- *#1: 06/10/2*
- **Úvod**
- **Lineární rovnice a jejich soustavy**
- **Matice**
- **Vektor**
- **Lineární rovnice a jejich soustavy (pokračování)**
- *#2: 06/10/9*
- **Řešení soustav**
- **Operace s maticemi, speciální typy matic.**
- *#3: 06/10/23*
- **Soustavy lineárních rovnic (doplnění minulé př.)**
- **Počítání s maticemi**
- *#4: 06/10/30*
- **Matice n×n**
- **Tělesa**
  - **Definice.** Je-li X nějaká množina, pak *binární operace* na X je libovolné zobrazení $X \times X \to X$
    - příklady operací
      - + **N**, **R**
      - násobení reg. matic
      - min{a, b}
  - **Definice.** *Těleso* je množina **T** spolu se dvěma binárními operacemi na **T** + a · (sčítání a násobení) splňujícími následující podmínky (tzv. axiomy)
    - **(sK)** sčítání je komutativní
      - $\forall a,b \in \mathbf{T}$: $a+b = b+a$
    - **(sA)** sčítání je asociativní
      - $\forall a, b, c \in \mathbf{T}$: $a+(b+c) = (a+b)+c$
    - **(sO)** existuje *neutrální* prvek sčítání
      - $\exists\, O \in \mathbf{T}\ \forall a \in \mathbf{T}$: $a+O = a$
    - **(sI)** existuje *opačný* prvek pro sčítání
      - $\forall a \in \mathbf{T}\ \exists b \in \mathbf{T}$ $a+b = O$
    - **(nK)** násobení je komutativní
    - **(nA)** …
    - **(n1)** *jednotkový* prvek pro násobení (podobně jako neutrální)
      - $\exists 1\ \forall a \in \mathbf{T}$ $1 \cdot a = a$
    - **(nI)** inversní prvek pro násobení
      - $\forall a \in \mathbf{T} - \{O\}\ \exists\, b \in \mathbf{T}$, $ab = 1$
    - **(d)** násobení je distributivní vzhledem ke sčítání, tj. $\forall a, b, c \in \mathbf{T}$
      - a(b+c) = ab+acß
    - **(01)** netrivialita
      - $0 \neq 1$
  - Značení
    - opačný: $-a$
    - inverzní: a^{-1}
    - vynechává se násobení
    - $a+(-b) = a-b$
    - $a \cdot b^{-1} = a/b$
  - Příklady
    - **R**, **Q**, **C**
    - $\mathbf{T} = \{a+\sqrt{2}b,\ a, b \in \mathbf{Q}\}$
  - (Ne)příklady
    - **Z**

- Pozorování 1: Prvky 0 a 1 jsou určeny jednoznačně
  - Důkaz sporem, kdyby existovala 0 a 0': 0+0'=0' & 0+0'=0 ⇒ 0=0' a to je spor, chtěli jsme dvě 0
  - Jednotkový obdobně
- Pozorování 2: ∀a∈**T**-{0} je prvek -a a a^{-1} určen jednoznačně
  - sporem: kdyby ex. -a≠(-a)'
    - -a = -a+ 0 = -a +(a+ (-a)' = (-a+a) + (-a)' = 0 +(-a)' = (-a)'

- *#5: 06/11/6*

- **Tělesa (pokračování)**
  - Úkol: Zkusit důkazy.
  - Pozorování 3: ∀a∈**T**: -(-a) = a, ∀a∈**T**-{0}: $(a^{-1})^{-1}$
    - Důkaz: -(-a) = -(-a) + 0 = -(-a) + (-a+a) = (-(-a)+(-a)) + a = 0 + a = a, inverzní prvek obdobně
  - Pozorování 4.1: ∀a∈**T**: 0a = 0
    - Důkaz: 0a = 0a + 0 = 0a + (0a - 0a) = (0a+0a) - 0a = (0+0)a - 0a = 0a - 0a = 0
      - šlo by i: 0a + (1a - 1a)
  - Pozorování 4.2: ∀a∈**T**: (-1)a = -a
    - Stačí ověřit, že (-1)a + a = 0 (víme pak, že (-1)a se musí rovnat -a)), nebo
    - Důkaz: (-1)a = (-1)a + (a-a) = ((-1)a+1a) = (((-1)+1)a)-a = 0 -a = -a
  - Pozorování 5: ab=0 ⇒ a=0 ∨ b=0
    - Důkaz sporem a≠0≠b:
    - $1 = 1 \cdot 1 = (a \cdot a^{-1}) \cdot (b \cdot b^{-1}) = (a \cdot b) \cdot (a^{-1} \cdot b^{-1}) = 0 \cdot (a^{-1} \cdot b^{-1}) = 0$ ⇒ spor
  - Pozorování 6: a + b = a + c ⇒ b = c; ab = ac & a≠0 ⇒ b=c
    - Důkaz:
      - b = b+ (a-a) = (b+a) - a = (c+a) - a = c + (a-a) = c + 0 = c
    - Obdobně důkaz, že rovnice a + x = b má jednoznačné řešení:
      - x = x + (a-a) = (x+a) -a = b - a = b + (-a); a to je jednoznačné
  - **Definice.** Pro číslo p ∈ **N** se množiny {0,p, 2p, …} = [0], {1,p+1, 2p+1, …} = [1], {2,p+2, 2p+2, …} = [2], … {p-1, 2p-1, 3p-1 …} = [p-1] nazývají *zbytkové třídy modulo* p.
    - Značení
      - x_p = třída obsahující *x*
      - $\mathbf{Z}_p$ = množina zbytkový tříd modulo *p*
    - $\forall p\ \forall a, b \in \mathbf{N}: a_p \oplus b_p = (a+b)_p$
    - $\forall p\ \forall a, b \in \mathbf{N}: a_p \odot b_p = (a \cdot b)_p$
    - **Tvrzení.** $\mathbf{Z}_n$ je těleso právě, když *n* je prvočíslo.
      - Důkaz:
        - *n* není prvočíslo, tedy *n* = *a* · *b*, [a]·[b] = [0], spor s pozorováním 5
        - *n* je prvočíslo: ověříme, že platí axiomy
          - (…)
          - opačný prvek k [a] je [(n-a) mod p]
          - (…)
          - inverzní prvek: a≠0, hledáme a^{-1}: $a \odot a^{-1}$ = [1]
            - uvažme 1a, 2a, 3a, (…), (n-1)a – nenulové, je jich n-1, a kdyby po dělení p dávala různé zbytky, tak jedno musí dávat zbytek [1]
              - Předpokládejme $(i \cdot a)_n = (j \cdot a)_n$, pro (n-1)>*i*>*j*, pak *ia* = *xn* + *c* & *ja* = *yn* + *c*
                - a(i-j) = n(x-y), n(x-y) je dělitelné *n*, a mezi 0 a n-1 a (i-j) mezi 0 a n-1 (součin není dělitelná přirozeným číslem *n*) ⇒ pravá str. dělitelná *n* a levá ne ⇒ spor, tedy čísla dávají různé zbytky
                -
              -
          - distributivita
      - Důkaz jinak:
        - pomocí *malé Fermatovy věty* (*p* prvočíslo, *a* nesoudělné s *p* ⇒ a^{p-1} dává zbytek 1 po dělení *p*
    - Značení (no fuj): a ⊜ b mod p ⇔ (a mod p) = (b mod p)
  - Těleso o *n* prvcích
    - o 4 prvcích
      - **T** = {0, 1, x, x+1}
      - +: jako sčítání polynomů, ale koeficienty mod 2
      - ·: jako násobení polynomů, ale mod (x^2+x+1)
        - x(x+1) = (x^2 + x + 1 + 1) mod (…) = 1 (Pozor: 1+1 = 0!)
      - Úkol: doma ověřit axiomy

- Věta (bez důkazu): Konečné těleso s n prvky existuje právě, když n je mocnina prvočísla. Pak existuje právě jedno (až na isomorfismus, tedy ‚přeznačení prvků‘)
  - Značení: GF(n): *Galoisovo těleso*
  - **Definice.** pokud existuje n takové, že 1+1+1+…+1 = 0, pak nejmenší takové n se nazývá *charakteristika tělesa*, jinak je charakteristika 0. (0 pro nekonečná tělesa)
  - **Tvrzení.** Charakteristika tělesa je buď 0 nebo prvočíslo.
    - Důkaz: Předpokládejme char. $0 \neq n = ab$, $a \neq n \neq b$
      - jedničky rozdělíme do b skupin po a jedničkách: $a \cdot b = 0$, takže a nebo b je ta charakteristika … spor!

