

• Reálný vektor

Def: Reálný vektor b s m složkami je usporiadana m-štrice r.č.:

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} = (b_1, b_2, \dots, b_m)^T, b \in \mathbb{R}^m$$

→ Nulový vektor $0 = (0, 0, \dots, 0)^T \in \mathbb{R}^m$

→ Vektor neznámych $x = (x_1, x_2, \dots, x_m)^T \in \mathbb{R}^m$

• Reálná matica

Def: Reálná matica A ťačka $m \times n$ je súbor $m \cdot n$ reálnych č. usporiadanych do tabuľky s m ťadkami a n sloupcami:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, A \in \mathbb{R}^{m \times n}$$

→ prvky značime a_{ij} , počas jde o nejaký 'složitejší' výraz ako A_{ij}

• Soustava lineárnych rovnic

Def: Nechť $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$ a $x = (x_1, x_2, \dots, x_n)^T$ je vektor neznámych. Soustava m lin. rovnic s n neznámych je

$$Ax = b,$$

Tedy:

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

$\left| \begin{array}{l} A \text{ je matice sústavy} \\ b \text{ je vektor pravých stran} \\ (A|b) \text{ je rozšírená matice sústavy} \end{array} \right.$

→ Vektor $x \in \mathbb{R}^m$ je riesenie sústavy $Ax = b$

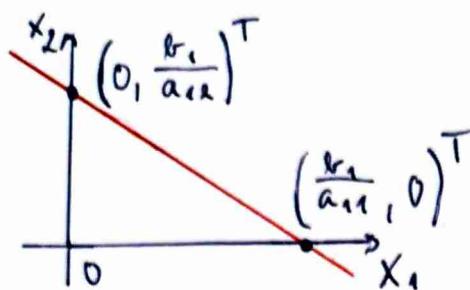
$$\Leftrightarrow \forall i \in \{1, 2, \dots, m\}: a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n = b_i$$

→ Sústavy $Ax = 0$ se nazývají homogenné a medzi uvažují $x = 0$

Geometrický pohled na řešení

1 rovnice o 2 neznámých

$$a_{11}x_1 + a_{12}x_2 = b_1 \equiv (a_{11} \ a_{12}) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ 0 \end{pmatrix}$$



→ je-li $a_{11} \neq 0 \vee a_{12} \neq 0$ pak množina řešení tvoří průsek 2D Eu. rovine
→ změna $b \Rightarrow$ posun průseku

degenerované případy

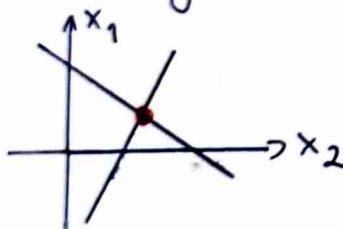
• $a_{11} = a_{12} = 0 \wedge b_1 \neq 0 \Rightarrow$ soustava nemá řešení

• $a_{11} = a_{12} = 0 \wedge b_1 = 0 \Rightarrow$ řešením jsou všechny body roviny

2 rovnice o 2 neznámých

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 &= b_1 \\ a_{21}x_1 + a_{22}x_2 &= b_2 \end{aligned} \equiv \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

① řádky



→ pokud jsou obě rovnice nedegenerované
⇒ průsek 2 průseků

→ více rovnice o 2 neznámých

a, 1. r. \Rightarrow všechny průseků se protínají v 1 bodě

b, ∞ r. \Rightarrow —||— jsou kolmé

c, $\emptyset \Rightarrow$ 2 průseků jsou || nebo rovnoběžné



② sloupec

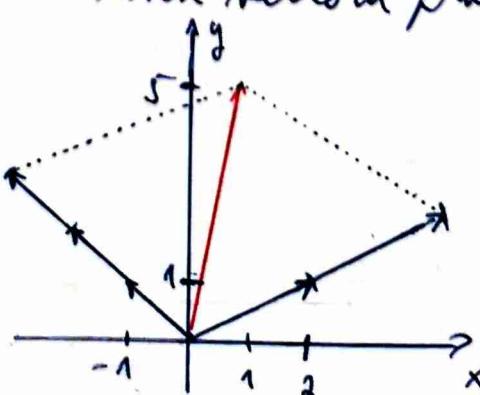
$$x_1 \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix} + x_2 \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

→ hledám takové x_1, x_2 , aby výsledný vektor rektoru na levé straně byl roven rektoru pravé strany

$$2x - y = 1$$

$$x + y = 5$$

$$(, x \begin{pmatrix} 2 \\ 1 \end{pmatrix} + y \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \end{pmatrix})$$



$$\Rightarrow x = 2$$

$$y = 3$$

$$(2, 3)^T$$

• 1 rovnice s 3 neznámých

$$a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = b_1$$

→ v nedegenerovaném případě $a_{11} \neq 0 \vee a_{12} \neq 0 \vee a_{13} \neq 0$ trojí množina řešení rovnice v 3-rozměrném Euklidovském prostoru

→ řádema b ⇒ posun roviny

→ degenerované případy - pro více rovnic o 3 neznámých

- nemá řešení ⇒ 2 roviny jsou II nebo rovná ~~X~~ nebo  nebo $OA = b, b \neq 0.$

- všechny body prostoru: $OA = 0$

• rovnice s 4 a více neznámých ⇒ množina řešení trojní nadvorina

• Elementární ekvivalentní řádkové úpravy

Def: $A \sim A'$ píšeme, pokud lze A' získat z A jednokrát z násil. úprav:

① vynásobení i-tého řádku reálnovým $\lambda \in \mathbb{R} \setminus \{0\}$

$$\hat{a}'_{k\ell} = \begin{cases} a_{k\ell} & \text{pro } k \neq i \\ \lambda \cdot a_{k\ell} & \text{pro } k = i \end{cases} \quad \begin{matrix} \leftarrow \text{nezměnilo} \\ \leftarrow \text{násobilo } \lambda \end{matrix}$$

② přičtení j-tého řádku k i-tému řádku

$$\hat{a}'_{k\ell} = \begin{cases} a_{k\ell} & \text{pro } k \neq i \\ a_{k\ell} + a_{j\ell} & \text{pro } k = i \end{cases} \quad \begin{matrix} \leftarrow \text{nezměnilo} \\ \leftarrow \text{přičtu aje} \end{matrix}$$

③ přičtení j-tého řádku vynásobeného $\lambda \in \mathbb{R}$ k i-tému řádku

- $\lambda = 0$: neděláme nic
- $\lambda \neq 0$: $(\frac{i}{j}) \sim (\frac{i}{\lambda j}) \sim (\frac{i+1}{\lambda j}, j) \sim (\frac{i+1}{j}, j)$

④ zámena dvou řádků

$$(\frac{i}{j}) \sim (\frac{i+j}{j}) \sim (-\frac{i-j}{j}, j) \sim (-\frac{i-j}{-i}, j) \sim (-\frac{i-j}{i}, j) \sim (\frac{-j}{i}, j) \sim (\frac{j}{i})$$

} úpravy ③, ④
lze získat
z úprav ①, ②

→ provedení posloupnosti el. úprav znacíme $A \sim \sim A'$

Použití elementárních úprav

Věta: Nechť $Ax = b$ a $A'x = b'$ jsou dvě soustavy splňující
 $(A|b) \sim \sim (A'|b')$,

pak obě soustavy mají zobecně možné řešení.

Důkaz: Staci' ukázat, že množina řešení je rovnováha pro provedení jediné úpravy ① nebo ②. Chceme ukázat, že platí:

$$\{x \in \mathbb{R}^m \mid Ax = b\} = \{x \in \mathbb{R}^m \mid A'x = b'\}.$$

Rovnost množin plyne ze dvou inequ \subseteq , které přepiseme do implikací:

$$a, Ax = b \Rightarrow A'x = b' \quad b, A'x = b' \Rightarrow Ax = b.$$

1a) $Ax = b \Rightarrow A'x = b'$ pro nynásobení i-tého řádku 1 ≠ 0

→ můžeme pouze i-ty řád \Rightarrow ostatní nemusíme ověřovat

$$a'_i x_1 + a'_{i2} x_2 + \dots + a'_{im} x_m = 1(a_{i1} x_1 + \dots a_{im} x_m) = 1 \cdot b_i = \underline{\underline{b'_i}} \quad \blacksquare$$

1b) $A'x = b' \Rightarrow Ax = b$ pro ①

$$a_{i1} x_1 + a_{i2} x_2 + \dots + a_{im} x_m = \frac{1}{1}(a'_{i1} x_1 + \dots a'_{im} x_m) = \frac{1}{1} b'_i = \underline{\underline{b_i}} \quad \blacksquare$$

2a) $Ax = b \Rightarrow A'x = b'$ pro přičtení j-tého řádku k i-temu

$$\begin{aligned} a'_{i1} x_1 + a'_{i2} x_2 + \dots + a'_{im} x_m &= (a_{i1} + a_{j1}) x_1 + \dots + (a_{im} + a_{jm}) x_m = \\ &= (a_{i1} x_1 + \dots a_{im} x_m) + (a_{j1} x_1 + \dots + a_{jm} x_m) = b_i + b_j = \underline{\underline{b'_i}} \quad \blacksquare \end{aligned}$$

2b) $A'x = b' \Rightarrow Ax = b$ pro ②

$$\begin{aligned} a_{i1} x_1 + a_{i2} x_2 + \dots + a_{im} x_m &= (a'_{i1} - a_{j1}) x_1 + \dots + (a'_{im} - a_{jm}) x_m = \\ &= (a'_{i1} x_1 + \dots + a'_{im} x_m) - (a_{j1} x_1 + \dots + a_{jm} x_m) = \\ &= b'_i - b_j = b_i + b_j - b_j = \underline{\underline{b_i}} \end{aligned}$$

Geometrický význam el. úprav

- ① ④ násobení nebo rozdělení řádku nemění polohu nadroviny
- ② ③ přičtení řádku změněné polohy nadroviny tak, že první řádková bude změny

Gaussova eliminace

① Sestavíme rozšířenou matici soustavy

② Pomocí elementárních úprav přivedeme matici do REF

③ Zpětovou substitucí popíšeme všechna řešení soustavy

Řádkově odstupňovaný tvar matice = REF

Def: Matice A je \sim REF, pokud jsou nenulové řádky seřazeny podle počtu počátečních nul a nulové řádky jsou pod nenulovými

\rightarrow pozice prvního nenulového prvku v i -ém řádku je

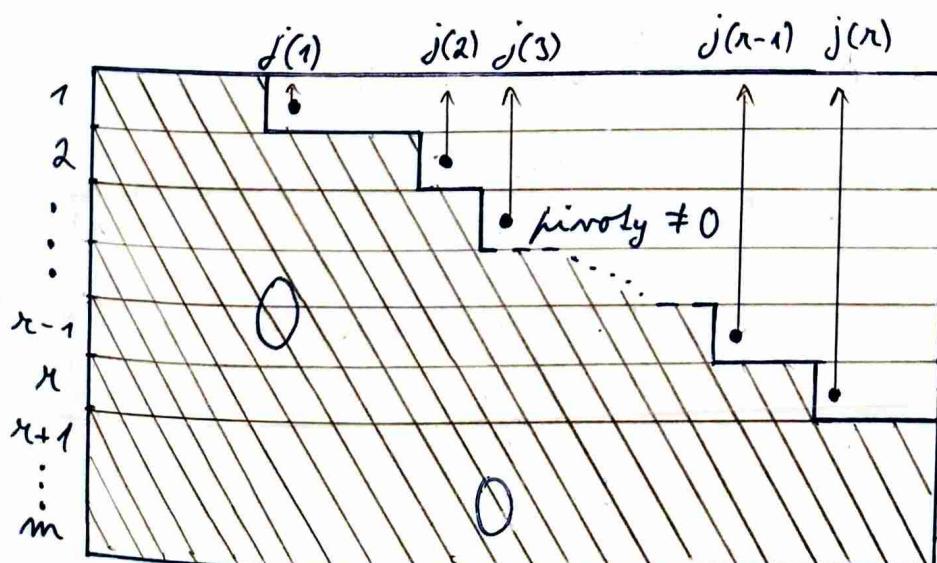
$$j(i) := \min \{ j \mid a_{ij} \neq 0 \}$$

\rightarrow první nenulové prvek $a_{ij(i)}$ se nazývají pivoly

\rightarrow Matice A je \sim REF, když $\exists r \in \{1, 2, \dots, m\}$:

$$a, j(1) < j(2) < \dots < j(r),$$

$$b, \forall i > r, \forall j: a_{ij} = 0.$$



$$\begin{pmatrix} 1 & 0 & 4 \\ 0 & -1 & 2 \\ 0 & 2 & 0 \end{pmatrix}$$

nemí \sim REF

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

je \sim REF

• Naivní algoritmus pro Gaussovu eliminaci

→ Input: Matice A

→ Output: Matice A \sim REF

→ $\forall i \in \{1, \dots, m\}$: určí $j(i)$ # nulový řádek: $j(i) = \infty$

→ Řeřad řádky A podle $j(i)$

→ Forever:

→ if $\exists i : j(i) = j(i+1) < \infty$:

i -tý a $(i+1)$ -mí řádky jsou nenuhore a mají stejný

počet počátečních nul

→ přičti $-\frac{a_{i+1,j(i)}}{a_{i,j(i)}}$ -násobek i -tého řádku k $(i+1)$ -ém řádku

myni: $a_{i+1,j(i)} = 0$

→ aktualizuj $j(i+1)$ a řeřad řádky podle $j(i)$

→ else:

všechny nenuhore řádky mají rovný počet počátečních nul

→ return A

→ Konečnost $\rightarrow O(\frac{n(n-1)}{2}) \in O(n^2)$ aritmetických operací

→ v každé iteraci roste celkový počet počátečních nul

• Zpětná substituce

Značení: $(A' | b')$ je rozšířená matice soustavy $A'x = b'$ \sim REF.

Pozorování: Je-li b' pivot, pak soustava nemá žádne řešení.

Definice: Pro soustavu $A'x = b'$ s $A' \sim$ REF jsou proměnné odpovídající sloupcům s pivots báječky, ostatní jsou volné.

Zpětná substituce

Věta: Pro $A'x = b'$ a $(A'|b') \sim \text{REF}$ a bez pivota v b' lze jakoukoli volbu volných proměnných jednoznačně rozšířit na řešení.

Důkaz: Chceme ukázat, že hodnoty bázičkých proměnných jsou jednoznačné.
 → Indukce podle $i = r, r-1, \dots, 1$.

1) v r-1é rovnici: pivot

$$0x_1 + \dots + 0x_{j(r)-1} + \underbrace{a'_{r,j(r)} x_{j(r)}}_{\text{základní proměnná}} + a'_{r,j(r)+1} x_{j(r)+1} + \dots + a'_{r,n} x_n = b'_r$$

\downarrow volné proměnné

→ hodnoty všech volných proměnných jsou známy

$$\Rightarrow x_{j(r)} = \frac{1}{a'_{r,j(r)}} (b'_r - a'_{r,j(r)+1} x_{j(r)+1} - \dots - a'_{r,n} x_n)$$

2) v i-1é rovnici, $i < r$:

$$0x_1 + \dots + 0x_{j(i)-1} + \underbrace{a'_{i,j(i)} x_{j(i)}}_{\text{pivot}} + a'_{i,j(i)+1} x_{j(i)+1} + \dots + a'_{i,n} x_n = b'_i$$

\downarrow základní proměnná

→ hodnoty všech volných proměnných jsou známy

→ hodnoty všech následujících základních proměnných

$$x_{j(i+1)}, \dots, x_{j(r)}$$

jsou známy z indukčního předpokladu

$$\Rightarrow x_{j(i)} = \frac{1}{a'_{i,j(i)}} (b'_i - a'_{i,j(i)+1} x_{j(i)+1} - \dots - a'_{i,n} x_n)$$

Q.E.D.

