Bonusový test

Definice (41)

definujte…

- rozšířená matice soustavy
    - soustava m lineárních rovnic o n neznámých … Ax = b
    - rozšířená matice soustavy … $(A|b) \in \mathbb{R}^{m\times(n+1)}$
    - matice soustavy … $A \in \mathbb{R}^{m\times n}$
    - vektor pravých stran … $b \in \mathbb{R}^m$
    - vektor neznámých … $x = (x_1, \ldots, x_n)^T$
    - vektor $x \in \mathbb{R}^n$ je řešení soustavy Ax = b, pokud splňuje všechny její rovnice
    - soustavy Ax = 0 se nazývají homogenní a vždy umožňují x = 0
- elementární řádkové operace
    - definujeme základní dvě elementární řádkové úpravy
        - vynásobení i-tého řádku nenulovým $t \in \mathbb{R} \setminus \{0\}$
        - přičtení j-tého řádku k i-tému řádku
    - z těch lze odvodit další dvě úpravy
        - přičtení t-násobku j-tého řádku k i-tému řádku (t může být i nulové)
        - záměna dvou řádků
    - provedení jedné elementární úpravy značíme $A \sim A'$
    - provedení posloupnosti úprav značíme $A \sim\sim A'$
- odstupňovaný tvar matice
    - matice je v řádkově odstupňovaném tvaru (REF = row echelon form), pokud jsou nenulové řádky seřazeny podle počtu počátečních nul a nulové řádky jsou pod nenulovými
    - první nenulový prvek nenulového řádku se nazývá pivot, pod pivotem jsou v REF všechny prvky nulové
- napište pseudokód pro Gaussovu eliminaci
    - // input: matice A
    - // output: matice A v REF
    - foreach i do určete j(i)

        - // j(i) = sloupec s pivotem daného řádku, $j(i) = min\{j : a_{i,j} \neq 0\}$
        - // prázdný řádek má j(i) = ∞
    - seřaďte řádky A podle j(i)
    - forever
        - if $\exists i : j(i) = j(i+1) < \infty$ then
            - // i-tý a (i+1)-ní řádky jsou nenulové a mají stejně počátečních nul
            - přičtěte $-a_{i+1,j(i)}/a_{i,j(i)}$-násobek i-tého řádku
            - // nyní je prvek ve sloupci j(i) řádku i+1 nulový
            - aktualizujte j(i + 1) a zařaďte (i + 1)-tý řádek na místo
        - else
            - // všechny nenulové řádky mají různý počet počátečních nul
            - return A
    - // konečnost: v každé iteraci roste celkový počet počátečních nul
- pivot
    - označme $j(i) = \min\{j : a_{i,j} \neq 0\}$
    - pivot = první nenulový prvek $a_{i,j(i)}$ v i-tém řádku matice v REF
- volné a bázické proměnné
    - pro soustavu $A'x = b'$ s A' v REF jsou proměnné odpovídající sloupcům s pivoty bázické, ostatní jsou volné
- hodnost matice
    - hodnost matice A, značená jako rank(A), je počet pivotů v libovolné A' v REF takové, že $A \sim\sim A'$
- jednotková matice
    - pro $n \in \mathbb{N}$ je jednotková matice $I_n \in \mathbb{R}^{n\times n}$ definovaná tak, že $(I_n)_{i,j} = 1 \iff i = j$, ostatní prvky jsou nulové
- transponovaná matice
    - transponovaná matice k matici $A \in \mathbb{R}^{m\times n}$ je matice $A^T \in \mathbb{R}^{n\times m}$ splňující $(A^T)_{i,j} = a_{j,i}$
- symetrická matice
    - čtvercová matice A je symetrická, pokud $A^T = A$, tedy $a_{i,j} = a_{j,i}$
- maticový součin
    - 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 $(AB)_{i,j} = \sum_{k=1}^{n} a_{i,k}b_{k,j}$
- inverzní matice

- pokud pro čtvercovou matici $A \in \mathbb{R}^{n \times n}$ existuje $B \in \mathbb{R}^{n \times n}$ taková, že $AB = I_n$, pak se B nazývá inverzní matice a značí se A^{-1}
- výpočet: $(A|I_n) \sim\sim (I_n|A^{-1})$

- regulární/singulární matice
  - pokud má matice A inverzi, pak se nazývá regulární, jinak je singulární
- binární operace
  - binární operace na množině X je zobrazení X × X → X
  - tedy např. podíl není binární operace na $\mathbb{R}$, rozdíl není binární operace na $\mathbb{N}$
- komutativní a asociativní binární operace
  - asociativní bin. operace na množině G: $\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$
  - komutativní bin. operace na množině G: $\forall a, b \in G : a \circ b = b \circ a$
- neutrální prvek
  - $(\exists e \in G)(\forall a \in G) : a \circ e = e \circ a = a$
- inverzní prvek
  - $(\forall a \in G)(\exists b \in G) : a \circ b = b \circ a = e$
  - inverzní prvek se obvykle značí a^{-1} (u aditivních grup jako $-a$)
- grupa
  - grupa $(G, \circ)$ je množina G spolu s binární operací ∘ na G splňující asociativitu operace ∘, existenci neutrálního prvku a existenci inverzních prvků
  - pokud je navíc operace ∘ komutativní, pak se jedná o abelovskou grupu
- permutace
  - permutace na množině $\{1, 2, \dots, n\}$ je bijektivní zobrazení $p : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$
- permutační matice
  - permutace může být popsána pomocí permutační matice P
  - $(P)_{i,j} = \begin{cases} 1 & \text{pokud } p(i) = j \\ 0 & \text{jinak} \end{cases}$
- transpozice
  - transpozice je permutace, která má pouze jeden netriviální cyklus o délce 2
  - jakoukoliv permutaci lze rozložit na transpozice
    - cyklus $(1, 2, 3, 4)$ lze rozložit na $(1, 4) \circ (1, 3) \circ (1, 2)$ nebo na $(1, 2) \circ (2, 3) \circ (3, 4)$