- *#6: 06/11/13*

Vektorové prostory

- **Definice.** *Vektorový prostor* nad tělesem (**T**, +, ·) je množina **V** (jeho prvky jsou vektory) s binárními operací ⊕ (sčítání vektorů) a operací ⊙ (násobení vektoru skalárami, **T**×**V** → **V**) splňující axiomy:
  - **(sK)** $\forall u, v \in \mathbf{V}$: $u \oplus v = v \oplus u$
  - **(sA)** $\forall u, v, w \in \mathbf{V}$: $(u \oplus v) \oplus w = u \oplus (v \oplus w)$
  - **(sO)** $\exists\, ⓪ \in \mathbf{V}$: $\forall u \in \mathbf{V}$: $u \oplus ⓪ = u$ (neutrální prvek)
  - **(sI)** $\forall v \in \mathbf{V}\ \exists\, w \in \mathbf{V}$: $v \oplus w = ⓪$
  - **(nA)** $\forall a, b \in \mathbf{T}, v \in \mathbf{V}$: $(a \cdot b) \odot v = a \odot (b \odot v)$
  - **(n1)** $\forall v \in \mathbf{V}$: $1 \odot v = v$ ($1 \in \mathbf{T}$)
  - **(d1)** $\forall a, b \in \mathbf{T}, v \in \mathbf{V}$: $(a+b) \odot v = a \odot v + b \odot v$
  - **(d2)** $\forall a \in \mathbf{T}; u, v \in \mathbf{V}$: $a \odot (u \oplus v) = a \odot u + a \odot v$
- Terminologie
  - *skaláry*: z tělesa
  - *vektory*: z vektorového prostoru, nemusí to tedy být uspořádané n-tice skalárů
- Příklady
  - Příklad 1
    - **V** = {⓪} – rozmyslet
  - Příklad 2 – aritmetický vektorový prostor
    - $\mathbf{V} = \mathbf{T}^n$ – uspořádané n-tice prvků **T** (třeba $\mathbf{R}^2$)
    - ⊕ po složkách
    - ⊙ po složkách vektoru násobíme skalárem
  - Příklad 3
    - libovolné **T**, **V** = množina všech matic $m \times n$ s prvky z **T**
    - obdoba příkladu 2
  - Příklad 4.1
    - **V** = množina všech polynomů s reálnými koeficienty (vlastně nekonečné n-tice reálných koeficientů)
  - Příklad 4.2
    - **V** = množina všech spojitých fcí na **R**
  - Příklad 5 (aneb legrácky s množinami)
    - **V** = množina všech podmnožin X; **T** = **GF**(2) (nula a jedna)
    - $\forall A, B \subseteq X$: $A \oplus B = (A \cup B) - (A \cap B)$
    - $\forall A \subseteq X$: $1 \odot A = A$; $0 \odot A = \varnothing$
  - Příklad 6
    - **V** = body přímky v $\mathbf{R}^2$ procházející počátkem
- Pozorování
  1. Prvek ⓪ je určen jednoznačně
     - Důkaz: Obdobně jako u tělesa.
  2. $\forall a$: $-a$ určen jednoznačně
     - Důkaz: Obdobně jako u tělesa.
  3. $\forall u \in \mathbf{V}$: $0 \odot u = ⓪$
     - Důkaz: $0 \odot u = 0 \odot u \oplus ⓪ = 0 \odot u \oplus (u \oplus -u) = (0 \odot u \oplus 1 \odot u) \oplus -u = (u \oplus 1) \odot u \oplus -u = ⓪$
  4. $\forall v \in \mathbf{V}$: $(-1) \odot v = -v$
  5. $\forall a \in \mathbf{T}$: $a \odot ⓪ = ⓪$
  6. $a \odot u = ⓪$, právě, když $a = 0 \vee u = ⓪$
     - Důkaz sporem: $u = 1 \odot u = (a^{-1} \cdot a) \odot u = a^{-1} \odot (a \odot u) = a^{-1} \odot ⓪ = ⓪$
- **Definice.** Nechť (**V**, +, ·) je vektorový prostor nad **T**, a nechť $\mathbf{U} \subseteq \mathbf{V}$ je taková, že splňuje následující vlastnosti, pak (**U**, +, ·) nazýváme *podprostorem* **V**. (Operace jsou převzaté z **V**.)
  - i) $\forall u, v \in \mathbf{U}$, $u+v \in \mathbf{U}$ (**U** je uzavřená na +)
  - ii) $\forall a \in \mathbf{T}$, $\forall u \in \mathbf{U}$, $a \cdot u \in \mathbf{U}$ (**U** je uzavřený na ·)

- Pozn.: Z toho plyne, že **U** musí obsahovat nulový prvek
- Pozorování: Podprostory $\mathbf{R}^2$ jsou:
  - přímky procházející počátkem
  - (0,0)
  - $\mathbf{R}^2$
  - (poslední dva *triviální*)
- **Tvrzení.** Nechť $\mathbf{U}_1$, $\mathbf{U}_2$, … jsou libovolné podprostory v. p. **V** (nad **T**) pro $i \in I$. Pak průnik $\mathbf{U} = \cap_{i \in I} \mathbf{U}_i$ je též podprostorem v. p. **V**.
  - Důkaz
    - Uzavřenost na sčítání (zřejmé)
    - Uzavřenost na násobení (stejně tak)
- **Definice.** Je-li (**V**, +, ·) vektorový prostor a $X \subseteq \mathbf{V}$, pak *podprostor generovaný množinou X* je průnik všech podprostorů **V** obsahujících *X*. Značíme ho L(*X*).
- Jsou-li $v_1, \ldots, v_k \in$ v. p. **V**, pak každý výraz $v_1 a_1 + v_2 a_2 + \ldots + v_k a_k$ se nazývá lineární kombinace $v_1, \ldots, v_k$ (vždy se uvažuje konečný počet vektorů). Lineární kombinace prázdné množiny vektorů je (vektorová) 0.
- **Tvrzení.** Pro vektorový prostor **V** nad **T** a pro $X \subseteq \mathbf{V}$ platí: Podprostor $L(X) = \{\sum_{i=1}^{n} a_i x_i: n \geq 0, a_i \in \mathbf{T}, x_i \in X\}$
  - Důkaz
    - Označme $\mathbf{U} = \{\sum_{i=1}^{n} a_i x_i: n \geq 0, a_i \in \mathbf{T}, x_i \in X\}$
    - $L(X) \subseteq \mathbf{U}$
      - **U** je vektorový prostor & **U** obsahuje *X*, takže Ok
        - To je jasné, že obsahuje *X*: beru n=1, a=1 a jednotlivé prvky *X*.
        - Vektorový prostor? – Uzavřenost na sčítání a násobení
          - sčítání funguje jako sčítání polynomů (lin. kombinace + lin. kombinace = lin. kombinace)
          - násobení (přenásobím lin. kombinaci skalárním koeficientem)
    - $\mathbf{U} \subseteq L(X)$
      - Prvky **U** jsme získali sčítáním a násobením prvků z *X*, takže musí být i v *X*, tedy i v L(*X*).

