- Reálný vektor

Def: Reálný vektor $b$ o $m$ složkách je uspořádaná $m$-tice 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 $O = (0, 0, \dots 0)^T \in \mathbb{R}^m$
- Vektor neznámých $x = (x_1, x_2, \dots x_m)^T \in \mathbb{R}^m$

- Reálná matice

Def: Reálná matice $A$ řádu $m \times n$ je soubor $m \cdot n$ reálných č. uspořádaných do tabulky s $m$ řádky a $n$ sloupci:

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

- prvky značíme $a_{ij}$, pokud jde o nějaký složitější výraz $Sad(A)_{ij}$

- Soustava lineárních 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 neznámých. Soustava $m$ lin. rovnic o $n$ neznámých je

$$Ax = b,$$

tedy:

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

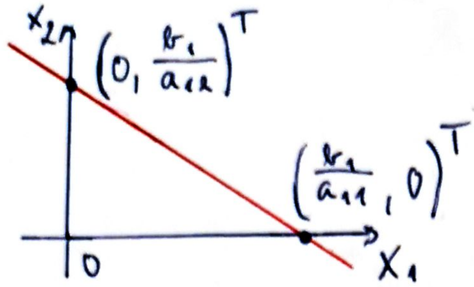
$A$ je matice soustavy
$b$ je vektor pravých stran
$(A|b)$ je rozšířená matice soustavy

- Vektor $x \in \mathbb{R}^n$ je řešení soustavy $Ax = b$
  $\iff \forall i \in \{1, 2, \dots m\}: a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n = b_i$
- Soustavy $Ax = 0$ se nazývají homogenní a vždy umožňují $x = 0$

## • Geometrický pohled na věc

### • 1 rovnice o 2 neznámých

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




→ je-li $a_{11} \neq 0 \vee a_{12} \neq 0$ pak množina řešení tvoří přímku ve 2D Eu. rovině

→ změna $b$ ⇒ posun přímky

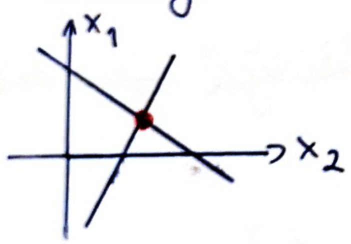
→ degenerované případy

- $a_{11} = a_{12} = 0 \wedge b_1 \neq 0$ ⇒ soustava nemá řešení
- $a_{11} = a_{12} = 0 \wedge b_1 = 0$ ⇒ 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
⇒ průsečík 2 přímek

→ více rovnic o 2 neznámých

a) 1 ř. ⇒ všechny přímky se protínají v 1 bodě

b) ∞ ř. ⇒ ——||—— jsou totožné

c) ∅ ⇒ 2 přímky jsou ∥ nebo vzniknul

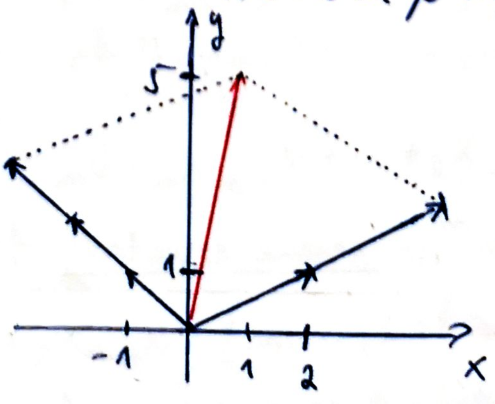
② sloupečky

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

→ hledám takové $x_1, x_2$, aby výsledný součet vektorů na levé straně byl roven vektoru pravých stran

- $2x - y = 1$
  $x + y = 5$

↳ $x\begin{pmatrix} 2 \\ 1 \end{pmatrix} + y\begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \end{pmatrix}$




⇒ $x = 2$
$y = 3$
$(2, 3)^T$

• **1 rovnice o 3 neznámých**

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

⇒ v nedegenerovaném případě $a_{11} \neq 0 \vee a_{12} \neq 0 \vee a_{13} \neq 0$ tvoří množina řešení rovina v 3-rozměrném Eukleidovském prostoru

→ změna $b$ ⇒ posun roviny

⇒ degenerované případy – pro více rovnic o 3 neznámých

- nemá řešení ⇒ 2 roviny jsou ∥ nebo vzniká  nebo 
  ↳ nebo $0A = b,\ b \neq 0$. 2r. 3r. 4r.
- všechny body prostoru: $0A = 0$

• rovnice o 4 a více neznámých ⇒ množina řešení tvoří nadrovina

## • Elementární ekvivalentní řádkové úpravy

Def: $A \sim A'$ píšeme, pokud lze $A'$ získat z $A$ jakoukoli z násl. úprav:

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

$$a'_{kl} = \begin{cases} a_{kl} & \text{pro } k \neq i \quad \leftarrow \text{neměním} \\ \lambda \cdot a_{kl} & \text{pro } k = i \quad \leftarrow \text{násobím } \lambda \end{cases}$$

② přičtení $j$-tého řádku k $i$-tému řádku

$$a'_{kl} = \begin{cases} a_{kl} & \text{pro } k \neq i \quad \leftarrow \text{neměním} \\ a_{kl} + a_{jl} & \text{pro } k = i \quad \leftarrow \text{přičtu } a_{jl} \end{cases}$$

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

- $\lambda = 0$: nedělám nic
- $\lambda \neq 0$: $\begin{pmatrix} i \\ j \end{pmatrix} \sim \begin{pmatrix} i \\ \lambda \cdot j \end{pmatrix} \sim \begin{pmatrix} i + \lambda \cdot j \\ \lambda \cdot j \end{pmatrix} \sim \begin{pmatrix} i + \lambda \cdot j \\ j \end{pmatrix}$

④ záměna dvou řádků

$\begin{pmatrix} i \\ j \end{pmatrix} \sim \begin{pmatrix} i+j \\ j \end{pmatrix} \sim \begin{pmatrix} -i-j \\ j \end{pmatrix} \sim \begin{pmatrix} -i-j \\ -i \end{pmatrix} \sim \begin{pmatrix} -i-j \\ i \end{pmatrix} \sim \begin{pmatrix} -j \\ i \end{pmatrix} \sim \begin{pmatrix} j \\ i \end{pmatrix}$

} úpravy ③, ④ lze získat z úprav ①, ②

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

• 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 totožné množiny řešení.

Důkaz: Stačí ukázat, že množina řešení je zachována po provedení jediné úpravy ① nebo ②. Chceme ukázat, že platí:

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

Rovnost množin plyne ze dvou inkluzí $\subseteq$, $\supseteq$, které přepíšeme do implikací:

$$a)\ Ax=b \Rightarrow A'x=b' \qquad b)\ A'x=b' \Rightarrow Ax=b.$$

1a) $Ax=b \Rightarrow A'x=b'$ pro vynásobení $i$-tého řádku $\lambda\neq 0$

→ mění se pouze $i$-tý ř. ⇒ ostatní nemusíme ověřovat

$$a'_{i1}x_1+a'_{i2}x_2+\dots+a'_{in}x_n=\lambda(a_{i1}x_1+\dots a_{in}x_n)=\lambda\cdot b_i=\underline{\underline{b'_i}}\ \blacksquare$$

1b) $A'x=b' \Rightarrow Ax=b$ pro ①

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

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

$$a'_{i1}x_1+a'_{i2}x_2+\dots a'_{in}x_n=(a_{i1}+a_{j1})x_1+\dots+(a_{in}+a_{jn})x_n=$$
$$=(a_{i1}x_1+\dots a_{in}x_n)+(a_{j1}x_1+\dots+a_{jn}x_n)=b_i+b_j=\underline{\underline{b'_i}}\ \blacksquare$$

2b) $A'x=b' \Rightarrow Ax=b$ pro ②

$$a_{i1}x_1+a_{i2}x_2+\dots+a_{in}x_n=(a'_{i1}-a_{j1})x_1+\dots+(a'_{in}-a_{jn})x_n=$$
$$=(a'_{i1}x_1+\dots+a'_{in}x_n)-(a_{j1}x_1+\dots+a_{jn}x_n)=$$
$$=b'_i-b_j=b_i+b_j-b_j=\underline{\underline{b_i}}$$

$\blacksquare$

- **Geometrický význam el. úprav**

① ④ násobení nebo záměna nemění polohu nadrovin

② ③ přičtení řádku změní polohu nadroviny tak, že průnik zůstává beze změny

- **Gaussova eliminace**

① Sestavíme rozšířenou matici soustavy

② Pomocí elementárních úprav převedeme matici do REF

③ Zpětnou substitucí popíšeme všechna řešení soustavy

- **Řádkově odstupňovaný tvar matice** = REF

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

→ pozice prvního nenulového prvku v i-tém řádku je

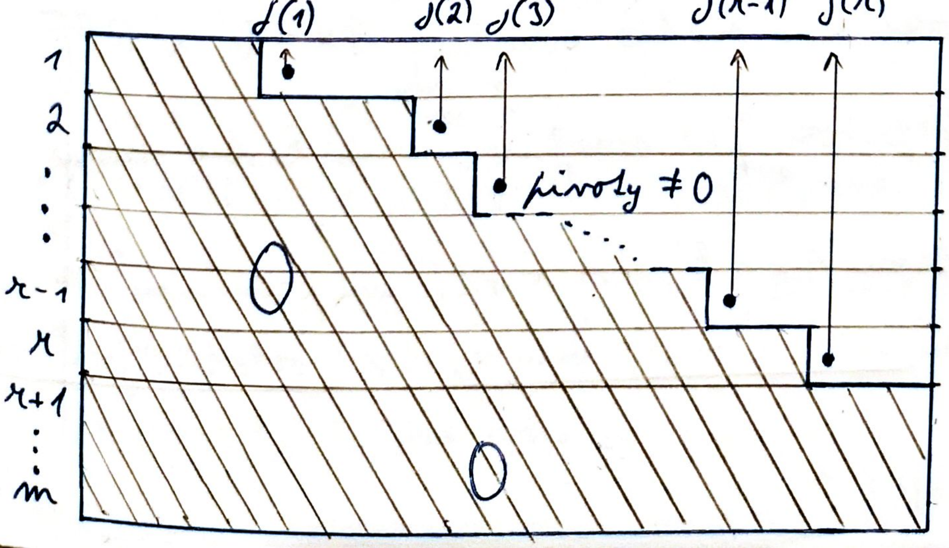
$$j(i) := \min(j \mid a_{ij} \neq 0)$$

→ první nenulové prvky $a_{ij(i)}$ se nazývají pivoty

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

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

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




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

není v REF

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

je v REF

- **Naivní algoritmus pro Gaussovu eliminaci**
  - → Input: Matice $A$
  - → Output: Matice $A$ v REF
  - → $\forall i \in \{1, \dots m\}$: urči $j(i)$ # nulový řádek : $j(i) = \infty$
  - → Seřaď řádky $A$ podle $j(i)$
  - → Forever:
    - → if $\exists i: j(i) = j(i+1) < \infty$:

      # $i$-tý a $(i+1)$-ní řádky jsou nenulové a mají stejný

      # počet počátečních nul

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

      # nyní: $a_{i+1, j(i)} = 0$

      - → aktualizuj $j(i+1)$ a seřaď řádky podle $j(i)$
    - → else:

      # všechny nenulové řádky mají různý počet počátečních nul

      - → return $A$
  - → **konečnost** → $O\left(\frac{m(m-1)}{2}\right) \in O(m^2)$ aritmetických operací
    - → v každé iteraci roste celkový počet počátečních nul

- **Zpětná substituce**

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

  **Pozorování**: Je-li v $b'$ pivot, pak soustava nemá žádné řešení.

  **Definice**: Pro soustavu $A'x = b'$ s $A'$ v REF jsou proměnné odpovídající sloupcům s pivoty bázické, ostatní jsou volné.

