Zkosení

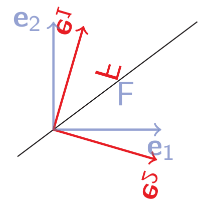
Další příklady lineárních zobrazení v $\mathbb{R}^2$



Projekce

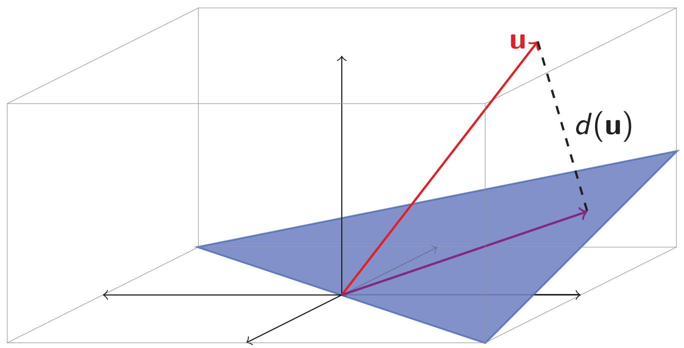


Zvětšení



Osová souměrnost

Lineární zobrazení z $\mathbb{R}^3$ do $\mathbb{R}$



orientovaná vzdálenost od roviny

Další příklady lineárních zobrazení

- identické zobrazení $id_{\mathbf{V}}$ na libovolném lineárním prostoru $\mathbf{V}$
- *nulové zobrazení* 0 z $\mathbf{V}$ do $\mathbf{W}$ přiřazující všem prvkům ve $\mathbf{V}$ nulový prvek ve $\mathbf{W}$
- je-li $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ báze lineárního prostoru $\mathbf{V}$, pak zobrazení f z V do T^n definované $f(\mathbf{v}) = [\mathbf{v}]_B$ je lineární
- zobrazení přiřazující matici nad $\mathbf{T}$ typu $n \times n$ součet prvků na diagonále (tzv. *stopu matice*)
- derivace je lineárním zobrazením (např.) z prostoru reálných diferencovatelných funkcí do prostoru všech reálných funkcí
- zobrazení přiřazující funkci její určitý integrál od 1 do 10 je lineárním zobrazením z prostoru všech reálných integrovatelných funkcí na $[1, 10]$ do $\mathbb{R}$

Lineární zobrazení je určené hodnotami na bázi

pro libovolné lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$ platí

$$f(t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_k\mathbf{v}_n) = t_1 f(\mathbf{v}_1) + t_2 f(\mathbf{v}_2) + \cdots + t_k f(\mathbf{v}_n)$$

pro prvky $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \in V$ a skaláry $t_1, t_2, \dots, t_k \in T$

tvrzení: jsou-li $\mathbf{V}$ a $\mathbf{W}$ lineární prostory nad tělesem $\mathbf{T}$,
$B = (\mathbf{v}_1,\ \mathbf{v}_2,\ \dots,\ \mathbf{v}_n)$ báze v prostoru $\mathbf{V}$,
a $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n \in \mathbf{W}$ libovolné prvky,
pak existuje právě jedno lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$
splňující $f(\mathbf{v}_i) = \mathbf{w}_i$ pro každé $i \in \{1, 2, \dots, n\}$

Důkaz

Lineární zobrazení mezi aritmetickými prostory

tvrzení: je-li $f : \mathbf{T}^n \to \mathbf{T}^m$ lineární zobrazení, pak existuje jednoznačně určená matice $A \in \mathbf{T}^{m \times n}$ taková, že $f = f_A$

důkaz:

Matice lineárního zobrazení

definice: jsou-li $\mathbf{V}, \mathbf{W}$ konečně generované lineární prostory nad tělesem $\mathbf{T}$, $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení, $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ je báze ve $\mathbf{V}$ a C je báze ve $\mathbf{W}$, pak *maticí lineárního zobrazení f vzhledem k bázím B a C* rozumíme matici

$$[f]^B_C = ([f(\mathbf{v}_1)]_C \,|\, [f(\mathbf{v}_2)]_C \,|\, \cdots \,|\, [f(\mathbf{v}_n)]_C)$$

tvrzení: jsou-li $\mathbf{V}, \mathbf{W}$ konečně generované lineární prostory nad tělesem $\mathbf{T}$, $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ báze prostoru $\mathbf{V}$, C báze prostoru $\mathbf{W}$, a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak pro libovolný prvek $\mathbf{x} \in V$ platí

$$[f(\mathbf{x})]_C = [f]^B_C \, [\mathbf{x}]_B \ .$$

Důkaz

Jednoznačnost matice lineárního zobrazení

tvrzení: jsou-li $\mathbf{V}, \mathbf{W}$ konečně generované lineární prostory nad tělesem $\mathbf{T}$, B báze ve $\mathbf{V}$, C báze ve $\mathbf{W}$, $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, a M matice nad tělesem $\mathbf{T}$ splňující $[f(\mathbf{x})]_C = M \, [\mathbf{x}]_B$ pro každý prvek $\mathbf{x} \in \mathbf{V}$, pak $M = [f]^B_C$

důkaz:

Lehké otázky

jsou-li B, C dvě báze lineárního prostoru $\mathbf{V}$, proč značíme matici přechodu od báze B k bázi C právě $[id]^B_C$?

je-li A matice typu $m \times n$ nad $\mathbf{T}$, čemu se rovná $[f_A]^{K_n}_{K_m}$?