- *#7: 06/11/20*

- ## Lineární rovnice (doplnění)
  - To, co jsme si říkali, platí pro libovolná tělesa (nejen **R**).

- ## Vektorové prostory (pokračování)
  - **Definice.** Nechť $\boldsymbol{A}$ je matice $m \times n$ nad tělesem **T**. Pak:
    - *Sloupcový prostor* $S(\boldsymbol{A})$ je podprostor $\mathbf{T}^m$ generovaný sloupci matice $\boldsymbol{A}$.
    - *Řádkový prostor* $\check{R}(\boldsymbol{A})$ je podprostor $\mathbf{T}^n$ generovaný (transponovanými) řádky matice $\boldsymbol{A}$.
    - *Jádro matice* $\boldsymbol{A}$ = Ker($\boldsymbol{A}$) je podprostor $\mathbf{T}^n$ tvořený všemi řešeními soustavy $\boldsymbol{Ax} = 0$.
      - Pozn.: Množina řešení je uzavřená na sčítání a násobení, je to tedy podprostor.
  - Pozorování:
    - $S(\boldsymbol{A}) = \{\boldsymbol{Ax} \mid \boldsymbol{x} \in \mathbf{T}^n\} \subseteq \mathbf{T}^m$ (česky: Sloupcový prostor matice $\boldsymbol{A}$ sestává z lineárních kombinací sloupců $\boldsymbol{A}$.)
    - $\check{R}(\boldsymbol{A}) = \{\boldsymbol{A}^T\boldsymbol{x} \mid \boldsymbol{x} \in \mathbf{T}^m\} \subseteq \mathbf{T}^n$
  - Pozorování (dle tvrzení z minula):
    - Soustava $\boldsymbol{Ax} = \boldsymbol{b}$ má řešení $\Leftrightarrow b \in S(\boldsymbol{A})$
      - $\boldsymbol{b}$ vlastně získáme lineární kombinací sloupců $\boldsymbol{A}$
  - Pozorování: Elementární řádkové úpravy nemění $\check{R}(\boldsymbol{A})$ ani Ker($\boldsymbol{A}$)
    - Důkaz:
      - řádkový prostor (je třeba ukázat tam i zpět)
        - násobení nenulovou konstantou: vynásobením inverzním prvkem ke konstantě získáme původní, zase lze nakombinovat totéž
        - přičtení řádku: obdobně co lze lineárně nakombinovat po přičtení, lze i před ním a naopak
      - EŘÚ nemění přece množinu řešení.
  - Pozorování: Sloupcový prostor se mění.
  - Pozorování: Nechť $\boldsymbol{v} \in \check{R}(\boldsymbol{A})$ a $\boldsymbol{x} \in$ Ker($\boldsymbol{A}$), pak $\boldsymbol{v}^T\boldsymbol{x} = 0$.
    - Důkaz:
      - $\boldsymbol{v} \in \check{R}(\boldsymbol{A})$ znamená $\boldsymbol{v}^T \in \boldsymbol{y}^T\boldsymbol{A}$
      - $\boldsymbol{x} \in$ Ker($\boldsymbol{A}$) znamená $\boldsymbol{Ax} = 0$
      - $\boldsymbol{v}^T\boldsymbol{x} =$
  - **Definice.** Vektory $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \in \mathbf{V}$ nad **T** jsou *lineárně nezávislé*, pokud rovnice $a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \ldots + a_n\boldsymbol{v}_n = 0$, $a_i \in \mathbf{T}$, má jediné řešení $a_1 = a_2 = \ldots = a_n = 0$
  - Poznámka:

- $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ lineárně závislé → **některé** z nich lze vyjádřit jako lineární kombinace těch ostatních (z definice plyne jak)
- (1; 0), (2; 0) a (1; 1) jsou tedy závislé, i když (2; 0) a (1; 1) jsou nezávislé, proto „**některé**"

- **Definice.** Nekonečný soubor vektorů (množina s opakováním) je *lineární nezávislý*, pokud každý konečný podsoubor je lineárně nezávislý.
- **Definice.** *Lineární obal* L(X) je podprostor generovaný množinou X, viz minulá hodina.
  - Další značení (psacím L):
    - $\mathcal{L}(X)$
  - Poznámka: Definice z minulé hodiny funguje i pro nekonečná X, bere z nich konečný počet prvků n.
- Příklady:
  - řádky I_n — nezávislé
  - nenulové řádky matice v odstupňovaném tvaru — nezávislé
  - $1, x, x^2, x^3, \ldots$ ve v. p. všech polynomů — nezávislé
- Pozorování:
  - 1. Nechť X je lineárně nezávislý a $Y \subseteq X$, pak Y je lineárně nezávislý
    - Důkaz:
      - Ex. (netriviální lin. kombinace y z Y) = 0, pak můžu stejnou lineární kombinaci udělat z prvků X – spor.
  - 2. Nechť X je lineárně závislý a $X \subseteq Y$, pak Y je lineárně závislý
    - Důkaz:
      - Obdobně jako předchozí bod.
  - 3. X je lineárně nezávislý ⇔ $\forall v \in X$: $v \notin L(X-\{v\})$
    - Důkaz sporem
- Domácí úkol
  - X je nekonečná, rozmyslet.
  - Jak funguje pro nearitmetické v. p.?
- Jak poznat, zda soubor $X \subseteq \mathbf{T}^n$ je lineárně závislý či nezávislý?
  - 1. Sestroj z X matici (vektory – řádky)
  - 2. Převedeme ji na odstupňovaný tvar.
  - 3. Nulový řádek ⇒ X je lineárně závislý, jinak nezávislý.
    - Elem. operace zase nic (tedy ani závislost, nezávislost) nepokazí.
- **Definice.** Soubor (množina s opakováním) B v. p. **V** se nazývá *systém generátorů* **V**, pokud L(B) = **V**
- **Definice.** Lineárně nezávislý systém generátorů se nazývá *báze vektorového prostoru*.
- Příklad:
  - e_i je vektor, jehož i-tý prvek je 1, osatní 0; $e_1, \ldots, e_n \in \mathbf{T}^n$ je báze $\mathbf{T}^n$
  - $1, x, x^2, x^3, \ldots$ je báze vektorového prostoru všech polynomů nad **T**
  - $\mathbf{V} = \mathbf{R}^2$, $\boldsymbol{u}, \boldsymbol{v}$ neležící na téže přímce procházející počátkem tvoří bázi $\mathbf{R}^2$

- *#8: 06/11/27*

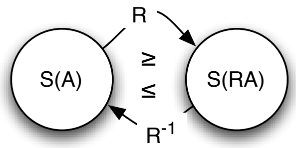
Vektorové prostory (pokračování)