Výkazka:

$$(A|b) \sim (A'|b') = \left(\begin{array}{ccccc|c} x_1 & x_2 & x_3 & x_4 & x_5 & \\ \hline 1 & 4 & 3 & 2 & 1 & 1 \\ 0 & 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 6 & 2 \end{array} \right)$$

→ proměnné x_1, x_3, x_5 jsou základní

→ proměnné x_2, x_4 jsou volné

→ Pro libovolné hodnoty v. proměnných, např.
 $x_2 = -1, x_4 = \frac{1}{3}$ dostaneme jednoznačné řešení

$$\text{III: } 6x_5 = 2 \Rightarrow x_5 = \frac{1}{3}$$

$$\text{II: } x_3 + 2 \cdot \frac{1}{3} + \frac{1}{3} = 1 \Rightarrow x_3 = 0$$

$$\text{I: } x_1 + 4(-1) + 3 \cdot 0 + \frac{2}{3} + \frac{1}{3} = 1 \Rightarrow x_1 = 4$$

$$\Rightarrow x = (4, -1, 0, \frac{1}{3}, \frac{1}{3})^T$$

Zpětná substituce

Věta: Zpětnou substitucí lze našest jakéholi řešení.

Důkaz: V libovolném řešení X jsou hodnoty bázičích proměnných X jednoznačně určeny volnými proměnnými x .

Věta: Pro libovolnou matici A a libovolnou A' v REF takovou, že $A \sim A'$ jsou indexy sloupců a ř�ely v A' určeny jednoznačně podle A .

Důkaz: Předpokládejme pro spor, že $A \sim A' \sim A''$. Nechť i je nejvyšší index, kde je charakter proměnných v A' a A'' různý.

Předpokládejme buďto, že x_i je bázička v A' a volná v A'' .

\Rightarrow všechny proměnné x_{i+1}, \dots, x_n mají stejný charakter v A' i v A'' .

\Rightarrow pro libovolnou volbu volných proměnných A' určuje soustava

$A'x = 0$ jednoznačnou hodnotu x_i .

\Rightarrow protože x_i je volná v A'' , můžeme zvolit volné proměnné pro A'' stejně jako nýže (což nám dá stejné hodnoty následujících bázičích proměn.), ale hodnota x_i odlišně

\Rightarrow získáme řešení $A''x = 0$, které ale není řešením $A'x = 0 \Rightarrow$ SPOR

\hookrightarrow v A je rovnice, kde je proměnná x_i u pravé strany:

Q.E.D.

$$0 + 0 + \dots + a_{xi}x_i + a_{xi+1}x_{i+1} + \dots + a_{xn}x_n = 0$$

předem určené & následujících rovnic

\hookrightarrow mym' do této rovnice dodačíme řešení soustavy $A''x = 0$:

$$0 + 0 + \dots + 0 \cdot x'_{i-1} + a_{xi}x'_i + \dots = 0$$

stejně jako

v soustavě $A''x = 0$

je bázičkou proměnná

v k -tém řádku

neníde před x_i

\Rightarrow víme, že $x'_i \neq x_i$, rovnost tedy nerovnost

Hodnot matic

Definice: Hodnot matic A, znacena jalo rank(A) je pocet pivotů
v libovolné A' v REF závore, že $A \sim A'$.

Frobeniova věta

Veta: Soustava $Ax = b$ má řešení právě tehdy, když $\text{rank}(A) = \text{rank}(A|b)$.

Diskaz: Zvolme libovolné $(A'|b')$ v REF závore, že $(A|b) \sim (A'|b')$.

Řešení X existuje $\Leftrightarrow b'$ nemá řádny pivot
 \Leftrightarrow pivotsy A' se shodují s pivotsy $(A'|b')$
 $\Leftrightarrow \text{rank}(A) = \text{rank}(A|b)$. Q.E.D.

Homogenní a nehomogenní soustavy

Pozorování:

$$(A|0) = \left(\begin{array}{ccccc|c} 1 & 4 & 3 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 \end{array} \right) \quad \begin{aligned} h_1 := x_2, h_2 := x_4 \\ \Rightarrow x_5 = 0 \\ \Rightarrow x_3 = -2h_2 \\ \Rightarrow x_1 = -4h_1 - 2h_2 + 6h_2 \end{aligned} \quad \left\{ \begin{aligned} \bar{x} = h_1 \begin{pmatrix} -4 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + h_2 \begin{pmatrix} 4 \\ 0 \\ -2 \\ 1 \\ 0 \end{pmatrix} \\ X = X_0 + \bar{x} \end{aligned} \right.$$

$$(A|b) = \left(\begin{array}{ccccc|c} 1 & 4 & 3 & 2 & 1 & 4 \\ 0 & 0 & 1 & 2 & 1 & 5 \\ 0 & 0 & 0 & 0 & 6 & 6 \end{array} \right) \quad \begin{aligned} \Rightarrow x_5 = 1 \\ \Rightarrow x_3 = 4 - 2h_2 \\ \Rightarrow x_1 = 3 - 2h_2 - 12 + 6h_2 - 4h_1 \end{aligned} \quad \left. \begin{aligned} X = X_0 + \bar{x} \\ x = \begin{pmatrix} -9 \\ 0 \\ 4 \\ 0 \\ 1 \end{pmatrix} + h_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + h_2 \begin{pmatrix} 4 \\ 0 \\ -2 \\ 1 \\ 0 \end{pmatrix} \end{aligned} \right)$$

→ řešení nehomogenní a homogenní soustavy se stejnou maticí soustavy A se liší pouze o rešení X_0 , který je řešením $Ax = b$.

Pozorování: Jestliže X a X_0 jsou dve řešení $Ax = b$, potom $\bar{x} = x - x_0$ je řešením $A\bar{x} = 0$.

Diskaz: $A\bar{x} = A(x - x_0) = Ax - Ax_0 = b - b = 0$ □

Pozorování: Jestliže x_0 je řešením $Ax = b$ a \bar{x} je řešením $A\bar{x} = 0$, pak $x = x_0 + \bar{x}$ je řešením $Ax = b$.

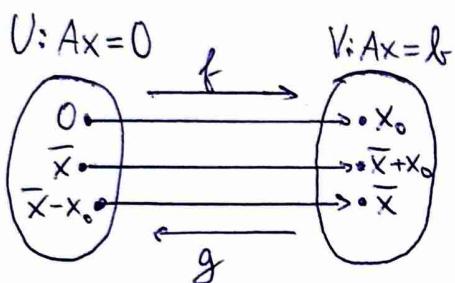
Diskaz: $Ax = A(x_0 + \bar{x}) = Ax_0 + A\bar{x} = b + 0 = b$ □

• Homogenní a nehomogenní soustavy

Věta: Nechť x_0 splňuje $Ax_0 = b$. Pak zobrazení $\bar{x} \mapsto \bar{x} + x_0$ je bijekce mezi množinami $U = \{\bar{x} \mid A\bar{x} = 0\}$ a $V = \{x \mid Ax = b\}$.

Důkaz 1: Označme zobrazení $f: U \rightarrow V$ s.ř. $f(\bar{x}) = \bar{x} + x_0$

$g: V \rightarrow U$ s.ř. $g(x) = x - x_0$.



→ Chceme ukázat, že f je bijekce
 $\Leftrightarrow f$ je prosté a f je "na"

• $f \circ g: U \rightarrow U \rightarrow U$ je identicka na $U \Rightarrow f$ je prosté

↳ kdyby f nebylo prosté, tak se stane $\begin{array}{c} U \\ \odot \end{array} \begin{array}{c} V \\ \odot \end{array}$ a když bych musel 1 vzdoru přiřadit 2 obrazy $\Rightarrow g$ by nebylo zobrazení \Rightarrow SPOR

• $g \circ f: V \rightarrow U \rightarrow V$ je identicka na $V \Rightarrow g$ je prosté $\Rightarrow f$ je "na"

↳ g je prosté \Rightarrow každý bod $\in V$ se zobrazi na právě 1 $\in U$

↳ kdyby f nebylo "na", tak se stane $\begin{array}{c} U \\ \odot \end{array} \begin{array}{c} V \\ \odot \end{array}$ $\Rightarrow f$ by nebylo prosté \Rightarrow SPOR

• f je prosté a f je "na" $\Rightarrow f$ je bijekce Q.E.D.

Důkaz 2: Označme zobrazení $f: U \rightarrow V$ s.ř., že $f(\bar{x}) = \bar{x} + x_0$, ukažeme, že f je bijekce.

• Předpokládejme pro spor, že f nemá prosté

↳ dveřma různým vstupům by přiřadilo stejný výstup

↳ ke vstupu různým $x_0 \Rightarrow$ nemůže pro různé vstupy dostat stejný výstup
 \Rightarrow SPOR

• Uvažme libovolné řešení x soustavy $Ax = b$.

$\Rightarrow x - x_0$ řeší $Ax = 0 \Rightarrow f(x - x_0) = x$

\Rightarrow k libovolnému $x \in V$ jsem našel jeho vztah $\Rightarrow f$ je "na"

• f je prosté a f je "na" $\Rightarrow f$ je bijekce Q.E.D.

• Řešení homogenních soustav

Věta: Je-li $A \in \mathbb{R}^{m \times n}$ matice hodnosti r, pak všechna řešení $A\bar{x}=0$

bude popsat jako $\bar{x} = p_1 \bar{x}^1 + p_2 \bar{x}^2 + \dots + p_{n-r} \bar{x}^{n-r}$, kde

- p_1, p_2, \dots, p_{n-r} jsou libovolné reálné parametry odpovídající volným proměnným
- $\bar{x}^1, \bar{x}^2, \dots, \bar{x}^{n-r}$ jsou vhodná řešení soustavy $A\bar{x}=0$.

Soustava má pouze triviální řešení $\bar{x}=0 \Leftrightarrow \text{rank}(A)=n$.

Důkaz: Prejmenujme volné proměnné na p_1, \dots, p_{n-r} .

Protože hodnoty bázických proměnných jsou jednoznačně určeny rovnici, musíme zároveň složku řešení vyjádřit jeho lineární kombinací s volnými proměnnými

$$\bar{x}_1 = d_{1,1} p_1 + \dots + d_{1,n-r} p_{n-r}$$

⋮

$$\bar{x}_m = d_{m,1} p_1 + \dots + d_{m,n-r} p_{n-r}.$$

→ Zvolíme

$$\bar{x}^1 = (d_{1,1}, \dots, d_{m,1})^T, \dots, \bar{x}^{n-r} = (d_{1,n-r}, \dots, d_{m,n-r})^T$$

→ Tyto nekteré řeší $A\bar{x}=0$, protože každý řádek soustavy \bar{x}^i dostaneme volbou parametru $p_i=1$, $\forall j \neq i: p_j=0$.

→ Je-li $\text{rank}(A)=n$, proměnné jsou jen bázické a 0 je jediné řešení.

• Řešení nehomogenních soustav

Q.E.D.

Důkaz předchozí věty:

Nechť soustava $Ax=b$ má neprázdnou množinu řešení, kde

$A \in \mathbb{R}^{m \times n}$ je matice hodnosti r. Pak všechna řešení $Ax=b$ bude popsat jako

$$x = x^0 + p_1 \bar{x}^1 + p_2 \bar{x}^2 + \dots + p_{n-r} \bar{x}^{n-r}, \text{ kde}$$

- p_1, \dots, p_{n-r} jsou reálné parametry odpovídající volným proměnným
- $\bar{x}^1, \dots, \bar{x}^{n-r}$ jsou vhodná řešení $\underline{Ax=0}$
- x^0 je libovolné řešení soustavy $Ax=b$.

- Buňková řešení soustavy $Ax = b$

① Převедeme rozšířenou matici $(A|b)$ do REF:

$$(A|b) = \left(\begin{array}{ccccc|c} 1 & 4 & 3 & 2 & 1 & 1 \\ 2 & 8 & 4 & 0 & 0 & 0 \\ 0 & 0 & 3 & 6 & 9 & 5 \\ 2 & 8 & 7 & 6 & 3 & 3 \end{array} \right) \sim \left(\begin{array}{ccccc|c} 1 & 4 & 3 & 2 & 1 & 1 \\ 0 & 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 6 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right) = (A'|b')$$

② Pokud je první a poslední sloupec, řádky řešení neexistuje.

③ Liničky řešíme nejdříve homogenní soustavu $A'x = 0$:

$$\bar{x}_3 = 0, \bar{x}_3 = -2\bar{x}_4, \bar{x}_1 = -4\bar{x}_2 - 3\bar{x}_3 - 2\bar{x}_4 = -4\bar{x}_2 + 4\bar{x}_4$$

④ Volné proměnné a popisu řešení \bar{x} nahradíme parametry:

$$\bar{x} = f_1(-4, 1, 0, 0, 0)^T + f_2(4, 0, -2, 1, 0)^T$$

⑤ Nakonec najdeme nějaké řešení nehomogenní soustavy $A'x = b'$

$$x_2 = 0, x_4 = 0 \Rightarrow x_5 = \frac{1}{3}, x_3 = \frac{2}{3}, x_1 = \frac{2}{3} - 2 = -\frac{4}{3}$$

$$\Rightarrow x = \left(-\frac{4}{3}, 0, \frac{2}{3}, 0, \frac{1}{3}\right)^T + f_1(-4, 1, 0, 0, 0)^T + f_2(4, 0, -2, 1, 0)^T$$

Gauss-Jordanova eliminace

Reducovaný odsupínací vektor - RREF

Def: Odsupínací vektor matice je redukovaný, pokud je každý prvotřídelný a všechny ostatní prvky ve sloupcích s prvními jsou nuly.

Věta: Každá matice A má jedinečný RREF A' takový, že $A \sim A'$.

Důkaz: Pro spor budeme předpokládat, že A', A'' jsou r-RREF a $A \sim A''$.

Poslední volnou proměnnou, která má v A' a A'' jiný koeficient označime x_k . Tento koeficient se nachází v nejnížím řádku i, je tedy a'_{ik} , a''_{ik} .

Volbu volných proměnných $x_k = 1$, $x_j \neq 0 : x_j = 0$ dostaneme v i -ém řádku:

$$x_{i,j}(a') + 0 + \dots + a'_{ik} + \dots + 0 = b_i \Rightarrow x_{i,j}(a') = b_i - a'_{ik}, x_{i,j}(a'') = b_i - a''_{ik}$$

Což je spor, protože báciče proměnné jsou všechny rovnou jednoznačné.

Vektor b musí být v A' i A'' stejný, neboť v.p. $x_j : x_j = 0$ bychom dostali spor.

• Libovolnou matici v REF lze redukovat takto

- 1) vydělíme řádky $a_{ij(i)}$, čímž si sláme 1 jako pivolg.
- 2) pro každé $i = r, \dots, 1$, eliminujeme každý $a_{ij(i)}$ s $i' < i$ přičtením $-a_{ij(i)}$ násobku i -tého řádku k i' -tému řádku, čímž nad pivolem $a_{ij(i)}$ dostaneme nuly.

