

1. Analýza

1.1 Posloupnosti a řady čísel a funkcí

1.1.1 Limity posloupností a součty řad

Definice Posloupností reálných čísel rozumíme jakékoliv zobrazení z množiny \mathbb{N} do množiny \mathbb{R} .

Definice Buď $M = \{a_n, n \in \mathbb{N}\}$. Pak posloupnost $\{a_n\}_{n \in \mathbb{N}}$ je (shora, zdola) omezená, pokud množina M je (shora, zdola) omezená v \mathbb{R} .

Definice Řekneme, že posloupnost $\{a_n\}_{n \in \mathbb{N}}$ je neklesající, jestliže $a_n \leq a_{n+1}, \forall n \in \mathbb{N}$.

Analogicky klesající, nerostoucí, rostoucí, monotónní, ryze monotónní.

Definice Řekneme, že $A \in \mathbb{R}$ je vlastní limita posloupnosti $\{a_n\}_{n \in \mathbb{N}}$, jestliže

$$\forall \epsilon > 0 \exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}, n \geq n_0 : |a_n - A| < \epsilon.$$

Definice Řekneme, že posloupnost $\{a_n\}_{n \in \mathbb{N}}$ má limitu ∞ , pokud

$$\forall K \in \mathbb{R} \exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}, n \geq n_0 : a_n > K.$$

Analogicky limita $-\infty$, tyto limity jsou nevlastní.

Věta (ekvivalentní podmínka limity) Nechť $K > 0$. Platí $\lim_{n \rightarrow \infty} a_n = A$ právě tehdy, když

$$\forall \epsilon > 0 \exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}, n \geq n_0 : |a_n - A| < K\epsilon.$$

Definice Řekneme, že posloupnost $\{a_n\}_{n \in \mathbb{N}}$ je konvergentní, pokud $\lim_{n \rightarrow \infty} a_n = A \in \mathbb{R}$

Věta (jednoznačnost limity) Každá posloupnost má nejvýše jednu limitu. Zde je vhodné znát důkaz.

Věta Každá konvergentní posloupnost je omezená.

Definice Nechť $\{a_n\}_{n \in \mathbb{N}}$ je posloupnost, pak řekneme, že posloupnost $\{b_k\}_{k \in \mathbb{N}}$ je vybraná z $\{a_n\}_{n \in \mathbb{N}}$, pokud existuje rostoucí posloupnost celých čísel $\{n_k\}_{k \in \mathbb{N}}$ taková, že $b_k = a_{n_k}, \forall k \in \mathbb{N}$.

Věta (o limitě vybrané posloupnosti) Pokud posloupnost $\{a_n\}_{n \in \mathbb{N}}$ má limitu $A \in \mathbb{R}^*$, pak každá vybraná posloupnost z posloupnosti $\{a_n\}_{n \in \mathbb{N}}$ má také limitu A .

Věta (o aritmetice limit) Nechť $\{a_n\}_{n \in \mathbb{N}}$ a $\{b_n\}_{n \in \mathbb{N}}$ jsou posloupnosti a platí $\lim_{n \rightarrow \infty} a_n = A$ a $\lim_{n \rightarrow \infty} b_n = B$. Pak

- i. $\lim_{n \rightarrow \infty} a_n \pm b_n = A \pm B$,
- ii. $\lim_{n \rightarrow \infty} a_n b_n = AB$,
- iii. Pokud $B \neq 0$, pak $\lim_{n \rightarrow \infty} \frac{a_n}{b_n} = \frac{A}{B}$.

Zde je vhodné znát důkaz.

Věta (o součinu omezené a nulové) Nechť $a_n \rightarrow 0$ a nechť $\{b_n\}_{n \in \mathbb{N}}$ je omezená posloupnost. Pak $a_n b_n \rightarrow 0$.

Zde je vhodné znát důkaz.

Věta (vztah uspořádání a limity) Nechť $\{a_n\}_{n \in \mathbb{N}}$, resp. $\{b_n\}_{n \in \mathbb{N}}$ jsou posloupnosti s limitami A , resp. B , a nechť platí

$$\exists n_0 \in \mathbb{N} \quad \forall n \in \mathbb{N}, \quad n \geq n_0 : a_n \leq b_n.$$

Pak $A \leq B$.