• Zpětná substituce

Věta: Pro $A'x = b'$ s $(A'|b')$ v REF a bez pivotu v $b'$ lze jakoukoli volbu volných proměnných jednoznačně rozšířit na řešení.

Důkaz: Chceme ukázat, že hodnoty bázických proměnných jsou jednoznačné.

→ Indukcí podle $i = r, r-1, \dots 1$.

1) v $r$-té rovnici:

pivot

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

bázická proměnná   volné proměnné

→ hodnoty všech volných proměnných jsou známy

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

2) v $i$-té rovnici, $i < r$:

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

pivot   bázická proměnná

→ hodnoty všech volných proměnných jsou známy

→ hodnoty všech následujících bázických proměnných

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

jsou známy z indukčního předpokladu

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

Q.E.D.

Ukázka:

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

→ proměnné $x_1, x_3, x_5$ jsou bázické

→ proměnné $x_2, x_4$ jsou volné

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

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

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

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

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

- Zpětná substituce

Věta: Zpětnou substitucí lze nalézt jakékoli řešení.

Důkaz: V libovolném řešení $X$ jsou hodnoty bázických proměnných $X$ jednoznačně určeny volnými proměnnými $X$.

Věta: Pro libovolnou matici $A$ a libovolnou $A'$ v REF takovou, že $A \sim\sim A'$ jsou indexy sloupců s pivoty v $A'$ určeny jednoznačně podle $A$

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

$\Rightarrow$ všechny proměnné $X_{i+1}, \dots X_n$ mají stejný charakter v $A'$ i $A''$

$\Rightarrow$ 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 $A''$ stejné jako výše (což nám dá stejné hodnoty následujících bázických proměn.), ale hodnotu $X_i$ odlišně

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

v $A$ je rovnice, kde je proměnná $X_i$ u pivotu:

Q.E.D.

$$0 + 0 + 0 + \dots + a_{ki} X_i + \underbrace{a_{k,i+1} X_{i+1} + \dots + a_{k,n} X_n}_{\text{předem určené z následujících rovnic}} = 0$$

nyní do této rovnice dosadíme řešení soustavy $A''x = 0$:

$$0 + 0 + \dots + 0 \cdot X'_{i-1} + a_{ki} X'_i + \underbrace{\dots\dots}_{\text{stejné jako}} = 0$$

v soustavě $A''x = 0$ je bázická proměnná v $k$-tém řádku někde před $X_i$

$\Rightarrow$ víme, že $X'_i \neq X_i$, rovnost tedy nenastane

- Hodnost matice

Definice: Hodnost matice $A$, značená jako $\text{rank}(A)$ je počet pivotů v libovolné $A'$ v REF takové, že $A \sim\sim A'$.

- Frobeniova věta

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

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

Řešení $x$ existuje $\iff$ $b'$ nemá žádný pivot
$\iff$ pivoty $A'$ se shodují s pivoty $(A'|b')$
$\iff$ $\text{rank}(A) = \text{rank}(A|b)$. Q.E.D.

- Homogenní a nehomogenní soustavy

Pozorování:

$$(A|0) = \left(\begin{array}{ccccc|c} 1 & 4 & 3 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 \end{array}\right) \quad \left.\begin{array}{l} p_1 := x_2,\ p_2 := x_4 \\ \Rightarrow x_5 = 0 \\ \Rightarrow x_3 = -2p_2 \\ \Rightarrow x_1 = -4p_1 - 2p_2 + 6p_2 \end{array}\right\} \bar{x} = p_1 \begin{pmatrix} -4 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + p_2 \begin{pmatrix} 4 \\ 0 \\ -2 \\ 1 \\ 0 \end{pmatrix}$$

$$(A|b) = \left(\begin{array}{ccccc|c} 1 & 4 & 3 & 2 & 1 & 4 \\ 0 & 0 & 1 & 2 & 1 & 5 \\ 0 & 0 & 0 & 0 & 6 & 6 \end{array}\right) \quad \left.\begin{array}{l} \Rightarrow x_5 = 1 \\ \Rightarrow x_3 = 4 - 2p_2 \\ \Rightarrow x_1 = 3 - 2p_2 - 12 + 6p_2 - 4p_1 \end{array}\right\} \begin{array}{l} x = x_0 + \bar{x} \\ x = \begin{pmatrix} -9 \\ 0 \\ 4 \\ 0 \\ 1 \end{pmatrix} + p_1 \begin{pmatrix} -4 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + p_2 \begin{pmatrix} 4 \\ 0 \\ -2 \\ 1 \\ 0 \end{pmatrix} \end{array}$$

→ řešení nehomogenní a homogenní soustavy se stejnou maticí soustavy $A$ se liší pouze o vektor $x_0$, který je řešením $Ax = b$.

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

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

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 $Ax = b$.

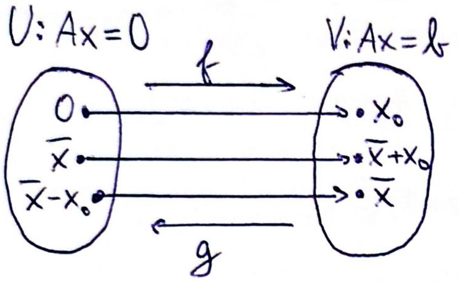
Důkaz: $Ax = A(x_0 + \bar{x}) = Ax_0 + A\bar{x} = b + 0 = b$ ▨

## • 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 $f: U \to V$ t.ž. $f(\bar{x}) = \bar{x} + x_0$

$g: V \to U$ t.ž. $g(x) = x - x_0$.




→ Chceme ukázat, že $f$ je bijekce

⟺ $f$ je prosté a $f$ je „na"

- $f \circ g: U \to V \to U$ je identita na $U$ ⇒ $f$ je prosté
  ↳ kdyby $f$ nebylo prosté, tak se stane a zpátky bych musel 1 vzoru přiřadit 2 obrazy ⇒ $g$ by nebylo zobrazení ⇒ SPOR

- $g \circ f: V \to U \to V$ je identita na $V$ ⇒ $g$ je prosté ⇒ $f$ je „na"
  ↳ $g$ je prosté ⇒ každý bod z $V$ se zobrazí na právě 1 z $U$
  ↳ kdyby $f$ nebylo „na", tak se stane ⇒ $f$ by nebylo prosté ⇒ SPOR

- $f$ je prosté a $f$ je „na" ⇒ $f$ je bijekce Q.E.D.

**Důkaz 2:** Označme zobrazení $f: U \to V$ takové, že $f(\bar{x}) = \bar{x} + x_0$, ukážeme, že $f$ je bijekce.

- Předpokládejme pro spor, že $f$ není prosté
  ↳ dvěma různým vstupům by přiřadilo stejný výstup
  ↳ ke vstupu vždy přičítám $x_0$ ⇒ nemůžu pro různé vstupy dostat stejný výstup
  ⇒ SPOR

- Vezměme libovolné řešení $x$ soustavy $Ax = b$.
  ⇒ $x - x_0$ řeší $Ax = 0$ ⇒ $f(x - x_0) = x$
  ⇒ k libovolnému $x \in V$ jsem našel jeho vzor ⇒ $f$ je „na"

- $f$ je prosté a $f$ je „na" ⇒ $f$ je bijekce Q.E.D.

## • Řešení homogenních soustav

**Věta:** Je-li $A \in \mathbb{R}^{m \times n}$ matice hodnosti $r$, pak všechna řešení $A\overline{x} = 0$ lze popsat jako $\overline{x} = p_1 \overline{x}^1 + p_2 \overline{x}^2 + \dots + p_{n-r} \overline{x}^{n-r}$, kde

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

Soustava má pouze triviální řešení $\overline{x} = 0 \iff \operatorname{rank}(A) = n$.

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

Protože hodnoty bázických proměnných jsou jednoznačně určeny volnými, můžeme každou složku řešení vyjádřit jako lineární fci volných proměnných

$$\overline{x}_1 = \alpha_{1,1} p_1 + \dots + \alpha_{1,n-r} p_{n-r}$$
$$\vdots$$
$$\overline{x}_n = \alpha_{n,1} p_1 + \dots + \alpha_{n,n-r} p_{n-r}.$$

→ Zvolíme

$$\overline{x}^1 = (\alpha_{1,1}, \dots \alpha_{n,1})^T, \dots \overline{x}^{n-r} = (\alpha_{1,n-r}, \dots \alpha_{n,n-r})^T$$

→ Tyto vektory řeší $A\overline{x} = 0$, protože každý takový $\overline{x}^i$ dostaneme volbou parametrů $p_i = 1$, $\forall j \neq i : p_j = 0$.

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

Q.E.D.

## • Řešení nehomogenních soustav

**Důsledek 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 $Ax = b$ lze popsat jako:

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

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

- Příklad řešení soustavy $Ax=b$

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

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

② Pokud je pivot v posledním sloupci, žádné řešení neexistuje.

③ Jinak vyřešíme nejprve homogenní soustavu $A'\bar{x}=0$:

$\bar{x}_5 = 0$ , $\bar{x}_3 = -2\bar{x}_4$ , $\bar{x}_1 = -4\bar{x}_2 - 3\bar{x}_3 - 2\bar{x}_4 = -4\bar{x}_2 + 4\bar{x}_4$

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

$\bar{x} = p_1(-4,1,0,0,0)^T + p_2(4,0,-2,1,0)^T$

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

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

$\Rightarrow x = (-\frac{4}{3}, 0, \frac{2}{3}, 0, \frac{1}{3})^T + p_1(-4,1,0,0,0)^T + p_2(4,0,-2,1,0)^T$

- Gauss-Jordanova eliminace

- Redukovaný odstupňovaný tvar - RREF

**Def:** Odstupňovaný tvar matice je redukovaný, pokud je každý pivot roven jedné a všechny ostatní prvky ve sloupcích s pivoty jsou nuly.

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

**Důkaz:** Pro spor budeme předpokládat, že $A'$, $A''$ jsou v RREF a $A \sim\sim A' \sim\sim A''$.
Poslední volnou proměnnou, která má v $A'$ a $A''$ jiný koeficient označíme $x_k$. Tento koeficient se nachází v nějakém řádku $i$, je tedy $a'_{ik}$, $a''_{ik}$.
Volbou volných proměnných $x_k = 1$, $\forall j \neq k: k_j = 0$ dostaneme v $i$-tých řádcích:

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

Což je spor, protože bázické proměnné jsou určeny volnými jednoznačně.
Vektor $b$ musí být v $A'$ i $A''$ stejný, volbou v.p. $\forall j: x_j = 0$ bychom dostali spor.

- Libovolnou matici v REF lze redukovat takto

1) vydělíme řádky $a_{ij(i)}$, čímž získáme 1 jako pivoty.

2) pro každé $i = r, \dots 1$, eliminujeme každé $a_{i'j(i)}$ s $i' < i$ přičtením $-a_{i'j(i)}$ násobku $i$-tého řádku k $i'$-tému řádku, čímž nad pivotem $a_{ij(i)}$ dostaneme nuly.

- Výhody RREF

→ vhodnou volbou volných proměnných lze RREF snadno přečíst řešení

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

1) volba $x_2 = x_4 = 0$ dává přímo 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 přímo první vhodné řešení $Ax = 0$:

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

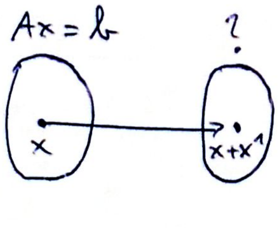
3) volba $x_2 = 0$, $x_4 = 1$ dává přímo druhé vhodné řešení $Ax = 0$

$$\text{I}: x_1 + 0 + 0 - 4 + 0 = 0 \Rightarrow x_1 = 4$$
$$\text{II}: x_3 + 2 + 0 = 0 \Rightarrow x_3 = -2$$
$$\Rightarrow \bar{x}^2 = (4, 0, -2, 1, 0)^T$$

→ když chci nějaké vhodné řešení $Ax = 0$, tak si vyberu proměnnou, třeba $x_4$ → 4. sloupeček → a hodnoty bázických proměnných = − hodnoty ve 4. sl.