• Výhody RREF

→ vhodnou volbou volných proměnných lze RREF snadno přečíst řešení

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

1, volba $x_2 = x_4 = 0$ dává prům. řešení $Ax = b$:

$$x_0 = \left(-\frac{4}{3}, 0, \frac{2}{3}, 0, \frac{1}{3} \right)^T$$

2, volba $x_2 = 1, x_4 = 0$ dává prům. první vhodné řešení $Ax = 0$:

$$\text{I: } x_1 + 4 + 0 + 0 + 0 = 0 \Rightarrow x_1 = -4 \Rightarrow \bar{x}^1 = (-4, 1, 0, 0, 0)^T$$

3, volba $x_2 = 0, x_4 = 1$ dává prům. druhé vhodné řešení $Ax = 0$

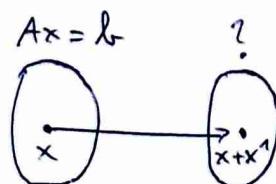
$$\text{I: } x_1 + 0 + 0 - 4 + 0 = 0 \Rightarrow x_1 = 4$$

$$\text{II: } x_3 + 2 + 0 = 0 \Rightarrow x_3 = -2 \Rightarrow \bar{x}^2 = (4, 0, -2, 1, 0)^T$$

→ když chceme nějaké vhodné řešení $Ax = 0$, tak si vyberu proměnnou, třeba $x_4 \rightarrow 4.$ sloupec → a hodnoty bázičích proměnných = - hodnoty ne 4. sl.

• Příklad

Označme $V = \{x \mid Ax = b\}$ a myslme $x^* \in V$. Jaky je obraz množiny V
v zobrazení $x \mapsto x + x^*$?



$$Ax = b \rightarrow A(x + x^*) = Ax + Ax^* = b + b$$

$$\Rightarrow \text{obrazem } V \text{ je } \{x \mid Ax = b + b\}$$

Operace s maticemi

Nulová matice

Def: Pro libovolné $m, n \in \mathbb{N}$ definujeme nulovou matici

$O_{m,n} \in \mathbb{R}^{m \times n}$ takovou, že splňuje $\forall i,j : (O_{m,n})_{i,j} = 0$. $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = O_{3,3}$

Jednotková matice - unit matrix

Def: Pro $n \in \mathbb{N}$ je jednotková matice $I_n \in \mathbb{R}^{n \times n}$ definovaná jako $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3$

$$(I_n)_{i,j} = 1 \text{ pro } i=j; \text{ a jinak } (I_n)_{i,j} = 0.$$

Hlavní diagonála

Def: Hlavní diagonální čívercové matice A svou prvek $a_{i,i}$.

Transponovaná matice

Def: Transponovaná matice k matici $A \in \mathbb{R}^{m \times n}$ je matice $A^T \in \mathbb{R}^{n \times m}$ splňující $(A^T)_{ij} = a_{ji}$.
 $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \rightarrow A^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$

Symetrická matice

Def: Čtvercová matice A je symetrická, pokud $A^T = A$, tedy $a_{ij} = a_{ji}$.

Součet matic

Def: Součet matic $A, B \in \mathbb{R}^{m \times n}$ je matice $(A+B) \in \mathbb{R}^{m \times n}$ definovaná
 $(A+B)_{i,j} = a_{ij} + b_{ij}$.

Násobek matice

Def: α -násobek matice $A \in \mathbb{R}^{m \times n}$, $\alpha \in \mathbb{R}$ je $(\alpha A) \in \mathbb{R}^{m \times n}$ taková, že
 $(\alpha A)_{i,j} = \alpha \cdot a_{ij}$.

Součin matic

Def: Pro $A \in \mathbb{R}^{m \times n}$, $B \in \mathbb{R}^{n \times k}$ je součin $(AB) \in \mathbb{R}^{m \times k}$ definován

$$(AB)_{ij} = \sum_{k=1}^n a_{ik} b_{kj} \rightarrow \text{složitý součin i-ého řádu A a j-ého s. B}$$

Díl:

$$A = \begin{pmatrix} 1 & 2 & 4 & 0 \\ 0 & 0 & 1 & 3 \\ 3 & 1 & 2 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 \\ 0 & 3 \\ 2 & 0 \\ 0 & 1 \end{pmatrix} \quad AB = \begin{pmatrix} 9 & 6 \\ 2 & 3 \\ 7 & 9 \end{pmatrix}$$

	1	2
	0	3
	2	0
	0	1
1	2	4 0 9 6
0	0	1 3 2 3
3	1	2 0 7 9

Průběhem: Maticevý součin AB pro $A \in \mathbb{R}^{m \times n}$, $B \in \mathbb{R}^{n \times k}$ významuje

- $m \cdot n \cdot k$ sčítání → A má $m \cdot n$ prvek, každý množením s B prvek
- $m \cdot k \cdot (n-1)$ sčítání → pro $m \cdot k$ prvek počítáme sumu n členů

⇒ Celkov. $m \cdot k \cdot (2n-1) = 2mnk - mk \approx mnk$ aritmetických operací

Vlastnosti pro operace s maticemi

Tvrdění: Jsou-li následující operace definovány, platí:

- ① $(A+B)+C = A+(B+C)$ Dle: $((A+B)+C)_{ij} = a_{ij} + b_{ij} + c_{ij} = (A+(B+C))_{ij}$ ■
- ② $A+B = B+A$ Dle: $(A+B)_{ij} = a_{ij} + b_{ij} = b_{ij} + a_{ij} = (B+A)_{ij}$ ■
- ③ $\exists ! B: A+B = A \wedge A+0 = A$ Dle: $A+B = A \Leftrightarrow a_{ij} + b_{ij} = a_{ij} \Leftrightarrow b_{ij} = 0$ ■
- ④ $\alpha(\beta A) = (\alpha\beta)A$ Dle: $(\alpha(\beta A))_{ij} = \alpha \cdot (\beta A)_{ij} = \alpha \cdot \beta \cdot a_{ij} = (\alpha\beta) \cdot A$ ■
- ⑤ $(\alpha+\beta)A = \alpha A + \beta A$ Dle: $((\alpha+\beta)A)_{ij} = (\alpha+\beta)a_{ij} = \alpha a_{ij} + \beta a_{ij} = \alpha A + \beta A$ ■
- ⑥ $(A+B)^T = A^T + B^T$ Dle: $((A+B)^T)_{ij} = (A+B)_{ji} = a_{ji} + b_{ji} = (A^T)_{ij} + (B^T)_{ij} = A^T + B^T$ ■
- ⑦ $(\alpha A)^T = \alpha A^T$ Dle: $((\alpha A)^T)_{ij} = (\alpha A)_{ji} = \alpha a_{ji} = \alpha (A^T)_{ij} = \alpha A^T$ ■
- ⑧ $(A^T)^T = A$ Dle: $((A^T)^T)_{ij} = (A^T)_{ji} = a_{ij}$ ■

Vlastnosti produktu matic

① Vražde, že AAT^T je symetrická pro libovolné A

$$A \in \mathbb{R}^{m \times m}, A^T \in \mathbb{R}^{n \times m} \Rightarrow AA^T \in \mathbb{R}^{m \times m}, AA^T \text{ je symetrická}$$

$$\left. \begin{aligned} (AA^T)_{ij} &= \sum_{k=1}^m (A)_{ik} \cdot (A^T)_{kj} = \sum_{k=1}^m a_{ik} \cdot a_{jk} \\ (AA^T)_{ji} &= \sum_{k=1}^m (A)_{jk} \cdot (A^T)_{ki} = \sum_{k=1}^m a_{jk} \cdot a_{ki} \end{aligned} \right\} \Leftrightarrow (AA^T)_{ij} = (AA^T)_{ji} \quad \square$$

② Vražde, že pro libovolnou $A \in \mathbb{R}^{m \times n}$ platí $I_m A = A I_m = A$

$$(I_m A)_{ij} = \sum_{k=1}^n (I_m)_{ik} \cdot (A)_{kj} = (I_m)_{ii} \cdot a_{ij} = a_{ij}, \text{ protože } (I_m)_{ik} = 0 \text{ } i \neq k$$

$$(A I_m)_{ij} = \sum_{k=1}^m a_{ik} \cdot (I_m)_{kj} = a_{ij} \cdot (I_m)_{jj} = a_{ij} \quad \square$$

→ Najděte čtvercové matice A, B takové, že $AB \neq BA$

$$A = \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} \quad \begin{array}{c|cc} 12 & & 10 \\ 34 & & 20 \\ \hline 10 & 12 & 12 \\ 20 & 34 & 110 \end{array} \quad AB = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

$$B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad BA = \begin{pmatrix} 5 & 0 \\ 11 & 0 \end{pmatrix}$$

Tvrdění: Dostali jsme sledovány operace definované, pak:

① $(AB)^T = B^T A^T$ $A \in \mathbb{R}^{m \times n} \Rightarrow B \in \mathbb{R}^{n \times k} \Rightarrow B^T \in \mathbb{R}^{k \times n} \wedge A^T \in \mathbb{R}^{n \times m}$

$$\text{Dle: } ((AB)^T)_{ij} = (AB)_{ji} = \sum_{k=1}^n a_{jk} b_{ki} = \sum_{k=1}^n b_{ki} a_{jk} = \sum_{k=1}^n (B^T)_{ik} (A^T)_{kj} = (B^T A^T)_{ij} \quad \square$$

② $(AB)C = A(BC)$ $A \in \mathbb{R}^{m \times n} \Rightarrow B \in \mathbb{R}^{n \times k} \Rightarrow C \in \mathbb{R}^{k \times q} \Rightarrow AB \in \mathbb{R}^{m \times k}, BC \in \mathbb{R}^{n \times q}$

$$\begin{aligned} \text{Dle: } ((AB)C)_{ij} &= \sum_{k=1}^k (AB)_{ik} c_{kj} = \sum_{k=1}^k \left(\sum_{l=1}^m a_{il} b_{lk} \right) c_{kj} = \sum_{k=1}^k \sum_{l=1}^m a_{il} b_{lk} c_{kj} = \\ &= \sum_{l=1}^m \sum_{k=1}^k a_{il} b_{lk} c_{kj} = \sum_{l=1}^m \left(a_{il} \sum_{k=1}^k b_{lk} c_{kj} \right) = \sum_{l=1}^m a_{il} (BC)_{lj} = \\ &= (A(BC))_{ij} \quad \square \end{aligned}$$

$$\textcircled{3} \quad \underline{(A+B)C = AC + BC} \quad A \in \mathbb{R}^{m \times m} \Rightarrow B \in \mathbb{R}^{m \times n} \Rightarrow C \in \mathbb{R}^{n \times k}$$

$$(A+B)_{ij} = \sum_{\ell=1}^n (A+B)_{i\ell} C_{\ell j} = \sum_{\ell=1}^n (a_{i\ell} c_{\ell j} + b_{i\ell} c_{\ell j}) = (AC)_{ij} + (BC)_{ij} = (AC + BC)_{ij} \blacksquare$$

$$\textcircled{4} \quad \underline{A(BC) = AB + AC} \quad A \in \mathbb{R}^{m \times m} \Rightarrow B, C \in \mathbb{R}^{m \times k}$$

$$(A(BC))_{ij} = \sum_{\ell=1}^m a_{i\ell} (BC)_{\ell j} = \sum_{\ell=1}^m (a_{i\ell} b_{\ell j} + a_{i\ell} c_{\ell j}) = (AB)_{ij} + (AC)_{ij} = (AB + AC)_{ij} \blacksquare$$

Efektivita výpočtu součinu

$$\rightarrow A \in \mathbb{R}^{m \times m}, B \in \mathbb{R}^{m \times n}, C \in \mathbb{R}^{n \times q} : (AB)C = A(BC)$$

B	C
A	AB

AB	(AB)C
----	-------

$AB \approx mnq$
 $(AB)C \approx mpq$

$BC \approx npq$
 $A(BC) \approx mnpq$

$\left\{ \begin{array}{l} mp(m+q) \text{ aritmetických operací} \\ mq(p+m) \text{ arit. operací} \end{array} \right.$

\rightarrow i když je konečný výsledek rovnou směrem stejný, vhodné pořadí dílčích součinů může ovlivnit celkovou výpočetní náročnost

Elementární matice

Przorování: Nechť B je matice výsledkem n řad směrem stejný, vzhodné pořadí dílčích součinů může ovlivnit celkovou výpočetní náročnost

1) Vynásobení i -tého řádku $\rightarrow E$ je jednotková matice s $E_{ii} = 1$ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$
řádku číslem $1 \neq 0$.

2) Přičtení j -tého řádku $\rightarrow E$ je jednotková matice s $E_{ij} = 1$ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
řádku k i -tému

3) Přičtení k -násobku j -tého řádku k i -tému řádku $\rightarrow E$ je jednotková matice s $E_{ij} = 1$ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

4) Zámena i -tého a j -tého řádku $\rightarrow E$ je jednotková matice
 $\rightarrow E_{ii} = E_{jj} = 0, E_{ij} = E_{ji} = 1$ $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$

Inverzní matice

Def: Pokud pro $A \in \mathbb{R}^{n \times n}$ existuje $B \in \mathbb{R}^{n \times n}$ taková, že $AB = I_n$,
poté se B nazývá inversní matice a značí se A^{-1}

Regulární a Singulární matice

Def: Pokud má A inverzi, poté se nazývá regulární, jinak je singulární.

Věta: $A \in \mathbb{R}^{n \times n}$ je regulární

$$1. \ Leftrightarrow \exists B \in \mathbb{R}^{n \times n}: AB = BA = I_n$$

$$2. \ Leftrightarrow \text{rank}(A) = n$$

$$3. \ Leftrightarrow A \sim I_n$$

$$4. \ Leftrightarrow Ax = 0 \text{ má pouze triviální řešení } x = 0.$$

Důkaz:

$$2. \Rightarrow 4. \text{ je triviální}$$

$$2. \Rightarrow 3. \text{ pomocí Gaus-Jordanovy eliminace, } 3 \Rightarrow 2 \text{ triviálně}$$

$$1. \text{ Inverzní matice splňuje } A^{-1}A = I_n$$

→ nejprve ukažeme, že A^{-1} je regulární

$$\rightarrow \text{pokud } A^{-1}x = 0 \text{ má řešení, poté } x = I_n x = A A^{-1}x = A(A^{-1}x) = A0 = 0. \quad (4.)$$

→ existuje řešení $(A^{-1})^{-1}$ a dostáváme

$$A^{-1}A = A^{-1}A I_n = A^{-1}A(A^{-1}(A^{-1})^{-1}) = A^{-1}(I_n)(A^{-1})^{-1} = A^{-1}(A^{-1})^{-1} = I_n \blacksquare$$

$$2. \Rightarrow 1. \text{ Označime } I_n = (e^1 | e^2 | \dots | e^n). \text{ Pro } i = 1, \dots, n \text{ uvažme soustavy} \\ Ax^i = e^i. \text{ Z } \text{rank}(A) = n \text{ dostaneme } B = (x^1 | x^2 | \dots | x^n).$$

1. \Rightarrow 2. Pro spor budeme předpokládat $\text{rank}(A) < n$, poté pro nějaké i může být i -tý řádek A eliminován oslabnoucí řádky.

Během řešení $Ax^i = e^i$ by i -tý řádek byl $0, 0, \dots, 0/1$, takže
 $Ax^i = e^i$ nemá žádné řešení $\Rightarrow A$ nemá inverzi \Rightarrow SPOR

Důsledek: Existuje-li inverzní matice, poté je jednoznačná.

Výpočet inversní matice

$$(A | I_m) \sim\sim (I_m | A^{-1})$$

Dle: Provádění elementárních úprav odpovídá mísťbene' el. maticemi

$$(A | I_m) \sim\sim (I_m | B)$$

$$\left. \begin{array}{l} \hookrightarrow E_1 \dots E_2 E_1 A = I_m \Rightarrow A^{-1} = E_1 \dots E_2 E_1 \\ \hookrightarrow E_1 \dots E_2 E_1 I_m = B \Rightarrow B = E_1 \dots E_2 E_1 \end{array} \right\} B = A^{-1}$$

→ sloupcy B jsou re řešenosti soustav $Ax^i = e^i$.