- **Tvrzení.** Nechť X je taková množina, že L(X) = **V**, a $\forall Y \subset X$ (⊊!): L(Y) ≠ **V**. Pak je báze V.
  - Důkaz:
    - Dle předpokladu: X je systém generátorů **V**.
    - $\forall$u∈X: L(X-{$\boldsymbol{u}$}) ≠ **V** (z 3. pozorování z minulé hodiny) ⇒ X je lineárně nezávislé.
    - Z předchozích dvou bodů: X je báze
  - Důsledek: Z každého konečného systému generátorů lze vybrat bázi.
    - Důkaz:
      - Buď ∃y∈X: L(X-{y}) = L(X),
      - nebo ∀y∈X: L(X-{y}) ≠ L(X) ⇒ máme bázi.
- **Věta.** Každý vektorový prostor má bázi.
  - Bez důkazu:(, i když pro konečně generované vektorové prostory plyne z předchozího.
- Pozorování: Je-li $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ báze vektorového prostoru **V** nad tělesem **T**, pak pro $\forall \boldsymbol{v} \in \mathbf{V}$ ∃! n-tice $a_1, \ldots, a_n \in \mathbf{T}$ taková, že $\boldsymbol{v} = a_1\boldsymbol{v}_1 + \ldots + a_n\boldsymbol{v}_n$.
  - Důkaz: Vezměme libovolný vektor $\boldsymbol{v} \in \mathbf{V}$, $\boldsymbol{v} = a_1\boldsymbol{v}_1 + \ldots + a_n\boldsymbol{v}_n$. Uvažme $b_1, \ldots, b_n$; $b_1\boldsymbol{v}_1 + \ldots + b_n\boldsymbol{v}_n = \boldsymbol{v}$:
    - $0 = \mathbf{v} - \mathbf{v} = (a_1-b_1)\boldsymbol{v}_1 + \ldots + (a_n-b_n)\boldsymbol{v}_n$, protože $\boldsymbol{v}_i$ jsou lineárně nezávislé, $\forall i\ a_i = b_i$
- **Definice.** Nechť $X = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ je konečná báze (uspořádaná množina) vektorového prostoru **V** nad tělesem **T**. Pak pro $\boldsymbol{v} \in \mathbf{V}$, $v = \sum a_i v_i$, $a_i \in T$, nazveme n-tici $(a_1, \ldots, a_n)$ *souřadnice* **v** *vzhledem k bázi* X.
  - Pozor: Záleží na bázi (a jejím pořadí)!
- Zápis $(\text{vektor})_X$ = (souřadnice) znamená: souřadnice (vektoru) vzhledem k bázi X jsou (souřadnice)
- Pozorování: Souřadnice „obyčejných" vektorů jsou vzhledem k bázi (1, 0, 0, …), (0, 1, 0, …), (0, 0, 1, …), …

- **Lemma** o výměně: Nechť $\{v_1, \ldots, v_n\}$ je systém generátorů vektorového prostoru **V** nad **T** a $\boldsymbol{w} \in$ **V** takové, že $\boldsymbol{w} = a_1\boldsymbol{v}_1 + \ldots + a_n\boldsymbol{v}_n$. Pak pro libovolné $a_i \neq 0$ je také $\{v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_n\}$ systém generátorů **V.**
  - Důkaz: $a_i \neq 0$, existuje inverzní, vyjádříme v_i pomocí ostatních, takže $v_i = a_i^{-1} (w - a_1\boldsymbol{v}_1 - a_2\boldsymbol{v}_2 - \ldots - a_{i-1}\boldsymbol{v}_{i-1} - a_{i+1}\boldsymbol{v}_{i+1} - \ldots - a_n\boldsymbol{v}_n)$. Uvažme libovolný $\boldsymbol{u} \in$ **V**: $\boldsymbol{u} = b_1\boldsymbol{v}_1 + \ldots + b_i\boldsymbol{v}_i + \ldots + b_n\boldsymbol{v}_n$, pro vhodná $b_i \in$ **T** ⇒ máme $\boldsymbol{u}$ jako lineární kombinaci $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{w}, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_n\}$
- **Věta.** Steinitzova věta o výměně
  - **(!)** Důkaz a lemma lépe na mff.lokisw.com/SteinitzovaVetaOVymene
  - Nechť **V** je vektorový prostor nad **T** a $X = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k\}$ jsou lineárně nezávislé a $Y = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ je systém generátorů. Pak ≤ a některých k vektorů z Y lze nahradit vektory $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k$ tak, že dostaneme opět systém generátorů
  - Nápověda ke zkoušce: Neříkat „nechť $k \leq n$“, ale *pak*. Rozlišit předpoklad!
  - Důkaz:
    - X lineárně nezávislý, tedy $\forall i\ w_i \neq 0$
    - Indukce podle l:
      - 1. $l = 1$
        - Y je systém generátorů: $w_1 = \sum_{j=1}^{n} a_j v_j$ & $\exists\ a_j \neq 0$, pak podle lemmatu o výměně můžeme zaměnit v_j za w_1, a stále budeme mít systém generátorů.
      - 2. $l \geq 2$
        - $w_l = \sum_{\text{zbylá } vi} c_i v_i + \sum_{j=1}^{l-1} d_j w_j$
        - Možný problém: Po (l-1) výměnách w_l vyjádřeno pouze jako lineární kombinace $w_1, \ldots, w_{l-1}$, to ale nenastane, protože w_i jsou lineárně nezávislé
    - Důsledky
      - 1. Pokud má **V** konečnou bázi, mají všechny báze stejný počet vektorů.
        - Důkaz: Uvažme báze X a Y, X je báze, množina lineárně nezávislých vektorů, Y je báze, systém generátorů, viz co o tom říká Steinitzova věta o výměně: k≤n, ale také (když se to udělá obráceně) n≤k, takže n=k, báze stejně velké.
        - **Definice.** *Dimenze* vektorového prostoru **V** je velikost (mohutnost) nějaké jeho báze. Označujeme ji dim(V).
      - 2. Libovolnou lineárně nezávislou množinu lze v konečně generovaném vektorovém prostoru dopplnit na bázi.
      - 3. Je-li **W** podprostor konečně generovaného vektorového prostoru **V**, pak platí dim(**W**) ≤ dim(**V**).
        - Důkaz: Vezmeme bázi X vektorového prostoru **W** a bázi Y vektorového prostoru **V**, a teď Steinitz: $|X| \leq |Y|$
        - Platí-li rovnost dim(**W**) = dim(**V**), pak **W**=**V**. (Celé Y nahradíme X, …)
- Aritmetický vektorový prostor $\mathbf{T}^n$ *dimenze n* ⇒ stejná dimenze jako jsme teď definovali.

- *#9: 06/12/04*

- ## Vektorové prostory (pokračování)
  - Pozorování: Je-li n dimenze vektorového prostoru a $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$, m>n, jsou vektory z **V**, pak $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ jsou lineárně závislé.
    - Důkaz sporem: Kdyby byl lineárně nezávislé…
  - Pozorování: Je-li n dimenze vektorového prostoru **V** a $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ je systém generátorů **V**, pak $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ jsou lineárně nezávislé.
    - Důkaz: Byli-li by závislé (?? –> vynech –> báze menší než n).
  - **Tvrzení.** Nechť **V** je vektorový prostor generovaný vektory $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathrm{T}^n$ a nechť A je matice (m×n), jejíž řádky jsou $\boldsymbol{v}_1^T, \ldots, \boldsymbol{v}_m^T$. Pak dim(**V**) je hodnost matice A.
    - Důkaz V = Ř(A) = Ř(U) (U je matice v odstupňovaném tvaru získaná elementrárními úpravami). Nenulové řádky U tvoří bázi V, jsou tedy lineárně nezávislé. Systém generátorů to je také (nenulové musí generovat celý prostor). Hodnost matice je tedy rovna dimenzi **V**.
  - **Věta.** Nechť A je matice m×n nad tělesem **T**. Pak dim(Ř(A)) = dim(S(A)).
    - Důkaz:
      - **Tvrzení.** Násobení regulární maticí zleva (tedy i elementární řádková úprava) nemění dimenzi sloupcového prostoru.
        - Důkaz: R·A = A'; R: m×m, A, A': m×n
          - Sloupce A: $u_1, \ldots u_n$
          - Sloupce A': $u_1', \ldots u_n'$
          - Báze S(A): $v_1, \ldots v_k$, tedy dim(S(A)) = k
          - Chceme ukázat, že $R \cdot v_1, \ldots, R \cdot v_k$ je báze S(A') = S(R·A).
            - Systém generátorů?
              - $w \in S(A')$, chceme vyjádřit jako lineární kombinaci $R \cdot v_1, \ldots, R \cdot v_k$.
              - $R \cdot u_i = u_i'$