Věta (o dvou policajtech) Nechť

$$\exists n_0 \in \mathbb{N} \quad \forall n \in \mathbb{N}, \quad n \geq n_0 : a_n \leq c_n \leq b_n$$

a nechť $\lim_{n \rightarrow \infty} a_n = A = \lim_{n \rightarrow \infty} b_n$. Pak $\lim_{n \rightarrow \infty} c_n = A$.

Plus jednostranné verze této věty.

Zde je vhodné znát důkaz.

Věta (o monotónní posloupnosti) Každá monotónní posloupnost má limitu.

Definice Nechť $\{a_n\}_{n \in \mathbb{N}}$ je posloupnost, definujeme

$$\alpha_k = \inf_{n \geq k} \{a_n\}, \quad \beta_k = \sup_{n \geq k} \{a_n\}.$$

Pak α_k je neklesající posloupnost, β_k je nerostoucí posloupnost a definujeme

$$\liminf_{n \rightarrow \infty} a_n = \lim_{k \rightarrow \infty} \alpha_k, \quad \limsup_{n \rightarrow \infty} a_n = \lim_{k \rightarrow \infty} \beta_k.$$

Věta Nechť $\{a_n\}_{n \in \mathbb{N}}$ je posloupnost. Pak

$$\lim_{n \rightarrow \infty} a_n = A \Leftrightarrow \liminf_{n \rightarrow \infty} a_n = A \wedge \limsup_{n \rightarrow \infty} a_n = A.$$

Definice Řekneme, že $H \in \mathbb{R}^*$ je hromadný bod posloupnosti $\{a_n\}_{n \in \mathbb{N}}$, pokud existuje vybraná posloupnost $\{b_k\}_{k \in \mathbb{N}}$ taková, že $b_k \rightarrow H$.

Věta (Bolzano - Weierstrass) Z každé omezené posloupnosti lze vybrat konvergentní.

Věta (Bolzano - Cauchy) Posloupnost $\{a_n\}_{n \in \mathbb{N}}$ má vlastní limitu \Leftrightarrow splňuje podmínu

$$(BC) \quad \forall \epsilon > 0 \exists n_0 \in \mathbb{N} \forall n, m \in \mathbb{N}, n, m \geq n_0 : |a_n - a_m| < \epsilon.$$

Zde je vhodné znát důkaz.

Definice Nechť $\{a_n\}_{n \in \mathbb{N}}$ je posloupnost reálných čísel. Částečným součtem řady $\sum_{n=0}^{\infty} a_n$ definujeme součet $s_n = \sum_{i=0}^n a_i$. Součtem řady $\sum_{n=0}^{\infty} a_n$ nazveme limitu posloupnosti $\{s_n\}_{n \in \mathbb{N}}$.

Definice Řekneme, že řada $\sum_{n=0}^{\infty} a_n$ konverguje (diverguje) pokud konverguje (diverguje) posloupnost $\{s_n\}_{n \in \mathbb{N}}$.

Věta (nutná podmínka konvergence) Platí

$$\sum_{n=0}^{\infty} a_n \text{ konverguje} \Rightarrow \lim_{n \rightarrow \infty} a_n = 0.$$

1.1.2 Kritéria absolutní a neabsolutní konvergence číselných řad

Řady s nezápornými členy

Věta (srovnávací kritérium) Nechť $\exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}, n \geq n_0 : a_n \leq b_n$, pak

- i. $\sum_{n=0}^{\infty} a_n$ diverguje $\Rightarrow \sum_{n=0}^{\infty} b_n$ diverguje,
- ii. $\sum_{n=0}^{\infty} b_n$ konverguje $\Rightarrow \sum_{n=0}^{\infty} a_n$ konverguje.

Zde je vhodné znát důkaz.