Příklad

zobrazení $f : \mathbb{Z}_5^3 \to \mathbb{Z}_5^2$ je dané předpisem

$$f\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2x_1 + 3x_2 + x_3 \\ 4x_1 + 2x_3 \end{pmatrix}$$

určíme matici f vzhledem k bázím

$$B = \left(\begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 4 \end{pmatrix}\right) \quad \text{a} \quad C = \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \end{pmatrix}\right)$$

Dokončení příkladu

Matice rotace v $\mathbb{R}^2$

najdeme znovu matici A takovou, že příslušné zobrazení f_A určené maticí A je rotace o úhel α kolem počátku

Příklad s derivováním polynomů

určíme matici derivace chápané jako lineární zobrazení f z prostoru polynomů stupně nejvýše 3 do stejného prostoru vzhledem k bázím $B = (1, x, x^2, x^3)$ a stejné bázi B

Matice složeného zobrazení

tvrzení: jsou-li $\mathbf{U}, \mathbf{V}, \mathbf{W}$ lineární prostory nad tělesem $\mathbf{T}$ a jsou-li $f : \mathbf{U} \to \mathbf{V}$ a $g : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak složené zobrazení gf je lineární zobrazení $gf : \mathbf{U} \to \mathbf{W}$

jsou-li navíc prostory $\mathbf{U}, \mathbf{V}, \mathbf{W}$ konečně generované a je-li B báze v $\mathbf{U}$, C báze ve $\mathbf{V}$, a D báze ve $\mathbf{W}$, pak platí

$$[gf]^B_D = [g]^C_D \, [f]^B_C$$

důkaz:

Matice inverzního zobrazení

tvrzení: jsou-li $\mathbf{U}, \mathbf{V}$ lineární prostory nad $\mathbf{T}$ a $f : \mathbf{U} \to \mathbf{V}$ vzájemně jednoznačné lineární zobrazení, pak $f^{-1} : \mathbf{V} \to \mathbf{U}$ je také lineární zobrazení

jsou-li navíc $\mathbf{U}, \mathbf{V}$ konečně generované lineátní prostory dimenze n, B báze v $\mathbf{U}$ a C báze ve $\mathbf{V}$, pak platí

$$[f^{-1}]^C_B = \left([f]^B_C\right)^{-1}$$

důkaz:

Příklad

otázka: jsou-li B, C báze v prostoru $\mathbf{V}$, čemu se rovná matice $[id]^B_B$

jaký je vztah mezi maticemi $[id]^B_C$ a $[id]^C_B$?

příklad: najdeme matici symetrie f v $\mathbb{R}^2$ určené přímkou procházející počátkem a bodem $(2, 5)$

Dokončení příkladu

Matice přechodu od báze B ke kanonické bázi K_n v $\mathbf{T}^n$

najdeme matici přechodu od báze

$$B = \left(\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}, \begin{pmatrix} 6 \\ 8 \\ 9 \end{pmatrix} \right)$$

ke kanonické bázi $K = (\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ v prostoru $\mathbb{R}^3$

je-li $B = (\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n)$ báze v aritmetickém prostoru $\mathbf{T}^n$ a $K = (\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$, pak

$[id]^B_K =$

Jeden příklad podruhé

zobrazení $f : \mathbb{Z}_5^3 \to \mathbb{Z}_5^2$ je dané předpisem

$$f \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2x_1 + 3x_2 + x_3 \\ 4x_1 + 2x_3 \end{pmatrix}$$

určíme znovu matici f vzhledem k bázím

$$B = \left(\begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 4 \end{pmatrix} \right) \quad \text{a} \quad C = \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \end{pmatrix} \right)$$

ale jinak

Dokončení příkladu podruhé

Terminologie lineárních zobrazení

definice: jsou-li $\mathbf{V}$, $\mathbf{W}$ lineární prostory nad tělesem $\mathbf{T}$ a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak říkáme že

- f je *monomorfismus*, pokud je f prosté
- f je *epimorfismus*, pokud je f na prostor $\mathbf{W}$
- f je *isomorfismus*, pokud je f je vzájemně jednoznačné
- f je *endomorfismus* prostoru $\mathbf{V}$ (nebo také *lineární operátor* na prostoru $\mathbf{V}$), pokud $\mathbf{V} = \mathbf{W}$
- f je *lineární forma* na $\mathbf{V}$, pokud $\mathbf{W} = \mathbf{T} = \mathbf{T}^1$
- f je *automorfismus* prostoru $\mathbf{V}$, pokud je f izomorfismus a endomorfismus

Matice lineárního operátoru

tvrzení: je-li $\mathbf{V}$ konečně generovaný lineární prostor nad tělesem $\mathbf{T}$, $f : \mathbf{V} \to \mathbf{V}$ lineární zobrazení, B, C dvě báze prostoru $\mathbf{V}$, a R matice přechodu od báze B k bázi C, pak

$$[f]_B^B = R^{-1}\,[f]_C^C\,R$$

důkaz:

Definice jádra a obrazu

definice: je-li $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak *jádro* f je množina

$$Ker\, f = \{\mathbf{x} \in V : f(\mathbf{x}) = \mathbf{o}\} \subseteq \mathbf{V}$$

obraz (obor hodnot) f je množina

$$Im\, f = \{f(\mathbf{x}) : \mathbf{x} \in V\} \subseteq \mathbf{W}$$

pozorování: $Ker\, f$ je podprostor $\mathbf{V}$, $Im\, f$ je podprostor $\mathbf{W}$

důkaz:

Věta o dimenzi jádra a obrazu

věta: je-li $\mathbf{V}$ lineární prostor konečné dimenze n nad tělesem $\mathbf{T}$ a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak

$$\dim(Ker\, f) + \dim(Im\, f) = n$$

důkaz:

Charakterizace monomorfismů pomocí jádra

tvrzení: lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$ je prosté právě tehdy, když $Ker\, f = \{\mathbf{o}\}$

důkaz:

tvrzení: je-li $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení a $f(\mathbf{u}) = \mathbf{b}$, pak

$$\{\mathbf{x} \in \mathbf{V} : f(\mathbf{x}) = \mathbf{b}\} = \mathbf{u} + Ker\, f = \{\mathbf{u} + \mathbf{y} : \mathbf{y} \in Ker\, f\}$$

Důkaz

Jádro a obraz zobrazení pomocí matice

tvrzení: jsou-li $\mathbf{V}, \mathbf{W}$ konečně generované lineární prostory, B báze ve $\mathbf{V}$, C báze ve $\mathbf{W}$ a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak platí

$$[Ker\, f]_B = Ker\, [f]^B_C\ , \quad [Im\, f]_C = Im\, [f]^B_C$$

důkaz:

Příklad

lineární zobrazení $f : \mathbb{R}^3 \to \mathbb{R}^2$ je dáno maticí $[f]^B_C$ vzhledem k následujícím bázím B v $\mathbb{R}^3$ a C v $\mathbb{R}^2$:

$$B = \left(\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \\ 0 \end{pmatrix} \right), \quad C = \left(\begin{pmatrix} 3 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right),$$

$$A = [f]^B_C = \begin{pmatrix} 2 & 1 & -3 \\ -4 & -2 & 6 \end{pmatrix}$$

určíme $Ker\, f$ a $Im\, f$

Dokončení příkladu

Charakterizace monomorfismů pomocí *LN* posloupností

tvrzení: jsou-li $\mathbf{V}$ a $\mathbf{W}$ lineární prostory nad tělesem $\mathbf{T}$, $\mathbf{V}$ konečně generovaný lineární prostor a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak jsou následující tvrzení ekvivalentní

1. zobrazení f je prosté (monomorfismus),
2. pro každou lineárně nezávislou posloupnost $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ ve $\mathbf{V}$ je posloupnost $(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_k))$ lineárně nezávislá ve $\mathbf{W}$,
3. existuje báze $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ prostoru $\mathbf{V}$ taková, že posloupnost $(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n))$ je lineárně nezávislá v $\mathbf{W}$

důkaz:

Dokončení důkazu

Charakterizace epimorfismů pomocí množin generátorů

tvrzení: jsou-li $\mathbf{V}$ a $\mathbf{W}$ lineární prostory nad tělesem $\mathbf{T}$, $\mathbf{V}$ konečně generovaný lineární prostor, a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak jsou následující tvrzení ekvivalentní

1. zobrazení f je na W (epimorfismus),
2. pro každou množinu generátorů $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ ve $\mathbf{V}$ je $\{f(\mathbf{v}_1), \ldots, f(\mathbf{v}_k)\}$ množina generátorů ve $\mathbf{W}$,
3. existuje báze $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ prostoru $\mathbf{V}$ taková, že $\{f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n)\}$ generuje $\mathbf{W}$

důkaz: přečíst ve skriptech

Charakterizace isomorfismů pomocí bází

tvrzení: jsou-li $\mathbf{V}$ a $\mathbf{W}$ lineární prostory nad tělesem $\mathbf{T}$, $\mathbf{V}$ konečně generovaný lineární prostor, a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak jsou následující tvrzení ekvivalentní

1. zobrazení f je izomorfismus,
2. pro každou bázi $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ ve $\mathbf{V}$ je $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_n))$ báze ve $\mathbf{W}$,
3. existuje báze $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ prostoru $\mathbf{V}$ taková, že $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_n))$ je báze ve $\mathbf{W}$.

důkaz:

Isomorfní prostory

definice: říkáme, že dva lineární prostory $\mathbf{V}$ a $\mathbf{W}$ jsou *isomorfní*, pokud existuje isomorfismus $f : \mathbf{V} \to \mathbf{W}$, **píšeme** $\mathbf{V} \cong \mathbf{W}$

isomorfní prostory jsou „v podstatě“ stejné, liší se pouze pojmenováním prvků

příklady isomorfismů

- mezi prostorem $\mathbb{R}_{\leq 4}$ reálných polynomů stupně nejvýše 4 a aritmetickým prostorem $\mathbb{R}^5$
- mezi lineárním prostorem $\mathbf{V}$ dimenze n nad $\mathbf{T}$ a aritmetickým vektorovým prostorem $\mathbf{T}^n$ dimenze n

Vlastnosti isomorfismů

tvrzení: je-li $f : \mathbf{V} \to \mathbf{W}$ izomorfismus konečně generovaných prostorů, pak platí

1. posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ je lineárně nezávislá ve $\mathbf{V}$ právě tehdy, když je posloupnost $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_k))$ lineárně nezávislá v $\mathbf{W}$
2. množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ generuje $\mathbf{V}$ právě tehdy, když množina $\{f(\mathbf{v}_1), \dots, f(\mathbf{v}_k)\}$ generuje $\mathbf{W}$
3. posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ je báze $\mathbf{V}$ právě tehdy, když je posloupnost $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_k))$ báze $\mathbf{W}$
4. $\dim V = \dim W$
5. množina $M \subseteq V$ je podprostorem prostoru $\mathbf{V}$ právě tehdy, když je $f(M) = \{f(\mathbf{m}) : \mathbf{m} \in M\}$ podprostorem prostoru $\mathbf{W}$
6. pokud $\mathbf{U} \leq \mathbf{V}$, pak f zúžené na U je izomorfismem $\mathbf{U} \to f(\mathbf{U})$, speciálně $\dim \mathbf{U} = \dim f(\mathbf{U})$

Kdy jsou dva prostory isomorfní

věta: jsou-li $\mathbf{V}$ a $\mathbf{W}$ dva konečně generované prostory nad tělesem $\mathbf{T}$, pak jsou následující tvrzení ekvivalentní

1. existuje izomorfismus $f : \mathbf{V} \to \mathbf{W}$
2. $\dim \mathbf{V} = \dim \mathbf{W}$

důkaz:

Kapitola 7

Determinanty

Motivace - obsah

- *Motivace*
  Řád 2
  Řád 3

Historie a motivace

definice: determinant čtvercové matice

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

nad tělesem **T** definujeme jako skalár

$$\det A = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

příklad: je-li $\det A \neq 0$, pak

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Cosinová věta pomocí souřadnic

jsou-li $\mathbf{a} = (a_1, a_2)^T$ a $\mathbf{b} = (b_1, b_2)^T$ reálné aritmetické vektory, spočítáme délku vektoru $\mathbf{b} - \mathbf{a}$:

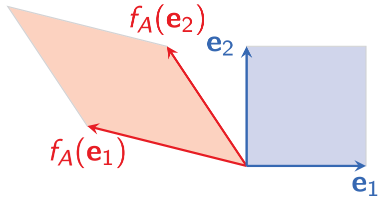
délku vektoru **a** budeme označovat $\|\mathbf{a}\|$, tj.

$$\|\mathbf{a}\| = \sqrt{a_1^2 + a_2^2}$$

Geometrický význam determinantu matice řádu 2

$$A = (\mathbf{a}|\mathbf{b}) = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$$