- inverze v permutaci
  - inverze v p je dvojice prvků $(i, j) : i < j \wedge p(i) > p(j)$
- znaménko permutace
  - znaménko permutace p je $\operatorname{sgn}(p) = (-1)^{\text{počet inverzí } p}$
  - permutace s kladným znaménkem jsou sudé, se záporným liché
  - v exponentu může být # inverzí, # transpozic, # sudých cyklů, $n-$# cyklů
- těleso
  - 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 platí distributivita $\forall a, b, c \in \mathbb{K} : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
- charakteristika tělesa
  - v tělese $\mathbb{K}$, pokud $\exists n \in \mathbb{N} : \underbrace{1 + 1 + \cdots + 1}_{n} = 0$, pak nejmenší takové n je charakteristika tělesa $\mathbb{K}$
  - jinak má těleso $\mathbb{K}$ charakteristiku 0
  - značí se $\operatorname{char}(\mathbb{K})$
- vektorový prostor
  - vektorový prostor $(V, +, \cdot)$ nad tělesem $(\mathbb{K}, +, \cdot)$ je množina spolu s binární operací $+$ na V a binární operací skalárního násobku $\cdot : \mathbb{K} \times V \to V$
  - $(V, +)$ je abelovská grupa
  - $\forall \alpha, \beta \in \mathbb{K}, \forall u, v \in V$
    - asociativita … $(\alpha \cdot \beta) \cdot u = \alpha \cdot (\beta \cdot u)$
    - neutrální prvek (skalár) vůči násobení skalárem … $1 \cdot u = u$
    - distributivita … $(\alpha + \beta) \cdot u = (\alpha \cdot u) + (\beta \cdot u)$
    - distributivita … $\alpha \cdot (u + v) = (\alpha \cdot u) + (\alpha \cdot v)$
  - prvky $\mathbb{K}$ se nazývají skaláry, prvky V vektory
  - rozlišujeme nulový skalár 0 a nulový vektor o
- podprostor vektorového prostoru
  - nechť V je vektorový prostor na $\mathbb{K}$, potom podprostor U je neprázdná podmnožina V splňující uzavřenost na součet vektorů a uzavřenost na násobení skalárem (z $\mathbb{K}$) – z toho nutně vyplývá $o \in U$
- lineární kombinace
  - lineární kombinace vektorů $v_1, \dots, v_k \in V$ nad $\mathbb{K}$ je libovolný vektor $u = \alpha_1 v_1 + \cdots + \alpha_k v_k$, kde $\alpha_1, \dots, \alpha_k \in \mathbb{K}$
- lineární obal (podprostor generovaný množinou)

- lineární obal $\mathcal{L}(X)$ podmnožiny X vektorového prostoru V je průnik všech podprostorů U z V, které obsahují X
- alternativní značení: span(X)
- pro $X \subseteq V$ platí $\text{span}(X) = \bigcap U : U \Subset V, X \subseteq U$
- jde o podprostor generovaný X, vektory v množině X se označují jako generátory podprostoru

- řádkový a sloupcový prostor matice $A \in \mathbb{K}^{m \times n}$
  - sloupcový prostor $\mathcal{S}(A) \subseteq \mathbb{K}^m$ je lineární obal sloupců A
  - řádkový prostor $\mathcal{R}(A) \subseteq \mathbb{K}^n$ je lineární obal řádků A
  - $\mathcal{S}(A) = \{u \in \mathbb{K}^m : u = Ax, x \in \mathbb{K}^n\}$
  - $\mathcal{R}(A) = \{v \in \mathbb{K}^n : v = A^T y, y \in \mathbb{K}^m\}$
- jádro matice $A \in \mathbb{K}^{m \times n}$
  - $\ker(A) = \{x \in \mathbb{K}^n : Ax = 0\}$
- lineárně nezávislé vektory
  - množina vektorů X je lineárně nezávislá, pokud nulový vektor nelze získat netriviální lineární kombinací vektorů z X; v ostatních případech je množina X lineárně závislá
  - vektory $v_1, \dots, v_n$ jsou lineárně nezávislé $\equiv$ $\sum_{i=1}^n \alpha_i v_i = o \iff \alpha_1 = \dots = \alpha_n = 0$
- báze vektorového prostoru
  - báze vektorového prostoru V je lineárně nezávislá množina X, která generuje V (tedy $\text{span}(X) = V$)
- dimenze vektorového prostoru
  - dimenze konečně generovaného vektorového prostoru V je mohutnost kterékoli z jeho bází; značí se dim(V)
- vektor souřadnic
  - nechť $X = (v_1, \dots, v_n)$ je uspořádaná báze vektorového prostoru V nad $\mathbb{K}$, potom vektor souřadnic $u \in V$ vzhledem k bázi X je $[u]_x = (\alpha_1, \dots, \alpha_n)^T \in \mathbb{K}^n$, kde $u = \sum_{i=1}^n \alpha_i v_i$
- lineární zobrazení
  - nechť U a V jsou vektorové prostory nad stejným tělesem $\mathbb{K}$
  - zobrazení $f : U \to V$ nazveme lineární, pokud splňuje $\forall u, v \in U, \forall \alpha \in \mathbb{K} :$
    - $f(u + v) = f(u) + f(v)$
    - $f(\alpha \cdot u) = \alpha \cdot f(u)$
      - z toho vyplývá, že pro lineární zobrazení obecně platí $f(o) = o$
- jádro lineárního zobrazení

- $\ker(f) = \{w \in U : f(w) = o\}$
- matice lineárního zobrazení
  - nechť U a V jsou vektorové prostory nad stejným tělesem $\mathbb{K}$ s bázemi $X = (u_1, \ldots, u_n)$ a $Y = (v_1, \ldots, v_m)$
  - matice lineárního zobrazení $f : U \to V$ vzhledem k bázím X a Y je $[f]_{X,Y} \in \mathbb{K}^{m \times n}$, jejíž sloupce jsou vektory souřadnic obrazů vektorů báze X vzhledem k bázi Y, tedy $[f(u_1)]_Y, \ldots, [f(u_n)]_Y$
  - pro $w \in U$ tedy platí, že $[f(w)]_Y = [f]_{X,Y}[w]_X$
- matice přechodu
  - nechť X a Y jsou dvě konečné báze vektorového prostoru U
  - matice přechodu od X k Y je $[id]_{X,Y}$
  - pro $u \in U$ tedy platí, že $[u]_Y = [id(u)]_Y = [id]_{X,Y}[u]_X$
  - matice přechodu je regulární, platí $[id]_{Y,X} = ([id]_{X,Y})^{-1}$
  - výpočet: $[id]_{X,Y} = Y^{-1}X$ nebo také $(Y|X) \sim\sim (I_n|[id]_{X,Y})$
- isomorfismus vektorových prostorů
  - vektorové prostory jsou isomorfní, pokud mezi nimi existuje isomorfismus, tedy bijektivní (vzájemně jednoznačné) lineární zobrazení
  - pro isomorfismus f platí, že existuje f^{-1} a je také isomorfismem
  - isomorfní prostory mají shodné dimenze
- afinní prostor a jeho dimenze
  - nechť W je podprostor vektorového prostoru U a $u \in U$
  - afinní podprostor $u + W$ je množina $\{u + w : w \in W\}$
  - dimenze afinního prostoru $u + W$ je $\dim(u + W) = \dim(W)$
  - prvky afinního prostoru se nazývají body