Vlastnosti regulární matice

• Kráćení matic: Pokud je R regulární, pak:

$$1, AR = BR \Leftrightarrow A = B. \quad \text{Dle: } A = A I_m = A R R^{-1} = B R R^{-1} = B I_m = B$$

$$2, RA = RB \Leftrightarrow A = B. \quad \text{Dle: } A = I_m A = R^{-1} R A = R^{-1} R B = I_m B = B$$

• Regulární matice A, B stejného řádu splňují

$$1, (A^{-1})^{-1} = A. \quad \text{Dle: } (A^{-1})^{-1} = (A^{-1})^{-1} A^{-1} A = I_m A = A$$

$$2, (AB)^{-1} = B^{-1} A^{-1}. \quad \text{Dle: } (AB)^T = B^{-1} B (AB)^{-1} = \underline{B^{-1}} (\underline{A^{-1} A}) B (AB)^{-1} = \underline{B^{-1} A^{-1}} I_m = B^{-1} A^{-1}$$

$$3, (A^T)^{-1} = (A^{-1})^T. \quad \text{Dle: } A A^{-1} = A^{-1} A = I_m \Rightarrow (AA^{-1})^T = (A^{-1} A)^T = I_m^T$$

$$\Rightarrow (A^{-1})^T A^T = A^T (A^{-1})^T = I_m \Rightarrow (A^T)^{-1} = (A^{-1})^T$$

$$4, AB \text{ je regulární.} \quad \text{Dle: } A A^{-1} = I_m \Rightarrow A B B^{-1} A^{-1} = I_m \Rightarrow (AB)^{-1} = B^{-1} A^{-1}$$

Maticeřnice

$$A + X = B \Rightarrow X = B - A = B + (-1)A$$

$$\alpha X = B \Rightarrow X = \frac{1}{\alpha} B$$

$$\left. \begin{array}{l} AX = B \\ XA = B \end{array} \right\} \Rightarrow X = A^{-1} B \quad \text{pro regulární } A$$

• Binární operace

Def: Binární operace na množině X je zobrazení $X \times X \rightarrow X$.

Príklady: $+, -, \cdot$ na \mathbb{R}

$\rightarrow + : \text{na } \mathbb{R} \setminus \{0\} \text{ nebo } \mathbb{R}^+$, ale ne na \mathbb{R}

$\rightarrow +, \cdot : \text{na } \mathbb{N}$, $-$ a \cdot nejsou bin. operace na \mathbb{N}

\rightarrow maticový součet na maticích stejného řádu

\rightarrow součin na čtvercových maticích stejného řádu

$\rightarrow (a, b) \rightarrow b$ je bin. operace na libovolné množině

$\rightarrow (f, g) \rightarrow r$, kde $\forall x \in \mathbb{R} : r(x) = f(x) + g(x)$ je binární operace na množině všech reálných funkcí $\mathbb{R}[x]$

• Grupa

Def: Grupa (G, \circ) je množina G a binární operace \circ na G splňující:

1, $\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c) \rightarrow \circ$ je asociativní

2) $\exists e \in G : \forall a \in G : a \circ e = e \circ a = a \rightarrow$ existuje neutralní prvek

3) $\forall a \in G : \exists b \in G : a \circ b = b \circ a = e \rightarrow b = a^{-1}$ je inverzní prvek k a

• Abelovská grufa

nejmenší grufa je $(\{e\}, \circ)$

Def: Grupa (G, \circ) je abelovská, pokud

$\forall a, b \in G : a \circ b = b \circ a \rightarrow \circ$ je komutativní na G

• Aditivní grupy

Def: Grupy (G, \circ) , kde \circ je odvozena od sčítání se nazývají aditivní.

$\Rightarrow (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{R}[x], +), (\mathbb{R}^{m \times n}, +)$ jsou aditivní

$\rightarrow (\mathbb{N}, +)$ není grufa, nesplňuje axiom inverze

\rightarrow Neutralní prvek se nazývá neutralní prvek a znací se 0.

\rightarrow Inverzní prvek se nazývá opacny a namísto a^{-1} se znací $-a$.

\rightarrow Lze rozést binární operaci rozdíl jako $a - b := a + (-b)$.

$\rightarrow (G, -)$ není grufa, nesplňuje asociativitu

Multiplicativní grupy

- Def: Grupy (G, \circ) , kde \circ je odvozena od součinu se nazývají multiplicativní
- $\Rightarrow (\mathbb{R} \setminus \{0\}, \cdot)$, (\mathbb{Q}^+, \cdot) , $(\{-1, 1\}, \cdot)$, $(\{z \in \mathbb{C}, |z|=1\}, \cdot)$ jsou abelovské mult.
 - $\rightarrow (\mathbb{R}, \cdot)$ není grupa, protože 0 nemá inverzi
 - $\rightarrow (\mathbb{R}^{n \times n}, \cdot)$ je m. grupa pro regulární matice.
 - \rightarrow neutrální prvek je nejdří vžací 1
 - \rightarrow lze rozložit podíl jako $a:b = a \cdot b^{-1}$.

Vlastnosti grup

Pozorování: Neutrální prvek je určen jednoznačně.

Důkaz: Pokud by e i e' byly neutrální, pak $e = e \cdot e' = e'$.

Pozorování: Inversní prvek k prveku a je určen jednoznačně.

Důkaz: Pokud by b i b' byly inversní k a , pak

$$b = b \circ e = b \circ (a \circ b') = (b \circ a) \circ b' = e \circ b' = b'$$

Pozorování: \Rightarrow v tabulce se nesmí v rádiu m. nebo s. zároveň užít dva různé c. dva ráz

$$a \circ c = b \circ c \Leftrightarrow a = b. \quad \text{Dk: } a = a \circ c \circ c^{-1} = b \circ c \circ c^{-1} = b \quad \blacksquare$$

$$c \circ a = c \circ b \Leftrightarrow a = b. \quad \text{Dk: } a = c^{-1} \circ c \circ a = c^{-1} \circ c \circ b = b \quad \blacksquare$$

Pozorování: Rovnice $a \circ x = b$, $y \circ a = b$ májí jednoznačná řešení.

$$\text{Dk: } x = e \circ x = \bar{a}^{-1} \circ a \circ x = \bar{a}^{-1} \circ b.$$

$$y = y \circ e = y \circ a \circ \bar{a}^{-1} = b \circ \bar{a}^{-1}.$$

Tvrcení:

$$(\bar{a}^{-1})^{-1} = a. \quad \text{Dk: } (\bar{a}^{-1})^{-1} = e \circ (\bar{a}^{-1})^{-1} = a \circ \bar{a}^{-1} \circ (\bar{a}^{-1})^{-1} = a \circ (\bar{a}^{-1} \circ (\bar{a}^{-1})^{-1}) = a \circ e = a \quad \blacksquare$$

$$(a \circ b)^{-1} = b^{-1} \circ \bar{a}^{-1}. \quad \text{Dk: } (a \circ b)^{-1} = b^{-1} \circ b \circ (a \circ b)^{-1} = b^{-1} \circ (\bar{a}^{-1} \circ a) \circ b \circ (a \circ b)^{-1} = \\ = b^{-1} \circ \bar{a}^{-1} \circ (a \circ b) \circ (a \circ b)^{-1} = b^{-1} \circ \bar{a}^{-1} \quad \blacksquare$$

$$\text{Dk: } a \circ \bar{a}^{-1} = e \Rightarrow a \circ b \circ b^{-1} \circ \bar{a}^{-1} = e$$

$$\Rightarrow (a \circ b) \circ (b^{-1} \circ \bar{a}^{-1}) = e \Rightarrow (a \circ b)^{-1} = b^{-1} \circ \bar{a}^{-1} \quad \blacksquare$$

• Permutace

$\rightarrow \{1, 2, \dots, n\}$

Def: Permutace na množině $[n]$ je bijektivní zobrazení $f: [n] \rightarrow [n]$.

• Znáromění permutace

1) sabalkou: $\begin{array}{c|c|c|c} i & 1 & 2 & 3 \\ \hline f(i) & 1 & 3 & 2 \end{array}$

2) matice: $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ nebo $f = (1, 3, 2)$

3) bijektivním grafem: $\begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & & \cancel{\downarrow} \\ 1 & 2 & 3 \end{array}$

4) grafem cyklu: $1 \circlearrowleft 2 \circlearrowright 3$

5) seznamem cyklu: $(1)(2, 3)$ nebo $(2, 3)$ a triviální cykly delky 1 nejsou

6) permutační matice P : $P_{ij} = \begin{cases} 1 & \text{edge } f(i) = j \\ 0 & \text{jinak} \end{cases}$ $P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

Pozorování: P je el. matice odpovídající zájmenej víc rádků.

$\Rightarrow PA$ zájmichá rádky A jsoule f

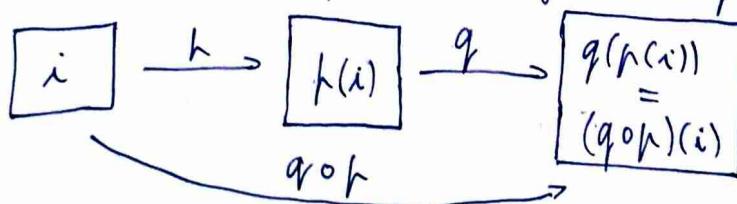
$\Rightarrow AP$ zájmichá sloupce A jsoule f

• Symetrická gruha

Pozorování: Množina všech permutací na n pravých S_n množinové

operaci sčítání o grupu (S_n, \circ) , která se nazývá symetrická

Zápis sčítání: $(q \circ f)(i) = q(f(i))$ → nejdříve uplatníme f , potom q



Důkaz:

1, \circ je bin. \circ . na S_n . \equiv složení dvou permutací je permutace

• $i \neq j \Rightarrow f(i) \neq f(j) \Rightarrow q(f(i)) \neq q(f(j)) \Rightarrow q \circ f$ je prosté

• $(\forall i \exists j: q(j)=i) \wedge (\forall j \exists k: f(k)=j) \Rightarrow (\forall i \exists k: q(f(k))=i) \Rightarrow q \circ f$ je na

2) (S_m, \circ) je grupa

- Skládání je asociativní: $\square \xrightarrow{h} \square \xrightarrow{g} \square \xrightarrow{r} \square \Rightarrow \square \xrightarrow{h} \square \xrightarrow{g} \square \xrightarrow{r} \square$

$$\xrightarrow{q \circ h}$$

$$(r \circ q) \circ h$$

$$r \circ (q \circ h)$$

- Neutralní prvek = Identita: $\text{id} \in S_m : \forall i : \text{id}(i) = i$

- Inverzní permutace: $h(i) = j \Leftrightarrow h^{-1}(j) = i$

→ otočení řadek, obrácení směru cyklu: $(1, 2, 3)^{-1} = (3, 2, 1)$



• Grupa S_3

$$S_3 = \{(1, 2, 3), (1, 3, 2), (3, 2, 1), (2, 1, 3), (2, 3, 1), (3, 1, 2)\}$$

$$= \{\text{id}, h_1, h_2, h_3, r_+, r_-\}$$

$$\begin{matrix} & 1 \\ 1 & \\ \curvearrowleft & 3 & 2 \end{matrix}$$

$\text{id}(1, 2, 3)$

$$\begin{matrix} & 1 \\ 3 & \xleftarrow{ } 2 \end{matrix}$$

$r_+(2, 3, 1)$

$$\begin{matrix} & 1 \\ 3 & \xrightarrow{ } 2 \end{matrix}$$

$r_-(3, 1, 2)$

$$\begin{matrix} & 1 \\ 3 & \xrightleftharpoons{ } 2 \end{matrix}$$

$h_1(1, 3, 2)$

$$\begin{matrix} & 1 \\ 3 & \xleftarrow{ } 2 \end{matrix}$$

$h_2(3, 2, 1)$

$$\begin{matrix} & 1 \\ 3 & \xrightarrow{ } 2 \end{matrix}$$

$h_3(2, 1, 3)$

Operace skládání:

\circ	id	h_1	h_2	h_3	r_+	r_-
id	id	h_1	h_2	h_3	r_+	r_-
h_1	h_1	id	r_+	r_-	h_2	h_3
h_2	h_2	r_-	id	r_+	h_3	h_1
h_3	h_3	r_+	r_-	id	h_1	h_2
r_+	r_+	h_3	h_1	h_2	r_-	id
r_-	r_-	h_2	h_3	h_1	id	r_+

inverzní permutace:

h	id	h_1	h_2	h_3	r_+	r_-
h^{-1}	id	h_1	h_2	h_3	r_-	r_+

$$\begin{array}{c} h_1 \circ h_3 \\ \hline h_3 \begin{matrix} 1 & 2 & 3 \\ \cancel{1} & \cancel{2} & 3 \\ 1 & 2 & 3 \end{matrix} \end{array} \quad \begin{array}{c} h_3 \circ h_1 \\ \hline h_1 \begin{matrix} 1 & 2 & 3 \\ 1 & \cancel{2} & \cancel{3} \\ 1 & 2 & 3 \end{matrix} \end{array}$$

$\Rightarrow (3, 1, 2) \quad \Rightarrow (2, 3, 1)$

• Pevný bod

Def: Pevný bod v permutations ρ je $i: \rho(i) = i$, t.j. trivialní cyclus délky 1.

• Transpozice

Def: Transpozice je permutace, která má pouze 1 netrivialní cyclus délky 2.

→ někdy se cyclus délky dva nazývá transpozice

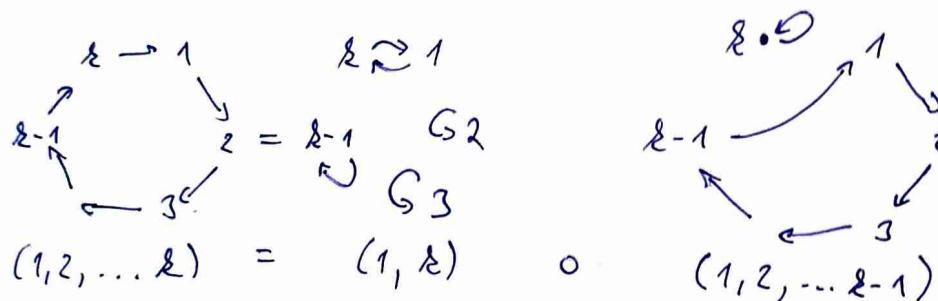
→ Transpozice $1\ 2\ 2\ 2\ ... \ i \xrightarrow{\rho} j \ ... \ m$ se zapisuje jako (i, j) .

Pozorování: Jakoukoliv permutaci lze rozložit na složení transpozic.

Důkaz: Cyclus $(1, 2, \dots, k)$ lze rozložit na

$$(1, 2, \dots, k) = (1, k) \circ (1, 2, \dots, k-1).$$

→ cyclus délky 1 lze * rozložit na 2 transpozice



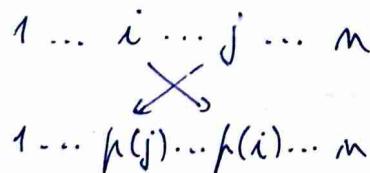
⇒ Potom lze cyclus $(1, 2, \dots, k-1)$ rozložit na $(1, k-1) \circ (1, 2, \dots, k-2)$ a indukčně dojdeme ke složení $k-1$ * transpozic

$$(1, 2, \dots, k) = (1, k) \circ (1, k-1) \circ \dots \circ (1, 2).$$

• Inverze

Def: Inverze v ρ je dvojice (i, j) : $i < j \wedge \rho(i) > \rho(j)$.