Geometrický význam znaménka determinantu matice řádu 2

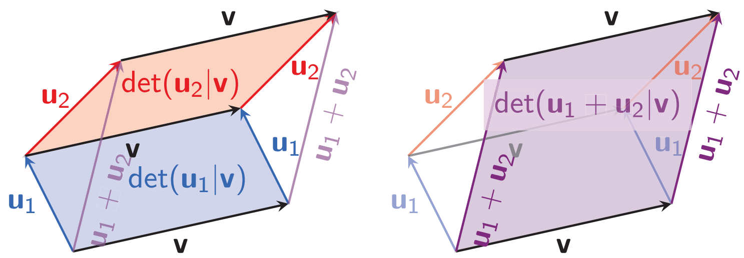


Lineární vlastnosti determinantu matice řádu 2

$$\det(t\mathbf{u}|\mathbf{v}) = t\ \det(\mathbf{u}|\mathbf{v}) = \det(\mathbf{u}|t\mathbf{v})$$

Lineární vlastnosti determinantu matice řádu 2

$$\det(\mathbf{u}_1 + \mathbf{u}_2|\mathbf{v}) = \det(\mathbf{u}_1|\mathbf{v}) + \det(\mathbf{u}_2|\mathbf{v})$$



$$\det(\mathbf{u}|\mathbf{v}_1 + \mathbf{v}_2) = \det(\mathbf{u}|\mathbf{v}_1) + \det(\mathbf{u}|\mathbf{v}_2)$$

Odvození determinantu obecné matice řádu 2

$$\det A = \det(\mathbf{a}_1|\mathbf{a}_2) = \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Definice

definice: pro matici

$$A = (\mathbf{a}_1|\mathbf{a}_2|\mathbf{a}_3) = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

nad tělesem **T** definujeme *determinant* $\det A$ matice A jako skalár

$$a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{11}a_{32}a_{23} - a_{31}a_{22}a_{13} - a_{21}a_{12}a_{33}$$

Geometrický význam

pro reálnou matici $A = (\mathbf{a}_1|\mathbf{a}_2|\mathbf{a}_3)$ řádu 3 očekáváme analogický geometrický význam jaký má determinant matice řádu 2, tj.

1. $|\det A|$ je objem rovnoběžnostěnu s hranami $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{a}_3$
2. znaménko $\det A$ je kladné (záporné), pokud je $(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$ pravotočivý (levotočivý) souřadný systém (báze) v $\mathbb{R}^3$

aby tomu tak bylo, musí platit

Odvození determinantu matice řádu 3

pro determinant matice $A = (\mathbf{a}_1|\mathbf{a}_2|\mathbf{a}_3) = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$

by muselo platit

Permutace - obsah

- *Permutace*
  Definice
  Znaménko permutace
  „15“
  Počet permutací

Definice permutace

definice: *permutace* na množině X je vzájemně jednoznačné zobrazení $\pi : X \to X$

množinu všech permutací na množině X značíme S_X

množinu všech permutací na množině $X = \{1, 2, \ldots, n\}$ označujeme také S_n

- identickou permutaci na množině Z označujeme ι_X
- ke každé permutaci $\pi \in S_X$ existuje *inverzní permutace* $\pi^{-1} \in S_X$
- permutace lze skládat, $\rho\pi$ je *složení* π s ρ

Vlastnosti skládání permutací

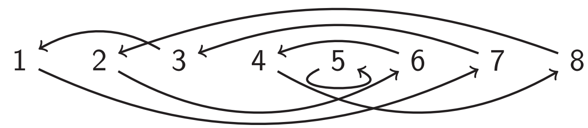
tvrzení: skládání permutací na množině X má následující vlastnosti

1. $\sigma(\rho\pi) = (\sigma\rho)\pi$ pro každé $\sigma, \rho, \pi \in S_X$
2. $\iota_X \pi = \pi \iota_X = \pi$ pro každé $\pi \in S_X$
3. $\pi\pi^{-1} = \pi^{-1}\pi = \iota_X$ pro každé $\pi \in S_X$

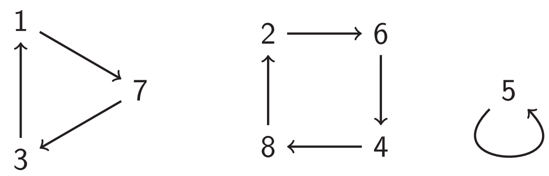
tabulka permutace $\pi \in S_n$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 1 & 8 & 5 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 4 & 7 & 2 & 8 & 1 & 3 & 5 \\ 4 & 8 & 3 & 6 & 2 & 7 & 1 & 5 \end{pmatrix}$$

Graf permutace



když graf trochu překreslíme, vidíme že permutace je sjednocením disjunktních cyklů



Cyklický zápis permutace

definice: *cyklus délky* $k \in \mathbb{N}$ je permutace na X splňující $\pi(x_1) = x_2$, $\pi(x_2) = x_3$, ..., $\pi(x_{k-1}) = x_k$, $\pi(x_k) = x_1$ a $\pi(y) = y$ pro každé $y \in X \setminus \{x_1, x_2, \dots, x_k\}$, kde x_1, x_2, ..., x_k jsou po dvou různé prvky X; zapisujeme $\pi = (x_1\ x_2\ \dots\ x_k)$

cykly nazýváme *nezávislé*, pokud jsou množiny prvků vyskytující se v cyklech disjunktní

transpozice je cyklus délky 2, tj. permutace tvaru $\pi = (x\ y)$

cyklický zápis permutace: každou permutaci na konečné množině lze zapsat jako složení nezávislých cyklů

Příklad

$\pi = (1\ 7\ 3)(2\ 6\ 4\ 8)$, $\quad \pi^{-1} =$

je-li dále $\rho = (1\ 7\ 4\ 6)(2\ 8)(3\ 5)$, pak

$\rho\pi = (1\ 7\ 4\ 6)(2\ 8)(3\ 5)\,(1\ 7\ 3)(2\ 6\ 4\ 8) = (1\ 4\ 2)(3\ 7\ 5)$

zatímco

$\pi\rho =$

pro každou transpozici $(x\ y)$ platí $(x\ y)^{-1} = (x\ y)$

pro každý cyklus $(x_1\ x_2\ \dots\ x_k)$ délky k platí

$(x_1\ x_2\ \dots\ x_k) = (x_1\ x_2)(x_2\ x_3)(x_3\ x_4)\dots(x_{k-2}\ x_{k-1})(x_{k-1}\ x_k)$