- Příklad

Označme $V = \{x \mid Ax = b\}$ a mějme $x^1 \in V$. Jaký je obraz množiny $V$ v zobrazení $x \mapsto x + x^1$?




$$Ax = b \rightarrow A(x + x^1) = Ax + Ax^1 = b + b$$

⇒ obrazem $V$ 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 $I_n \in \mathbb{R}^{n \times n}$ definována jako $(I_n)_{i,j} = 1$ pro $i = j$; a jinak $(I_n)_{i,j} = 0$.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3$$

### Hlavní diagonála

**Def:** Hlavní diagonálu čtvercové matice $A$ tvoří prvky $a_{i,i}$.

### 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:** $\alpha$-násobek matice $A \in \mathbb{R}^{m \times n}$, $\alpha \in \mathbb{R}$ je $(\alpha A) \in \mathbb{R}^{m \times n}$ taková, že

$$(\alpha A)_{ij} = \alpha \cdot a_{ij}.$$

- **Součin matic**

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

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik}\, b_{kj}.$$ → skalární součin i-tého ř. A a j-tého s. B

Př.:

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

$$\begin{array}{cccc|cc} & & & & 1 & 2 \\ & & & & 0 & 3 \\ & & & & 2 & 0 \\ & & & & 0 & 1 \\ \hline 1 & 2 & 4 & 0 & 9 & 6 \\ 0 & 0 & 1 & 3 & 2 & 3 \\ 3 & 1 & 2 & 0 & 7 & 9 \end{array} \longrightarrow \quad \begin{array}{c|c} & B \\ \hline A & AB \end{array}$$

Pozorování: Maticový součin $AB$ pro $A \in \mathbb{R}^{m\times n}$, $B \in \mathbb{R}^{n\times p}$ vyžaduje

- $m\cdot n\cdot p$ násobení → $A$ má $m\cdot n$ prvků, každý násobím s $p$ prvky
- $m\cdot p\cdot(n-1)$ sčítání → pro $m\cdot p$ prvků počítám sumu o $n$ členech

⇒ celkem $mp(2n-1) = 2mnp - mp \approx$ $mnp$ aritmetických operací

- **Vztahy platící pro operace s maticemi**

Tvrzení: Jsou-li výsledky operací definovány, pak:

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

- Vztahy platící pro součin matic

① Ukažte, že $AA^T$ je symetrická pro libovolné $A$

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

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

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

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

$$(A I_n)_{ij} = \sum_{k=1}^{n} a_{ik}(I_n)_{kj} = a_{ij}(I_n)_{jj} = a_{ij} \quad \blacksquare$$

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

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

$$\begin{array}{cc|cc} & & 1 & 2 \\ & & 3 & 4 \\ \hline 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 2 \end{array} \qquad \begin{array}{cc|cc} & & 1 & 0 \\ & & 2 & 0 \\ \hline 1 & 2 & 5 & 0 \\ 3 & 4 & 11 & 0 \end{array}$$

$$AB = \begin{pmatrix}1 & 2\\ 2 & 2\end{pmatrix} \qquad BA = \begin{pmatrix}5 & 0\\ 11 & 0\end{pmatrix}$$

Tvrzení: Jsou-li výsledky operací definovány, pak:

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

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

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

Dk: $$((AB)C)_{ij} = \sum_{k=1}^{p} (AB)_{ik} c_{kj} = \sum_{k=1}^{p} \left(\sum_{l=1}^{n} a_{il} b_{lk}\right) c_{kj} = \sum_{k=1}^{p}\sum_{l=1}^{n} a_{il} b_{lk} c_{kj} =$$

$$= \sum_{l=1}^{n}\sum_{k=1}^{p} a_{il} b_{lk} c_{kj} = \sum_{l=1}^{n}\left(a_{il} \sum_{k=1}^{p} b_{lk} c_{kj}\right) = \sum_{l=1}^{n} a_{il}(BC)_{lj} =$$

$$= (A(BC))_{ij} \quad \blacksquare$$

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

$$((A+B)C)_{ij} = \sum_{k=1}^{n} (A+B)_{ik} c_{kj} = \sum_{k=1}^{n} (a_{ik} c_{kj} + b_{ik} c_{kj}) = (AC)_{ij} + (BC)_{ij} = (AC+BC)_{ij} \quad \blacksquare$$

④ $A(B+C) = AB + AC \quad A \in \mathbb{R}^{m \times n} \Rightarrow B, C \in \mathbb{R}^{n \times p}$

$$(A(B+C))_{ij} = \sum_{k=1}^{n} a_{ik} (B+C)_{kj} = \sum_{k=1}^{n} (a_{ik} b_{kj} + a_{ik} c_{kj}) = (AB)_{ij} + (AC)_{ij} = (AB+AC)_{ij} \quad \blacksquare$$

• Efektivita výpočtu součinu

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

| | B | C |
|---|---|---|
| A | AB | (AB)C |

$$\left.\begin{aligned} AB &\approx mnp \\ (AB)C &\approx mpq \end{aligned}\right\} mp(n+q) \text{ aritmetických operací}$$

| | C |
|---|---|
| B | BC |
| A | A(BC) |

$$\left.\begin{aligned} BC &\approx npq \\ A(BC) &\approx mnq \end{aligned}\right\} nq(p+m) \text{ arit. operací}$$

→ i když je konečný výsledek v obou směrech stejný, vhodné pořadí dílčích součinů může ovlivnit celkovou výpočetní náročnost

• Elementární matice

Pozorování: Nechť $B$ je matice získaná z $A$ pomocí elementární úpravy, potom existuje elementární matice $E$ t.ž. $B = EA$

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

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

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

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

- Inverzní matice

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

- Regulární a Singulární matice

Def: Pokud má $A$ inverzi, pak se nazývá regulární, jinak je singulární

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

1. $\iff \exists B \in \mathbb{R}^{n \times n} : AB = BA = I_n$
2. $\iff rank(A) = n$
3. $\iff A \sim\sim I_n$
4. $\iff Ax = 0$ má pouze triviální řešení $x = 0$.

Důkaz:

2.$\iff$4. je triviální

2.$\Rightarrow$3. pomocí Gauss-Jordanovy eliminace, $3 \Rightarrow 2$ triviálně

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

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

→ pokud $A^{-1}x = 0$ má řešení, pak $x = I_n x = AA^{-1}x = A(A^{-1}x) = A0 = 0$. (4.)

⇒ existuje tedy $(A^{-1})^{-1}$ a dostáváme

$$A^{-1}A = A^{-1}A\,I_n = A^{-1}A\left(A^{-1}(A^{-1})^{-1}\right) = A^{-1}(I_n)(A^{-1})^{-1} = A^{-1}(A^{-1})^{-1} = I_n \quad \blacksquare$$

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

1.$\Rightarrow$2. Pro spor budeme předpokládat $rank(A) < n$, pak pro nějaké $i$ může být $i$-tý řádek $A$ eliminován ostatními 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 ⇒ $A$ nemá inverzi ⇒ SPOR

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

- Výpočet inverzní matice

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

Dk.: Provádění elementárních úprav odpovídá násobení el. maticemi

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

$\hookrightarrow E_k \dots E_2 E_1 A = I_n \Rightarrow A^{-1} = E_k \dots E_2 E_1$
$\hookrightarrow E_k \dots E_2 E_1 I_n = B \Rightarrow B = E_k \dots E_2 E_1$
$\Big\}\ B = A^{-1}$ $\blacksquare$

→ sloupce $B$ jsou ve skutečnosti řešení soustav $Ax^i = e^i$.

- Vlastnosti regulární matice

  - Krácení matic: Pokud je $R$ regulární, pak:

    1, $AR = BR \Leftrightarrow A = B$. Dk: $A = AI_n = ARR^{-1} = BRR^{-1} = BI_n = B$ $\blacksquare$

    2, $RA = RB \Leftrightarrow A = B$. Dk: $A = I_n A = R^{-1}RA = R^{-1}RB = I_n B = B$ $\blacksquare$

  - Regulární matice $A, B$ stejného řádu splňují

    1, $(A^{-1})^{-1} = A$. Dk: $(A^{-1})^{-1} = (A^{-1})^{-1}A^{-1}A = I_n A = A$ $\blacksquare$

    2) $(AB)^{-1} = B^{-1}A^{-1}$. Dk: $(AB)^{-1} = B^{-1}B(AB)^{-1} = \underbrace{B^{-1}(A^{-1}}\underbrace{A)B}(AB)^{-1} = B^{-1}A^{-1}I_n = B^{-1}A^{-1}$ $\blacksquare$

    3) $(A^T)^{-1} = (A^{-1})^T$. Dk: $AA^{-1} = A^{-1}A = I_n \Rightarrow (AA^{-1})^T = (A^{-1}A)^T = I_n^T$
    $\Rightarrow (A^{-1})^T A^T = A^T (A^{-1})^T = I_n \Rightarrow (A^T)^{-1} = (A^{-1})^T$ $\blacksquare$

    4) $AB$ je regulární. Dk: $AA^{-1} = I_n \Rightarrow ABB^{-1}A^{-1} = I_n \Rightarrow (AB)^{-1} = B^{-1}A^{-1}$ $\blacksquare$

  - Maticové rovnice

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

$aX = B \Rightarrow X = \frac{1}{a}B$

$AX = B \Rightarrow X = A^{-1}B$
$XA = B \Rightarrow X = BA^{-1}$
$\Big\}$ pro regulární $A$

• **Binární operace**

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

Příklady: $+, -, \cdot$ na $\mathbb{R}$

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

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

→ maticový součet na maticích stejného řádu

→ součin na čtvercových maticích stejného řádu

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

→ $(p, q) \to r$, kde $\forall x \in \mathbb{R}: r(x) = p(x) + q(x)$ je binární operace na množině všech reálných fcí $\mathbb{R}[x]$

• **Grupa**

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

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

2) $\exists e \in G: \forall a \in G: a \circ e = e \circ a = a$ → existuje neutrální prvek

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

↳ nejmenší grupa je $(\{e\}, \circ)$

• **Abelovská grupa**

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

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

• **Aditivní grupy**

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

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

→ $(\mathbb{N}, +)$ není grupa, nesplňuje axiom inverze

→ Neutrální prvek se nazývá nulový prvek a značí se $0$.

→ Inverzní prvek se nazývá opačný a namísto $a^{-1}$ se značí $-a$.

→ lze zavést binární operaci rozdíl jako $a - b := a + (-b)$.

→ $(G, -)$ není grupa, nesplňuje asociativitu

• Multiplikativní grupy

Def: Grupy $(G, \circ)$, kde $\circ$ je odvozena od součinu se nazývají multiplikativní

$\Rightarrow (\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q}^+, \cdot)$, $(\{-1, 1\}, \cdot)$, $(\{z \in \mathbb{C}, |z| = 1\}, \cdot)$ jsou abelovské mult.

- $(\mathbb{R}, \cdot)$ není grupa, protože 0 nemá inverzi
- $(\mathbb{R}^{n \times n}, \cdot)$ je m. grupa pro regulární matice.
- neutrální prvek se někdy značí 1
- lze zavést podíl jako $a : b = a : b^{-1}$.

• Vlastnosti grup

Pozorování: Neutrální prvek je určen jednoznačně.

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

Pozorování: Inverzní prvek k prvku a je určen jednoznačně.