Věty a důkazy (15)

vyslovte a dokažte… / uveďte a dokažte…

- vztah mezi elementárními řádkovými operacemi a soustavami rovnic

  - 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

- dokážeme, že množina řešení je zachována, pokud je provedena jediná úprava prvního nebo druhého typu (1. typ = vynásobení řádku, 2. typ = přičtení jiného řádku)
- ukazujeme rovnost $\{x \in \mathbb{R}^n : Ax = b\} = \{x \in \mathbb{R}^n : A'x = b'\}$
- rovnost plyne ze dvou inkluzí, které převedeme na implikace
    - $Ax = b \implies A'x = b'$
    - $A'x = b' \implies Ax = b$
- elementární úpravou se vždy mění jenom i-tý řádek matice, ostatní zůstávají zachovány, tedy ověříme dvakrát dvě implikace pro i-tý řádek
- násobení
    - $Ax = b \implies A'x = b'$
        - předpoklad: $a_{i,1}x_1 + \cdots + a_{i,n}x_n = b_i$
        - chceme: $a'_{i,1}x_1 + \cdots + a'_{i,n}x_n = b'_i$
        - víme: $\forall k \in \{1, \ldots, n\} : a'_{i,k} = ta_{i,k}, b'_i = tb_i$
        - důkaz: $a'_{i,1}x_1 + \cdots + a'_{i,n}x_n = ta_{i,1}x_1 + \cdots + ta_{i,n}x_n$
          $= t(a_{i,1}x_1 + \cdots + a_{i,n}x_n) = tb_i = b'_i$
    - $a_{i,1}x_1 + \cdots + a_{i,n}x_n = \frac{1}{t}(ta_{i,1}x_1 + \cdots + ta_{i,n}x_n)$
      $= \frac{1}{t}(a'_{i,1}x_1 + \cdots + a'_{i,n}x_n) = \frac{1}{t}b'_i = \frac{1}{t}tb_i = b_i$
- přičtení
    - $a'_{i,1}x_1 + \cdots + a'_{i,n}x_n = (a_{i,1} + a_{j,1})x_1 + \cdots + (a_{i,n} + a_{j,n})x_n$
      $= (a_{i,1}x_1 + \cdots + a_{i,n}x_n) + (a_{j,1}x_1 + \cdots + a_{j,n}x_n) = b_i + b_j = b'_i$
    - $a_{i,1}x_1 + \cdots + a_{i,n}x_n = a_{i,1}x_1 + \cdots + a_{i,n}x_n + b_j - b_j$
      $= (a_{i,1}x_1 + \cdots + a_{i,n}x_n) + (a_{j,1}x_1 + \cdots + a_{j,n}x_n) - b_j$
      $= (a_{i,1} + a_{j,1})x_1 + \cdots + (a_{i,n} + a_{j,n})x_n - b_j$
      $= (a'_{i,1}x_1 + \cdots + a'_{i,n}x_n) - b_j = b'_i - b_j = b_i + b_j - b_j = b_i$
    - pozor, druhá implikace se dokazuje pomocí $+b_j - b_j$

- věta o jednoznačnosti volných a bázických proměnných

    - 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 se charakter proměnných v A' a A'' liší.
        - Předpokládejme BÚNO, že x_i je bázická v A' a volná v A''.

        - Pro libovolnou volbu proměnných A' určuje soustava $A'x = 0$ jednoznačnou hodnotu x_i (protože x_i je v A' bázická).
        - Protože proměnná x_i je volná v A'', můžeme její hodnotu zvolit odlišně. Všechny ostatní volné proměnné zvolíme u obou matic stejně.
        - Získáme řešení $A''x = 0$, které není řešením $A'x = 0$, což je spor.

- Frobeniova věta
    - věta: Soustava $Ax = b$ má řešení právě tehdy, když se hodnost matice A rovná hodnosti rozšířené matice $(A|b)$.
    - důkaz
        - zvolíme libovolné $(A'|b')$ v REF takové, že $(A|b) \sim\sim (A'|b')$
        - řešení x existuje $\iff$ b' nemá žádný pivot $\iff$ počet pivotů A' se shoduje s počtem pivotů $(A'|b')$ $\iff$ $\mathrm{rank}(A) = \mathrm{rank}(A|b)$
        - protože převod $A \sim\sim A'$ lze provést stejnými elementárními úpravami jako $(A|b) \sim\sim (A'|b')$

- věta o vztahu mezi řešeními $Ax = b$ a $Ax = 0$
    - věta: Nechť x^0 splňuje $Ax^0 = b$. Poté zobrazení $\bar{x} \mapsto \bar{x} + x^0$ je bijekce mezi množinami $\{\bar{x} : A\bar{x} = 0\}$ a $\{x : Ax = b\}$.
    - důkaz
        - $U = \{\bar{x} : A\bar{x} = 0\}, \quad V = \{x : Ax = b\}$
        - $f : U \to V, \quad \bar{x} \mapsto \bar{x} + x^0$
        - $g : V \to U, \quad x \mapsto x - x^0$
        - f je bijekce, neboť
            - $g \circ f$ je identita na $U \implies f$ je prosté
            - $f \circ g$ je identita na $V \implies f$ je „na“
        - jiný mechanismus důkazu
            - f je zobrazení: $A\bar{x} = 0 \implies A(\bar{x} + x_0) = A\bar{x} + Ax_0 = 0 + b = b$
            - f je prosté: $x \neq x' \implies x + x^0 \neq x' + x^0$, což zjevně platí
            - f je na: $(\forall x \in V)(\exists \bar{x} \in U) : x = \bar{x} + x^0$, takové $\bar{x}$ lze určit jako $\bar{x} = x - x^0$

- věta popisující všechna řešení $Ax = b$
    - věta

- 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 $x = x^0 + p_1\bar{x}^1 + \cdots + p_{n-r}\bar{x}^{n-r}$.
  - p jsou libovolné reálné parametry
  - $\bar{x}$ jsou vhodná řešení soustavy $A\bar{x} = 0$
  - x^0 je libovolné řešení soustavy $Ax = b$
- Soustava $A\bar{x} = 0$ má pouze triviální řešení $\bar{x} = o \iff \operatorname{rank}(A) = n$.