Věta (limitní srovnávací kritérium) Nechť $\exists \lim_{n \rightarrow \infty} \frac{a_n}{b_n} = K \in \langle 0, \infty \rangle$, pak

- i. $K \in (0, \infty) \Rightarrow \left(\sum_{n=0}^{\infty} a_n \text{ konverguje} \Leftrightarrow \sum_{n=0}^{\infty} b_n \text{ konverguje} \right)$,
- ii. $K = 0 \Rightarrow \left(\sum_{n=0}^{\infty} b_n \text{ konverguje} \Rightarrow \sum_{n=0}^{\infty} a_n \text{ konverguje} \right)$,
- iii. $K = \infty \Rightarrow \left(\sum_{n=0}^{\infty} a_n \text{ konverguje} \Rightarrow \sum_{n=0}^{\infty} b_n \text{ konverguje} \right)$.

Věta (D'Alambertovo podílové kritérium)

- Pokud

$$\exists q \in (0, 1) \exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}, n \geq n_0 : \frac{a_{n+1}}{a_n} < q,$$

pak $\sum_{n=0}^{\infty} a_n$ konverguje. Speciálně, je-li $\lim_{n \rightarrow \infty} \frac{a_{n+1}}{a_n} < 1$ pak $\sum_{n=0}^{\infty} a_n$ konverguje.

- Pokud

$$\exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}, n \geq n_0 : \frac{a_{n+1}}{a_n} \geq 1,$$

pak $\sum_{n=0}^{\infty} a_n$ diverguje. Speciálně, je-li $\lim_{n \rightarrow \infty} \frac{a_{n+1}}{a_n} > 1$ pak $\sum_{n=0}^{\infty} a_n$ diverguje.

Zde je vhodné znát důkaz.

Věta (Cauchyho odmocninové kritérium)

- Pokud

$$\exists q \in (0,1) \exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}, n \geq n_0 : \sqrt[n]{a_n} < q,$$

pak $\sum_{n=0}^{\infty} a_n$ konverguje. Speciálně, je-li $\lim_{n \rightarrow \infty} \sqrt[n]{a_n} < 1$ pak $\sum_{n=0}^{\infty} a_n$ konverguje.

- Pokud $\sqrt[n]{a_n} \geq 1$ pro nekonečně mnoho $n \in \mathbb{N}$, pak $\sum_{n=0}^{\infty} a_n$ diverguje. Speciálně je-li $\lim_{n \rightarrow \infty} \sqrt[n]{a_n} > 1$, pak $\sum_{n=0}^{\infty} a_n$ diverguje.

Zde je vhodné znát důkaz.

Věta (Raabeovo kritérium)

- Nechť $\lim_{n \rightarrow \infty} n \left(\frac{a_n}{a_{n+1}} - 1 \right) > 1$ pak $\sum_{n=0}^{\infty} a_n$ konverguje.
- Nechť $\lim_{n \rightarrow \infty} n \left(\frac{a_n}{a_{n+1}} - 1 \right) < 1$ pak $\sum_{n=0}^{\infty} a_n$ diverguje.

Věta (kondenzační kritérium) Nechť $\exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}, n \geq n_0 : a_{n+1} \leq a_n$, pak

$$\sum_{n=0}^{\infty} a_n \text{ konverguje} \Leftrightarrow \sum_{n=0}^{\infty} 2^n a_{2^n} \text{ konverguje.}$$

Obecné řady

Definice Řekneme, že řada $\sum_{n=0}^{\infty} a_n$ konverguje *absolutně*, jestliže konverguje řada $\sum_{n=0}^{\infty} |a_n|$. Pokud řada $\sum_{n=0}^{\infty} a_n$ konverguje, ale ne absolutně, řekneme, že konverguje *neabsolutně*.

Věta (Bolzano - Cauchy pro řady) Platí

$$\sum_{n=0}^{\infty} a_n \text{ konverguje} \Leftrightarrow \forall \epsilon > 0 \exists n_0 \in \mathbb{N} \forall n, k \in \mathbb{N}, n \geq n_0 : \left| \sum_{i=n+1}^{n+k} a_i \right| < \epsilon.$$

Zde je vhodné znát důkaz.

Věta (vztah konvergence a absolutní konvergence) Pokud řada $\sum_{n=0}^{\infty} a_n$ konverguje absolutně, pak konverguje.