Důkaz: Pokud by $b$ i $b'$ byly inverzní 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 žádném ř. nebo s. opakovat stejné č. dvakrát

$a \circ c = b \circ c \iff a = b$. Dk: $a = a \circ c \circ c^{-1} = b \circ c \circ c^{-1} = b$ ∎

$c \circ a = c \circ b \iff a = b$. Dk: $a = c^{-1} \circ c \circ a = c^{-1} \circ c \circ b = b$ ∎

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

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

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

Tvrzení:

$(a^{-1})^{-1} = a$. Dk: $(a^{-1})^{-1} = e \circ (a^{-1})^{-1} = a \circ a^{-1} \circ (a^{-1})^{-1} = a \circ (a^{-1} \circ (a^{-1})^{-1}) = a \circ e = a$ ∎

$(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ Dk: $(a \circ b)^{-1} = b^{-1} \circ b \circ (a \circ b)^{-1} = b^{-1} \circ (a^{-1} \circ a) \circ b \circ (a \circ b)^{-1} =$

$= b^{-1} \circ a^{-1} \circ (a \circ b) \circ (a \circ b)^{-1} = b^{-1} \circ a^{-1}$. ∎

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

$\Rightarrow (a \circ b) \circ (b^{-1} \circ a^{-1}) = e \Rightarrow (a \circ b)^{-1} = b^{-1} \circ a^{-1}$ ∎

• **Permutace**

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

Def: Permutace na množině $[n]$ je bijektivní zobrazení $p: [n] \to [n]$.

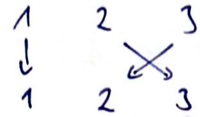
• **Znázornění permutace**

1) tabulkou:

| $i$ | 1 | 2 | 3 |
|---|---|---|---|
| $p(i)$ | 1 | 3 | 2 |

2) maticí $p = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ nebo $p = (1, 3, 2)$

3) bipartitním grafem



4) grafem cyklů

5) seznamem cyklů $(1)(2,3)$ nebo $(2,3)$ a triviální cykly délky 1 nepíšeme

6) permutační maticí $P$ $\quad P_{ij} = \begin{cases} 1 & \text{když } p(i) = j \\ 0 & \text{jinak} \end{cases} \qquad P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

↳ Pozorování: $P$ je el. matice odpovídající záměně více řádků.

$\Rightarrow$ $PA$ zamíchá řádky $A$ podle $p$

$\Rightarrow$ $AP$ zamíchá sloupce $A$ podle $p$

• **Symetrická grupa**

Pozorování: Množina všech permutací na $n$ prvcích $S_n$ tvoří s operací skládání $\circ$ grupu $(S_n, \circ)$, která se nazývá symetrická

Zápis skládání: $(q \circ p)(i) = q(p(i))$ → nejdříve uplatníme $p$, potom $q$

$$\begin{tikzcd} \boxed{i} \arrow[r, "p"] \arrow[rr, bend right, "q \circ p"'] & \boxed{p(i)} \arrow[r, "q"] & \boxed{q(p(i)) = (q \circ p)(i)} \end{tikzcd}$$

Důkaz:

1) $\circ$ je bin. o. na $S_n$ $\equiv$ složení dvou permutací je permutace

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

• $(\forall i \, \exists j: q(j) = i) \wedge (\forall j \, \exists k: p(k) = j) \Rightarrow (\forall i \, \exists k: q(p(k)) = i)$ $\Rightarrow$ $q \circ p$ je „na"

2) $(S_n, \circ)$ je grupa

- Skládání je asociativní:

$$\begin{tikzcd} \square \arrow[r, "p"] \arrow[rr, bend right, "q \circ p"'] & \square \arrow[r, "q"] \arrow[rr, bend left, "r \circ q"] & \square \arrow[r, "r"] & \square \end{tikzcd} \Rightarrow \begin{tikzcd} \square \arrow[r, "p"] \arrow[rrr, bend left, "(r \circ q) \circ p"] \arrow[rrr, bend right, "r \circ (q \circ p)"'] & \square \arrow[r, "q"] & \square \arrow[r, "r"] & \square \end{tikzcd}$$

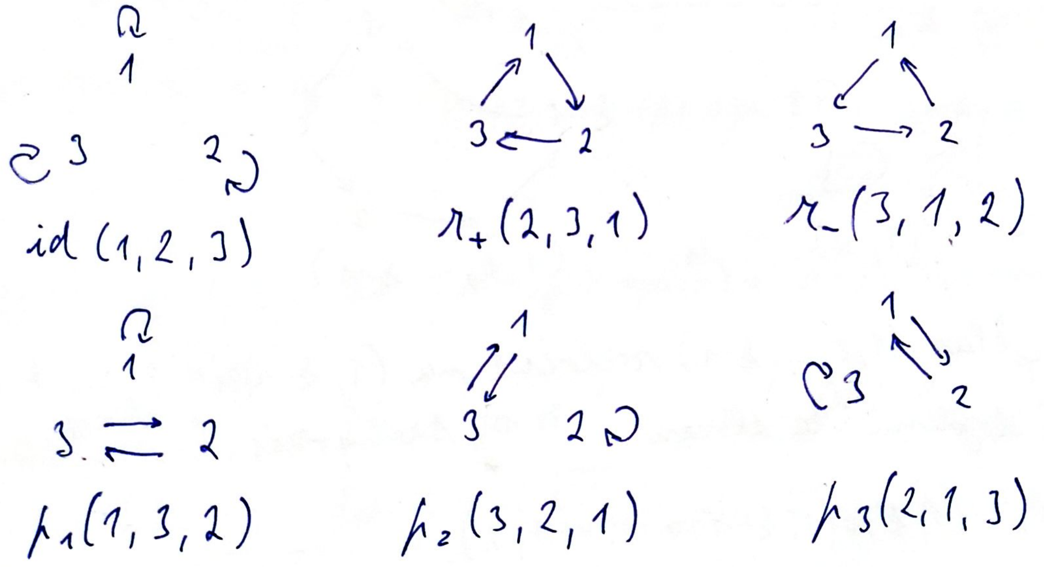
- Neutrální prvek = Identita: $id \in S_n : \forall i : id(i) = i$

- Inverzní permutace: $p(i) = j \iff p^{-1}(j) = i$ $\quad \begin{tikzcd} i \arrow[r, shift left, "p"] & j \arrow[l, shift left, "p^{-1}"] \end{tikzcd}$

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

- Grupa $S_3$

$$S_3 = \{(1,2,3), (1,3,2), (3,2,1), (2,1,3), (2,3,1), (3,1,2)\}$$
$$= \{ id, p_1, p_2, p_3, r_+, r_- \}$$



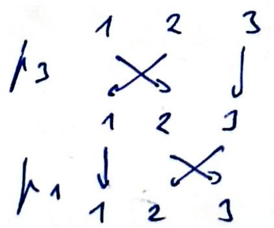

Operace skládání:

| $\circ$ | $id$ | $p_1$ | $p_2$ | $p_3$ | $r_+$ | $r_-$ |
|---|---|---|---|---|---|---|
| $id$ | $id$ | $p_1$ | $p_2$ | $p_3$ | $r_+$ | $r_-$ |
| $p_1$ | $p_1$ | $id$ | $r_+$ | $r_-$ | $p_2$ | $p_3$ |
| $p_2$ | $p_2$ | $r_-$ | $id$ | $r_+$ | $p_3$ | $p_1$ |
| $p_3$ | $p_3$ | $r_+$ | $r_-$ | $id$ | $p_1$ | $p_2$ |
| $r_+$ | $r_+$ | $p_3$ | $p_1$ | $p_2$ | $r_-$ | $id$ |
| $r_-$ | $r_-$ | $p_2$ | $p_3$ | $p_1$ | $id$ | $r_+$ |

inverzní permutace:

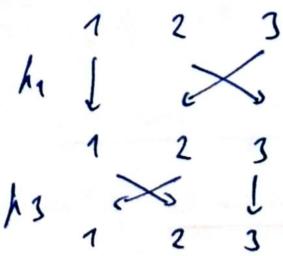
| $p$ | $id$ | $p_1$ | $p_2$ | $p_3$ | $r_+$ | $r_-$ |
|---|---|---|---|---|---|---|
| $p^{-1}$ | $id$ | $p_1$ | $p_2$ | $p_3$ | $r_-$ | $r_+$ |

$p_1 \circ p_3$




$\Rightarrow (3,1,2)$

$p_3 \circ p_1$




$\Rightarrow (2,3,1)$

• <u>Pevný bod</u>

<u>Def</u>: <u>Pevný bod</u> v permutaci $p$ je $i: p(i) = i$, t.j. triviální cyklus délky 1.

• <u>Transpozice</u>

<u>Def</u>: <u>Transpozice</u> je permutace, která má pouze 1 netriviální cyklus délky 2.

→ někdy se cyklu délky dva říká transpozice

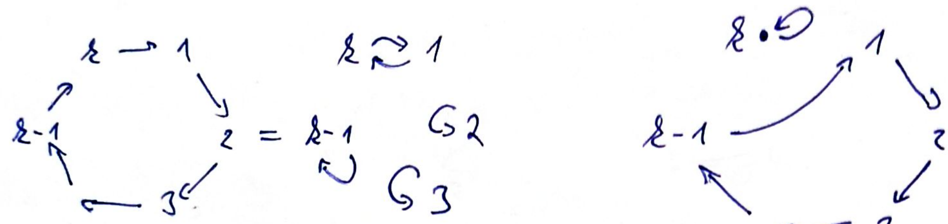
⇒ transpozice 1↺ 2↺ ... $i \rightleftarrows j$ ... n↺ se zapisuje jako $(i, j)$.

<u>Pozorování</u>: Jakoukoli permutaci lze rozložit na složení transpozic.

<u>Důkaz</u>: Cyklus $(1, 2, \dots k)$ lze rozložit na

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

→ cyklus délky 1 lze * rozložit na 2 transpozice



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

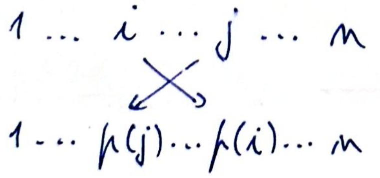
⇒ Potom lze cyklus $(1, 2, \dots k-1)$ rozložit na $(1, k-1) \circ (1, 2, \dots k-2)$ a indukcí dojdeme ke složení $k-1$ transpozic *

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

• <u>Inverze</u>

<u>Def</u>: Inverze v $p$ je dvojice $(i, j): i < j \wedge p(i) > p(j)$.

<u>Pozorování</u>: Inverze odpovídá křížení šipek v bipartitním grafu permutací




Počet inverzí $p = I(p)$

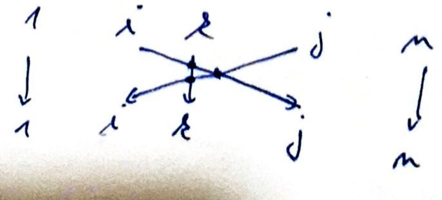
• <u>Znaménko permutace</u>

<u>Def</u>: <u>Znaménko</u> permutace $p$ je $sgn(p) = (-1)^{I(p)}$.

Permutace s kladným znaménkem jsou sudé, se záporným liché.