Složení permutace s transpozicí

tvrzení: každou permutaci lze složit z transpozic

tvrzení: je-li π permutace na konečné množině X a $(x\ y) \in S_X$ transpozice, pak počet cyklů v permutacích π a $(x\ y)\pi$ se liší o 1; také počet cyklů sudé délky v permutacích π a $(x\ y)\pi$ se liší o 1

důkaz: případ, kdy x, y leží ve stejném cyklu $(x = x_1\ x_2\ \dots\ x_k\ y = y_1\ y_2\ \dots\ y_l)$ permutace π

případ, kdy x, y leží v různých cyklech $(x = x_1\ x_2\ \dots\ x_k)$, $(y = y_1\ y_2\ \dots\ y_l)$

Sudé a liché permutace

důsledek: pro každou permutaci π na konečné množině X nastává právě jedna z následujících možností

1. každé vyjádření π jako složení transpozic obsahuje sudý počet transpozic; nastane to právě tehdy, když počet cyklů sudé délky v (redukovaném) cyklickém zápisu permutace π je sudý
2. každý vyjádření π jako složení transpozic obsahuje lichý počet transpozic; nastane to právě tehdy, když počet cyklů sudé délky v (redukovaném) cyklickém zápisu permutace π je lichý

důkaz: je-li $\pi = \rho_k \rho_{k-1} \cdots \rho_2 \rho_1 \iota_X$, kde ρ_i jsou transpozice, má

- ι_X sudý počet (nula) sudých cyklů
- $\rho_1 \iota_X$ lichý počet (jedna) sudých cyklů
- $\rho_2 \rho_1 \iota_X$ sudý počet sudých cyklů
- atd.
- $\rho_k \rho_{k-1} \cdots \rho_2 \rho_1 \iota_X$ počet sudých cyklů sudý nebo lichý v závislosti na tom, je-li k sudé nebo liché číslo

Znaménko permutace

definice: permutace π na konečné množině X se nazývá *sudá*, pokud nastane možnost (1) v předchozím důsledku; říkámetaké, že *znaménko* π *je* 1 a píšeme $sgn(\pi) = 1$
v opačném případě je π *lichá*, má znaménko -1 a definujeme $sgn(\pi) = -1$

příklad: $sgn((1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9)(10\ 11)) = -1$

pozorování:

- $sgn(\iota_X) =$
- $sgn(\pi^{-1}) =$
- $sgn(\pi\rho) =$

„15“

Počet permutací

počet permutací na n-prvkové množině je

počet sudých permutací na n-prvkové množině je

počet lichých permutací na n-prvkové množině je

tvrzení: pro libovolnou množinu X a permutaci $\pi \in S_X$ jsou následující zobrazení vzájemně jednoznačná

1. $f : S_X \to S_X$ definované předpisem $f(\rho) = \rho^{-1}$
2. $g : S_X \to S_X$ definované předpisem $g(\rho) = \pi\,\rho$
3. $h : S_X \to S_X$ definované předpisem $h(\rho) = \rho\,\pi$

Důkaz

důsledek: je-li X konečná množina s aspoň dvěma prvky, pak počet sudých permutací na množině X se rovná počtu lichých permutací na X

důkaz:

Permutace a permutační matice

příklad: permutační matici jsme definovali jako čtvercovou matici, která má v každém řádku a každém sloupci právě jeden prvek rovný 1 a ostatní 0

každá permutační matice $P = (p_{ij})$ řádu n určuje permutaci $\rho \in S_n$ předpisem

$$\rho(j) = i \quad \text{právě když} \quad p_{ij} = 0$$

naopak, každá permutace $\rho \in S_n$ určuje permutační matici $P_\rho = (p_{ij})$ řádu n předpisem

$$p_{ij} = \begin{cases} 1, & \text{pokud} \quad \rho(j) = i \\ 0, & \text{jinak} \end{cases}$$

Součin matice s permutační maticí

pozorování: je-li $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ matice typu $m \times n$ nad $\mathbf{T}$ a P_ρ permutační matice řádu n, pak

$$A\,P_\rho = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)\,P_\rho = (\mathbf{a} \quad |\mathbf{a} \quad |\cdots|\mathbf{a} \quad)$$

je-li navíc $B = \begin{pmatrix} \tilde{\mathbf{b}}_1^T \\ \tilde{\mathbf{b}}_2^T \\ \vdots \\ \tilde{\mathbf{b}}_n^T \end{pmatrix}$ matice typu $n \times q$, pak

$$P_\rho\,B = P_\rho \begin{pmatrix} \tilde{\mathbf{b}}_1^T \\ \tilde{\mathbf{b}}_2^T \\ \vdots \\ \tilde{\mathbf{b}}_n^T \end{pmatrix} = \begin{pmatrix} \tilde{\mathbf{b}}^T \\ \tilde{\mathbf{b}}^T \\ \vdots \\ \tilde{\mathbf{b}}^T \end{pmatrix}$$

Obecné determinanty - obsah

- *Obecné determinanty*
  Základní vlastnosti
  Vliv elementárních úprav
  Rozvoj determinantu podle řádku nebo sloupce
  Adjungovaná matice
  Vandermondův determinant a sdílení tajemství

Definice

definice: je-li $A = (a_{ij})$ čtvercová matice řádu n nad tělesem $\mathbf{T}$, pak *determinant* matice A definujeme jako

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

příklad: je-li $A = (a_{ij})$ matice řádu 2, pak

$$\det A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12}$$

Determinant matice řádu 3

příklad: je-li $A = (a_{ij})$ matice řádu 3, má množina všech permutací na množině $\{1, 2, 3\}$ celkem 6 prvků