        - $w = \sum_{i=1}^{n} a_i u_i' = \sum_{i=1}^{n} a_i(Ru_i) = R\cdot \sum_{i=1}^{n} a_i u_i$ (kde $\sum_{i=1}^{n} a_i u_i \in S(A)) = R\sum_{j=1}^{k} b_j v_j = \sum_{j=1}^{k} b_j(Rv_j)$ je lin. kombinace $R\cdot v_1 + \dots + R\cdot v_k$, tedy je systém generátorů.
      - Lineárně nezávislé?
        - Sporem: Předpokládejme netriviální lineární kombinaci $a_1\cdot R\cdot v_1, \dots, a_k\cdot R\cdot v_k = 0 \in \mathbf{T}^m$
        - $R(a_1\cdot v_1, \dots, a_k\cdot v_k) = 0$, R regulární, tedy $(a_1\cdot v_1, \dots, a_k\cdot v_k)$ musí být 0, protože v_i jsou lineárně nezávislé (báze), tak všechna $a_i = 0$, i=1, …, k (triviální kombinace.)
        -
    - Oba vektorové prostory mají tedy stejně velké báze, tedy stejně velké dimenze: dim(S(A) = dim(S(RA))
    - Poznámka, z první části víme dim(S(A)) ≥ dim(S(RA)). Pak využijeme regularity matice R: A' = RA ⇒ A = R^{-1}A', opět násobíme regulární maticí, pak dim(S(R^{-1}A') ≤ dim(S(A'), R^{-1}A' = A, A = RA. Tradá.
    - 

    - Opakování:
      - Nechť U je A v odst. tvaru.
      - U = RA, pro R regulární.
      - Víme
        - dim(R(A)) = rank(A) (hodnost A) = # nenulových řádků v odst tvaru (dle tvrzení před touto větou)
        - dim(S(A) = dim(S(U) = # nenulových řádků v odst. tvaru (stačí si to představit, skutečně to tak je)
    - Tím je věta dokázána.
- Příklad:
  - matice A = (10/00), R = (01/10)
  - RA = (00/10), S(A) ≠ S(RA) mění sloupcový prostor (nemění jeho dimenzi a řádkový) – rozlišovat!
- Důsledek 1: Pro matici A, m×n, platí rank(A) = rank(A^T) (z toho jak si odpovídají řádkové a sloupcové prostory).
- Pozorování:
  - dim(Ker(A) (jádro je prostor řešení homogenní soustavy) = # volných rádků matice v odstupňovaného tvaru = # volných proměnných (bázové proměné odpovídají pivotům, ostatní jsou volné)
  - Obecné řešení Ax = 0 lze zapsat $x = t_1 z_1 + \dots + t_k z_k$, kde k je počet volných proměnných (parametrů), takže dimenze ≥ # volných
  - Dále je třeba nahlédnout, že vektory jsou lineárně nezávislé: vždy x bazická = lineární kombinace nebázických (takhle jsme zapisovali řešení), z toho to plyne (prý se nějak prodlužují nezávislé vektory, a jsou pak stále nezávislé – prý promyslet před spaním).
- Důsledek 2: Pro matici A, m×n, platí: dim(Ker(A)) + rank(A) = n = # sloupců.
  - Důkaz:
    - Pro matici v odstupňovaném tvaru m×n využijeme pozorování.
    - Pro matici, která není v odstupňovaném tvaru: Převedeme ji do něj pomocí regulární matice R: U = R·A. Elementární řádkové úpravy nemění prostor řešení, tím spíš dim(Ker(A)) = dim(Ker(U)) = n - rank(U) = n - rank(A).
- Důsledek 3: rank(AB) ≤ min(rank(A), rank(B)), je-li definováno.
  - Mé zdůvodnění (tohle mě napadlo, když se mi nechtělo číst následující odpudivě vypadající důkaz, dost nejspíš je to ale to samé, ono se toho moc vymyslet nedá…):
    - Řádky AB jsou lineární kombinací řádků z B, tedy: rank(AB) = dim(Ř(AB)) ≤ dim(Ř(B)) ≤ rank(B)
    - Sloupce AB jsou lineární kombinací sloupců z A, tedy: rank(AB) = dim(S(AB)) ≤ dim(S(A)) ≤ rank(A)
  - Důkaz: $A_{m\times n} \cdot B_{n\times k} = AB_{m\times k}$
    - S(AB) = {ABu | u ∈ $\mathbf{T}^k$} = {Av|v ∈ S(B)} ⊆ {Av|v∈$\mathbf{T}^n$} = S(A)
    - Proto dim(S(AB)) ≤ dim(S(A)). Přitom vždy dim(S(AB) = dim(Ř(AB)) = rank(AB).
    - Ř(AB) = {uAB | u ∈ T^m} = {vB | v ∈ Ř(A)}⊆ (vB | v∈ T^n} = Ř(B)
- Důsledek 4: Pro regulární matici R a matici A platí, že rank(RA) = rank(A), je-li součin definován.

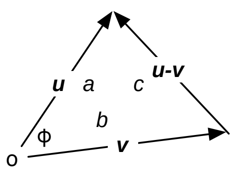
- *#10: 06/12/11*

- **Lineární Zobrazení**
  - Na úvod: Mějme matici A: *m×n* a vektorové prostory $\mathbf{T}^n$, $\mathbf{T}^m$, násobení vektoru maticí je pak lineární zobrazení $\mathbf{T}^n \to \mathbf{T}^m$,
    - A(u+u') = Au + A'
  - **Definice.** *Zobrazení f*: **U**→**V**, kde **U** a **V** jsou vektorové prostory nad tělesem **T**, je *lineární*, pokud
    - ∀***u***,***v*** ∈ **U**: *f*(***u***+***v***) = *f*(***u***) + *f*(***v***) (Prý aditivita, ale na přednášce jsme tomu nijak neříkali.)
    - ∀***u*** ∈ **U**,∀*c* ∈ **T**:*f*(*c**u***) = *c f*(***u***) (Prý homogenita.)
  - Příklady:

- 1. Libovolný vektorový prostor V, f:V→V, ∀u∈V: f(u) = 0 je lineární.
- 2. Libovolný vektorový prostor V, f:V→V, ∀u∈V: f(u) = u je lineární
- 3. V = T^n, n≥13, f((u_1, …, u_n)) = u_7; f: T^n→T^1 je *projekce na sedmou osu*, také lineární zobrazení
- 4. V=$\mathbf{R}^2$
  - Takhle nějak by to vypadalo, kdybych to hezky vysázel, ale na to nemám čas:($f(\binom{x}{y}) = \binom{x+2}{y+3}$
  - f(x,y) = f($(x,y)^T$) = $(x+2, y+3)^T$ – není splněna první podmínka, není lineární zobrazení
  - f(x,y) = $(\alpha x,\alpha y)^T$ = ((α, 0)(0, α))(x,y) – lze zapsat maticovým násobením, podmínky platí, je lineární
  - f(x,y) = $(-x,y)^T$ = ((-1, 0)(0, 1))(x,y) – dtto
  - f(x,y) = $(-x,-y)^T$ = ((-1, 0)(0, -1))(x,y) – dtto
  - f(x,y) = $(ax+by,cx+by)^T$ = ((a, b)(c, d))(x,y) – dtto
    - Poslední příklad je obecné lineární zobrazení (v $\mathbf{R}^2$). Žádná jiná už nejsou. (Třeba posunutí (x+2, y+3) není.)
      - Rozmyslet: Mohu *jen* lineárně kombinovat (násobit maticí).
- 5. U = {$\sum_{i=0}^n a_i x^i$ | n≥0, a_i ∈ **R**, i=0, …, n}
  - f(p(x)) = p'(x), ∀p(x)∈U, f:U→U (p: mnohočlen)
  - g(p(x)) = p(x)(x-7), ∀p(x)∈U, f:U→U
- 6. U_n = {$\sum_{i=0}^n a_i x^i$ | n≥0, a_i ∈ **R**, i=0, …, n}
  - f(p(x)) = p'(x), ∀p(x)∈U_n, f:U_n→U_{n-1}
  - g(p(x)) = p(x)(x-7), ∀p(x)∈U_n, f:U_n→U_{n+1}
- Pozorování: f:U→V, f(U) = {f(v)|v ∈ U}, f(U) je podprostor V (f je lineární zobrazení)
- Pozorování:
  - 1. dim(f(U)) ≤ dim(U)
    - Důkaz:
      - Vezměme bázi U: u_1, …., u_n
      - Uvažme f(u_1), …., f(u_k), chceme dokázat, že je systém generátorů
      - Lib. v ∈ f(U) je obrazem nějakého u ∈ U, tj. v=f(u), f(u) = f($\sum_{i=0}^n a_i u_i$) = $\sum_{i=0}^n a_i f(u_i)$
  - 2. Jsou-li f: U→V a g: V→W lineární zobrazení, potom i složení h = g○f je lineární zobrazení U→W
    - Poznámka: g○f znamená, že se nejdříve aplikuje f, pak g
    - Důkaz:
      - h(u+v) = g(f(u+v)) = g(f(u)+f(v)) = g(f(u)) + g(f(v))
- **Věta.** Nechť **V** a **W** jsou vektorové prostory nad T a v_1, …, v_n je báze **V**. Pak pro každou uspořádanou n-tici w_1, …, w_n ∈ W, existuje právě jedno lineární zobrazení f:V→W takové, že f(v_i) = w_i, i=1,…,n. (česky asi takhle: Lineární zobrazení je jednoznačně určené obrazem báze **V**.)
  - Důkaz:
    - Libovolné x ∈ V lze jednoznačně zapsat x = $\sum_{i=1}^n a_i v_i$
    - f(x) = f($\sum_{i=1}^n a_i v_i$) = $\sum_{i=1}^n a_i f(v_i)$ = $\sum_{i=1}^n a_i w_i$
- Příklad: V = $\mathbf{R}^2$, uvažme rotaci kolem počátku o úhel α (proti směru ručiček)
  - Zobrazení bázových vektorů:
    - f(1, 0) = (cosα, sinα)
    - f(0, 1) = (-sinα, cosα)
  - Víme, že se dá vyjádřit jako maticové násobení:
    - $f(\binom{x}{y}) = \begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}\cdot\binom{x}{y}$
  - h=g○f
  - h(x,y) = g(f(x,y)) = … = (cos b -sin b / sin b cos b) (cos b -sin b / sin b cos b) (x y) =
  - = (cos a cos b - sin a sin b -sin a cos b - cos a sin b / cos a sin b + sin a cos b - sin a sin b + cos a cos b)(x / y) = (cos (a+b) -sin (a+b) / sin (a+b) cos (a+b)) (x / y)
  - Takže mimochodem máme odvozeny vzorce pro součty argumentů sinu a cosinu
  - Nechť v_1, …, v_n jsou vrcholy pravidelného n-úhelníka se středem v počátku.
    - Úkoly:
      - s = $\sum_{i=1}^n v_i$ = ? (součet vrcholů, že by nula/počátek?)
      - Vezměme rotaci o tau = 2π/n. Pak tau(v_i) = $v_{i \bmod n + 1}$. Pak s = $\sum_{i=1}^n v_i$ = $\sum_{i=1}^n$ tau(v_i) = tau($\sum_{i=1}^n$) ⇒ s je nulový vektor (pže s ním rotace nic neudělá)
- **Definice.** Nechť **V** a **W** jsou vektorové prostory nad tělesem **T** a nechť ($\boldsymbol{v}_1$, …, $\boldsymbol{v}_n$) = *X* je báze **V** a ($\boldsymbol{w}_1$, …, $\boldsymbol{w}_m$) = *Y* je báze **W**, a *f*: **V**→**W** je lineární zobrazení. Označme $[f(\boldsymbol{v}_i)]_Y$ souřadnice $f(\boldsymbol{v}_i)$ vůči bázi *Y*. Pak matici ($[f(\boldsymbol{v}_1)]_Y$, …, $[f(\boldsymbol{v}_n)]_Y$] nazýváme *maticí zobrazení* f *vůči bázím* X *a* Y. Označujeme ji $[f]_{XY}$