<u>Pozorování</u>: $sgn(id) = (-1)^0 = 1$

transpozice: $sgn((i, j)) = -1$

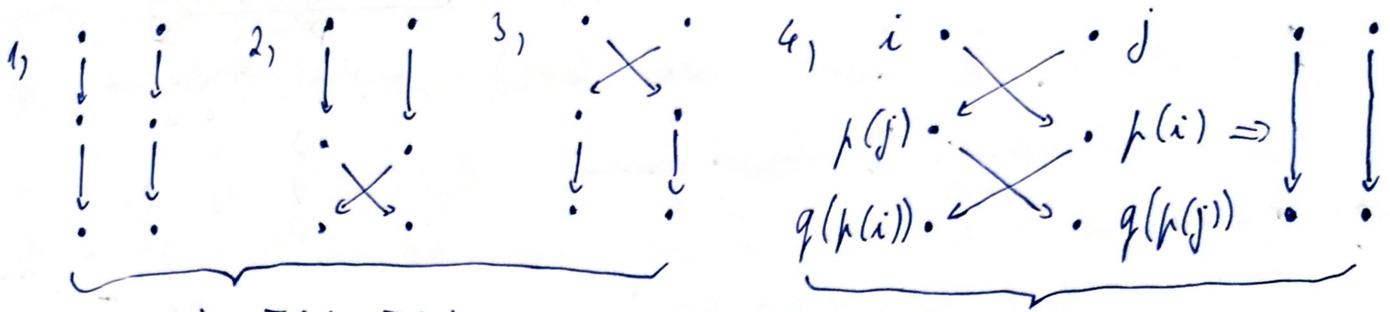



$I(n) = 2(j-i-1) + 1$

$\Rightarrow (-1)^{I(n)} = -1$

**Věta:** Pro libovolné $p, q \in S_n$: $sgn(q \circ p) = \underline{sgn(p \circ q) = sgn(p) \cdot sgn(q)}$

**Důkaz:** $sgn(q \circ p) = (-1)^{I(q \circ p)}$. Při skládání mohou nastat 4 situace:




$I(q \circ p) = I(p) + I(q)$

inverze v $p$ a $q$ se navzájem vyruší

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

$\Rightarrow sgn(q \circ p) = (-1)^{I(p)+I(q)} = (-1)^{I(p)} \cdot (-1)^{I(q)} = sgn(p) sgn(q)$

$\Rightarrow sgn(p \circ q) = sgn(q) \cdot sgn(p) = sgn(p) \cdot sgn(q) = sgn(q \circ p)$ ∎

**Důsledky:**

- $sgn(p^{-1}) = sgn(p)$. Dk: $sgn(p^{-1}) \cdot sgn(p) = sgn(p^{-1} \circ p) = sgn(id) = 1$ ∎

- $\underline{sgn(p) = (-1)^r}$, kde $r$ je # transpozic libovolného rozkladu $p$ na transp.

  Dk: $p = t_1 \circ t_2 \circ \ldots \circ t_r \Rightarrow sgn(p) = sgn(t_1) \cdot \ldots \cdot sgn(t_r) = (-1)^r$ ∎

- $sgn(p) = (-1)^s$, kde $s$ je # sudých cyklů $p$. $\rightarrow$ pro $k=1$ na 2 t.

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

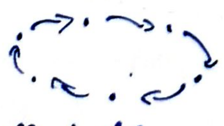
  $\Rightarrow$ sudé cykly $\rightarrow$ lichý počet $\Rightarrow sgn(s_c) = -1$

  $\Rightarrow$ liché cykly $\rightarrow$ sudý počet $\rightarrow sgn(l_c) = 1$ ∎

- $\underline{sgn(p) = (-1)^{n-k}}$, kde $p \in S_n$ a $k$ je počet cyklů $p$.

Dk:

**1 cyklus**



$n$ prvků

$\Rightarrow$ rozklad na $n-1$ t.

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

**2 cykly**

$a + b = n$

$\downarrow$

$a-1 + b-1$ t.

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

$\Rightarrow sgn(p) = (-1)^{n-2}$

**k cyklů**

$a_1 + a_2 + \ldots + a_k = n$

$a_1 - 1 + a_2 - 1 + \ldots + a_k - 1$ t.

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

$\rightarrow$ pokud délka $a_i = 1$, pak rozklad na 2 transpozice a vyvčíráme

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

Q.E.D.

• Těleso

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

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

$\Rightarrow$ Musí být splněny následující axiomy:

- $\forall a,b \in \mathbb{K}: a+b = b+a$
- $\forall a,b,c \in \mathbb{K}: (a+b)+c = a+(b+c)$
- $\exists 0 \in \mathbb{K}: \forall a \in \mathbb{K}: a+0 = a$
- $\forall a \in \mathbb{K}: \exists -a \in \mathbb{K}: a+(-a) = 0$

- $\forall a,b \in \mathbb{K}: a\cdot b = b\cdot a$ $\leftarrow$ včetně 0!
- $\forall a,b,c \in \mathbb{K}: (a\cdot b)\cdot c = a\cdot(b\cdot c)$
- $\exists 1 \in \mathbb{K}\setminus 0: \forall a \in \mathbb{K}: a\cdot 1 = a$ $\leftarrow 1 \neq 0$!
- $\forall a \in \mathbb{K}\setminus 0: \exists a^{-1} \in \mathbb{K}: a\cdot a^{-1} = 1$ $\leftarrow$ 0 nemá inverzi vůči $\cdot$
- $\forall a,b,c \in \mathbb{K}: a\cdot(b+c) = (a\cdot b)+(a\cdot c)$

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 inverzní prvek

$\mathbb{Z}_2$:

| $x$ | 0 | 1 |
|---|---|---|
| $-x$ | 0 | 1 |
| $x^{-1}$ | – | 1 |

$\mathbb{Z}_3$:

| $x$ | 0 | 1 | 2 |
|---|---|---|---|
| $-x$ | 0 | 2 | 1 |
| $x^{-1}$ | – | 1 | 2 |

$\mathbb{Z}_5$:

| $x$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $-x$ | 0 | 4 | 3 | 2 | 1 |
| $x^{-1}$ | – | 1 | 3 | 2 | 4 |

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

Metavěta: Všechna dosud uvedená tvrzení o soustavách rovnic, maticích a výpočtech nad $\mathbb{R}$ jsou platná i v libovolném tělese $\mathbb{K}$.

Metadůkaz: Provedené důkazy využívaly z $\mathbb{R}$ jen axiomy tělesa.

Vlastnosti tělesa

- jednoznačnost prvků 0 a 1
- jednoznačnost $-a$, $a^{-1}$
- $x = y \Leftrightarrow ax+b = ay+b$
  $ax+b = c \Leftrightarrow x = (c-b)\cdot a^{-1}$ $\Big\}$ pro $a \neq 0$

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

- $\forall a \in \mathbb{K}: 0 \cdot a = 0$

Dk: $0a = 0a + 0 = 0a + (0a - 0a) = (0+0)a - 0a = 0a - 0a = 0$ ☒

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

Dk: $(-1) \cdot a = (-1) \cdot a + 0 = (-1) \cdot a + a - a = (-1+1)a - a = 0a - a = -a$ ☒

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

Dk: Kdyby $ab = 0$ pro $a \neq 0$, $b \neq 0$, pak $\exists a^{-1}, b^{-1}$: $1 = aa^{-1}bb^{-1} = \overset{0}{\overbrace{ab}}a^{-1}b^{-1} = 0$ ↯ SPOR

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

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

→ navíc násobky $a, b$ nebudou mít inverze vůči $\cdot$

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

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

Nechť $f_a: [p-1] \to [p-1]$ t.ž. $f_a(x) = (ax) \bmod p$. $\Rightarrow f_a(a^{-1}) = 1$

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

→ Kdyby nebylo prosté, tak $\exists\, b, c$ búno $b > c$ t.ž.

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

$$\Rightarrow a(b-c) \equiv 0 \pmod p \Rightarrow a = p \cdot 0 \vee b - c = p \cdot 0$$

$\Rightarrow$ spor protože $a, b-c \in [p-1]$

- Galoisovo těleso

Věta: Těleso o velikosti $n$ existuje $\iff$ $n$ je mocninou prvočísla.

Je jednoznačné až na izomorfismus a značí se $GF(n) = GF(p^k)$

- Charakteristika tělesa

Def: V tělese $\mathbb{K}$, pokud $\exists n \in \mathbb{N}: \overbrace{1 + 1 + \dots + 1}^{n\text{-krát}} = 0$, pak nejmenší takové $n$ je charakteristika tělesa $\mathbb{K}$, jinak $\operatorname{char}(\mathbb{K}) = 0$.

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

Věta: Charakteristika tělesa je vždy prvočíslo nebo nula.

Dk: Pokud by $\operatorname{char}(\mathbb{K}) = n = a \cdot b$, pak

$$0 = \underbrace{1 + 1 + \dots + 1}_{n} = \underbrace{(1 + 1 + \dots + 1)}_{a \neq 0}\underbrace{(1 + 1 + \dots + 1)}_{b \neq 0} \neq 0 \Rightarrow \text{SPOR} ↯$$

Pozorování: V tělesech char $= 2$ je každý prvek svojí inverzí a $-$ lze nahradit $+$.

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

- Malá Fermatova věta

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

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

Proto v $\mathbb{Z}_p$ platí

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

- Vektorový prostor

Def: Vektorový prostor $(V, +, \bullet)$ nad tělesem $(\mathbb{K}, +, \cdot)$ je množina $V$ spolu s binární operací $+$ na $V$ a binární operací skalárního násobku $\mathbb{K} \bullet V \to V$.

- $\to$ $(V,+)$ je Abelovská grupa
- $\to$ $\forall a, b \in \mathbb{K}, \forall v \in V: (a \cdot b) \bullet v = a \bullet (b \bullet v)$ asociativita
- $\to$ $\forall v \in V: 1 \bullet v = v$ neutrální prvek
- $\to$ $\forall a, b \in \mathbb{K}, \forall v \in V: (a+b) \bullet v = (a \bullet v) + (b \bullet v)$ distributivita
- $\to$ $\forall a \in \mathbb{K}, \forall u, v \in V: a \bullet (u+v) = (a \bullet u) + (a \bullet v)$

Prvky $\mathbb{K}$ se nazývají skaláry, prvky $V$ vektory.
Rozlišujeme nulový skalár $0 \in \mathbb{K}$ a nulový vektor $\sigma \in V$.
Máme opačný skalár $-a \in \mathbb{K}$ i opačný vektor $-v \in V$.
Existuje inverzní skalár $a^{-1} \in \mathbb{K}$, ale ne inverzní vektor! $\begin{cases} v \cdot a \\ u v \end{cases}$ nedef.

Vzácky

- Aritmetický vektorový prostor dimenze $n$ nad $\mathbb{K}$ $\to \mathbb{K}^n$
  - $\to$ vektory jsou uspořádané $n$-tice prvků z $\mathbb{K}$
  - $\to$ sčítání a skalární násobky se provádějí po souřadnicích
  - $\to$ každé těleso $\mathbb{K}$ dává vektorový prostor $\mathbb{K}^1$ stejné mohutnosti.
- $\mathbb{K}^{m \times n}$ matice řádu $m \times n$ nad $\mathbb{K}$
- $V = \{\sigma\}$ triviální vektorový prostor nad libovolným $\mathbb{K}$
- Polynomy s koeficienty v $\mathbb{K}$
- Polynomy omezeného stupně
- Vektorový prostor reálných funkcí nad tělesem $\mathbb{R}$

- **Množinové systémy pro vektorové prostory**

$\mathcal{X}$ je systém podmnožin množiny $X$ uzavřený na symetrický rozdíl $\Delta$.