Věta (Leibnizovo kritérium) Nechť $\{a_n\}_{n \in \mathbb{N}}$ je nerostoucí posloupnost. Pak

$$\sum_{n=0}^{\infty} (-1)^{n+1} a_n \text{ konverguje} \Leftrightarrow \lim_{n \rightarrow \infty} a_n = 0.$$

Definice Řekneme, že řada $\sum_{n=0}^{\infty} a_n$ má omezené částečné součty, pokud platí

$$\exists K > 0 \forall m \in \mathbb{N} : \left| \sum_{i=0}^m a_i \right| < K.$$

Věta (Ábel - Dirichlet). Nechť $\{a_n\}_{n \in \mathbb{N}}$ je posloupnost a $\{b_n\}_{n \in \mathbb{N}}$ je nerostoucí nezáporná posloupnost. Jestliže platí alespoň jedna z podmínek

(A) $\sum_{n=0}^{\infty} a_n$ konverguje,

(D) $\sum_{n=0}^{\infty} a_n$ má omezené částečné součty a $\lim_{n \rightarrow \infty} b_n = 0$,

pak $\sum_{n=0}^{\infty} a_n b_n$ konverguje.

1.1.3 Stejnoměrná konvergence posloupností a řad funkcí

Definice Nechť $f, f_n, n \in \mathbb{N}$ jsou funkce definované na množině $M \subseteq \mathbb{R}$ (nebo na metrickém prostoru (M, ρ)) s hodnotami v \mathbb{R} . Řekneme, že posloupnost $\{f_n\}_{n=1}^{\infty}$ konverguje bodově k f na M , jestliže $\lim_{n \rightarrow \infty} f_n(x) = f(x), \forall x \in M$, tj. pokud

$$\forall x \in M \forall \epsilon > 0 \exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}, n \geq n_0 : |f_n(x) - f(x)| < \epsilon.$$

Tento vztah značíme $f_n \rightarrow f$.

Řekneme, že posloupnost $\{f_n\}_{n=1}^{\infty}$ konverguje k f na M stejnoměrně, pokud

$$\forall \epsilon > 0 \exists n_0 \in \mathbb{N} \forall x \in M \forall n \in \mathbb{N}, n \geq n_0 : |f_n(x) - f(x)| < \epsilon,$$

značíme $f_n \rightrightarrows f$.

Řekneme, že posloupnost $\{f_n\}_{n=1}^{\infty}$ konverguje k f na M lokálně stejnoměrně, pokud $\forall x \in M \exists r > 0 : f_n \rightrightarrows f$ na $\mathcal{U}(x, r)$.

Věta (charakterizace stejnoměrné konvergence) Nechť $f, f_n, n \in \mathbb{N}$ jsou funkce definované na množině $M \subseteq \mathbb{R}$ s hodnotami v \mathbb{R} . Platí $f_n \rightrightarrows f$ právě tehdy, když

$$\lim_{n \rightarrow \infty} \sup_{x \in M} |f_n(x) - f(x)| = 0.$$

Definice Řekneme, že posloupnost $\{f_n\}_{n=1}^{\infty}$ je cauchyovská, pokud

$$\forall x \in M \forall \epsilon > 0 \exists n_0 \in \mathbb{N} \forall n, m \in \mathbb{N}, n, m \geq n_0 : |f_n(x) - f_m(x)| < \epsilon.$$

Řekneme, že posloupnost $\{f_n\}_{n=1}^{\infty}$ je stejnoměrně cauchyovská, pokud

$$\forall \epsilon > 0 \exists n_0 \in \mathbb{N} \forall x \in M \forall n, m \in \mathbb{N}, n, m \geq n_0 : |f_n(x) - f_m(x)| < \epsilon.$$

Definice Řekneme, že množina M (metrický prostor (M,ρ)) je *úplná*, pokud každá cauchyovská posloupnost v ní je konvergentní.