Pozorování: Inverze odpovídá křížení řádek v bipartitním grafu permutací



Počet inverzí $\rho = I(\rho)$

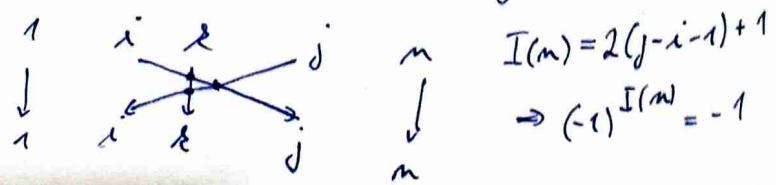
• Znaménko permutace

Def: Znaménko permutace ρ je $\text{sgn}(\rho) = (-1)^{I(\rho)}$.

Permutace s kladným znaménkem jsou sudé, se záporným liché.

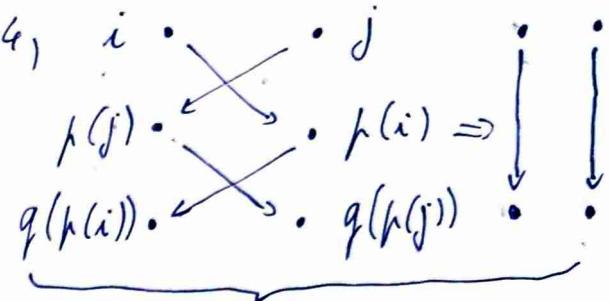
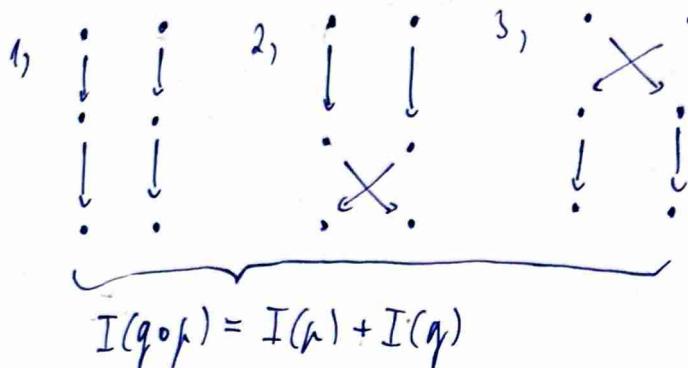
Pozorování: $\text{sgn}(\text{id}) = (-1)^0 = 1$

Transpozice: $\text{sgn}((i, j)) = -1$



Věta: Pro libovolné $f, g \in S_m$: $\text{sgn}(g \circ f) = \underline{\text{sgn}(f \circ g)} = \text{sgn}(f) \cdot \text{sgn}(g)$

Důkaz: $\text{sgn}(g \circ f) = (-1)^{I(g \circ f)}$. Vrátíme si vlastnosti funkce:



inverse v $f \circ g$
se nazývá směrnicí

$$\Rightarrow I(g \circ f) = I(f) + I(g) - 2 \left| \left\{ (i, j) : i < j \wedge f(i) > f(j) \wedge g(f(i)) < g(f(j)) \right\} \right|$$

$$\Rightarrow \text{sgn}(g \circ f) = (-1)^{I(f) + I(g)} = (-1)^{I(f)} \cdot (-1)^{I(g)} = \text{sgn}(f) \text{sgn}(g)$$

$$\Rightarrow \text{sgn}(f \circ g) = \text{sgn}(g) \cdot \text{sgn}(f) = \text{sgn}(f) \cdot \text{sgn}(g) = \text{sgn}(g \circ f) \quad \blacksquare$$

Důkaz:

$$\bullet \text{sgn}(f^{-1}) = \text{sgn}(f). \quad \text{Dk: } \text{sgn}(f^{-1}) \cdot \text{sgn}(f) = \text{sgn}(f^{-1} \circ f) = \text{sgn}(\text{id}) = 1 \quad \blacksquare$$

$$\bullet \text{sgn}(f) = (-1)^m, \quad \text{kde } r \neq \# \text{ transpozic libovolného rozkladu } f \text{ na transpozice.}$$

Dk: $f = t_1 \circ t_2 \circ \dots \circ t_r \Rightarrow \text{sgn}(f) = \text{sgn}(t_1) \cdot \dots \cdot \text{sgn}(t_r) = (-1)^r \quad \blacksquare$

$$\bullet \text{sgn}(f) = (-1)^s, \quad \text{kde } s \neq \# \text{ sudých cyklů } f. \quad \text{pro } s=1 \text{ na 2.}$$

Dk: cyklus délky k lze rozložit na $k-1$ transpozic.

$$\Rightarrow \text{sudé cykly} \rightarrow \text{lých' počet} \Rightarrow \text{sgn}(s_c) = -1$$

$$\Rightarrow \text{lící' cykly} \rightarrow \text{sudý' počet} \Rightarrow \text{sgn}(l_c) = 1 \quad \blacksquare$$

$$\bullet \text{sgn}(f) = (-1)^{m-k}, \quad \text{kde } f \in S_m \text{ a } k \text{ je počet cyklů } f.$$

Dk: 1 cyklus



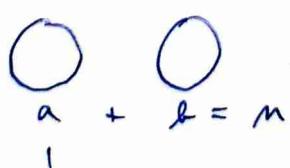
\Rightarrow rozložit na $n-1$ 1.

$$\Rightarrow \text{sgn}(f) = (-1)^{n-1}$$

$$\Rightarrow (-1)^{a+b-2}$$

$$\Rightarrow \text{sgn}(f) = (-1)^{m-2}$$

2 cykly



$$a-1 + b-1 \text{ 1.}$$

$$\Rightarrow (-1)^{a+b-2}$$

$$\Rightarrow \text{sgn}(f) = (-1)^{m-2}$$

ℓ cykly

$$a_1 + a_2 + \dots + a_\ell = m$$

$$a_1-1 + a_2-1 + \dots + a_\ell-1 \cdot 1.$$

$$\Rightarrow \text{sgn}(f) = (-1)^{m-\ell}$$

\rightarrow počet delen $a_i = 1$, když rozložit na

2 transpozice a směrnicí

$$(-1)^2 = (-1)^0 = (-1)^{a_i-1}$$

Q.E.D.

Těleso

Def: Těleso je množina K spolu se dříma komutativními binárními operacemi $+ \text{ a } \cdot$, kde $(K, +)$ a $(K \setminus 0, \cdot)$ jsou Abelovské grupy a navíc

$$\forall a, b, c \in K : a \cdot (b + c) = (a \cdot b) + (a \cdot c). \quad \leftarrow \text{distributivita}$$

\Rightarrow Musí být splněny následující axiomy:

- $\forall a, b \in K : a + b = b + a$
- $\forall a, b, c \in K : (a + b) + c = a + (b + c)$
- $\exists 0 \in K : \forall a \in K : a + 0 = a$
- $\forall a \in K : \exists -a \in K : a + (-a) = 0$
- $\forall a, b \in K : a \cdot b = b \cdot a \quad \leftarrow$ včetně 0!
- $\forall a, b, c \in K : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $\exists 1 \in K \setminus 0 : \forall a \in K : a \cdot 1 = a \quad \leftarrow 1 \neq 0 !$
- $\forall a \in K \setminus 0 : \exists \bar{a} \in K : a \cdot \bar{a} = 1 \quad \leftarrow 0$ nemá inversi ručí.
- $\forall a, b, c \in K : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Příklady: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ jsou tělesa

$\rightarrow \mathbb{Z}_p$, kde $p \in \mathbb{P}$ jsou tělesa \Rightarrow např. \mathbb{Z}_4 není, protože 2 nemá inversu prok

$$\mathbb{Z}_2 : \begin{array}{c|cc} x & 0 & 1 \\ \hline -x & 0 & 1 \\ \hline \bar{x} & -1 & 1 \end{array} \quad \mathbb{Z}_3 : \begin{array}{c|ccc} x & 0 & 1 & 2 \\ \hline -x & 0 & 2 & 1 \\ \hline \bar{x} & -1 & 1 & 2 \end{array} \quad \mathbb{Z}_5 : \begin{array}{c|cccc} x & 0 & 1 & 2 & 3 & 4 \\ \hline -x & 0 & 4 & 3 & 2 & 1 \\ \hline \bar{x} & -1 & 3 & 2 & 4 & \end{array}$$

\rightarrow množina $\left\{ \frac{p(x)}{q(x)} \right\}$ s polynomy p, q s reálnými koeficienty kromě těleso $\mathbb{R}(x)$ reálných racionálních funkcí.

Metaměta: Všechna dospělá uvedená tvrzení o soustavách rovnic, maticech a výpočtech nad \mathbb{R} jsou platné i v libovolném tělesu K .

Metadůkza: Provedení důkazy pouze pro \mathbb{R} ještě axiomu tělesa.

Vlastnosti tělesa

- jednoznačnost prvek 0 a 1
- jednoznačnost $-a$, \bar{a}
- $x = y \Leftrightarrow ax + b = ay + b$
- $ax + b = c \Leftrightarrow x = (c - b) \cdot \bar{a}$

} pro $a \neq 0$

} protože $(K, +), (K \setminus 0, \cdot)$
jsou grupy

- $\forall a \in K: 0 \cdot a = 0$

Dle: $0a = 0a + 0 = 0a + (0a - 0a) = (0+0)a - 0a = 0a - 0a = 0$ \blacksquare

- $\forall a \in K: (-1) \cdot a = -a$

Dle: $(-1) \cdot a = (-1) \cdot a + 0 = (-1) \cdot a + a - a = (-1+1)a - a = 0a - a = -a$ \blacksquare

- $a \cdot b = 0 \Leftrightarrow a = 0 \vee b = 0$

Dle: Když $ab = 0$ pro $a \neq 0, b \neq 0$, pak $\exists \bar{a}^1, \bar{b}^1: 1 = a\bar{a}^1 b\bar{b}^1 = ab\bar{a}^1\bar{b}^1 = 0$

Věta: \mathbb{Z}_p je těleso $\Leftrightarrow p$ je prvočíslo.

Důkaz: \Rightarrow : Když $p = a \cdot b$, pak $a \cdot b \equiv 0 \pmod{p}$.

→ může násobek a, b nebo oba mít inverse míci.

\Leftarrow : Většina axiomů plyne z vlastnosti $+ a \cdot$ na \mathbb{Z}_p , kromě existence \bar{a}^1 .

Cíl: $\forall a \in [p-1] \exists \bar{a}^1 \in [p-1]: a \cdot \bar{a}^1 \equiv 1 \pmod{p}$.

Nechť $f_a: [p-1] \rightarrow [p-1]$ t.j. $f_a(x) = (ax) \pmod{p} \Rightarrow f_a(\bar{a}^1) = 1$

\Rightarrow stačí ukázat, že $1 \in H(f_a)$. Uvážme, že f_a je prosté \Rightarrow bude i "na".

→ Když nebylo prosté, pak $\exists b, c$ brno $b > c$ t.j.

$$f_a(b) = f_a(c) \Rightarrow 0 = f_a(b) - f_a(c) \equiv ab - ac \equiv a(b-c) \pmod{p}$$

$$\Rightarrow a(b-c) \equiv 0 \pmod{p} \Rightarrow a = p, 0 \vee b-c = p, 0$$

\Rightarrow pro první $a, b-c \in [p-1]$

• Galiosovo těleso

Věta: Těleso o reliabiliti m existuje $\Leftrightarrow m$ je mocnina prvočísla.

Je jednoznačné až má izomorfismus a znací se $GF(m) = GF(p^n)$

• Charakteristika tělesa

Def: V tělesu K , pokud $\underbrace{\exists m \in \mathbb{N}: 1+1+\dots+1=0}$, pak nejménší takové m je charakteristika tělesa K , jinak $\text{char}(K)=0$.

Výuka: $\text{char}(\mathbb{R})=0$, $\text{char}(\mathbb{Z}_p)=p$.

Věta: Charakteristika tělesa je rádý prvočísel nebo nula.

Dle: Pokud by $\text{char}(K)=m=a \cdot b$, pak

$$0 = \underbrace{1+1+\dots+1}_m = (\underbrace{1+1+\dots+1}_{a \neq 0}) (\underbrace{1+1+\dots+1}_{b \neq 0}) + 0 \Rightarrow \text{SPOR} \quad \mathfrak{S}$$

Pozorování: V tělesech $\text{char} = 2$ je rádý prvek srovnávání $a = b$ neobsahuje +.

Důkaz: $1+1=0 \Rightarrow -1=1 \Rightarrow -a=a \Rightarrow a-b=a+b$.

Mala' fermatova věta

Květa: Nechť je $p \in \mathbb{P}$, $a \in [p-1]$, potom $\underline{a^{p-1} \equiv 1 \pmod p}$

Důkaz: Zobrazení $f_a: x \mapsto ax$ je $\nu \mathbb{Z}_p$ bijekce na $[p-1]$.

Proto $\nu \mathbb{Z}_p$ platí

$$\prod_{x=1}^{p-1} x = \prod_{x=1}^{p-1} ax = a^{p-1} \prod_{x=1}^{p-1} x \Rightarrow 1 = a^{p-1}. \quad \blacksquare$$

Vektorový prostor

Def: Vektorový prostor $(V, +, \cdot)$ nad körtem $(\mathbb{K}, +, \cdot)$ je množina V s těmi

- binární operací $+$ na V a binární operací skalárního nasobku $\mathbb{K} \cdot V \rightarrow V$.
- $(V, +)$ je Abelova skupina
- $\forall a, b \in \mathbb{K}, \forall v \in V: (a \cdot b) \cdot v = a \cdot (b \cdot v)$ asociativita
- $\forall v \in V: 1 \cdot v = v$ neutralní prvek
- $\forall a, b \in \mathbb{K}, \forall v \in V: (a+b) \cdot v = (a \cdot v) + (b \cdot v)$ distributivita
- $\forall a \in \mathbb{K}, \forall u, v \in V: a \cdot (u+v) = (a \cdot u) + (a \cdot v)$ distributivita

Počet \mathbb{K} se nazývají skalary, prvek V vektory.

Rozlišujeme nulový skalar $0 \in \mathbb{K}$ a nulový vektor $0 \in V$.

Máme opačný skalar $-a \in \mathbb{K}$ i opačný vektor $-v \in V$.

Existuje inverzní skalar $a^{-1} \in \mathbb{K}$, ale ne inverzní vektor! $\begin{cases} 0 \cdot a \\ a \cdot 0 \end{cases}$ nedef.

Vlastnosti

• Aritmetický vektorový prostor dimenze n nad $\mathbb{K} \rightarrow \mathbb{K}^n$

→ vektory jsou uspořádání n -tice prvků $\nu \mathbb{K}$

→ sčítání a skalární nasobky se provádějí po souřadnicích

→ kdežto körtem \mathbb{K} dává vektorový prostor \mathbb{K}^n stejnou mohutnost.

• $\mathbb{K}^{m \times n}$ matice řádu $m \times n$ nad \mathbb{K}

• $V = \{0\}$ triviální vektorový prostor nad libovolným \mathbb{K}

• Polynomy s koeficienty $\nu \mathbb{K}$

• Polynomy omezeného stupně

• Vektorový prostor reálných funkcí nad körtem \mathbb{R}

Množinové systémy pro rektoričné prostory

X je systém podmnožin množiny X uspořádán symetricky rovídlem Δ .

(X, Δ, \cdot) je r.v.p. mod \mathbb{Z}_2 , kde \cdot definujeme jako $0 \cdot A = \emptyset$, $1 \cdot A = A$, $\forall A \in X$.