- *#11: 06/12/18*

- **Lineární zobrazení**
  - Dneska prý nahlédneme, že lineární zobrazení se dá vždy vyjádřit násobením matic:
    - (Že to platí naopak už víme, plyne to z pravidel pro počítání s maticemi.)
    - Mějme $\boldsymbol{u} \in \mathbf{V}$, $\boldsymbol{u} = \sum_{i=1}^{n} a_i x_i$; $[\boldsymbol{u}]_X = (a_1, \ldots, a_n)^T$
    - $[\, f(\boldsymbol{u})\,]_X = ?$
    - $f(\boldsymbol{u}) = f(\, \sum_{i=1}^{n} a_i \boldsymbol{x}_i\,) = \sum_{i=1}^{n} a_i\, f(\boldsymbol{x}_i)$
    - $[\, f(\boldsymbol{u})\,]_X = [f]_{XY} \cdot [\boldsymbol{u}]_X$; kde $[f]_{XY}$ je matice zobrazení vůči bázím X a Y.
  - **Tvrzení.** Pro vektorové prostory **V** s bází $X = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ a **W** s bází Y a lineární zobrazení f: $\mathbf{V} \to \mathbf{W}$ platí: $\forall \boldsymbol{u} \in V$: $[\, f(\boldsymbol{u})\,]_X = [f]_{XY} \cdot [\boldsymbol{u}]_X$.
  - Důsledek: Každé lineární zobrazení f: $\mathbf{R}^n \to \mathbf{R}^m$ má tvar f(u) = A u, kde u $\in \mathbf{R}^n$ a A je matice m×n, kde i-tý sloupec je roven obrazu bázového vektoru e_i = (0 0 1 (na i-té složce) 0 0)^T.
    - $u \in \mathbf{R}^n$, $K_n = \{e_1, \ldots, e_n\}$ (kanonická báze)
    - „$u = [u]_{Kn}$“, takže:
    - $[f(u)]_{Kn} = [f]_{KnKm}\, [u]_{Kn} = [f]_{KnKm}\, u$ ($[f]_{KnKm}$ je matice A z předchozího tvrzení)
  - Zvláštní případ (*identita*): id: $\mathbf{V} \to \mathbf{V}$: $\forall \boldsymbol{v} \in \mathbf{V}$: $id(\boldsymbol{v}) = \boldsymbol{v}$
  - **Definice.** Matice identického zobrazení vzhledem k bázím X a Y se nazývají *matice přechodu* od X k Y.
    - $[\boldsymbol{u}]_Y = [id]_{XY} \cdot [\boldsymbol{u}]_X$
  - Příklad: $\mathbf{V} = \mathbf{R}^2$, K_2 = { (1;0), (0;1) }, B = { (1;0), (1;1) }
    - $[id]_{K2\,B}$ = (1 -1 / 0 1)
  - **Tvrzení.** Nechť U, V, W jsou vektorové prostory nad T s konečnými bázemi X, Y a Z, nechť f: U→V a g:V→W jsou lineární zobrazení. Pak $[g \circ f]_{XZ} = [g]_{YZ}[f]_{XY}$.
    - Důkaz:
      - Vezmi libovolné u ∈ U:
      - $[f(u)]_Y = [f]_{XY}[u]_X$
      - $[g(f(u))]_z = [g]_{YZ}[f(u)]_Y = [g]_{YZ}[f]_{XY}\, [u]_X$
  - Jak vyjádřit, že následující jsou vlastně stejné vektorové prostory?
    - V_1: $a_0 + a_1 x + a_2 x^2 + a_3 x^3$
    - $V_2 = T^4$
  - **Definice:** Nechť V a W jsou vektorové prostory nad T. Pak lineární zobrazení f: V→W, které je prosté a na, nazýváme *isomorfismem* vektorových prostorů V a W.
  - Pozorování: *f* je bijekce, takže existuje inverzní zobrazení f^{-1}, a f^{-1} je lineární zobrazení
    - Důkaz: ∀z, z' ∈ W:
    - $f^{-1}(z+z') = f^{-1}(f(x) + f(x')) = f^{-1}(f(x + x')) = x + x' = f^{-1}(z) + f^{-1}(z')$
    - Promyslet $f^{-1}(c \cdot z)$
  - **Věta.** Nechť V a W jsou vektorové prostory nad T s konečnými bázemi X a Y. Pak zobrazení f: V→W je isomorfismus právě tehdy, když je matice $[f]_{XY}$ regulární. Pak též platí: $([f]_{XY})^{-1} = [f^{-1}]_{YX}$
    - Důkaz
      - ⇐:
        - *f* je prosté:
          - Uvažme zobrazení g: $\mathbf{W} \to \mathbf{V}$ popsané maticí $[g]_{YX} = (\, [f]_{XY}\,)^{-1}$.
          - Pak $[g \circ f]_{XX}$ = (dle předchozího tvrzení) $[g]_{YX} \cdot [f]_{XY} = I = [id]_{XX}$
        - *f* je na:
          - Podobně: $[f \circ g]_{YY} = [f]_{XY} \cdot [g]_{YX} = I = [id]_{YY}$
        - Tedy *f* je isomorfismus.
      - ⇒:
        - Abychom ukázali, že je regulární, hledáme inversní matici.
        - *f* isomorfismus ⇒ $\exists f^{-1}$: W→V, lineární zobrazení, platí:
          - $[f]_{XY} \cdot [f^{-1}]_{YX} = [f \circ f^{-1}]_{YY} = [id]_{YY} = I_{|Y|}$ (to ale neznamená, že máme inverzní matici, mohou to být nějaké obdélníkové potvory)
          - $[f^{-1}]_{YX} \cdot [f]_{XY} = [f^{-1} \circ f]_{XX} = [id]_{XX} = I_{|X|}$
          - Víme: rank(AB) ≤ min(rank(A), rank(B))
          - $[f]_{XY}$: |Y| × |X| (a $[f^{-1}]_{YX}$: |X| × |Y|) hodnost matice je tedy aspoň |Y| a taky aspoň |X| (protože takové jsou hodnosti těch jednotkových matic $I_{|Y|}$, resp. $I_{|X|}$), tedy máme rank($[f]_{XY}$) ≥max(|Y|, |X|) ⇒ |Y| = |X| (viz předchozí řádek)
          - Tradá.

- **Ke zkoušce**
  - Máme mít udělený zápočet.
  - Zkouška písemná.
  - Jeden teoretický příklad: důkaz nebo úkaz;)
- *#12: 07/01/08*
  Přednášející: Fiala.
- **Prostory se skalárním součinem**
  - Tělesa, se kterými budeme pracovat:
    - **C**: komplexní čísla
      - algebraicky uzavřené těleso
        - komplexně sdružené číslo $\bar{x}$
        - $|x| = \sqrt{(a^2+b^2)}$
    - **R**: reálná čísla
      - uspořádané těleso ≤ (reflexivní, antisymetrická, transitivní)
      - ∀a,b: buď a ≤ b nebo b ≤ a
      - ∀a,b: a, b ≥ 0 ⇒ a+b ≥ 0, ab ≥ 0
      - ∀a,b: a ≤ b ⇒ -a+b ≥ 0
    - $\mathbf{R}^+_0$
      - odmocnina √a
  - **Definice.** Nechť **V** je vektorový prostor nad **C**. Zobrazení, které dvojici vektorů ***u***, ***v*** ∈ **V** přiřadí komplexní číslo 〈***u***|***v***〉, se nazývá skalární součin, pokud splňuje následující axiomy:
    - (N) ∀***u*** ∈ **V**: 〈***u***|***u***〉 = 0 ⇔ u = 0
    - (L1) ∀***u***, ***v*** ∈ **V**, ∀ a∈**C**: 〈a***u***|***v***〉 =a ·〈***u***|***v***〉
    - (L2) ∀***u***, ***v***, ***w*** ∈ **V**: 〈***u***+***v***|***w***〉 = 〈***u***|***v***〉 + 〈***v***|***w***〉
    - (KS) ∀***u***, ***v*** ∈ **V**: 〈***v***|***u***〉 = sdružené(〈***u***|***v***〉)
      To jako, že celý součin je „nadtržený“, nechce se mi to sázet.
    - (P) ∀***u*** ∈ **V**: 〈***u***|***u***〉 ≥ 0
  - Formálně je skalární součin zobrazení
    - 〈·|·〉: **V**×**V**→**C**
  - Skalární součin pro prostor nad **R** se definuje stejně až na axiom KS:
    - (KS) ∀***u***, ***v*** ∈ **V**: 〈***u***|***v***〉 = 〈***v***|***u***〉
  - Příklady: Standardní skalární součin na aritmetických vektorových prostorech:
    - pro $\mathbf{V}=\mathbf{R}^n$: $\langle \boldsymbol{u}|\boldsymbol{v}\rangle = \sum_{i=1}^{n} \boldsymbol{u}_i \cdot \boldsymbol{v}_i$
    - pro $\mathbf{V}=\mathbf{C}^n$: $\langle \boldsymbol{u}|\boldsymbol{v}\rangle = \sum_{i=1}^{n} \boldsymbol{u}_i \cdot \overline{\boldsymbol{v}}_i$
      Pozor, véčko je nadtržené!
    - Skalární součin na $\mathbf{R}^n$ definovaný promocí regulární matice A řádu n:
      - $\langle \boldsymbol{u}|\boldsymbol{v}\rangle = u^T A^T A v$ Při $V=R^2$, A=(1 2 / 0 1) $\langle \boldsymbol{u}|\boldsymbol{v}\rangle = u^T(1\ 2\ /\ 2\ 5)v$ = u1v1 + 2u1v2 + 2u2v1 + 5v1v2
    - Skalární součin na prostoru spojitých integrovatelných funkcí na intervalu (a, b)
      - 〈*f(x)*|*g(x)*〉 = ∫ f(x)g(x)dx
  - **Definice.** Nechť **V** je prostor se skalárním součinem. Potom *norma určená skalárním součinem* je zobrazení ||·||: **V**→**R** dané předpisem ||***u***|| = √〈***u***|***u***〉 (〈***u***|***u***〉 je nezáporné z definice)
  - Geometrická interpretace:
    - ||***u***|| délka vektoru
    - ||***u***-***v***|| vzdálenost vektorů ***u*** a ***v***
    - 〈***u***|***v***〉 udává pozici, „úhel“ mezi vektory
      - Pozorování: Pro skalární součin a jím určenou normu na $\mathbf{R}^n$ platí:
        - 〈***u***|***v***〉 = ||***u***||·||***v***||·cosφ, kde φ je úhel sevřený vektory ***u*** a ***v***
        - Důkaz:
          - 