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

- **Vlastnosti vektorových prostorů**

$\left.\begin{array}{l} \text{- jednoznačnost } \sigma, -u \\ - \; u = v \iff u + w = v + w \\ - \; x + u = v \iff x = v - u \end{array}\right\}$ protože $(V,+)$ je grupa

- $\forall v \in V, \forall a \in \mathbb{K}: 0v = a\sigma = \sigma$

Dk: $0v = 0v + \sigma = 0v + 0v - 0v = (0+0)v - 0v = 0v - 0v = \sigma$

$a\sigma = a\sigma + \sigma = a\sigma + a\sigma - a\sigma = a(\sigma + \sigma) - a\sigma = a\sigma - a\sigma = \sigma$ ∎

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

Dk: $(-1)v = (-1)v + \sigma = (-1)v + v - v = (-1+1)v - v = 0v - v = \sigma - v = -v$ ∎

- $a \cdot v = \sigma \iff a = 0 \vee v = \sigma$

Dk: pokud $a \neq 0$, pak $v = 1v = a^{-1}av = a^{-1}\sigma = \sigma$ ∎

- **Podprostor**

Def: Nechť $V$ je vektorový prostor nad $\mathbb{K}$, potom podprostor $U$ je neprázdná podmnožina $V$ splňující

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

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

značení: $U \Subset V$

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

Pozorování: Jakýkoli podprostor je také vektorový prostor, protože $(U,+)$ je grupa plyne z uzavřenosti $\sigma = 0 \cdot v \in U$, $-v = (-1)v \in U$.

- **Průnik podprostorů**

Věta: Nechť $(U_i, i \in I)$ je libovolný systém podprostorů prostoru $V$. Průnik tohoto systému $\bigcap_{i \in I} U_i$ je také podprostor $V$.

Důkaz: Ukážeme, že $W = \bigcap_{i \in I} U_i$ je uzavřen na $+$ a $\cdot$.

$\forall u, v \in W: u, v \in W \Rightarrow \forall i: u, v \in U_i \Rightarrow \forall i: u + v \in U_i \Rightarrow \underline{u + v \in W}$.

$\forall v \in W, a \in \mathbb{K}: v \in W \Rightarrow \forall i: v \in U_i \Rightarrow \forall i: av \in U_i \Rightarrow \underline{a \cdot v \in W}$

• Lineární obal

Def: Lineární obal $L(X)$ podmnožiny $X$ vektorového prostoru $V$ je průnik všech podprostorů $U$ z $V$, 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 $v_1, \dots v_n \in V$ nad $\mathbb{K}$ je libovolný vektor $u = a_1 v_1 + \dots + a_n v_n$, kde $a_1, \dots a_k \in \mathbb{K}$. $\quad u = \sum_i a_i v_i$

Věta: Nechť $V$ je vektorový prostor nad $\mathbb{K}$ a $X$ je podmnožina $V$.
Potom $\text{span}(X)$ je množina všech lineárních kombinací vektorů z $X$.

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

→ $X \subseteq W_2$, ukážeme, že $W_2$ je podprostor ⇒ je v tom $\bigcap U_i$ ⇒ $W_1 \subseteq W_2$.

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

→ Všechny $U_i$ obsahují $X$ a jsou uzavřené na $\oplus$ a $\odot$ ⇒ obsahují všechny lineární kombinace vektorů $X$

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

• Prostory určené maticí

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

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

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

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

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

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

Dk: $\exists y$: $v = A^T y \Rightarrow v^T x = (A^T y)^T x = y^T A x = y^T 0 = 0$. $\blacksquare$

• Pozorování: Nechť $R$ je regulární.

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

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

## • Lineární nezávislost

<u>Def:</u> Množina vektorů $X = \{v_1, \dots v_n\}$ je <u>lineárně nezávislá</u>
$\equiv \sum_{i=1}^{n} a_i v_i = 0$ má pouze triviální řešení $\forall_i\ a_i = 0$.

<u>Pozorování:</u> Pokud jsou $v_1, \dots v_n$ lin. závislé, pak

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

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

<u>Důsledek:</u> Pokud lze nějaký z vektorů $v_1, \dots v_n$ vyjádřit jako lineární kombinaci těch ostatních, pak jsou tyto vektory lin. závislé.

<u>Ukázky:</u>

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

② Řádky matice v REF jsou lineárně nezávislé

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

## • Testování nezávislosti

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

a, vektory zapíšeme do matice jako řádky a pokusíme se jeden z nich eliminovat

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

vznikl nulový řádek $\Rightarrow X$ je závislá

b, vektory zapíšeme do matice jako sloupečky a pokusíme se najít netriviální řešení $\sum_i a_i v_i = 0$

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

↳ máme volnou proměnou $\Rightarrow \exists$ netr. řeš. $\Rightarrow X$ je z.

## • Vlastnosti nezávislosti

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

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

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

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

Dk: Sporem: $Y = \{v_1, \dots v_n\}$ a $\{u_1, \dots u_{n+1}\} \subseteq X$, každé $u_i$ vyjádříme:

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

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

## • Báze vektorového prostoru

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

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

Dk: Sporem: $u = \sum_i a_i v_i = \sum_i b_i v_i$

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

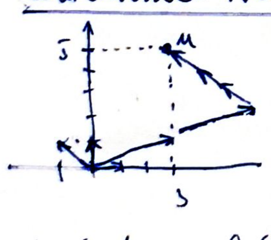
Def: Nechť $X = (v_1, \dots v_n)$ je uspořádaná báze prostoru $V$ nad $\mathbb{K}$.
Vektor souřadnic vektoru $u \in V$ vzhledem k bázi $X$ je:

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

## • Kanonická báze

→ v aritm. v.p. $\mathbb{K}^n$ tvoří sloupce $e_1, \dots e_n$ jednotkové matice $I_n$ kan. bázi $K$.

## • Souřadnice vektoru vzhledem k různým bázím




$X = \{(3,1)^T, (-1,1)^T\}$

$[u]_K = (3,5)^T \qquad [u]_X = (2,3)^T$

## • Existence báze

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

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

Dk: $\forall v \in Y$: když $v \in span(Y \setminus \{v\})$, pak odebereme $v$ z $Y$ dokud $Y$ není lin. nezávislá.

Věta: Každý vektorový prostor má bázi.

↳ pro konečně generované dokázáno, pro nekonečně gen. se nedokazuje.

• Změna báze

• **Lemma (o výměně):** Nechť $Y$ generuje $V$ nad $\mathbb{K}$. Nyní $u \in V$ zapíšeme pomocí $v_1, \dots v_n \in Y$, $a_1, \dots a_n \in \mathbb{K}$: $u = \sum_i a_i v_i$

→ $\forall i : a_i \neq 0$ můžeme provést výměnu $v_i$ za $u$.

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

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

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

$\hookrightarrow u \leftrightarrow v_4$.

Důkaz:

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

$\hookrightarrow a_j \neq 0$

→ jakékoli $w \in V$ lze zapsat jako lin. kom. prvků $Y$. Pokud se v této kombinaci vyskytuje $v_j$, tak ho nahradíme výrazem výše. ■

• **Věta (Steinitzova)** Nechť $Y$ generuje $V$ a $X$ je konečná l.n. množina ve $V$. Potom lze $X$ doplnit vektory z $Y$ na $Z$ t.ž. $|Y| = |Z|$ a $Z$ také generuje $V$.

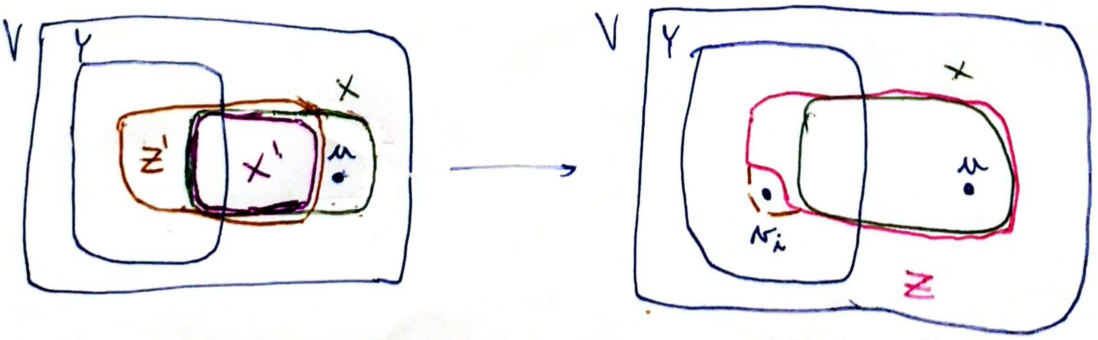
$$\Rightarrow X \subseteq Z, \quad Z \setminus X \subseteq Y, \quad |Z| = |Y|, \quad span(Z) = V.$$

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

1. $|X \setminus Y| = 0 \Rightarrow X \subseteq Y \Rightarrow Z = Y$ ✓

2. $n \to n+1$. Najdu $u \in X$, ale $u \notin Y \Rightarrow u \in X \setminus Y$ a položím $X' = X \setminus \{u\}$.
   Podle i.p. $\exists Z'$ pro $X'$ a $Y$ t.ž. $X' \subseteq Z'$, $Z' \setminus X' \subseteq Y$, $|Z'| = |Y|$, $span(Z') = V$.
   Použijeme lemma o výměně pro $u$ a $Z' = \{v_1, \dots v_n\}$.
   $u = \sum_i a_i v_i \rightarrow u \in X$ a $X$ je l.n. $\Rightarrow a_i \neq 0$ pro nějaké $v_i \in Z' \setminus X'$.

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



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

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

→ postupnou aplikací lemmatu o výměně vytvoříme $Z$.

$(1,1,0,0)^T=(1,0,0,0)^T+(0,1,0,0)^T$

$(1,1,0,1)^T=(1,1,0,0)^T+(0,0,0,1)^T$

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

Důsledek: Je-li v.p. konečně generován, pak lze jakoukoli l.n. množinu rozšířit na bázi.

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

Dk: Mějme báze $X, Y$ prostoru $V$, pak:

- $X$ je nezávislá, $Y$ generuje $V \Rightarrow |X| \le |Y|$
- $Y$ je nezávislá, $X$ generuje $V \Rightarrow |Y| \le |X|$

$\Big\}\ |Y| = |X|$

- Dimenze vektorového prostoru

Def: Dimenze konečně generovaného v.p. $V$ je mohutnost kterékoli z jeho bází. Značí se $\dim(V)$.

Ukázky: $\dim(\mathbb{K}^n)=n$, $\dim(\mathcal{R}(A)) = \operatorname{rank}(A)$.

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

Dk: Báze $V$ je l.n. ve $W$ a lze ji rozšířit na bázi $W$.

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

$$\dim(U)+\dim(V) = \dim(U\cap V) + \dim(\operatorname{span}(U\cup V)).$$

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

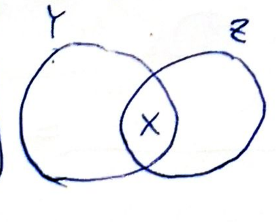
$\Rightarrow \dim(U\cap V)=|X|$, $\dim(U)=|Y|$, $\dim(V)=|Z|$.

$\Rightarrow \dim(\operatorname{span}(U\cup V)) = |Y\cup Z|$.

→ všimnu si, že $X\subseteq Y$, $X\subseteq Z \Rightarrow |Y|+|Z| = |X| + |Y\cup Z|$ ■

Pozorování: $|U| = |\mathbb{K}|^{\dim(U)}$

∵ vektory zapíšeme jako vektory souř. vůči nějaké bázi ⇒ vektorů souřadnic je




$\Updownarrow$

$|Y|+|Z| - |Y\cap Z| = |Y\cup Z|$.