Věta (vztah konvergence a cauchyovskosti) Nechť funkce $f, f_n, n \in \mathbb{N}$ zobrazují do úplného prostoru. Pak je posloupnost $\{f_n\}_{n=1}^{\infty}$ (stejnoměrně) konvergentní právě tehdy, když je (stejnoměrně) cauchyovská.

Věta (o stejnoměrné konvergenci a spojitosti) Nechť jsou funkce $f_n, n \in \mathbb{N}$ spojité a nechť $f_n \rightrightarrows f$. Pak f je také spojité.

Věta (Moore-Osgoodova) Nechť jsou funkce $f, f_n, n \in \mathbb{N}$ definované na M , $x_0 \in M$ a nechť platí

- i. $f_n \rightrightarrows f$ na M ,
- ii. $\forall n \in \mathbb{N} \exists \lim_{x \rightarrow x_0} f_n(x) =: \alpha_n \in \mathbb{R}$.

Potom existuje $\lim_{n \rightarrow \infty} \alpha_n$ a platí $\lim_{n \rightarrow \infty} \alpha_n = \lim_{x \rightarrow x_0} f(x)$.

Věta (záměna limity a derivace) Nechť jsou funkce $f_n, n \in \mathbb{N}$ definované na intervalu (a,b) , $a < b$ a nechť platí

- i. f_n mají vlastní derivaci na $(a,b) \forall n \in \mathbb{N}$,
- ii. $\exists c \in (a,b) : \{f_n(c)\}_{n=1}^{\infty}$ je konvergentní,
- iii. $\{f'_n\}_{n=1}^{\infty}$ je stejnoměrně konvergentní na (a,b) .

Pak existuje funkce f taková, že posloupnost $\{f_n\}_{n=1}^{\infty}$ konverguje lokálně stejnoměrně k f , f má vlastní derivaci na (a,b) a posloupnost $\{f'_n\}_{n=1}^{\infty}$ konverguje lokálně stejnoměrně k f' na (a,b) .

Věta (limita a primitivní funkce) Nechť funkce $f_n, n \in \mathbb{N}$ mají na intervalu (a,b) , $a < b$ primitivní funkce $F_n, n \in \mathbb{N}$ a posloupnost $\{f_n\}_{n=1}^{\infty}$ konverguje stejnoměrně k f na (a,b) . Pak posloupnost $\{F_n\}_{n=1}^{\infty}$ konverguje lokálně stejnoměrně k F , kde F je primitivní funkce k f .

Věta (záměna limity a integrálu) Nechť jsou funkce $f_n, n \in \mathbb{N}$ newtonovsky integrovatelné na intervalu $\langle a,b \rangle$ a nechť $f_n \rightrightarrows f$ na $\langle a,b \rangle$. Pak funkce f je také newtonovsky integrovatelná na $\langle a,b \rangle$ a platí

$$\int_a^b f(x) dx = \lim_{n \rightarrow \infty} \int_a^b f_n(x) dx.$$

Definice Řekneme, že množina K (metrický prostor (K,ρ)) je *kompaktní*, pokud z každé posloupnosti v něm lze vybrat konvergentní podposloupnost.

Věta (Diniho) Nechť je množina K (metrický prostor (K, ρ)) kompaktní a nechť funkce $f, f_n, n \in \mathbb{N}$ jsou spojité, zobrazující z K do \mathbb{R} , a $f_n \rightarrow f$. Pokud $\forall x \in K$ je $\{f_n(x)\}_{n=1}^{\infty}$ monotónní, pak $f_n \rightrightarrows f$ na K .

Definice Nechť jsou funkce $f_n, n \in \mathbb{N}$ definované na množině M . Řekneme, že řada funkcí $\sum_{n=1}^{\infty} f_n$ je (*stejnoměrně, lokálně stejnoměrně*) konvergentní, pokud je (stejnoměrně, lokálně stejnoměrně) konvergentní posloupnost jejích částečných součtů.

Definice Řekneme, že řada $\sum_{n=1}^{\infty} g_n$ je *majorantní* řadě $\sum_{n=1}^{\infty} f_n$ na M , pokud $|f_n(x)| \leq g_n(x), \forall x \in M, \forall n \in \mathbb{N}$.