π	$sgn(\pi)$	
ι	1	$a_{11}a_{22}a_{33}$
$(1, 2, 3)$	1	$a_{21}a_{32}a_{13}$
$(1, 3, 2)$	1	$a_{31}a_{12}a_{23}$
$(1, 2)(3)$	-1	$-a_{21}a_{12}a_{33}$
$(1, 3)(2)$	-1	$-a_{31}a_{22}a_{13}$
$(1)(2, 3)$	-1	$-a_{11}a_{32}a_{23}$

proto $\det A = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} =$

$a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{21}a_{12}a_{33} - a_{31}a_{22}a_{13} - a_{11}a_{32}a_{23}$

Determinant trojúhelníkové matice

tvrzení: je-li $A = (a_{ij})$ horní trojúhelníková matice, pak platí $\det A = a_{11}a_{22}\cdots a_{nn}$

důkaz:

Determinant transponované matice

tvrzení: pro každou čtvercovou matici $A = (a_{ij})$ řádu n nad $\mathbf{T}$ platí $\det A = \det(A^T)$

důkaz: označíme $A^T = (b_{ij})$, tedy $b_{ij} = a_{ji}$ pro každé $i, j = 1, \dots, n$

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

Lineární vlastnosti determinantu

tvrzení: pro čtvercovou matici $A = (a_{ij}) = (\mathbf{a}_1|\cdots|\mathbf{a}_n)$ řádu n nad $\mathbf{T}^n$, libovolný vektor $\mathbf{b} = (b_1, \dots, b_n)^T$, každé $j \in \{1, \dots, n\}$ a skalár $t \in \mathbf{T}$ platí

1. $\det(\mathbf{a}_1|\cdots|\mathbf{a}_{j-1}|\mathbf{a}_j + \mathbf{b}|\mathbf{a}_{j+1}|\cdots|\mathbf{a}_n) =$
   $\det(\mathbf{a}_1|\cdots|\mathbf{a}_{j-1}|\mathbf{a}_j|\mathbf{a}_{j+1}|\cdots|\mathbf{a}_n) + \det(\mathbf{a}_1|\cdots|\mathbf{a}_{j-1}|\mathbf{b}|\mathbf{a}_{j+1}|\cdots|\mathbf{a}_n)$
2. $\det(\mathbf{a}_1|\cdots|\mathbf{a}_{j-1}|t\mathbf{a}_j|\mathbf{a}_{j+1}|\cdots|\mathbf{a}_n) =$
   $t\det(\mathbf{a}_1|\cdots|\mathbf{a}_{j-1}|\mathbf{a}_j|\mathbf{a}_{j+1}|\cdots|\mathbf{a}_n) = t\det A$

důkaz:

Další elementární sloupcové a řádkové úpravy

druhá část předchozího tvrzení říká, že pokud vynásobíme nějaký sloupec matice A skalárem t, determinant nové matice získáme tak, že vynásobíme determinant původní matice t

protože $\det A = \det(A^T)$, stejný vliv na hodnotu determinantu matice má vynásobení nějakého řádku matice A skalárem t

tvrzení: prohození dvou řádků čtvercové matice $A = (a_{ij})$ změní znaménko $\det A$; podobně prohození dvou sloupců matice A změní znaménko $\det A$

důkaz:

Dokončení důkazu

Determinant permutační matice

tvrzení: pro permutační matici P_ρ řádu n platí $\det P_\rho = sgn\,\rho$

důkaz:

důsledek: pro každou permutaci $\rho \in S_n$ platí
$\det(\mathbf{a}_{\rho(1)}|\mathbf{a}_{\rho(2)}|\cdots|\mathbf{a}_{\rho(n)}) = sgn\,(\rho)\det(\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$

důkaz:

Pomocné tvrzení

tvrzení: má-li matice $A = (a_{ij}) = (\mathbf{a}_1|\cdots|\mathbf{a}_n)$ nad $\mathbf{T}$ dva stejné sloupce, platí $\det A = 0$

důkaz:

Efekt třetí elementární sloupcové (řádkové) úpravy

tvrzení: přičteme-li v matici $A = (\mathbf{a}_1|\cdots|\mathbf{a}_n)$ násobek jednoho řádku (sloupce) k jinému řádku (sloupci), determinant $\det A$ se nezmění

důkaz: dokážeme pro sloupce a použijeme $\det A = \det(A^T)$

První metoda výpočtu determinantů

známe efekt *eřú* a *esú* na determinant; pomocí těchto úprav matici převedeme do horní trojúhelníkové nebo dolní trojúhelníkové matice a pak vynásobíme prvky na hlavní diagonále

příklad: spočteme

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 4 & 6 \\ 6 & 8 & 9 \end{vmatrix} =$$

Determinanty elementárních matic

tvrzení: pro každou elementární matici E a libovolnou matici A, obě řádu n, platí $\det(EA) = \det(E) \cdot \det(A)$

důkaz: každou elementární matici dostaneme z jednotkové matice I_n jednou *eřú*; $\det I_n = 1$

matici E pro přehození řádků, dostaneme z I_n prohozením dvou řádků, tedy $\det E = -1$ a $\det(EA) = (-1)\det A = \det(E)\det(A)$

matice E pro vynásobení řádku nenulovým skalárem je diagonální, tedy $\det E = t$ a $\det(EA) = t \det A = \det(E)\det(A)$

a nakonec matice E pro přičtení t-násobku jednoho řádku k jinému je horní (nebo dolní) trojúhelníková s jednotkami na hlavní diagonále, proto $\det E = 1$ a $\det(EA) = \det A = \det(E)\det(A)$

Charakterizace regularity pomocí determinantu

tvrzení: pro čtvercovou matici A nad $\mathbf{T}$ je ekvivalentní

1. matice A je regulární

15. $\det A \neq 0$

důkaz: pomocí *eřú* převedeme A do *řot* C

Věta o součinu determinantů

věta: pro každé dvě čtvercové matice A, B řádu n platí
$\det(AB) = \det(A)\det(B)$

důkaz:

geometrický význam věty o součinu determinantů

Důsledky věty o součinu determinantů

důsledek: pro regulární matici A platí $\det(A^{-1}) = (\det A)^{-1}$

důkaz:

důsledek: pro každou permutaci $\rho \in S_n$ platí
$\det(\mathbf{a}_{\rho(1)}|\mathbf{a}_{\rho(2)}|\cdots|\mathbf{a}_{\rho(n)}) = sgn(\rho)\det(\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$

důkaz:

Cramerovo pravidlo

Cramerovo pravidlo: je-li $A = (\mathbf{a}_1|\cdots|\mathbf{a}_n)$ regulární matice řádu n nad tělesem $\mathbf{T}$, $\mathbf{b} \in \mathbf{T}^n$ a $\mathbf{x} = (x_1, \ldots, x_n)^T$ jednoznačně určený vektor řešení soustavy $A\mathbf{x} = \mathbf{b}$, pak platí pro každé $j = 1, \ldots, n$

$$x_j = \frac{\det A_j}{\det A},$$

kde $A_j = (\mathbf{a}_1|\cdots|\mathbf{a}_{j-1}|\mathbf{b}|\mathbf{a}_{j+1}|\cdots|\mathbf{a}_n)$ je matice, kterou dostaneme z A nahrazením j-tého sloupce $\mathbf{a}_j$ sloupcem pravých stran $\mathbf{b}$

důkaz:

Dokončení důkazu Cramerova pravidla

příklad: najdeme druhou složku řešení soustavy $\left(\begin{array}{ccc|c} 1 & 2 & 3 & 2 \\ 4 & 4 & 6 & 4 \\ 6 & 8 & 9 & 0 \end{array}\right)$:

$$\det A = \begin{vmatrix} 1 & 2 & 3 \\ 4 & 4 & 6 \\ 6 & 8 & 9 \end{vmatrix} = 12, \qquad \det A_2 = \begin{vmatrix} 1 & 2 & 3 \\ 4 & 4 & 6 \\ 6 & 0 & 9 \end{vmatrix} = -36,$$

proto $x_2 = -3$

Algebraický doplněk

definice: je-li $A = (a_{ij})$ čtvercová matice řádu n nad $\mathbf{T}$ a $i, j \in \{1, 2, \ldots, n\}$ pak *algebraický doplněk* nebo také *kofaktor* prvku a_{ij} je skalár $m_{ij} = (-1)^{i+j} \det M_{ij}$, kde M_{ij} je matice, kterou dostaneme z A vynecháním i-tého řádku a j-tého sloupce

příklad: v matici $A = (a_{ij}) = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 4 & 6 \\ 6 & 8 & 9 \end{pmatrix}$ spočteme kofaktor

m_{21} prvku a_{21}: $m_{21} = (-1)^{1+2} \begin{vmatrix} 2 & 3 \\ 8 & 9 \end{vmatrix} = (-1)(18 - 24) = 6$

m_{22} prvku a_{22}: $m_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 3 \\ 6 & 9 \end{vmatrix} = 9 - 18 = -9$

Rozvoj determinantu podle sloupce

věta: je-li $A = (a_{ij})$ matice řádu n a $j \in \{1, 2, \ldots, n\}$, pak platí
$\det A = a_{1j} m_{1j} + a_{2j} m_{2j} + \cdots + a_{nj} m_{nj} = \sum_{i=1}^{n} a_{ij} m_{ij}$

důkaz: v každém sčítanci v

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

je právě jeden činitel z j-tého sloupce matice A a to $a_{\pi(j),j}$

pro každý prvek a_{ij} sdružíme sčítance, které prvek a_{ij} obsahují, a vytkneme jej; dostaneme

1. krok důkazu

$$\begin{aligned} \det A &= \sum_{\pi \in S_n} sgn\,(\pi) a_{\pi(1),1} \cdots a_{\pi(n),n} \\ &= \sum_{i=1}^{n} \sum_{\pi \in S_n, \pi(j)=i} sgn\,(\pi) a_{\pi(1),1} \cdots a_{\pi(n),n} \\ &= \sum_{i=1}^{n} a_{ij} \sum_{\pi \in S_n, \pi(j)=i} sgn\,(\pi) a_{\pi(1),1} \cdots a_{\pi(j-1),j-1} a_{\pi(j+1),j+1} \cdots a_{\pi(n),n} \end{aligned}$$

dokážeme, že po vytknutí zůstane součet rovný m_{ij}

1. krok důkazu: budeme předpokládat, že $\mathbf{a}_n = \mathbf{e}_n$ a $j = n$

2. krok důkazu

2. krok důkazu: nyní předpokládáme, že $\mathbf{a}_j = \mathbf{e}_i$ pro $i \in \{1, \ldots, n\}$

matici A upravíme tak, že napřed pomocí $n - j - 1$ transpozic sloupců přesuneme sloupec $\mathbf{a}_j = \mathbf{e}_i$ na místo n-tého sloupce tak, aby se pořadí ostatních sloupců nezměnilo

dále pomocí $n - i - 1$ transpozic řádků upravíme matici tak, aby se poslední sloupec matice rovnal $\mathbf{e}_n$ a pořadí ostatních řádků se nezměnilo; dostaneme tak matici B, jejíž minor N_{nn} se rovná minoru M_{ij} matice A a n-tý sloupec $\mathbf{b}_n = \mathbf{e}_n$; podle 1. kroku

Rozvoj determinantu podle řádku

3. krok důkazu: obecný vektor $\mathbf{a}_j$ matice A se rovná $\sum_{i=1}^{n} a_{ij}\mathbf{e}_i$; pak

opětovným použitím rovnosti $\det A = \det(A^T)$ dostaneme

větu o rozvoji determinantu podle řádku: pro matici A řádu n a libovolné $i \in \{1, 2, \dots n\}$ platí $\det A = \sum_{j=1}^{n} a_{ij} m_{ij}$

Příklad

příklad: spočteme rozvojem podle prvního řádku ještě jednou

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 4 & 6 \\ 6 & 8 & 9 \end{vmatrix} = (-1)^{1+1} \cdot 1 \cdot \begin{vmatrix} 4 & 6 \\ 8 & 9 \end{vmatrix} + (-1)^{1+2} \cdot 2 \cdot \begin{vmatrix} 4 & 6 \\ 6 & 9 \end{vmatrix}$$

$$+(-1)^{1+3} \cdot 3 \cdot \begin{vmatrix} 4 & 4 \\ 6 & 8 \end{vmatrix} = (36 - 48) - 2(36 - 36) + 3(32 - 24) = 12$$