- důkaz
  - pro $A\bar{x} = 0$
    - přejmenujeme volné proměnné na $p_1, \ldots p_{n-r}$
    - zpětnou substitucí můžeme vyjádřit každou složku řešení jako lineární funkci volných proměnných
      - $\bar{x}_1 = \alpha_{1,1}p_1 + \cdots + \alpha_{1,n-r}p_{n-r}$
      - ...
      - $\bar{x}_n = \alpha_{n,1}p_1 + \cdots + \alpha_{n,n-r}p_{n-r}$
    - zvolíme $\bar{x}^1 = (\alpha_{1,1}, \ldots, \alpha_{n,1})^T, \ldots, \bar{x}^{n-r} = (\alpha_{1,n-r}, \ldots, \alpha_{n,n-r})^T$
    - ty řeší $A\bar{x} = 0$, což lze ověřit tak, že pro každý z nich vynulujeme všechny volné proměnné (tedy parametry p) kromě toho s odpovídajícím indexem, který nastavíme jako 1
    - je-li $\operatorname{rank}(A) = n$, proměnné jsou jen bázické a o je jediné řešení
  - pro $Ax = b$ vztah plyne z přechozí věty a důkazu této věty pro $Ax = 0$
    - ale lze dokázat také pomocí $x_1 = \beta_1 + \alpha_{1,1}p_1 + \cdots + \alpha_{1,n-r}p_{n-r}$

- věta o ekvivalentních definicích regulárních matic

  - věta: pro čtvercovou matici $A \in \mathbb{R}^{n \times n}$ jsou následující podmínky ekvivalentní
    1. matice A je regulární, tedy k ní existuje inverzní matice … $\exists B : AB = I_n$
    2. $\operatorname{rank}(A) = n$
    3. $A \sim\sim I_n$
    4. systém $Ax = 0$ má pouze triviální řešení $x = 0$
  - důkaz
    - $2. \iff 4.$ vyplývá z předchozí věty

    - $\implies$ lze také dokázat tak, že do rovnic dosazujeme zespodu
    - $\impliedby$ lze dokázat sporem (matice s $\mathrm{rank}(A) < n$ musí mít nutně více řešení, protože do volné proměnné lze dosadit libovolnou hodnotu)
  - $2. \implies 3.$ podle Gauss-Jordanovy eliminace, $2. \impliedby 3.$ triviálně
  - $2. \implies 1.$
    - označme $I_n = (e^1|\dots|e^n)$
    - pro $i \in \{1, \dots, n\}$ uvažme soustavy $Ax^i = e^i$
    - z $\mathrm{rank}(A) = n$ dostaneme $B = (x^1|\dots|x^n)$
  - $1. \implies 2.$
    - pokud $\mathrm{rank}(A) < n$, tak pro jedno (či více) i bude i-tý řádek matice A eliminován ostatními řádky
    - konkrétní rovnice $Ax^i = e^i$ tedy nebude mít žádné řešení, protože onu jedinou jedničku v e^i není možné eliminovat nulami

- věta o znaménku složené permutace

  - věta: Pro libovolné $p, q \in S_n : \mathrm{sgn}(q \circ p) = \mathrm{sgn}(p) \cdot \mathrm{sgn}(q)$.
  - důkaz
    - # inverzí $(q \circ p) =$ # inverzí $p +$ # inverzí q $- 2|\{(i,j) : i < j \land p(i) > p(j) \land q(p(i)) < q(p(j))\}|$
    - od součtu odečítáme dvojité inverze – ty se totiž ve složené permutaci „rozmotají“ (každou takovou inverzi odečítáme dvakrát – jednou za každou permutaci)
    - protože od součtu odečítáme sudé číslo, sudost/lichost součtu je zachována – tedy postačí součin znamének obou permutací (exponenty se sčítají)

- věta charakterizující, kdy $\mathbb{Z}_n$ je těleso

  - věta: $\mathbb{Z}_p$ je těleso, právě když je p prvočíslo.
  - důkaz
    - $\implies$ pokud by p bylo složené $p = ab$, pak $ab \equiv 0 \mod p$, což je spor s pozorováním, že pokud $ab = 0$, pak $a = 0$ nebo $b = 0$
      - důkaz pozorování (sporem)
        - pro nenulová a, b by existovaly inverzní prvky a^{-1}, b^{-1}

      - $1 = aa^{-1}bb^{-1} = aba^{-1}b^{-1} = 0a^{-1}b^{-1} = 0$
  - $\Longleftarrow$
    - většina axiomů plyne z vlastností $+$ a $\cdot$ na $\mathbb{Z}$, kromě existence inverzních prvků a^{-1}, protože $\mathbb{Z}$ není uzavřená na dělení
    - $A = \{1, \dots, p-1\}$
    - chceme: $(\forall a \in A)(\exists a^{-1} \in A) : aa^{-1} \equiv 1 \mod p$
    - nechť $f_a : A \to A, \quad x \mapsto ax \mod p$
    - hledané a^{-1} splňuje $f_a(a^{-1}) = 1$
    - tedy stačí ukázat, že 1 je v oboru hodnot f_a
    - dokážeme dokonce, že f_a je surjektivní („na")
    - protože f_a zobrazuje konečnou množinu na sebe samu, pak platí, že je surjektivní, právě když je prosté
    - pokud by pro spor f_a nebylo prosté, pak $\exists b, c : b > c \land f_a(b) = f_a(c)$ $\implies 0 = f_a(b) - f_a(c) = ab - ac = a(b-c) \mod p$
    - což je spor, neboť $a, (b-c) \in A$