Věta (srovnávací kritérium pro stejnoměrnou konvergenci) Nechť je řada $\sum_{n=1}^{\infty} g_n$ majorantní řadě $\sum_{n=1}^{\infty} f_n$ na M a nechť $\sum_{n=1}^{\infty} g_n$ je stejnoměrně konvergentní na M . Pak i řady $\sum_{n=1}^{\infty} f_n$ a $\sum_{n=1}^{\infty} |f_n|$ jsou stejnoměrně konvergentní na M .

Věta (Weierstrassovo kritérium) Nechť platí $|f_n(x)| \leq a_n \forall n \in \mathbb{N}, \forall x \in M$ a nechť $\sum_{n=1}^{\infty} a_n < \infty$. Pak jsou řady $\sum_{n=1}^{\infty} f_n$ a $\sum_{n=1}^{\infty} |f_n|$ stejnoměrně konvergentní na M .

Věta (záměna sumy a derivace) Nechť mají funkce $f_n, n \in \mathbb{N}$ vlastní derivace na intervalu (a, b) , $a < b$ a nechť

- i. $\exists x_0 \in (a, b) : \sum_{n=1}^{\infty} f_n(x_0)$ konverguje,
- ii. $\sum_{n=1}^{\infty} f'_n$ konverguje lokálně stejnoměrně na (a, b) ,

pak i řada $\sum_{n=1}^{\infty} f_n$ konverguje lokálně stejnoměrně $\forall x \in (a, b)$ platí

$$\left(\sum_{n=1}^{\infty} f_n(x) \right)' = \sum_{n=1}^{\infty} f'_n(x).$$

Věta (záměna sumy a integrálu) Nechť platí $\sum_{n=1}^{\infty} f_n \rightrightarrows f$ na (a, b) , $a < b$ a nechť jsou funkce $f_n, n \in \mathbb{N}$ newtonovsky integrovatelné na (a, b) . Pak i funkce f je newtonovsky integrovatelná na (a, b) a platí

$$\int_a^b f(x) dx = \sum_{n=1}^{\infty} \int_a^b f_n(x) dx.$$

Definice Řekneme, že posloupnost funkcí $f_n, n \in \mathbb{N}$ je *stejnoměrně omezená* na $M \subseteq \mathbb{R}$, pokud $\exists K > 0 \forall n \in \mathbb{N}, \forall x \in M : |f_n(x)| < K$.

Věta (Abel-Dirichlet) Nechť funkce $f_n, g_n, n \in \mathbb{N}$ zobrazují z M do \mathbb{R} a nechť platí alespoň jedna z podmínek

- (A) i. $\sum_{n=1}^{\infty} f_n \rightrightarrows$ na M ,
- ii. $\{g_n\}_{n=1}^{\infty}$ je stejnoměrně omezená na M ,

iii. $\forall x \in M$ je $\{g_n(x)\}_{n=1}^{\infty}$ monotónní.

- (D) i. $\{\sum_{i=1}^n f_i\}_{n=1}^{\infty}$ je stejnoměrně omezená,
ii. $g_n \rightharpoonup 0$,
iii. $\forall x \in M$ je $\{g_n(x)\}_{n=1}^{\infty}$ monotónní.

Pak $\sum_{n=1}^{\infty} g_n f_n$ je stejnoměrně konvergentní na M .

1.1.4 Mocninné řady

Definice Nechť $\{a_n\}_{n=0}^{\infty}$ je posloupnost reálných čísel a nechť $x_0 \in \mathbb{R}$. Pak řadu funkcí $\sum_{n=0}^{\infty} a_n(x - x_0)^n$ nazýváme *mocninnou řadou* s *koefficienty* a_n a *středem* x_0 .

Věta (o existenci poloměru konvergence) Nechť $\sum_{n=0}^{\infty} a_n(x - x_0)^n$ je mocninná řada. Pak existuje právě jedno číslo $R \in \langle 0, \infty \rangle$ takové, že $\forall x : |x - x_0| < R$ platí, že řada $\sum_{n=0}^{\infty} a_n(x - x_0)^n$ konverguje absolutně a pro $\forall x : |x - x_0| > R$ tato řada diverguje. Pro toto R platí vztah

$$R = \frac{1}{\limsup_{n \rightarrow \infty} \sqrt[n]{|a_n|}}.$$

Zde je vhodné znát myšlenku důkazu.