• **Dimenze prostorů určených maticí** $\Rightarrow$ = pro $B$ regulární

**Lemma**: Pokud $A' = BA$, pak $\dim(S(A')) \leq \dim(S(A))$.

**Dk**: Označme $u_1, \dots u_n$ sloupce matice $A$ a $u'_1, \dots u'_n$ sloupce $A'$.

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

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

$$w' = \sum_i a_i u'_i = \sum_i a_i B u_i = B \sum_i a_i u_i = B \cdot w.$$

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

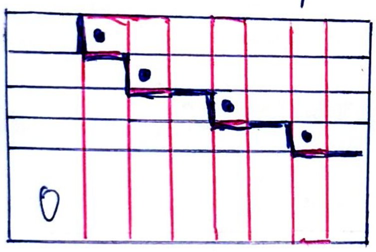
$\therefore u'_1, \dots u'_d$ generují $S(A') \Rightarrow \dim(S(A')) \leq \dim(S(A))$. ∎

**Věta**: Jakákoli $A \in \mathbb{K}^{m \times n}$ splňuje: $\dim(R(A)) = \dim(S(A)) = \operatorname{rank}(A)$.

**Důkaz**: Nechť $A \sim\sim A'$ v REF, $\Leftrightarrow \exists R$ regulární t.ž. $A' = RA$.

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

Pro $A'$ v REF věta platí přímo:




$$\dim(R(A')) = \underbrace{\operatorname{rank}(A')}_{= \operatorname{rank}(A)} = \dim(S(A'))$$

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

**Důsledky**:

• $\operatorname{rank}(A^T) = \operatorname{rank}(A)$

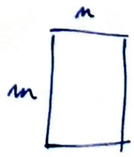
• $\operatorname{rank}(A) = \operatorname{rank}(RA) = \operatorname{rank}(AR')$ pro libovolné $A \in \mathbb{K}^{m \times n}$ a regulární $R \in \mathbb{K}^{m \times m}$, $R' \in \mathbb{K}^{n \times n}$

• $\underbrace{R(BA) \subseteq R(A)}_{\text{kombinace řádků z } A}$, $\underbrace{S(BA) \subseteq S(B)}_{\text{kombinace sloupců z } B}$

násobení nemůže zvýšit hodnost

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

**Věta**: Pro libovolnou $A \in \mathbb{K}^{m \times n}$: $\dim(\operatorname{Ker}(A)) + \operatorname{rank}(A) = n$.




**Dk**: $d := n - \operatorname{rank}(A)$ = # volných proměnných $\rightarrow$ ukážeme $d = \dim(\operatorname{Ker}(A))$.

$x_1, \dots x_d$ jsou řešení $Ax = 0$ daná zpětnou substitucí. Jsou l.n. $\because$ pro $\forall i$ platí, že $x_i$ je mezi $x_1, \dots x_d$ jediné s $i$-tou složkou nenulovou. Takže $x_1, \dots x_d$ tvoří bázi $\operatorname{Ker}(A) \Rightarrow \dim(\operatorname{Ker}(A)) = d$ ∎

• <u>Lineární zobrazení</u>

<u>Def:</u> Nechť $U$ a $V$ jsou vektorové prostory nad stejným tělesem $\mathbb{K}$.

Zobrazení $f: U \to V$ je lineární $\equiv$

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

$$\forall u \in U, \alpha \in \mathbb{K}: \ f(\alpha u) = \alpha \cdot f(u) \qquad \leftarrow \text{roztáhnutí}$$

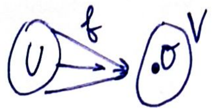
<u>Pozorování:</u> Počátek se zobrazí sám na sebe $\because$ $f(\underbrace{0}_{\in U}) = f(0 \cdot u) = 0 \cdot f(u) = \underbrace{0}_{\in V}$.

• <u>Jednoduchá lin. zobrazení</u>

→ Mezi obecnými v.p. $f: U \to V$ nad stejným $\mathbb{K}$.

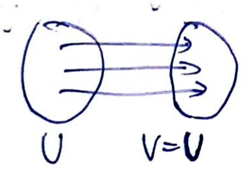
• <u>Triviální</u>

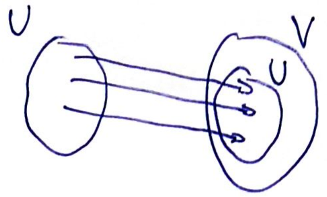
$$\forall u \in U: \ f(u) = 0$$




• <u>Identita</u> - id jako zobrazení na $U$ nebo když $U \subseteq V$

$$\forall u \in U: \ id(u) = u$$




$U \subseteq V$

• <u>Geometrická lineární zobrazení</u>

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

- rotace okolo počátku
- osová souměrnost podle osy procházející počátkem
- stejnolehlost se středem v počátku

} jakákoli kombinace je l.z.

• <u>Vlastnosti lineárních zobrazení</u>

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

<u>Dk:</u>
- $(g \circ f)(u+v) = g(f(u+v)) = g(f(u) + f(v)) = g(f(u)) + g(f(v))$
- $(g \circ f)(\alpha u) = g(f(\alpha u)) = g(\alpha f(u)) = \alpha g(f(u))$ ■

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

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

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

**Def:** Bijektivní lineární zobrazení se nazývá isomorfismus.

• **Transformace na vektor souřadnic**

**Tvrzení:** Nechť $V$ je prostor nad $\mathbb{K}$ s bází $X=(u_1,\dots u_n)$.
Potom $f: V \to \mathbb{K}^n$, $f(w)=[w]_X$ je l.z.

**Dk:** Pro $w, w' \in V$ vyjádříme $w=\sum_i a_i u_i$. $w'=\sum_i b_i u_i$, čili
$[w]_X=(a_1,\dots a_n)^T$, $[w']_X=(b_1,\dots b_n)^T$.

$$\bullet\ f(w+w)=[w+w']_X=\Big[\sum_i a_i u_i+\sum_i b_i u_i\Big]_X=\Big[\sum_i (a_i+b_i)u_i\Big]_X=$$
$$=(a_1+b_1,\dots a_n+b_n)^T=[w]_X+[w']_X=f(w)+f(w')$$
$$\bullet\ f(\alpha w)=[\alpha w]_X=\Big[\sum_i \alpha a_i u_i\Big]=(\alpha a_1,\dots \alpha a_n)^T=\alpha\cdot[w]_X=\alpha f(w) \quad \blacksquare$$

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

• **Věta (o rozšiřitelnosti):** Nechť $U$ a $V$ jsou prostory nad $\mathbb{K}$ a $X$ je báze $U$.
Pak pro jakékoli zobrazení $f_0: X \to V$ existuje jediné l.z. $f: U \to V$ rozšiřující $f_0$ t.j. $\forall u \in X: f(u)=f_0(u)$.

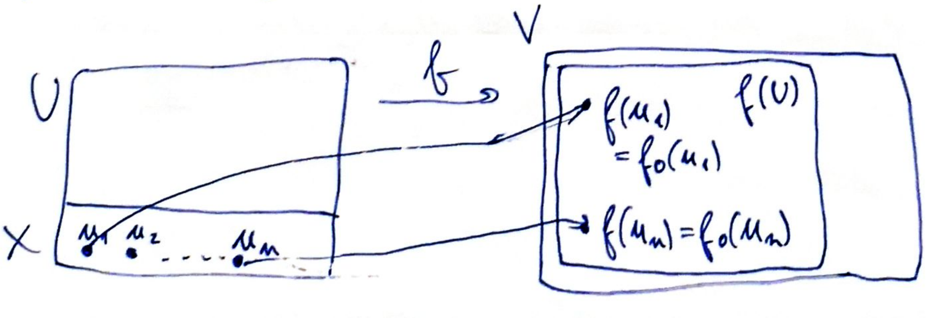
$\Rightarrow$ když vím, kam se mi zobrazí báze, tak je to zobrazení jednoznačně určeno.

**Dk:** Libovolný $w \in U$ si zapíšu jako l.k. vektorů z báze – pro konečnou bázi lze použít všechny vektory, pro nekonečnou vynechám násobení nulou $\Rightarrow \exists n \in \mathbb{N}_0$:
$a_1,\dots a_n \in \mathbb{K}\setminus\{0\}$ a $u_1,\dots u_n \in X$ a $w=\sum_{i=1}^n a_i u_i$

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

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

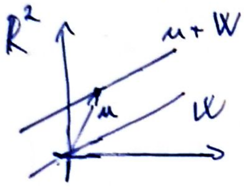
**Dk:** Báze $X$ prostoru $U$ se zobrazí na $f(X)$, která generuje $f(U)$, ale $f(X)$ může být lineárně závislá, potom je báze $f(U)$ podmnožinou $f(X)$.



- Afinní prostory

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

Ukázka: V $\mathbb{R}^2$ je přímka procházející počátkem podprostor → přímka v obecné poloze je afinní prostor.



$0 \to u$

$w \to u + w$

- Jádro lineárního zobrazení

$\nearrow$ $0 \in Ker(f)$ !

Def: Jádro lineárního zobrazení $f: U \to V$ je $Ker(f) = \{u \in U \mid f(u) = 0\}$.

Pozorování: Jádro je vektorový podprostor.

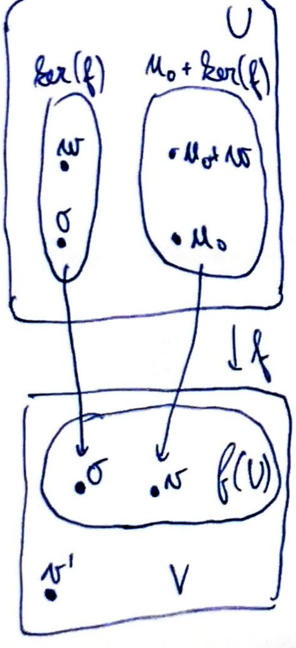
Ukázka: Pro $f: \mathbb{K}^n \to \mathbb{K}^m$, $f(x) = Ax$ je $Ker(f) = Ker(A)$.

Věta: Nechť $f: U \to V$ je l.z. Pro libovolné $v \in V$ rovnice $f(u) = v$ buď nemá řešení, nebo řešení tvoří afinní podprostor

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

→ ukázka: řešení soustav $Ax = b$.

Důkaz: Ukážeme, že každý vektor z $u_0 + Ker(f)$ se zobrazí na $v$ a že každý vektor, co se zobrazí na $v$ je v $u_0 + Ker(f)$.




1, $u \in u_0 + Ker(f) \Rightarrow u = u_0 + w$, $w \in Ker(f)$.

$\Rightarrow f(u) = f(u_0) + f(w) = v + 0 = v$

2, $f(u) = v \Rightarrow f(u - u_0) = f(u) - f(u_0) = v - v = 0$

$\Rightarrow u - u_0 \in Ker(f) \Rightarrow u \in u_0 + Ker(f)$

$\blacksquare$

- **Matice lineárního zobrazení**

**Def:** Nechť $U$ a $V$ jsou v.p. nad stejným tělesem $\mathbb{K}$, s bázemi $X = \{u_1, \dots u_n\}$ a $Y = \{v_1, \dots v_m\}$.
Matice l.z. $f: U \to V$ vzhledem k $X, Y$ je ${}_Y[f]_X \in \mathbb{K}^{m \times n}$,
jejíž sloupce jsou vektory souřadnic obrazů vektorů báze $X$ vzhledem k $Y$.

$$ {}_Y[f]_X = \left( [f(u_1)]_Y, \dots [f(u_n)]_Y \right) $$

**Pozorování:** Pro $w \in U$ platí $[f(w)]_Y = {}_Y[f]_X [w]_X$

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

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

$$ \Rightarrow [f(w)]_Y = \sum_i a_i [f(u_i)]_Y = {}_Y[f]_X [w_X] $$

$$ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} [w]_X $$

$$ \boxed{[f(u_1)]_Y, \dots [f(u_n)]_Y} \to [f(w)]_Y $$

∎

**Příklad:** Vzhledem ke kanonické bázi $K$ urči
matici zobrazení $f: \mathbb{R}^2 \to \mathbb{R}^2$, $f(2,1) = (7,0)$, $f(-1,1) = (-2,3)$. $\to {}_K[f]_K = ?$