- malá Fermatova věta
  - věta: Pro prvočíslo p a každé $a \in \{1, \dots, p-1\} : a^{p-1} \equiv 1 \mod p$.
  - důkaz
    - zobrazení $f_a : x \mapsto ax$ je v $\mathbb{Z}_p$ bijekcí na $\{1, \dots, p-1\}$ (viz výše)
    - proto v $\mathbb{Z}_p$ platí $\prod_{x=1}^{p-1} x = \prod_{x=1}^{p-1} f_a(x) = \prod_{x=1}^{p-1} ax = a^{p-1} \prod_{x=1}^{p-1} x$
    - a po zkrácení $\prod_{x=1}^{p-1} x$ dostaneme $1 = a^{p-1}$
  - důsledek: $a = a^p$ (v tělese $\mathbb{Z}_p$)

- věta o průniku vektorových prostorů
  - věta
    - Nechť $(U_i, i \in I)$ je libovolný systém podprostorů prostoru V
    - Průnik tohoto systému $\bigcap_{i \in I} U_i$ je také podprostorem V.
  - důkaz
    - nechť $W = \bigcap_{i \in I} U_i$, ukážeme, že W je uzavřen na $+$ a $\cdot$
    - $\forall u, v \in W : u, v \in W \implies \forall i \in I : u, v \in U_i$ $\implies \forall i \in I : u + v \in U_i \implies u + v \in W$
    - $\forall \alpha \in \mathbb{K}, v \in W : v \in W \implies \forall i \in I : v \in U_i$ $\implies \forall i \in I : \alpha v \in U_i \implies \alpha v \in W$

        - věta platí i pro $I = \emptyset$, neboť prázdný průnik $\equiv V \Subset V$

- věta o ekvivalentních definicích lineárního obalu
    - věta
        - Nechť V je vektorový prostor nad $\mathbb{K}$ a X je podmnožina V.
        - Potom $\mathcal{L}(X)$ je množina všech lineárních kombinací vektorů z X.
    - důkaz
        - $W_1 = \bigcap U : U \Subset V, X \subseteq U$
        - $W_2 = \{\sum_{i=1}^k \alpha_i v_i : k \in \mathbb{N}, \alpha_i \in \mathbb{K}, v_i \in X\}$
        - chceme ukázat $W_1 = \mathcal{L}(X) = W_2$
        - W_2 je podprostor, protože je uzavřen na skalární násobky
          $u \in W_2 \implies u = \sum_{i=1}^k \alpha_i v_i$
          $\implies \beta u = \beta \sum_{i=1}^k \alpha_i v_i = \sum_{i=1}^k (\beta\alpha_i) v_i \implies \beta u \in W_2$
        - a analogicky také na součty
        - protože $X \subseteq W_2$, máme W_2 mezi protínajícími se podprostory U_i
        - z toho plyne $W_1 \subseteq W_2$
        - každý U_i obsahuje X a je uzavřen na sčítání a skalární násobky
        - každý U_i tedy obsahuje všechny lineární kombinace vektorů X
        - proto $\forall U_i : W_2 \subseteq U_i \implies W_2 \subseteq W_1$

- Steinitzova věta o výměně (včetně lemmatu, pokud jej potřebujete)
    - lemma o výměně
        - Buď $y_1, \dots, y_n$ systém generátorů vektorového prostoru V a nechť vektor $x \in V$ má vyjádření $x = \sum_{i=1}^n \alpha_i y_i$.
        - Pak pro libovolné k takové, že $\alpha_k \neq 0$, je $y_1, \dots, y_{k-1}, x, y_{k+1}, \dots, y_n$ systém generátorů prostoru V.
    - důkaz lemmatu
        - $x = \sum_i \alpha_i y_i = \sum_{i \neq k} \alpha_i y_i + \alpha_k y_k$
        - $y_k = \frac{1}{\alpha_k}(x - \sum_{i \neq k} \alpha_i y_i)$
        - libovolný vektor $z \in V$ lze vyjádřit jako
          $z = \sum_i \beta_i y_i = \sum_{i \neq k} \beta_i y_i + \beta_k y_k = \sum_{i \neq k} \beta_i y_i + \frac{\beta_k}{\alpha_k}(x - \sum_{i \neq k} \alpha_i y_i)$
          $= \frac{\beta_k}{\alpha_k} x + \sum_{i \neq k} (\beta_i - \frac{\beta_k}{\alpha_k} \alpha_i) y_i$
    - S. věta
        - Buď V vektorový prostor, buď $x_1, \dots, x_m$ lineárně nezávislý systém ve V a nechť $y_1, \dots, y_n$ je systém generátorů V.

    - Pak platí $m \leq n$ a existují navzájem různé indexy $k_1, \ldots, k_{n-m}$ takové, že $x_1, \ldots, x_m, y_{k_1}, \ldots, y_{k_{n-m}}$ tvoří systém generátorů V.
  - důkaz věty *matematickou indukcí podle* m
    - je-li $m = 0$, tvrzení platí triviálně
    - předpokládejme, že tvrzení platí pro $m - 1$ a ukážeme, že platí i pro m
    - kdyby $m - 1 = n$, pak by vektory $x_1, \ldots, x_{m-1}$ byly generátory prostoru V, což by byl spor s lineární nezávislostí $x_1, \ldots, x_m$
      - $\implies m - 1 < n \implies m \leq n \quad \square_1$
    - během indukce vektory postupně nahrazujeme pomocí lemmatu o výměně
    - vycházíme z toho, že věta platí pro $m - 1$ vektorů z LN množiny a $n - m + 1$ vektorů z množiny generátorů
    - takže m-tý vektor z LN množiny vyjádříme z ostatních a pomocí lemmatu o výměně jím nahradíme (n-m+1)-tý vektor z množiny generátorů
    - lemma o výměně bude možné uplatnit, protože alespoň u jednoho z $n - m + 1$ vektorů z množiny generátorů bude ve vyjádření doplňovaného vektoru nenulový koeficient (jinak by to bylo ve sporu s LN) – viz skripta