Vlastnosti rektoričních prostorů

- jednoznačnost $0, -n$
- $n = n \Leftrightarrow n + n = n + n$
- $x + n = n \Leftrightarrow x = n - n$
- $\forall n \in V, \forall a \in \mathbb{K}: 0n = a0 = 0$

} protože $(V, +)$ je grufa

$$\text{D\acute{e}lka: } 0n = 0n + 0 = 0n + 0n - 0n = (0+0)n - 0n = 0n - 0n = 0$$

$$a0 = a0 + 0 = a0 + a0 - a0 = a(0+0) - a0 = a0 - a0 = 0$$

- $\forall n \in V: (-1)n = -n$

$$\text{D\acute{e}lka: } (-1)n = (-1)n + 0 = (-1)n + n - n = (-1+1)n - n = 0n - n = 0 - n = -n$$

- $a \cdot n = 0 \Leftrightarrow a = 0 \vee n = 0$

$$\text{D\acute{e}lka: } \text{pokud } a \neq 0, \text{ potom } n = 1n = \bar{a}^1 a n = \bar{a}^1 0 = 0$$

Podprostor

Def. Nechť V je rektoriční prostor mod \mathbb{K} , potom podprostor U je

neprázdná podmnožina V splňující

$$\forall u, v \in U: u + v \in U$$

$$\text{znacení: } U \subseteq V$$

$$\forall v \in U, \forall a \in \mathbb{K}: a \cdot v \in U \Rightarrow 0 \in U!$$

Vlastnosti: Rovina U procházející počátkem je podprostorem \mathbb{R}^3 , prímka $W \subset U$ procházející počátkem je podprostor $U \subset \mathbb{R}^3$.

Pozorování: Jakožkolik podprostor je také rektoriční prostor, protože $(U, +)$ je grufa plyne z uvažování $0 = 0 \cdot n \in U, -n = (-1)n \in U$.

Brušek podprostoru

Věta: Nechť $(V_i, i \in I)$ je libovolný systém podprostoru prostoru V .

Brušek tohoto systému $\bigcap_{i \in I} V_i$ je také podprostor V .

Důkaz: Uvažme, že $W = \bigcap_{i \in I} V_i$ je uspořádán na $+ \circ \bullet$.

$$\forall u, v \in W: u, v \in W \Rightarrow \forall i: u, v \in V_i \Rightarrow \forall i: u + v \in V_i \Rightarrow u + v \in W$$

$$\forall w \in W, a \in \mathbb{K}: w \in W \Rightarrow \forall i: w \in V_i \Rightarrow \forall i: aw \in V_i \Rightarrow aw \in W$$

• Lineární obal

Def: Lineární obal $L(X)$ podmnožiny X rektoričkého prostoru V je průnik všech podprostorů $U \subseteq V$, které obsahují X .

$$L(X) = \bigcap \{U : X \subseteq U, U \text{ je podprostor } V\}$$

$L(X) = \text{span}(X) = \text{podprostor generovaný } X.$

Def: Lineární kombinace vektorů $v_1, \dots, v_m \in V$ nad \mathbb{K} je libovolný vektor $u = a_1 v_1 + \dots + a_m v_m$, kde $a_1, \dots, a_m \in \mathbb{K}$.

Věta: Nechť V je rektoričký prostor nad \mathbb{K} a X je podmnožina V .

Potom $\text{span}(X)$ je množina všech lineárních kombinací vektorů z X .

Dоказ: Pro $W_1 = \bigcap_{x \subseteq U_i \in V} U_i$, $W_2 = \left\{ \sum_i a_i v_i \mid a_i \in \mathbb{K}, v_i \in X \right\}$ chceme ukázat $W_1 = \text{span}(X) = W_2$.

$\rightarrow X \subseteq W_2$, máme, že W_2 je podprostor \Rightarrow je rovnoučko $\bigcap U_i \Rightarrow W_1 \subseteq W_2$.

- uvažujeme na $\mathbf{0}$: $u \in W_2 \Rightarrow u = \sum_i a_i v_i = \sum_i (a_i \cdot 1) v_i \Rightarrow u \in W_2$.

- uvažujeme na \oplus : $u, u' \in W_2 \Rightarrow u + u' = \sum_i (a_i + a'_i) v_i \Rightarrow u + u' \in W_2$

\rightarrow Když všechny v_i obsahují X a jsou uvaženy na \oplus a $\mathbf{0}$ \Rightarrow obsahují všechny lineární kombinace vektorů X

$$\Rightarrow \forall i: W_2 \subseteq U_i \Rightarrow W_2 \subseteq W_1 \Rightarrow W_2 = W_1 \quad \blacksquare$$

• Prostupy určené matice

- Def: Jádro matice $A \in \mathbb{K}^{m \times n}$ je $\ker(A) := \{x \in \mathbb{K}^n \mid Ax = \mathbf{0}\}$. $\ker(A) \subseteq \mathbb{K}^n$

- Def: Řádkový prostor $R(A) \subseteq \mathbb{K}^m$ je lineární obal řádků A .

- Def: Sloupcový prostor $S(A) \subseteq \mathbb{K}^m$ je lineární obal sloupců A .

$$S(A) = \{u \in \mathbb{K}^m \mid u = Ax, x \in \mathbb{K}^n\}$$

$$R(A) = \{v \in \mathbb{K}^m \mid v = A^T y, y \in \mathbb{K}^n\}$$

- Pozorování: Elementární úpravy nemění $\ker(A)$ ani $R(A)$.

- Pozorování: $\forall v \in R(A), \forall x \in \ker(A): v^T x = 0$.

Dоказ: $\exists y: v = A^T y \Rightarrow v^T x = (A^T y)^T x = y^T A x = y^T \mathbf{0} = 0$. \blacksquare

- Pozorování: Nechť R je regulární.

1, Pokud $A = R \cdot B \Rightarrow \ker(A) = \ker(B)$, $R(A) = R(B) \rightarrow$ el. úpravy

2, Pokud $A = D \cdot R \Rightarrow S(A) = S(B) \rightarrow$ el. úpravy na sloupcích

Lineární nerávnislost

Def: Množina vektorů $X = \{v_1, \dots, v_m\}$ je lineárně nerávnislá
 $\Leftrightarrow \sum_{i=1}^m a_i v_i = 0$ má pouze triviální řešení $\forall i: a_i = 0$.

Pozorování: Pokud jsou v_1, \dots, v_m lin. závislé, pak

$$\sum_i a_i v_i = 0, \text{ kde nějaké } a_i \neq 0, \text{ tedy}$$

$$v_i = - \sum_{j \neq i} \frac{a_j}{a_i} v_j.$$

Důsledek: Pokud bude nějaký z vektorů v_1, \dots, v_m nezávislý jde lineární kombinací všech ostatních, pak jsou tyto vektory lin. závislé.

Vrátily:

① Když $0 \in X$, pak je X lineárně závislá $\because 1 \cdot 0 = 0$.

② Řádky matice v REF jsou lineárně nerávnislosti

③ Ve vektorném prostoru reálných polynomů je $\{x^0, x^1, x^2, \dots\}$ lin. nerávnislosti

Testování nerávnislosti

$$X = \{(2, 1, 0, 3)^T, (4, 1, 3, 4)^T, (0, 2, 2, 1)^T, (3, 4, 1, 0)^T, (0, 2, 2, 2)^T\} \text{ nad } \mathbb{Z}_5^4$$

a) vektory zapišeme do matice jako řádky a počasime se jeden z nich eliminovat

$$\begin{pmatrix} 2 & 1 & 0 & 3 \\ 4 & 1 & 3 & 4 \\ 0 & 2 & 2 & 1 \\ 3 & 4 & 1 & 0 \\ 0 & 2 & 2 & 2 \end{pmatrix} \sim \sim \begin{pmatrix} 2 & 1 & 0 & 3 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \text{vzniklo nulový řádek} \Rightarrow X \text{ je závislá}$$

b) vektory zapišeme do matice jako sloupcity a počasime se najít nekonečnou řešení

$$\begin{pmatrix} 2 & 4 & 0 & 3 & 0 \\ 1 & 1 & 2 & 4 & 2 \\ 0 & 3 & 2 & 1 & 2 \\ 3 & 4 & 1 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 0 & 3 & 0 \\ 0 & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{řešení } \sum_i a_i v_i = 0$$

\hookrightarrow máme volnou proměnnou $\Rightarrow \exists$ nebr. řeš. $\Rightarrow X \notin \mathcal{L}$.

Klasifikaci nerávnislosti

① Je-li X nerávnislost a $Y \subseteq X \Rightarrow Y$ je nerávnislost

② Je-li Y závisla a $Y \subseteq X \Rightarrow X$ je závisla

③ X je nerávnislost $\Leftrightarrow \forall v \in X: v \notin \text{span}(X \setminus \{v\})$.

Tvrdění: Jestliže Y je konečná generující množina prostoru V a X je LN ne V , potom $|X| \leq |Y|$.

Důkaz: Spolem: $Y = \{v_1, \dots, v_n\}$ a $\{u_1, \dots, u_{n+1}\} \subseteq X$, kdežto u_i vyjadřuje:

$$\forall i \quad u_i = \sum_{j=1}^n a_{ij} v_j$$

Z konstant a_{ij} uděláme matice $A \in \mathbb{K}^{(n+1) \times n}$, která má $n+1$ řád a n sloupců \Rightarrow el. úpravami můžeme některý z nich eliminovat $\Rightarrow X$ je rán.

• Báze rektoričkového prostoru

Def: Báze v.r.p. V je lineárně nezávislá množina vektorů X , generující V .

Pozorování: Každý vektor $u \in V$ je unikátní lin. kom. vektorů z báze X .

Důkaz: Spolem: $u = \sum_i a_i v_i = \sum_i b_i v_i$

$$\Rightarrow 0 = u - u = \sum_i v_i (a_i - b_i) \Rightarrow \forall i: a_i = b_i$$

Def: Nechť $X = (v_1, \dots, v_m)$ je uspořádaná báze prostoru V nad \mathbb{K} .

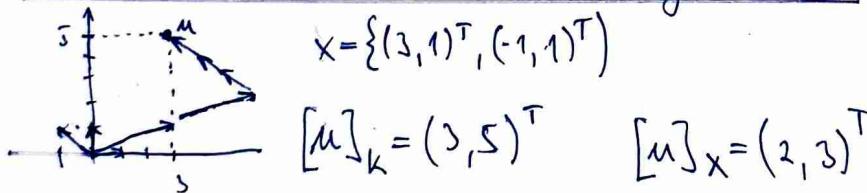
Vector souřadnice vektoru $u \in V$ vzhledem k bázi X je:

$$[u]_X = (a_1, \dots, a_m)^T \in \mathbb{K}^m, \text{ kde } u = \sum_i a_i v_i.$$

• Kanonická báze

\rightarrow v arit. v.r.p. \mathbb{K}^n jsou sloupce e_1, \dots, e_n jednotkové matice I_n kan. bázi \mathbb{K} .

• Souřadnice vektoru vzhledem k různým bázím



• Existence báze

Pozorování: Pokud $\text{span}(X) = V$ a $\forall v \in X: v \notin \text{span}(X - \{v\})$, potom X je báze V .

Důkaz: Každá konečná generující množina Y prostoru V obsahuje bázi X . $X \subseteq Y$.

Důkaz: $\forall v \in Y: \exists y \in \text{span}(Y - \{v\})$, když odebereme $v \in Y$ oblast Y není lin. nezávislá.

Výta: Každý rektoričkový prostor má bázi.

(pro konečné generované doložit, pro nekonečné gen. se nedokazuje.)

Změna bare

- Lemma o výměně: Nechť Y generuje V nad \mathbb{K} . Nyní $u \in V$ lze zapsat pomocí $v_1, \dots, v_m \in Y$, $a_1, \dots, a_n \in \mathbb{K}$: $u = \sum_i a_i v_i$
 $\rightarrow \forall i: a_i \neq 0$ můžeme provést výměnu v_i za u .

$$\Rightarrow \text{span}((Y \setminus \{v_i\}) \cup \{u\}) = V.$$

Vrážku: $Y = \{(1, 0, 0)^T, (0, 1, 0)^T, (0, 0, 1)^T, (1, 1, 0)^T\}$ $u = (1, 1, 1)$

$$\rightarrow u = \underbrace{(1, 0, 0)^T + (0, 1, 0)^T + (0, 0, 1)^T}_{u \text{ lze vyměnit za } v_1, v_2, v_3} = (0, 0, 1)^T + (1, 1, 0)^T$$

Důkaz: $u \leftrightarrow v_4$.

$$u = a_1 v_1 + \dots + a_j v_j + \dots + a_m v_m \Rightarrow v_j = \frac{1}{a_j} \left(u - \sum_{i \neq j} a_i v_i \right)$$

$\hookrightarrow a_j \neq 0$

\rightarrow jakékoli $w \in V$ lze zapsat jako lin. kom. funkci Y . Potom se v nějto kombinaci vyskytuje v_j , tak ho nahradíme výrazem w . ■

- Věta (Steinitzova): Nechť Y generuje V a X je konečná l.m. množina ve V . Potom lze X doplnit vektoru $z \in Y$ na Z t.ž. $|Y| = |Z|$ a Z lze generovat V .

$$\Rightarrow X \subseteq Z, Z \setminus X \subseteq Y, |Z| = |Y|, \text{span}(z) = V.$$

Důkaz: Indukce podle $|X \setminus Y|$.

$$\textcircled{1} \quad |X \setminus Y| = 0 \Rightarrow X \subseteq Y \Rightarrow Z = Y \quad \checkmark$$

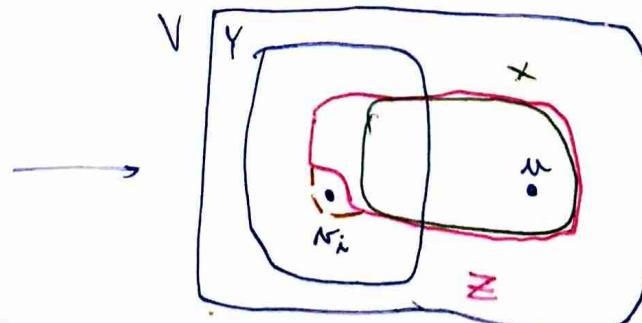
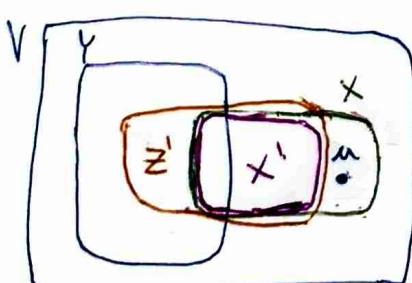
$$\textcircled{2} \quad n \rightarrow n+1. \text{ Najdu } u \in X, \text{ ale } u \notin Y \Rightarrow u \in X \setminus Y \text{ a položím } X' = X \setminus \{u\}.$$

Po dle i.p. $\exists z' \text{ pro } X' \text{ a } Y$ t.ž. $X' \subseteq z'$, $z' \setminus X' \subseteq Y$, $|Z'| = |Y|$, $\text{span}(z') = V$.

Použijeme lemma o výměně pro u a $Z' = \{v_1, \dots, v_m\}$.

$$u = \sum_i a_i v_i \rightarrow u \in X \text{ a } X \text{ je l.m.} \Rightarrow a_i \neq 0 \text{ pro nejake } v_i \in Z' \setminus X'.$$

Potom $z = z' \setminus v_i \cup u$ splňuje všechny vlastnosti. ■



Vážela: $Y = \{(1, 0, 0, 0)^T, (0, 1, 0, 0)^T, (0, 0, 1, 0)^T, (0, 0, 0, 1)^T, (1, 1, 1, 1)^T\}$
 $X = \{(1, 1, 0, 0)^T, (1, 1, 0, 1)^T\}$

→ prostorovou aplikací lemmatu o rozšíření výběru základny Z .

$$(1, 1, 0, 0)^T = \underbrace{(1, 0, 0, 0)^T}_{\curvearrowright} + (0, 1, 0, 0)^T$$

$$(1, 1, 0, 1)^T = \underbrace{(1, 1, 0, 0)^T}_{\curvearrowright} + (0, 0, 0, 1)^T$$

$$\Rightarrow Z = \{(1, 1, 0, 0)^T, (0, 1, 0, 0)^T, (0, 0, 1, 0)^T, (1, 1, 0, 1)^T, (1, 1, 1, 1)^T\}$$

Důsledek: Je-li v.p. konečně generován, pak lze jeho l.m. rozšířit na bázi.