**Víme:**
$$ {}_K[f]_K [(2,1)^T]_K = [(7,0)^T]_K \Rightarrow {}_K[f]_K \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 7 \\ 0 \end{pmatrix} $$
$$ {}_K[f]_K [(-1,1)^T]_K = [(-2,3)^T]_K \Rightarrow {}_K[f]_K \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ 3 \end{pmatrix} $$
$$ \Big\} \; {}_K[f]_K \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 7 & -2 \\ 0 & 3 \end{pmatrix} $$

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

$$ \hookrightarrow \left( \begin{array}{cc|cc} 2 & -1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) \sim \left( \begin{array}{cc|cc} 1 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{3}{2} & -\frac{1}{2} & 1 \end{array} \right) \sim \left( \begin{array}{cc|cc} 1 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & -\frac{1}{6} & \frac{1}{3} \end{array} \right) \sim \left( \begin{array}{cc|cc} 1 & 0 & \frac{1}{3} & \frac{1}{3} \\ 0 & 1 & -\frac{1}{3} & \frac{2}{3} \end{array} \right) $$

$$ \to e^1 = (1,0)^T \Rightarrow f(e_1) = (3,-1)^T $$
$$ e^2 = (0,1)^T \Rightarrow f(e_2) = (1,2)^T $$

je to vůči $K$

- **Složení lineárních zobrazení**

**Pozorování:** Nechť $U, V, W$ jsou v.p. nad $\mathbb{K}$ s konečnými bázemi $X, Y, Z$.
Pro matice l.z. $f: U \to V$ a $g: V \to W$ platí:

$$ {}_Z[g \circ f]_X = {}_Z[g]_Y \, {}_Y[f]_X \qquad g(f(u)) \qquad \Rightarrow {}_Y[f]_X = {}_Y[id]_K \, {}_K[f]_X $$

**Dk:** Pro $\forall u \in U$: $[(g \circ f)(u)]_Z = {}_Z[g \circ f]_X [u]_X \;\wedge\; [(g \circ f)(u)]_Z = {}_Z[g]_Y [f(u)]_Y = {}_Z[g]_Y \, {}_Y[f]_X [u]_X$
→ Nyní ověříme, že ty dvě matice jsou stejné. Volbou $u$ = $i$-tý vektor báze $X$
máme $[u]_X = e^i \Rightarrow {}_Z[g \circ f]_X e^i = {}_Z[g]_Y \, {}_Y[f]_X e^i \Rightarrow$ matice mají
shodné $i$-té sloupce. Takto lze sloupec po sloupci ověřit ${}_Z[g \circ f]_X = {}_Z[g]_Y \, {}_Y[f]_X$ ∎

$id(u) = u$: identita

- ## Matice přechodu

**Def:** Nechť $X$ a $Y$ jsou konečné báze v.p. $U$. Matice přechodu od $X$ k $Y$ je ${}_Y[id]_X$.

**Pozorování:** Pro $\forall u \in U$: $[u]_Y = [id(u)]_Y = {}_Y[id]_X [u]_X$ ∎

**Pozorování:** Protože ${}_X[id]_Y\,{}_Y[id]_X = {}_X[id \circ id]_X = {}_X[id]_X = I_{dim(U)}$,
je každá matice přechodu regulární a $({}_Y[id]_X)^{-1} = {}_X[id]_Y$.

**Postup:** Výpočet matice přechodu ${}_Y[id]_X$ od báze $X=(x_1,\dots x_n)$ k $Y=(y_1,\dots y_n)$ v $\mathbb{K}^n$.
Do sloupečků $\mathbb{X}$ zapíšeme vektory báze $X$ a do $\mathbb{Y}$ vektory $Y$. $\Rightarrow \mathbb{X}, \mathbb{Y} \in \mathbb{K}^{n\times n}$

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

$$\left.\begin{array}{l} \bullet\ u = \sum_i a_i x_i = \mathbb{X}\cdot[u]_X \\ \bullet\ u = \sum_i b_i y_i = \mathbb{Y}[u]_Y \end{array}\right\} \begin{array}{l}\mathbb{Y}[u]_Y = \mathbb{X}[u]_X \\ \Rightarrow [u]_Y = \mathbb{Y}^{-1}\mathbb{X}[u]_X\end{array}$$

$\mathbb{Y}$ je regulární, protože $rank(\mathbb{Y}) = dim(S(\mathbb{Y})) = n$.

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

**Výpočet:** $(\mathbb{Y}|\mathbb{X}) \sim\sim (I_n | \mathbb{Y}^{-1}\mathbb{X}) = (I_n | {}_Y[id]_X)$

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

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

- ## Charakterizace matic isomorfismu

**Věta:** Lineární z. $f: U \to V$ je isomorfismus prostorů $U$ a $V$ s konečnými bázemi
$X$ a $Y$ $\iff$ ${}_Y[f]_X$ je regulární.

→ ${}_Y[f]_X$ je reg $\Rightarrow |X| = |Y|$

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

${}_X[g\circ f]_X = {}_X[g]_Y\,{}_Y[f]_X = I_{|X|} = {}_X[id]_X \Rightarrow f$ je prostá

${}_Y[f\circ g]_Y = {}_Y[f]_X\,{}_X[g]_Y = I_{|Y|} = {}_Y[id]_Y \Rightarrow f$ je „na"

$$U \underset{f^{-1}}{\overset{f}{\rightleftarrows}} V$$

$\Rightarrow$: 

$$\left.\begin{array}{l} {}_X[f^{-1}]_Y\,{}_Y[f]_X = {}_X[id]_X = I_{|X|} \xRightarrow{*} |Y| \ge |X| \\ {}_Y[f]_X\,{}_X[f^{-1}]_Y = {}_Y[id]_Y = I_{|Y|} \xRightarrow{*} |X| \ge |Y| \end{array}\right\}$$

$|X| = |Y| \Rightarrow {}_Y[f]_X$ je čtvercová $\wedge\ {}_X[f^{-1}]_Y\,{}_Y[f]_X = I \Rightarrow$ je reg.

$*$: $dim(S(BA)) \le dim(S(A)) \to rank(BA) \le rank(A)$

$rank(I_{|X|}) = |X| \Rightarrow |X| \le rank({}_Y[f]_X) \le |Y|$


∎

Důsledek: $({}_Y[f]_X)^{-1}\,\cancel{{}_Y[f]_X} = {}_X[f^{-1}]_Y\,\cancel{{}_Y[f]_X} \Rightarrow {}_X[f^{-1}]_Y = ({}_Y[f]_X)^{-1}$ pro $f$ izomorfismus.

## • Počet sudých podgrafů

Def: Nechť $G$ je souvislý graf a $U$ obsahuje množiny hran $A \subseteq E(G)$ t.ž. $\forall v \in V(G)$: $v$ je incidentní se sudým počtem hran v $A$. Tyto množiny $A$ určují sudé podgrafy $G$.

A B

$* \rightarrow |A \triangle B| = |A| + |B| - 2|A \cap B|$

G  U 

Problém: Kolik sudých podgrafů obsahuje $G$?

- Vektorový p. sudých podgrafů: $(U, \triangle, \cdot)$ nad $\mathbb{Z}_2$ tvoří v.p.

  Ověříme, že $(U, \triangle)$ je abelovská grupa; $\emptyset$ je neutrální prvek

  $\forall A \in U$: $A$ je inverzní k $A$, asociativita ✓

  Ověříme, že $U$ je uzavřená na $\triangle$: $*$ $|A \triangle B|$ je sudá pro $|A|, |B|$ sudé ✓

  ↳ ∴ $\triangle$ zachovává sudé stupně

- pro prostory konečné mohutnosti platí $|U| = |K|^{\dim(U)}$ ⇒ stačí najít bázi $U$
- Konstrukce báze $X$ v.p. $U$

  Zvolíme libovolnou kostru $T$ grafu $G$. Pro každou nekosterní hranu $e_i \in E(G) \setminus E(T)$ definujeme $A_i$ jako unikátní kružnici co vznikne v $T + e_i$.

  → množina $X = \{A_i \mid e_i \in E(G) \setminus E(T)\}$ je l. nezávislá, protože žádná hrana $e_i$ nemůže být eliminována sym. rozdílem $A_i$ △ ostatními grafy z $X$. (neobsahují $e_i$)

  G  X: $A_1$  $A_2$ 

  → ukážeme, že $X$ generuje $U$ → zvolíme libovolný $B \in U$

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

  ↳ graf $B \triangle A_{i_1} \triangle A_{i_2} \triangle \dots \triangle A_{i_k}$ je sudým podgrafem $G$, ale také je podgrafem $T$, protože neobsahuje žádné nekosterní hrany

  ⇒ strom nemá cykly ⇒ jediným s. podgrafem $T$ je prázdný graf $O$

  ⇒ $B \triangle A_{i_1} \triangle \dots \triangle A_{i_k} = O \Rightarrow B = A_{i_1} \triangle \dots \triangle A_{i_k}$ ⇒ $X$ generuje $U$

→ velikost báze $X$

$\dim(U) = |X| = |E(G)| - \overbrace{|E(T)|}^{|V(T)|-1} = |E(G)| - |V(G)| + 1$

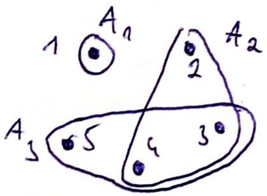
⇒ každý souvislý graf $G$ má $2^{|E(G)| - |V(G)| + 1}$ sudých podgrafů.

## • Množinové systémy s omezeními na mohutnosti

Problém: Kolik podmnožin může mít $n$-prvková množina, pokud každá množina má mít lichou mohutnost a průnik každé dvojice různých podmnožin sudou mohutnost?

Hledáme: $\max\{k \mid \exists A_1, \dots A_k \subseteq \{1, \dots n\}: \forall i \neq j: 2 \nmid |A_i| \wedge 2 \mid |A_i \cap A_j|\}$

Ukázka: $n=5$, $k=3$:




Pozorování: Jednoprvkové podmnožiny dávají $k=n$.

Tvrzení: Vždy platí $k \leq n$. $\Rightarrow$ hledané maximum je $n$.

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

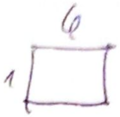
Pro příklad výše máme $M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$.

Matice splňuje $MM^T = I_k$, protože nad $\mathbb{Z}_2$ máme

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

Nyní $\operatorname{rank}(I_k) = k = \operatorname{rank}(MM^T) \leq \operatorname{rank}(M) \leq n \Rightarrow k \leq n$ ■

• **Dělení obdélníku na čtverce**



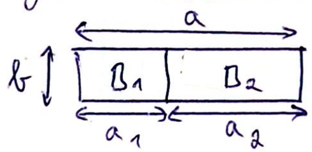

Problém: Lze obdélník s iracionálním poměrem délek stran rozdělit na konečně mnoho čtverců? (pro racionální $p:q$ lze $p\cdot q$ čtverci)

Tvrzení: Pro iracionální poměr žádné takové rozdělení neexistuje.

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

- Všimněme si, že $\mathbb{R}$ tvoří v.p. nad $\mathbb{Q}$, kde jsou $1$ a $x$ l. nezávislé
  $\because \nexists q \in \mathbb{Q}: q\cdot x = -1. \Rightarrow \{1, x\}$ lze rozšířit na bázi.
- Zvolme libovolné l.z. $f: \mathbb{R} \to \mathbb{R}$ t.ž. $f(1) = 1$, $f(x) = -1$.
- Pro obdélník $A$ o stranách $a, b$ definujeme „plocha" $v(A) := f(a)\cdot f(b)$.
- Pokud postupně svisle rozdělíme $A$ na $B_1, \dots B_k$, pak $v(A) = \sum_i v(B_i)$.

  $\because$ když $A$ dělíme na $B_1$ a $B_2$, tak $v(A) = v(B_1) + v(B_2)$ → indukcí




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

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

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