- věta o jedinečnosti lineárního zobrazení

  - věta
    - Nechť U a V jsou prostory nad $\mathbb{K}$ a X je báze U.
    - Pak pro jakékoliv zobrazení $f_0 : X \to V$ existuje jediné lineární zobrazení $f : U \to V$ rozšiřující f_0, tj. $\forall u \in X : f(u) = f_0(u)$.
    - (Jinými slovy: To, kam se zobrazí vektory báze, jednoznačně definuje lineární zobrazení jako celek – tedy i zobrazení všech ostatních vektorů daného prostoru.)
  - důkaz
    - vektor $w \in U$ lze jednoznačně vyjádřit jako lineární kombinaci bázických vektorů, tedy $w = \sum_i \alpha_i u_i$
    - potom $f(w) = f(\sum_i \alpha_i u_i) = \sum_i \alpha_i f(u_i) = \sum_i \alpha_i f_0(u_i)$
  - důsledek: pokud je $f : U \to V$ lineární, pak $\dim(U) \geq \dim(f(U))$, protože obraz $f(X)$ báze X prostoru U generuje $f(U)$

- věta o charakterizaci isomorfismu mezi vektorovými prostory
  - věta: Lineární zobrazení $f : U \to V$ je isomorfismus prostorů U a V s konečnými bázemi X a Y právě tehdy, když $[f]_{X,Y}$ je regulární.
  - důkaz
    - $\Longleftarrow$ uvažme $g : V \to U$ takové, že $[g]_{Y,X} = [f]^{-1}_{X,Y}$, pak
      - $[g \circ f]_{X,X} = [f]^{-1}_{X,Y}[f]_{X,Y} = I_{|X|} = [id]_{X,X} \implies f$ je prosté
      - $[f \circ g]_{Y,Y} = [f]_{X,Y}[f]^{-1}_{X,Y} = I_{|Y|} = [id]_{Y,Y} \implies f$ je „na“
    - $\implies$
      - $[f^{-1}]_{Y,X}[f]_{X,Y} = [id]_{X,X} = I_{|X|} \implies |Y| \geq |X|$
      - $[f]_{X,Y}[f^{-1}]_{Y,X} = [id]_{Y,Y} = I_{|Y|} \implies |X| \geq |Y|$
      - $\implies |X| = |Y|$
      - matice jsou navzájem inverzní (a čtvercové), takže jejich součinem získáváme jednotkovou matici – lze tedy říci, že jsou regulární
  - důsledek: když f je isomorfismus, pak platí $[f^{-1}]_{Y,X} = [f]^{-1}_{X,Y}$

- věta o vektorových prostorech souvisejících s maticí A
  - lemma: Pokud $A' = BA$, pak $\dim(\mathcal{S}(A')) \leq \dim(\mathcal{S}(A))$.
  - zkrácený důkaz lemmatu
    - BÚNO předpokládejme, že bázi $\mathcal{S}(A)$ tvoří d prvních sloupcových vektorů u
    - $w \in A, w' \in A'$
    - $w' = Bw = B\sum_{i=1}^d \alpha_i u_i = \sum_{i=1}^d \alpha_i B u_i = \sum_{i=1}^d \alpha_i u'_i$
    - bázi $\mathcal{S}(A')$ tedy tvoří nejvýše d prvních sloupcových vektorů u'
  - věta: Jakákoli $A \in \mathbb{K}^{m \times n}$ splňuje $\dim(\mathcal{R}(A)) = \dim(\mathcal{S}(A))$.
  - důkaz věty
    - nechť $A \sim\sim A'$ v odstupňovaném tvaru, neboli existuje regulární R taková, že $A' = RA$
    - podle lemmatu $\dim(\mathcal{S}(A')) \leq \dim(\mathcal{S}(A))$
    - z $A = R^{-1}A'$ dostaneme $\dim(\mathcal{S}(A')) \geq \dim(\mathcal{S}(A))$, a tudíž i rovnost dimenzí
    - pro matice A' v odstupňovaném tvaru platí věta přímo
      - $\dim(\mathcal{R}(A')) = \#$ pivotů $= \operatorname{rank}(A') = \dim(\mathcal{S}(A'))$
    - protože $\mathcal{R}(A) = \mathcal{R}(A')$, dostaneme

- $\dim(\mathcal{R}(A)) = \dim(\mathcal{R}(A')) = \dim(\mathcal{S}(A')) = \dim(\mathcal{S}(A))$

- tvrzení o mohutnostech lineárně nezávislé množiny a generující množiny
  - tvrzení: Jestliže Y je konečná generující množina prostoru V a X je lineárně nezávislá ve V, potom $|X| \leq |Y|$.
  - důkaz (sporem)
    - předpokládejme, že $Y = \{v_1, \ldots, v_n\}$ a že z X lze vybrat různá $u_1, \ldots, u_{n+1}$
    - každé u_i vyjádříme jako $u_i = \sum_{j=1}^{n} a_{i,j} v_j$, přičemž $a_{i,j} \in A$
    - matice A má $n+1$ řádků a n sloupců, z čehož po Gaussově eliminaci nutně plyne nulový řádek, tedy je některý řádek lineární kombinací ostatních
    - to je spor s lineární nezávislostí vektorů $u_1, \ldots, u_{n+1}$

- věta o dimenzi průniku vektorových prostorů
  - věta: Jsou-li U, V podprostory konečné generovaného prostoru W, pak $\dim(U) + \dim(V) = \dim(U \cap V) + \dim(\mathcal{L}(U \cup V))$.
  - důkaz: rozšíříme bázi X průniku $U \cap V$ na bázi Y prostoru U a také na bázi Z prostoru V, potom $|Y| + |Z| = |X| + |Y \cup Z|$

- věta o dimenzi jádra matice
  - věta: Pro libovolné $A \in \mathbb{K}^{m \times n} : \dim(\ker(A)) + \operatorname{rank}(A) = n$.
  - důkaz
    - nechť $d = n - rank(A)$ je počet volných proměnných a $x_1, \ldots, x_d$ jsou řešení soustavy $Ax = 0$ daná zpětnou substitucí
    - tato řešení jsou lineárně nezávislá, protože pro každé i platí, že x_i je mezi $x_1, \ldots, x_d$ jediné, které má složku odpovídající i-té volné proměnné nenulovou
    - vektory $x_1, \ldots, x_d$ tudíž tvoří bázi $\ker(A)$, a proto $\dim(\ker(A)) = d = n - rank(A)$

- věta o řešení rovnice s lineárním zobrazením
  - věta: Nechť $f : U \to V$ je lineární zobrazení. Pro libovolné $v \in V$ rovnice $f(u) = v$ buď nemá žádné řešení, nebo řešení tvoří afinní podprostor $u_0 + \ker(f)$, kde u_0 je libovolné řešení $f(u) = v$.