Důsledek: Je-li v.p. konečně generován, pak všechny jeho báze mají stejnou mohutnost.

Def: Mejdme báze X, Y prostoru V , pak:

- X je nezávislá, Y generuje $V \Rightarrow |X| \leq |Y| \quad \left. \begin{array}{l} |Y|=|X| \\ |Y| \leq |X| \end{array} \right\} |Y|=|X|$
- Y je nezávislá, X generuje $V \Rightarrow |Y| \leq |X| \quad \left. \begin{array}{l} |Y|=|X| \\ |Y| \leq |X| \end{array} \right\} |Y|=|X|$

* Dimenze nelineárního prostoru

Def: Dimenze konečně generovaného v.p. V je možnost sestavit k němu bázi.
 Značí se $\dim(V)$.

Vážky: $\dim(K^n) = n$, $\dim(R(A)) = \text{rank}(A)$.

Pozorování: Je-li V podprostorem konečně generovaného W , pak $\dim(V) \leq \dim(W)$.

Def: Báze V je l.m. ve W a lze ji rozšířit na bázi W .

Věta: Jom-li U, V podprostory konečně generovaného prostoru W , pak

$$\dim(U) + \dim(V) = \dim(U \cap V) + \dim(\text{span}(UV)).$$

Def: Bázi X průniku $U \cap V$ rozšíříme na bázi Y prostoru U a na Z prostoru V .

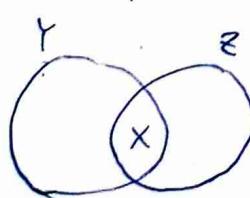
$$\Rightarrow \dim(U \cap V) = |X|, \dim(U) = |Y|, \dim(V) = |Z|.$$

$$\Rightarrow \dim(\text{span}(UV)) = |YZ|.$$

$$\rightarrow všimně si, že $X \subseteq Y$, $X \subseteq Z \Rightarrow |Y| + |Z| = |X| + |YZ|$ ■$$

Pozorování: $|U| = |K| \dim(U)$

\because vektory zapíšeme jako
větory souč. něči nejale'
bázi \Rightarrow vektory součadné je



$$\begin{aligned} &\uparrow \\ &|Y| + |Z| - |Y \cap Z| = |YZ|. \end{aligned}$$

• Dimenze prostoru všechných matic $\rightarrow = \text{pro } B \text{ regulární}$

Lemma: Pro lib. $A' = BA$, pro $\dim(S(A')) \leq \dim(S(A))$.

Děl: Označme u_1, \dots, u_m sloupcy matice A a u'_1, \dots, u'_m sloupcy A' .

$$\Rightarrow \forall i: u'_i = Bu_i \quad \Rightarrow d := \dim(S(A)).$$

Buďo nechť u_1, \dots, u_d tvoří bázi $S(A)$. Když si nechne libovolný $w' \in S(A')$:

$$w' = \sum_i a_{i1} u'_i = \sum_i a_{i1} Bu_i = B \sum_i a_{i1} u_i = B \cdot w.$$

$$\Rightarrow w = \sum_{i=1}^d b_i u_i \Rightarrow w' = B \cdot \sum_{i=1}^d b_i u_i = \sum_{i=1}^d b_i Bu_i = \sum_{i=1}^d b_i u'_i.$$

$$\therefore u'_1, \dots, u'_d \text{ generují } S(A') \Rightarrow \dim(S(A')) \leq \dim(S(A)). \quad \blacksquare$$

Věta: Jakákoliv $A \in K^{m \times n}$ splňuje: $\dim(R(A)) = \dim(S(A)) = \text{rank}(A)$.

Důkaz: Nechť $A \sim A' \sim \text{REF}$, $\Leftrightarrow \exists R \text{ regulární} \text{ až } A' = RA$.

- podle lemmaho $\dim(S(A')) \leq \dim(S(A))$
 - $A = R^{-1}A' \Rightarrow \dim(S(A)) \leq \dim(S(A'))$
- $\left. \begin{array}{l} \dim(S(A')) = \dim(S(A)) \\ \dim(S(A')) = \dim(S(A)) \end{array} \right\} \dim(S(A')) = \dim(S(A))$

Pro $A' \sim \text{REF}$ věta platí jízdní:

1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	1
0	0	0	0

$$\dim(R(A')) = \text{rank}(A') = \dim(S(A'))$$

($\hookrightarrow \text{rank}(A)$)

Protože $R(A) = R(A')$: $\dim(R(A)) = \dim(S'(A)) = \dim(S(A))$ \blacksquare

Důsledky:

$$\bullet \text{rank}(A^T) = \text{rank}(A)$$

$$\bullet \text{rank}(A) = \text{rank}(RA) = \text{rank}(AR') \quad \text{pro libovolné } A \in K^{m \times n} \text{ a regulární } R \in K^{m \times m}, R' \in K^{n \times n}$$

$$\bullet \underbrace{R(BA)}_{\sim} \subseteq R(A), \quad \underbrace{S(BA)}_{\sim} \subseteq S(B)$$

komboinace řádků $\times A \hookrightarrow$ komboinace sloupců $\times B \quad \nearrow$ násobení nemáže využít hodnot

$$\Rightarrow \underline{\text{rank}(BA) \leq \min\{\text{rank}(A), \text{rank}(B)\}}$$

Věta: Pro libovolnou $A \in K^{m \times n}$: $\dim(\ker(A)) + \text{rank}(A) = n$.



Děl: $d := n - \text{rank}(A) = \# \text{ volných proměnných} \rightarrow \text{násobené } d = \dim(\ker(A))$.

x_1, \dots, x_d jsou řešení $Ax=0$ dané specifickou substitucí. Jsou l.m. \because pro $\forall i$ platí,

že x_i je mezi x_1, \dots, x_d jedinečná a i-tou sloučenou nemůžou. Takhle x_1, \dots, x_d tvoří bázi $\ker(A) \Rightarrow \dim(\ker(A)) = d$. \blacksquare

Lineární zobrazení

Def: Nechť U a V jsou vektorové prostory nad stejným tělesem \mathbb{K} .

Zobrazení $f: U \rightarrow V$ je lineární =

$$\forall u, v \in U: f(u+v) = f(u) + f(v) \quad \leftarrow \text{otocení}$$

$$\forall u \in U, \lambda \in \mathbb{K}: f(\lambda u) = \lambda \cdot f(u) \quad \leftarrow \text{roztažení}$$

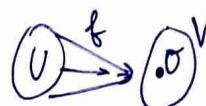
Pozorování: Při této se zobrazení sám na sebe $\therefore f(0) = f(0 \cdot u) = 0 \cdot f(u) = 0$.

Jednoduchá lin. zobrazení

→ Meri obecnější v.f. $f: U \rightarrow V$ nad stejným \mathbb{K} .

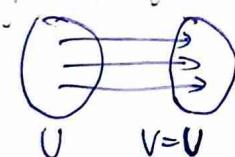
Triviale

$$\forall u \in U: f(u) = 0$$



Identita - id je zobrazení na U nebo $U \subseteq V$

$$\forall u \in U: \text{id}(u) = u$$



$$U \subseteq V$$

Geometrická lineární zobrazení

↳ transformace v \mathbb{R}^2 nebo \mathbb{R}^3 fixující počátek

• rotace okolo počátku

• osy souměrnosti podél osy procházející počátkem } galáktické
• stejnoběhlost se středem v počátku } kombinace je l.z.

Vlastnosti lineárních zobrazení

① Pokud $f: U \rightarrow V$ a $g: V \rightarrow W$ jsou l.z. poté je i $(g \circ f): U \rightarrow W$ l.z.

$$\text{Dle: } \bullet (g \circ f)(u+v) = g(f(u+v)) = g(f(u) + f(v)) = g(f(u)) + g(f(v))$$

$$\bullet (g \circ f)(\lambda u) = g(f(\lambda u)) = g(\lambda f(u)) = \lambda g(f(u)) \quad \blacksquare$$

② Pokud $f: U \rightarrow V$ je bijektivní l.z. poté je i $f^{-1}: V \rightarrow U$ l.z.

→ pro libovolná $v, v' \in V$ nechť $u = f^{-1}(v)$, $u' = f^{-1}(v')$

$$\bullet f^{-1}(v+v') = f^{-1}(f(u) + f(u')) = f^{-1}(f(u+u')) = u+u' = f^{-1}(v) + f^{-1}(v')$$

$$\bullet f^{-1}(\lambda v) = f^{-1}(\lambda f(u)) = f^{-1}(f(\lambda u)) = \lambda u = \lambda f^{-1}(v) \quad \blacksquare$$

Def: Bijektivní lineární zobrazení se nazývá isomorfismus.

• Transformace na vektor souřadnic

Tvrdění: Nechť V je prostor nad \mathbb{K} s bází $X = (u_1, \dots, u_m)$.

Potom $f: V \rightarrow \mathbb{K}^m$, $f(w) = [w]_X$ je l.z.

Dk: Pro $w, w' \in V$ vyjádřime $w = \sum_i a_i u_i$, $w' = \sum_i b_i u_i$, tedy

$$[w]_X = (a_1, \dots, a_m)^T, \quad [w']_X = (b_1, \dots, b_m)^T$$

$$\begin{aligned} f(w+w') &= [w+w']_X = \left[\sum_i a_i u_i + \sum_i b_i u_i \right]_X = \left[\sum_i (a_i+b_i) u_i \right]_X = \\ &= (a_1+b_1, \dots, a_m+b_m)^T = [w]_X + [w']_X = f(w) + f(w') \end{aligned}$$

$$\bullet f(\alpha w) = [\alpha w]_X = \left[\sum_i \alpha a_i u_i \right]_X = (\alpha a_1, \dots, \alpha a_m)^T = \alpha \cdot [w]_X = \alpha f(w) \quad \blacksquare$$

Pozorování: Zobrazení $w \leftrightarrow [w]_X$ je isomorfismus.

• Věta o rozšířitelnosti: Nechť U a V jsou prostory nad \mathbb{K} a X je báze U .

Pak pro jdeček zobrazení $f_0: X \rightarrow V$ existuje jediné l.z. $f: U \rightarrow V$ rozšiřující f_0 t.j. $\forall u \in X: f(u) = f_0(u)$.

\Rightarrow když nám, kam se má zobrazení báze, tak je to zobrazení podmnožinou určenou.

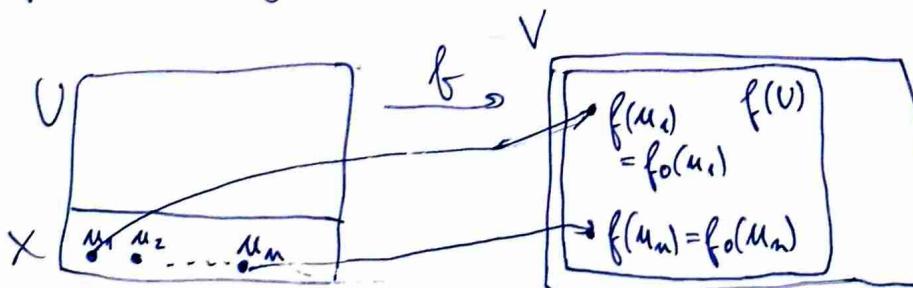
Dk: Libovolný $w \in U$ si zapišme jako l.k. vektoru z báze - pro konečnou bázi lze použít všechny vektory, pro nekonečnou využíváme násobení nulou $\Rightarrow \exists n \in \mathbb{N}_0:$

$$a_1, \dots, a_n \in \mathbb{K} \setminus \{0\} \text{ a } u_1, \dots, u_n \in X \text{ a } w = \sum_{i=1}^n a_i u_i$$

$$\Rightarrow f(w) = f\left(\sum_i a_i u_i\right) = \sum_i a_i f(u_i) = \sum_i a_i f_0(u_i) \quad \blacksquare$$

Důsledek: Pokud je $f: U \rightarrow V$ l.z. potom $\dim(U) \geq \dim(f(U))$.

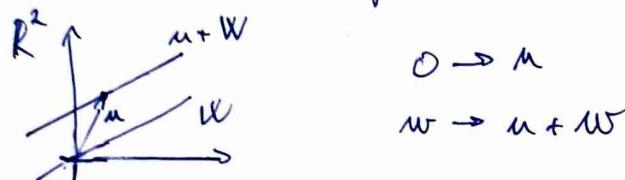
Dk: Báze X prostoru U se zobrazi na $f(X)$, která generuje $f(U)$, ale $f(X)$ může být lineárně závislá, potom je báze $f(U)$ podmnožinou $f(X)$.



• Afinní prostor

Def: Nechť W je podprostor v.p. V a $u \in V$. Afinní prostor $u + W$ je množina $\{u + w \mid w \in W\}$. Dimenze $u + W$ je $\dim(u + W) = \dim(W)$.

Václavka: $V \subset \mathbb{R}^2$ je prímka procházející fikčním podprostорem \rightarrow prímka v obecné poloze je affinní prostor.



$$\nearrow O \in \text{ker}(f) !$$

• Jádro lineárního zobrazení

Def: Jádro lineárního zobrazení $f: V \rightarrow V$ je $\text{ker}(f) = \{u \in V \mid f(u) = 0\}$.

Pozorování: Jádro je vektorový podprostor.

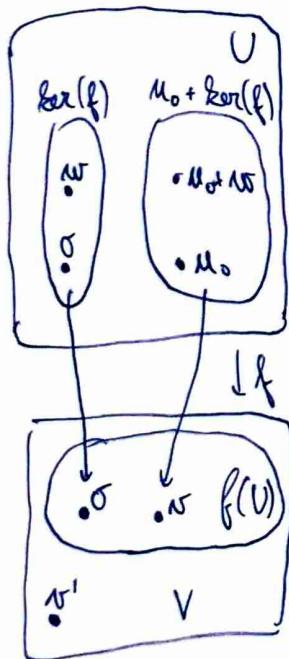
Václavka: Pro $f: K^n \rightarrow K^m$, $f(x) = Ax$ je $\text{ker}(f) = \text{ker}(A)$.

Věta: Nechť $f: V \rightarrow V$ je l.r. Pro libovolné $v \in V$ rovnice $f(u) = v$ bud' nema' řešení, nebo řešení tvorí affinní podprostor

$u_0 + \text{ker}(f)$, kde u_0 je libovolné řešení $f(u) = v$.

\rightarrow Václavka: řešení soustavy $Ax = b$.

Důkaz: Uvažme, že každý vektor $v \in u_0 + \text{ker}(f)$ se zobrazen na v a že každý vektor, co se zobrazen na v je $v \in u_0 + \text{ker}(f)$.



$$\begin{aligned} 1, \quad u \in u_0 + \text{ker}(f) &\Rightarrow u = u_0 + w, \quad w \in \text{ker}(f). \\ &\Rightarrow f(u) = f(u_0) + f(w) = v + 0 = v \\ 2, \quad f(u) = v &\Rightarrow f(u - u_0) = f(u) - f(u_0) = v - v = 0 \\ &\Rightarrow u - u_0 \in \text{ker}(f) \Rightarrow u \in u_0 + \text{ker}(f) \end{aligned}$$



• Matice lineárních obrazem

Def: Nechť U a V jsou v.r.p. nad stejným tělesem K , s bázemi $X = \{u_1, \dots, u_m\}$ a $Y = \{v_1, \dots, v_n\}$.