          - Z cosinové věty: c^2 = a2 + b2 - 2ab cosφ
          - a = ||u||, b=||v||, c=||u-v||
          - 〈***u***-***v***|***u***-***v***〉 = 〈***u***|***u***〉 + 〈***v***|***v***〉 -2||u|| ||v|| cosφ
          - 〈***u***-***v***|***u***-***v***〉 = 〈***u***|***u***〉 - 〈***u***|***v***〉 - 〈***v***|***u***〉 + 〈***v***|***v***〉

- **Věta.** (Cauchy-Schwarzova nerovnost) Nechť V je vektorový prostor nad **C** se skalárním součinem a příslušnou normou. Potom platí:
  - $|\langle \boldsymbol{u}|\boldsymbol{v}\rangle| \leq \|\boldsymbol{u}\|\cdot\|\boldsymbol{v}\|$
    Pozor, vlevo je komplexní číslo, proto je v absolutní hodnotě, abychom mohli porovnávat.
- Důsledky:
  - Nerovnost mezi aritmetickým a kvadratickým průměrem: $\forall u \in R^n$ $1/n \sum_{i=1}^n u_i \leq \sqrt{(1/n \sum_{i=1}^n u_i^2)}$
    - Důkaz: zvolme $v=(1, \ldots, 1)^T$
      - $\sum_{i=1}^n u_i = \langle \boldsymbol{u}|\boldsymbol{v}\rangle \leq \|u\| \|v\| = \sqrt{(\sum_{i=1}^n u_i^2)}\sqrt{n}$
  - Důsledek: Norma určená součinem splňuje trojúhelníkovou nerovnost $\|u+v\| \leq \|u\| + \|v\|$
    - Důkaz: $\|u+v\| = \sqrt{(\langle \boldsymbol{u+v}|\boldsymbol{v+v}\rangle)} = \sqrt{(\langle \boldsymbol{u}|\boldsymbol{u}\rangle + \langle \boldsymbol{u}|\boldsymbol{v}\rangle + \langle \boldsymbol{v}|\boldsymbol{u}\rangle + \langle \boldsymbol{v}|\boldsymbol{v}\rangle)} \leq$
    - $\leq \sqrt{(\langle \boldsymbol{u}|\boldsymbol{u}\rangle + 2|\langle \boldsymbol{u}|\boldsymbol{v}\rangle| + \langle \boldsymbol{v}|\boldsymbol{v}\rangle)} \leq$ (Cauchy-Schwarz)
    - $\leq \sqrt{(\langle \boldsymbol{u}|\boldsymbol{u}\rangle + 2\|u\| \|v\| + \langle \boldsymbol{v}|\boldsymbol{v}\rangle)} = \sqrt{(\|u\|^2 + 2\|u\| \|v\| + \|v\|^2)} = \|u\|+\|v\|$
  - Obecně je norma zobrazení $\|\cdot\|$: **V**→**R**, které splňuje následující podmínky:
    - $\|\boldsymbol{u}\| \geq 0$
    - $\|\boldsymbol{u}\| = 0 \Leftrightarrow u = 0$
    - $\|\boldsymbol{u}+\boldsymbol{v}\| \leq \|\boldsymbol{u}\| + \|\boldsymbol{v}\|$
      Trojúhelníková nerovnost.
    - $\|a\cdot\boldsymbol{u}\| = |a|\cdot\|\boldsymbol{u}\|$
    - Příklad obecně definované normy:
      - L_p norma na $\mathbf{R}^n$ (No, řekl bych, že to má být spíš L^p, ale pak si nedokážu vysvětlit, proč jsem si napsal tohle…)
        - $||u||_p = \sqrt[p]{\sum_{i=1}^{n} |u_i|^p}$
      - L_2 norma, norma určená std. skalárním součinem
      - L_1, L_∞ – to jsem nějak nepobral, ale při přednášce se to vyskytlo
      - další normy, která splňují výše uvedené axiomy, ale nejsou odvozeny od vektorových prostorů se skalárním součinem
- Ortogonalita
  - **Definice.** Vektory u a v z prostoru se skalárním součinem nazveme *kolmé*, pokud platí $\langle \boldsymbol{u}|\boldsymbol{v}\rangle = 0$. Značíme $\boldsymbol{u} \perp \boldsymbol{v}$.
  - Pozorování: Každý systém vzájemně kolmých vektorů je lineárně nezávislý.
    - Důkaz: Sporem, předpokládám lineárně závislé: $u_0 = \sum_{i=1}^n a_i u_i$
      - $0 \neq \langle \boldsymbol{u}_0|\boldsymbol{u}_0\rangle = \langle \sum_{i=1}^n a_i \boldsymbol{u}_i|\boldsymbol{u}_0\rangle = \sum_{i=1}^n a_i \langle \boldsymbol{u}_i|\boldsymbol{u}_0\rangle = \sum_{i=1}^n a_i 0 = 0$
- **Definice.** Nechť je prostor se skalárním součinem a *Z* je jeho báze taková, že $\forall \boldsymbol{v} \in Z$: $\|\boldsymbol{v}\| = 1$ a navíc $\forall \boldsymbol{v},\boldsymbol{v}' \in Z$: $\boldsymbol{v} \neq \boldsymbol{v}' \Rightarrow \boldsymbol{v} \perp \boldsymbol{v}'$. Potom *Z* se nazývá *ortonormální báze* prostoru **V**.
- Poznámka: Když ortonormální bázi R^n narovnám do matice A (tzv. ortogonální matice). $A^T \cdot A = I_n$
- Příklad ortonormální báze
  - v R^3: $(-2/3, 2/3, 1/3)^T$, $(2/3, 1/3, 2/3)^T$, $(1/3, 2/3, -2/3)^T$
- **Tvrzení.** Nechť $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ je ortonormální báze prostoru **V**. Potom pro $\forall \boldsymbol{u} \in \mathbf{V}$ platí, že $\boldsymbol{u} = \langle \boldsymbol{u}|\boldsymbol{v}_1\rangle \boldsymbol{v}_1 + \ldots + \langle \boldsymbol{u}|\boldsymbol{v}_n\rangle \boldsymbol{v}_n$.
  - Koeficienty $\langle \boldsymbol{u}|\boldsymbol{v}_i\rangle$ se nazývají Fourierovy koeficienty vektoru u vůči bázi $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$