- poznámka: tato věta přímo souvisí s větou o vztahu $Ax = b$ a $Ax = 0$
- důkaz
  - když $u \in u_0 + \ker(f)$, pak $u = u_0 + w$ pro $w \in \ker(f)$
  - nyní $f(u) = f(u_0 + w) = f(u_0) + f(w) = v + o = v$
  - naopak pro $f(u) = v$ platí $f(u - u_0) = f(u) - f(u_0) = v - v = 0$
  - čili $u - u_0 \in \ker(f)$, tudíž $u \in u_0 + \ker(f)$

- pozorování o matici složeného lineárního zobrazení
  - pozorování: Nechť U, V, W jsou vektorové prostory nad $\mathbb{K}$ s konečnými bázemi X, Y, Z. Pro matice lineárních zobrazení $f : U \to V$ a $g : V \to W$ platí, že $[g \circ f]_{X,Z} = [g]_{Y,Z}[f]_{X,Y}$
  - důkaz
    - pro všechny $u \in U$ platí
      - $[(g \circ f)(u)]_Z = [g \circ f]_{X,Z}[u]_X$
      - $[(g \circ f)(u)]_Z = [g(f(u))]_Z = [g]_{Y,Z}[f(u)]_Y = [g]_{Y,Z}[f]_{X,Y}[u]_X$
      - tedy $[g \circ f]_{X,Z}[u]_X = [g]_{Y,Z}[f]_{X,Y}[u]_X$
    - dosadíme-li za u i-tý vektor báze X, máme $[u]_X = e^i$ a tedy nám ze vztahu $[g \circ f]_{X,Z}e^i = ([g]_{Y,Z}[f]_{X,Y})e^i$ plyne, že matice mají i-té sloupce shodné $\square$

- zformulujte problém o počtu sudých podgrafů a vyřešte jej
  - problém: Kolik sudých podgrafů obsahuje souvislý graf G?
  - řešení
    - sudý podgraf je podgraf, který má sudé stupně všech vrcholů
    - symetrický rozdíl $\triangle$ zachovává sudé stupně, protože symetrický rozdíl dvou množin sudé mohutnosti má také sudou mohutnost
    - proto $(U, \triangle, \cdot)$ tvoří vektorový prostor nad $\mathbb{Z}_2$
    - pro prostory konečné mohutnosti platí $|U| = |\mathbb{K}|^{\dim(U)}$
    - ekvivalentní problém: sestrojte bázi U
    - zvolme libovolnou kostru T grafu G
    - pro každou hranu $e_i \in E_G \setminus E_T$ definujme A_i jako unikátní cyklus z $T \cup e_i$
    - množina takových cyklů je lineárně nezávislá, protože hrana e_i nemůže být eliminována symetrickým rozdílem A_i s ostatními prvky množiny, neboť ty e_i neobsahují

    - pro libovolný sudý podgraf B označme $B \setminus E_T = \{e_{i_1}, \ldots, e_{i_k}\}$
    - graf $B \triangle A_{i_1} \triangle \cdots \triangle A_{i_k}$ je sudým podgrafem G, ale také je podgrafem T, neboť hrany e_i jsou eliminovány
    - strom nemá žádné cykly, tudíž tento rozdíl (výše) je roven nule
    - odtud $B = A_{i_1} \triangle \cdots \triangle A_{i_k}$
    - dostáváme, že X generuje U
    - tedy $\dim(U) = |X| = |E_G| - |E_T| = |E_G| - |V_G| + 1$
    - každý souvislý graf G má $2^{|E_G|-|V_G|+1}$ sudých podgrafů

- zformulujte problém o množinových systémech s omezeními na mohutnosti a vyřešte jej

  - problém: Kolik podmnožin může mít n-prvková množina, pokud každá podmnožina má mít lichou velikost, ale průnik každé dvojice různých podmnožin má mít sudou velikost?
  - věta: Vždy platí, že $k \leq n$, neboli existuje nejvýše n takových podmnožin.
  - důkaz
    - uvažujme soustavu podmnožin, která splňuje zadání
    - sestrojíme matici incidence $M \in \mathbb{Z}_2^{k \times n}$ předpisem $m_{i,j} = \begin{cases} 1 & \text{pokud } j \in A_i \\ 0 & \text{pokud } j \notin A_i \end{cases}$
    - matice splňuje $MM^T = I_k$, protože v součinu řádku a sloupce se stejným indexem je prvků lichý počet (tedy 1 v $\mathbb{Z}_2$) a u nesouhlasných řádků a sloupců se prvky posčítají na nulu, protože průnik je sudý
    - nyní $k = \text{rank}(I_k) = \text{rank}(MM^T) \leq \text{rank}(M) \leq n$

- zformulujte problém o dělení obdélníku na čtverce a vyřešte jej

  - problém: Lze obdélník s iracionálním poměrem délek jeho stran rozdělit na konečně mnoho čtverců?
  - věta: Pro iracionální poměr žádné takové rozdělení neexistuje.
  - zjednodušený důkaz (sporem)
    - nechť má obdélník R délky stran $1 : x$, kde x je iracionální
    - $\mathbb{R}$ tvoří vektorový prostor nad $\mathbb{Q}$, zde jsou 1 a x lineárně nezávislé
    - zvolme libovolné lineární zobrazení $f : \mathbb{R} \to \mathbb{R}$, kde $f(1) = 1$ a $f(x) = -1$
    - pro A o stranách a, b definujeme plochu jako $v(A) = f(a)f(b)$

        - R rozdělíme na čtverce A o stranách délek a
        - $-1 = f(1)f(x) = v(R) = \sum v(A) = \sum f(a)^2 \geq 0$

Přehledy (13)

přehledově sepište, co víte o…

uveďte definice, tvrzení, věty, příklady a souvislosti – důkazy nejsou vyžadovány