Matice l.z. $f: U \rightarrow V$ vzhledem k X, Y je $\gamma[f]_X \in K^{n \times m}$,

ježíž sloupce jsou vektorové souřadnice obrazu vektoru báze X vzhledem k Y .

$$\gamma[f]_X = \left([f(u_1)]_Y, \dots, [f(u_m)]_Y \right)$$

Pozorám: Pro $w \in U$ platí $[f(w)]_Y = \gamma[f]_X [w]_X$

Dk: Nechť $w = \sum_i a_i u_i$, tedy $[w]_X = (a_1, \dots, a_m)^T$. Potom

$$f(w) = f\left(\sum_i a_i u_i\right) = \sum_i a_i f(u_i) \quad f(w) \rightarrow [f(w)]_Y \text{ je l.z.}$$

$$\Rightarrow [f(w)]_Y = \sum_i a_i [f(u_i)]_Y = \gamma[f]_X [w]_X$$

$$\begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix} [w]_X \xrightarrow{\gamma[f]_X} [f(w)]_Y$$

Beispiel: Vzhledem k kanonické bázi K určit

matice obrazem $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $f(2,1) = (7,0)$, $f(-1,1) = (-2,3)$. $\rightarrow \kappa[f]_K = ?$

$$\begin{aligned} \text{Vime: } \kappa[f]_K [(2,1)]_K &= [(7,0)]_K \Rightarrow \kappa[f]_K \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 7 \\ 0 \end{pmatrix} \\ \kappa[f]_K [(-1,1)]_K &= [(-2,3)]_K \Rightarrow \kappa[f]_K \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ 3 \end{pmatrix} \end{aligned} \quad \left\{ \begin{array}{l} \kappa[f]_K \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 7 & -2 \\ 0 & 3 \end{pmatrix} \end{array} \right.$$

$$\Rightarrow \kappa[f]_K = \begin{pmatrix} 7 & -2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}^{-1} = \frac{1}{3} \begin{pmatrix} 7 & -2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix} = \frac{1}{3} \begin{pmatrix} 9 & 3 \\ -3 & 6 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ -1 & 2 \end{pmatrix}$$

$$\hookrightarrow \begin{pmatrix} 2 & -1 & | & 1 & 0 \\ 1 & 1 & | & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & -\frac{1}{2} & | & \frac{1}{2} & 0 \\ 0 & \frac{3}{2} & | & -\frac{1}{2} & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & -\frac{1}{2} & | & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & | & -\frac{1}{6} & \frac{1}{3} \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & | & \frac{1}{3} & \frac{1}{2} \\ 0 & 1 & | & -\frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

$$\rightarrow e^1 = (1,0)^T \Rightarrow f(e_1) = (3, -1)^T$$

$$e^2 = (0,1)^T \Rightarrow f(e_2) = (1, 2)^T$$

je to násobek K

• Slezem lineárních obrazem

Pozorám: Nechť U, V, W jsou v.r.p. nad K s koncovými bázemi X, Y, Z .

Pro matice l.z. $f: U \rightarrow V$ a $g: V \rightarrow W$ platí:

$$z[gof]_X = z[g]_Y \gamma[f]_X$$

$$\Rightarrow \gamma[f]_X = \gamma[id]_{K \times K} [f]_X$$

Dk: Pro $\forall u \in U$: $[(gof)(u)]_Z = z[gof]_X [u]_X \wedge [(gof)(u)]_Z = z[g]_Y [f(u)]_Y = z[g]_Y \gamma[f]_X [u]_X$

\rightarrow Nyní ověřime, že ty dve matice jsou stejné. Vektory $u = i\text{-tý vektor báze } X$
máme $[u]_X = e^i \Rightarrow z[gof]_X e^i = z[g]_Y \gamma[f]_X e^i \Rightarrow$ matice mají

shodné i -té sloupce. Tato tři sloupce lze sloupce po sloupce ověřit $z[gof]_X = z[g]_Y \gamma[f]_X$

• Matice prechodu

$\text{id}(u) = u$: identita

Def: Nechť X a Y jsou konečné báze v.r.p. V . Matice prechodu od X k Y je ${}_{\gamma}[\text{id}]_X$.

Poznámka: Pro $\forall u \in V$: $[u]_Y = [\text{id}(u)]_Y = {}_{\gamma}[\text{id}]_X [u]_X$ ■

Poznámka: Proloží ${}_{\gamma}[\text{id}]_Y$ a ${}_{\gamma}[\text{id}]_X$ $= [\text{id} \circ \text{id}]_X = {}_{\gamma}[\text{id}]_X = I_{\dim(V)}$,

je tedy matice prechodu regulární a $({}_{\gamma}[\text{id}]_X)^{-1} = {}_{\gamma}[\text{id}]_Y$.

Postup: Vyjádří matice prechodu ${}_{\gamma}[\text{id}]_X$ od báze $X = (x_1, \dots, x_n)$ k $Y = (y_1, \dots, y_m)$ v \mathbb{K}^m .

Do sloupců X zapišeme vektory báze X a do řad Y vektory Y . $\Rightarrow X, Y \in \mathbb{K}^{n \times n}$

→ myší zapišeme libovolný $u \in \mathbb{K}^n$ pomocí obou bází:

$$\begin{aligned} u &= \sum_i a_i x_i = X [u]_X \\ u &= \sum_i b_i y_i = Y [u]_Y \end{aligned} \quad \left\{ \begin{array}{l} Y [u]_Y = X [u]_X \\ \Rightarrow [u]_Y = Y^{-1} X [u]_X \end{array} \right. \quad \begin{array}{l} Y \text{ je regulární, protože} \\ \text{rank}(Y) = \dim(S(Y)) = m. \end{array}$$

→ volbou $u = x_i$ získáme $[u]_X = e^i$ → můžeme po sloupcích ověřit, že
 ${}_{\gamma}[\text{id}]_X e^i = Y^{-1} X e^i \Rightarrow {}_{\gamma}[\text{id}]_X = Y^{-1} X$

Výpočet: $(Y|X) \sim (I_m | Y^{-1} X) = (I_m | {}_{\gamma}[\text{id}]_X)$

Příklad: V \mathbb{R}^2 určí matici prechodu od $A = \{(1,1)^T, (1,-1)^T\}$ k $B = \{(1,3)^T, (2,5)^T\}$.

$$\left(\begin{matrix} 1 & 2 \\ 3 & 5 \end{matrix} \middle| \begin{matrix} 1 & 1 \\ 1 & -1 \end{matrix} \right) \sim \left(\begin{matrix} 1 & 2 \\ 0 & -1 \end{matrix} \middle| \begin{matrix} 1 & 1 \\ -2 & 4 \end{matrix} \right) \sim \left(\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} \middle| \begin{matrix} -3 & -7 \\ 2 & 4 \end{matrix} \right) \Rightarrow {}_B[\text{id}]_A = \begin{pmatrix} -3 & -7 \\ 2 & 4 \end{pmatrix}$$

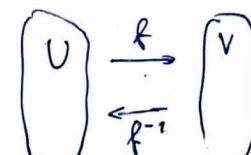
• Charakterizace matic izomorphismu

Věta: Lineární z. $f: V \rightarrow V$ je izomorfismus prostorů V a V s konkrétními bázemi X a Y $\Leftrightarrow {}_{\gamma}[f]_X$ je regulární.

Důkaz: \Leftarrow : Nechť $g: V \rightarrow V$ l.z. ${}_{\gamma}[g]_Y = ({}_{\gamma}[f]_X)^{-1}$. Pak

$${}_{\gamma}[g \circ f]_X = {}_{\gamma}[g]_Y {}_{\gamma}[f]_X = I_{1 \times 1} = {}_{\gamma}[\text{id}]_X \Rightarrow f \text{ je prostá'}$$

$${}_{\gamma}[f \circ g]_Y = {}_{\gamma}[f]_X {}_{\gamma}[g]_Y = I_{1 \times 1} = {}_{\gamma}[\text{id}]_Y \Rightarrow f \text{ je "na"}$$



$$\Rightarrow: {}_{\gamma}[f^{-1}]_Y {}_{\gamma}[f]_X = {}_{\gamma}[\text{id}]_X = I_{|X|} \xrightarrow{*} |Y| \geq |X| \quad \left\{ \begin{array}{l} |X| = |Y| \Rightarrow {}_{\gamma}[f]_X \text{ je čtvercová} \\ \wedge {}_{\gamma}[f^{-1}]_Y {}_{\gamma}[f]_X = I \Rightarrow \text{je reg.} \end{array} \right.$$

$$*: \dim(S(BA)) \leq \dim(S(A)) \rightarrow \text{rank}(BA) \leq \text{rank}(A)$$

$$\text{rank}(I_{|X|}) = |X| \Rightarrow |X| \leq \text{rank}({}_{\gamma}[f]_X) \leq |Y| \quad \boxed{|Y| \leq |X|}$$



Důsledek: $(\gamma[f]_x)^{-1} \gamma[f]_x = x[f^{-1}]_x \gamma[f]_x \Rightarrow x[f^{-1}]_x = (\gamma[f]_x)^{-1}$ pro f izomorfismus.

Počet sudých podgrafů

Def: Nechť G je souvislý graf a V obsahuje množinu hran $A \subseteq E(G)$.
• $\forall v \in V(G)$: v je incidentní se sudým počtem hran v A . Tyto množiny

A určují sudé podgrafy G .



$$|A \Delta B| = |A| + |B| - 2|A \cap B|$$

Problém: Kolik sudých podgrafů obsahuje G ?

• Kelatorny f. sudých podgrafů: (V, Δ, \circ) nad Z_2 krouží n.f.

Okoušme, že (V, Δ) je abelovská grupa; \emptyset je neutrální prvek

$\forall A \in V: A$ je inverzem \emptyset a A asociativita V

Okoušme, že V je uravnená na Δ : * $|A \Delta B|$ je sudá pro $|A|, |B|$ sudé ✓

↳ Δ zachovává sude stupeň

• pro prostor konečné možnosti platí $|V| = |K|^{\dim(V)}$ \Rightarrow stačí najít bázi V

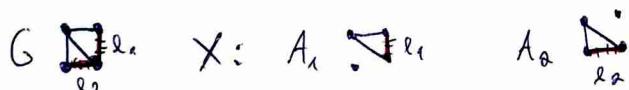
• Konstrukce báze \times n.f. V

Zvolíme libovolnou podmnožinu T grafu G . Pro každou neobsahující hranci $e_i \in E(G) \setminus E(T)$

definujeme A_i jako unikátní součinitel související s $T + e_i$.

\rightarrow množina $X = \{A_i \mid e_i \in E(G) \setminus E(T)\}$ je l.m. nezávislá, protože žádná hrana

e_i nemůže být eliminována agm. rozdílem A_i s ostatními grafy z X . (neobsahují e_i)



\rightarrow užádeme, že X generuje V \rightarrow zvolíme libovolný $B \in V$

\hookrightarrow najdeme jeho neobsahující hrany: $B \setminus E(T) = \{e_{i_1}, e_{i_2}, \dots, e_{i_k}\}$

\hookrightarrow graf $B \setminus A_{i_1} \setminus A_{i_2} \setminus \dots \setminus A_{i_k}$ je sudým podgrafem G , ale tato je podgrafem T , protože neobsahuje žádné neobsahující hrany

\Rightarrow strom nemá cykly \Rightarrow jediným s. podgrafem T je prázdny graf \emptyset

$\Rightarrow B \setminus A_{i_1} \setminus \dots \setminus A_{i_k} = \emptyset \Rightarrow B = A_{i_1} \cup \dots \cup A_{i_k} \Rightarrow X$ generuje V

\rightarrow velikost báze X $\rightarrow |V(T)| - 1$

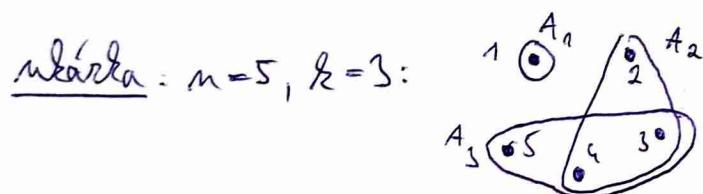
$$\dim(V) = |X| = |E(G)| - |E(T)| = |E(G)| - |V(G)| + 1$$

\Rightarrow když souvislý graf G má $2^{|E(G)| - |V(G)| + 1}$ sudých podgrafů.

• Množinové systémy s omezením na mohutností

Problém: Kolik podmnožin může mít n -prvová množina, pokud každá množina má mít lichou mohutnost a prvník každé dvojice různých podmnožin súdu mohutnost?

Hledáme: $\max \{ \ell \mid \exists A_1, \dots, A_\ell \subseteq \{1, \dots, n\} : \forall i \neq j : |A_i| \text{ je liché} \wedge |A_i \cap A_j| = 1 \}$



Pozorám: Jedenopravové podmnožiny dávají $\ell=n$.

Tvrzení: Vždy platí $\ell \leq n$. \rightarrow hledané maximum je n .

Důkaz: Postrojme matici incidence $M \in \mathbb{Z}_2^{\ell \times n}$: $m_{ij} = \begin{cases} 1, & \text{pokud } j \in A_i, \\ 0, & \text{jinak.} \end{cases}$

Pro příklad výše máme $M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$.

Matice splňuje $MM^T = I_\ell$, protože mod \mathbb{Z}_2 máme

$$(MM^T)_{ij} = \begin{cases} 1 & \text{pro } i=j \rightarrow \text{skalární součin se stejným rázem} \\ & \Rightarrow \text{lichý počet jedniček} \Rightarrow 1 \\ 0 & \text{pro } i \neq j \rightarrow |A_i \cap A_j| \text{ je sudý} \rightarrow \text{sudý počet jedniček} \Rightarrow 0. \end{cases}$$

Nyní $\text{rank}(I_\ell) = \ell = \text{rank}(MM^T) \leq \text{rank}(M) \leq n \Rightarrow \ell \leq n \quad \square$

Dělení obdélníku na čtverce

Problém: Ze obdélník s iracionálním poměrem délky stran rozdělit na konečně mnoho čtverců? (pro racionalní $f: \mathbb{R} \rightarrow \mathbb{Q}$ lze $f(g)$ čtvrtci)

Tworem: Pro iracionální poměr žádné takové rozdělení neexistuje.

Dle: Nechť má obdélník R délky strana $1:x$, kde $x \in \mathbb{R} \setminus \mathbb{Q}$.

- Všimněme si, že R nerozšířitelný nad \mathbb{Q} , kde jsou 1 a x l. nezávislé
 $\therefore \nexists q \in \mathbb{Q}: q \cdot x = -1 \Rightarrow \{1, x\}$ lze rozšířit na bázi.

- Zvolme libovolné l.z. $f: \mathbb{R} \rightarrow \mathbb{R}$ l.z. $f(1) = 1$, $f(x) = -1$.

- Pro obdélník A o stranách a, b definujeme „plochu“ $v(A) := f(a) \cdot f(b)$.

- Potom postupně svíle rozdělíme A na B_1, \dots, B_k , pak $v(A) = \sum_i v(B_i)$.

\therefore když A dělíme na B_1 a B_2 , pak $v(A) = v(B_1) + v(B_2)$ — indukce

$$f(a) f(b) = f(a_1 + a_2) f(b) = f(a_1) f(b) + f(a_2) f(b) = v(B_1) + v(B_2)$$

- Pro spor předpokládejme, že R lze rozdělit na čtverce A_1, \dots, A_k o stranách délky a_1, \dots, a_k . Nyní prodloužíme jejich strany, čímž získáme jemnější tabulkové rozdělení R na obdélníky B_1, \dots, B_m . Pak:

$$-1 = f(1) f(x) = v(R) = \sum_j v(B_j) = \sum_i v(A_i) = \sum_i f(a_i)^2 \geq 0. \quad \square$$