Obecný postup: pro rozvoj determinantu obvykle vybíráme řádek nebo sloupec s velkým počtem prvků rovných 0

takový řádek nebo sloupec často napřed vytvoříme pomocí elementárních řádkových nebo sloupcových úprav

Adjungovaná matice

definice: *kofaktorová matice* ke čtvercové matici $A = (a_{ij})$ je matice $M = (m_{ij})$ tvořená algebraickými doplňky prvků a_{ij}, *adjungovaná matice* k matici A je matice M^T transponovaná ke kofaktorové matici M, **značení**: *adj A*

tvrzení o falešném rozvoji: pro čtvercovou matici A řádu n a libovolné dva různé indexy $k, l \in \{1, 2, \dots, n\}$ platí

$a_{1l}m_{1k} + a_{2l}m_{2k} + \cdots + a_{nl}m_{nk} = \sum_{i=1}^{n} a_{il}m_{ik} = 0$

důkaz:

Formulka pro inverzní matici

tvrzení: pro čtvercovou matici A řádu n platí $\mathit{adj}\,(A) \cdot A = A \cdot \mathit{adj}\,(A) = \det(A) \cdot I_n$

důkaz: prvek na místě (k, l) v součinu $\mathit{adj}\,(A) \cdot A$ se rovná skalárnímu součinu k-tého řádku matice $\mathit{adj}\,A = M^T$ s l-tým sloupcem matice A, tj. k-tého sloupce kofaktorové matice M s l-tým sloupcem matice A

důsledek: je-li matice A regulární, pak platí

$$A^{-1} = \frac{\mathit{adj}\,A}{\det A}$$

Inverzní matice k maticím řádu 2 a 3

pro regulární matici $A = (a_{ij})$ řádu 2 tak platí

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}^{-1} = (\det A)^{-1} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

inverzní matice A^{-1} k regulární matici $A = (a_{ij})$ řádu 3 je

$$(\det A)^{-1} \begin{pmatrix} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} & -\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} & \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \\ -\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} & \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} & -\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} \\ \begin{vmatrix} a_{21} & a_{21} \\ a_{31} & a_{31} \end{vmatrix} & -\begin{vmatrix} a_{11} & a_{12} \\ a_{31} & a_{31} \end{vmatrix} & \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{21} \end{vmatrix} \end{pmatrix}$$

Vandermondova matice

úloha: je dáno těleso $\mathbf{T}$, n jeho navzájem různých prvků $a_1, \ldots, a_n$ a dalších n prvků $b_1, \ldots, b_n \in \mathbf{T}$

máme najít polynom $f(x) = k_0 + k_1 x + \cdots + k_{n-1} x^{n-1}$ stupně nejvýše $n-1$ s koeficienty v tělese $\mathbf{T}$, který v zadaném bodě a_i nabývá předepsané hodnoty b_i pro každé $i = 1, \ldots, n$

řešení: musí platit $f(a_i) = k_0 + k_1 a_i + \cdots + k_{n-1} a_i^{n-1} = b_i$ pro každé $i = 1, \ldots, n$

neznámé koeficienty $k_0, \ldots, k_{n-1} \in \mathbf{T}$ tak musí splňovat soustavu lineárních rovnic

$$\begin{pmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{pmatrix} \begin{pmatrix} k_0 \\ k_1 \\ \vdots \\ k_{n-1} \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

Vandermondův determinant

matice této soustavy se nazývá *Vandermondova matice* a její determinant *Vandermondův determinant*

tvrzení: pro libovolné $n \geq 2$ a prvky $a_1, \ldots, a_n \in \mathbf{T}$ platí

$$V(a_1, a_2, \ldots, a_n) = \begin{vmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (a_j - a_i)$$

důkaz: přečíst ve skriptech

jsou-li prvky $a_1, \ldots, a_n$ navzájem různé, je Vandermondova matice regulární, soustava pro neznámé koeficienty $k_0, \ldots, k_{n-1}$ má jednoznačné řešení a polynom $f(x)$ je proto určený jednoznačně

nazývá se *Lagrangeův interpolační polynom*

Digitální klíče ke korunovačním klenotům

zvolíme nějaké dostatečně velké prvočíslo p, sejf s korunovačními klenoty otevře náhodně zvolené číslo $d \in \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$

klíčník musí informaci o klíči d rozdělit mezi 7 státních a církevních hodnostářů tak, aby jej bylo možné zjistit pouze tehdy, když se všichni sejdou

udělá to tak, že zvolí náhodně koeficienty $k_1, k_2, \ldots, k_6 \in \mathbb{Z}_p$ a získá tím polynom $f(x) = d + k_1 x + \cdots + k_6 x^6$

platí $f(0) = d$

dále zvolí náhodně 7 navzájem různých nenulových čísel $a_1, \ldots, a_7$

i-tému hodnostáři přidělí dvojici $(a_i, b_i = f(a_i))$

Otevírání sejfu

při významné příležitosti se sejde všech 7 hodnostářů

polynom $f(x)$ je jednoznačně určený hodnotami $f(a_i) = b_i$ pro $i = 1, \ldots, 7$, všechny prvky a_i, b_i jsou k dispozici

řešením soustavy na str. 6-54 najdou jednoznačně určený Lagrangeův interpolační polynom f a tedy také klíč $d = f(0)$

Co když je pan president indisponovaný?

zbylých 6 hodnostářů má k dispozici dvojice (a_i, b_i) pro $i = 2, \ldots, 7$

pro jakékoliv $d \in \mathbb{Z}_p$ existuje právě jeden polynom stupně nejvýše 6, pro který platí $f(a_i) = b_i$ pro $i = 2, \ldots, 7$ a $f(0) = d$ (proto jsme volili prvky $a_1, \ldots, a_7$ nenulové)

všechny možné hodnoty klíče jsou při znalosti pouhých šesti dvojic (a_i, b_i) stejně pravděpodobné

bez pana presidenta si ostatní hodnostáři ani neškrtnou