- elementární řádkové operace a Gaussova eliminace
    - rozšířená matice soustavy
    - 4 typy elementárních řádkových úprav
        - elementární matice
    - odstupňovaný tvar matice
    - věta o totožnosti řešení
    - Gaussova eliminace
    - zpětná substituce
    - věta o libovolné volbě volných proměnných (jakoukoli volbu volných proměnných lze jednoznačně rozšířit na řešení)
    - věta o jednoznačnosti sloupců s pivoty (o jednoznačnosti volných a bázických proměnných)
    - bázické a volné proměnné
    - hodnost matice
    - Frobeniova věta
- řešení homogenních a nehomogenních soustav lineárních rovnic
    - homogenní × nehomogenní soustava rovnic
    - věta o vztahu mezi řešeními $Ax = b$ a $Ax = 0$
    - věta popisující všechna řešení $Ax = b$
    - homogenní soustava má triviální řešení $x = 0$, když $\mathrm{rank}(A) = n$
    - provedení zkoušky (dosazení řešení včetně parametrů do původní soustavy)
    - redukovaný odstupňovaný tvar
- maticové operace
    - nulová matice, jednotková matice, hlavní diagonála
    - transponovaná matice, symetrická matice
    - součet matic, α-násobek matice
    - součin matic, jeho asociativita

- elementární matice
- inverzní matice
- maticové rovnice (viz níže)

- regulární a singulární matice
  - inverzní matice, její jednoznačnost
  - regulární × singulární matice
  - věta o ekvivalentních definicích regulárních matic
  - výpočet inverzní matice
  - vlastnosti regulárních matic
    - pro R regulární: $A = B \iff AR = BR \iff RA = RB$
    - pro A, B regulární (stejného řádu)
      - $(A^{-1})^{-1} = A$
      - AB je regulární
      - $(AB)^{-1} = B^{-1}A^{-1}$
      - $(A^T)^{-1} = (A^{-1})^T$
  - maticové rovnice (viz prezentace)
    - $A + X = B \implies X = B - A$
    - $\alpha X = B \implies X = \frac{1}{\alpha}B$
    - $AX = B \implies X = A^{-1}B$ pro regulární A
    - $XA = B \implies X = BA^{-1}$ pro regulární A
- binární operace a jejich vlastnosti
  - binární operace jako zobrazení
  - komutativita, asociativita
  - neutrální prvek, inverzní prvek
- (obecné) grupy
  - definice grupy
  - binární operace a jejich vlastnosti
  - aditivní a multiplikativní grupy
  - vlastnosti grup (jednoznačnost neutrálního prvku, jednoznačnost inverzního prvku, ekvivalentní úpravy, jednoznačnost řešení rovnic)
- permutační grupy
  - permutace jako zobrazení (bijekce)
  - způsob popisu permutace (tabulkou, jejím druhým řádkem, pomocí bipartitního grafu, podle grafu cyklů, seznamem cyklů, pomocí permutační matice P)

    - množina S_n všech permutací na n prvcích s operací skládání tvoří symetrickou grupu
        - identita je neutrální prvek
    - pevný bod, transpozice, inverze
    - znaménko permutace (sudé/liché permutace)
    - věta o znaménku složené permutace
- tělesa
    - definice tělesa
    - distributivita
    - konečná tělesa – zbytkové třídy modulo prvočíslo p, Galoisovo těleso (těleso o velikosti n existuje $\iff n$ je mocninou prvočísla)
    - metavěta – tvrzení o soustavách rovnic, maticích a výpočtech nad reálnými čísly platí i v libovolném tělese
    - vlastnosti tělesa (jednoznačnost neutrálních a inverzních prvků, korektnost ekvivalentních úprav, řešitelnost rovnic)
    - pokud $ab = 0$, pak $a = 0$ nebo $b = 0$
    - charakteristika tělesa
    - věta charakterizující, kdy $\mathbb{Z}_n$ je těleso
    - malá Fermatova věta
- vektorové prostory a jejich podprostory
    - definice vektorového prostoru nad tělesem
    - binární operace ve vektorovém prostoru
    - aritmetický vektorový prostor, vektorový prostor matic, triviální vektorový prostor (pouze nulový vektor)
    - vlastnosti vektorových prostorů (jednoznačnost nulového a opačného vektoru, korektnost ekvivalentních úprav, řešitelnost rovnic)
    - definice podprostoru
    - věta o průniku podprostorů
    - lineární obal, generátory podprostoru
    - lineární kombinace
    - věta o ekvivalentních definicích lineárního obalu
- vektorové prostory určené maticí A
    - jádro, řádkový prostor, sloupcový prostor
    - elementární úpravy nemění jádro ani řádkový prostor
    - (technické) lemma o dimenzích sloupcového prostoru

    - věta o dimenzích sloupcového a řádkového prostoru matice
    - počet řádků matice je roven součtu dimenze jádra a hodnosti matice (tedy dimenzi sloupcového/řádkového prostoru)
- lineární závislost
    - definice lineární nezávislosti (LN)
    - lineární nezávislost řádků matice v odstupňovaném tvaru
    - lineární nezávislost podmnožin (podmnožina lineárně nezávislé množiny bude rovněž nezávislá apod.)
    - báze vektorového prostoru
- báze vektorových prostorů
    - definice báze
    - lineární nezávislost
    - vektor souřadnic
    - kanonická báze v aritmetickém vektorovém prostoru
    - věta o existenci báze (každý vektorový prostor má bázi)
    - lemma o výměně
    - Steinitzova věta o výměně
    - jakoukoliv LN množinu lze rozšířit na bázi
    - všechny báze konečně generovaného prostoru mají stejnou mohutnost
    - dimenze vektorového prostoru
- lineární zobrazení a jejich matice
    - definice lineárního zobrazení
    - triviální lineární zobrazení (na nulový vektor), identita
    - geometrická lineární zobrazení (rotace, osová souměrnost podle osy procházející počátkem, stejnolehlost se středem v počátku)
    - skládání lineárních zobrazení, existence inverze pro bijektivní zobrazení (isomorfismus)
    - transformace na vektor souřadnic
    - věta o rozšiřitelnosti (jedinečnosti) lineárního zobrazení
    - afinní prostor a jeho dimenze
    - matice lineárního zobrazení
    - matice přechodu
    - isomorfismus vektorových prostorů