Definice Číslo R z předchozí věty nazýváme *poloměr konvergence* mocninné řady $\sum_{n=0}^{\infty} a_n(x - x_0)^n$.

Věta (derivace mocninné řady) Označme $f(x) := \sum_{n=0}^{\infty} a_n(x - x_0)^n$ s poloměrem konvergence R . Pak řada $\sum_{n=1}^{\infty} n a_n(x - x_0)^{n-1}$ má stejný poloměr konvergence R a v něm platí $f'(x) = \sum_{n=1}^{\infty} n a_n(x - x_0)^{n-1}$.

Věta (o integrování mocninné řady) Nechť má mocninná řada $\sum_{n=0}^{\infty} a_n(x - x_0)^n$ poloměr konvergence $R \in (0, \infty)$, pak pro $|x - x_0| < R$ platí

$$\int \left(\sum_{n=0}^{\infty} a_n(x - x_0)^n \right) dx = \sum_{n=0}^{\infty} \frac{a_n}{n+1} (x - x_0)^{n+1} + C.$$

Věta (Abelova) Nechť má mocninná řada $\sum_{n=0}^{\infty} a_n(x - x_0)^n$ poloměr konvergence $R \in (0, \infty)$ a nechť suma $\sum_{n=0}^{\infty} a_n R^n$ konverguje. Pak řada $\sum_{n=0}^{\infty} a_n(x - x_0)^n$ konverguje stejnoměrně pro $x \in \langle x_0, x_0 + R \rangle$ a platí

$$\lim_{r \rightarrow R_-} \sum_{n=0}^{\infty} a_n r^n = \sum_{n=0}^{\infty} a_n R^n.$$

Zde je vhodné znát důkaz (alespoň první části věty).

1.2 Diferenciální počet funkcí jedné reálné proměnné

1.2.1 Spojitost a derivace funkcí jedné reálné proměnné

Definice Funkce jedné reálné proměnné je funkce $f : M \rightarrow \mathbb{R}$, kde $M \subseteq \mathbb{R}$.

Definice Nechť $a \in \mathbb{R}$ a nechť funkce f je definována na nějakém redukovaném okolí bodu a . Řekneme, že $A \in \mathbb{R}^*$ je *limita* funkce f v bodě a , pokud

$$\forall \epsilon > 0 \exists \delta > 0 : x \in \mathcal{U}(a, \delta) \Rightarrow f(x) \in \mathcal{U}(A, \epsilon),$$

kde \mathcal{U} značí okolí bodu. Tento vztah značíme $\lim_{x \rightarrow a} f(x) = A$.

Definice Nechť $a \in \mathbb{R}$ a funkce f je definovaná v bodě a . Řekneme, že funkce f je *spojitá* v bodě a , pokud $\lim_{x \rightarrow a} f(x) = f(a)$.

Definice pro limitu a spojitost zprava a zleva analogicky.

Věta (Heineho) Nechť $f : M \rightarrow \mathbb{R}$, $M \subseteq \mathbb{R}$, $a \in \mathbb{R}^*$ a nechť f je definována na nějakém redukovaném okolí bodu a . Pak platí

$$\lim_{x \rightarrow a} f(x) = A \Leftrightarrow \forall \text{ posloupnost } \{x_n\}_{n=1}^{\infty}, x_n \rightarrow a, x_n \neq a : f(x_n) \rightarrow A.$$

Zde je vhodné znát myšlenku důkazu.

Věta (Heineho věta pro spojitost) Nechť $f : M \rightarrow \mathbb{R}$, $M \subseteq \mathbb{R}$, $a \in \mathbb{R}$ a navíc f definována v nějakém okolí bodu a . Pak f je spojité v bodě a právě tehdy, když pro každou posloupnost $\{x_n\}_{n=1}^{\infty}$, $x_n \rightarrow a$ platí $f(x_n) \rightarrow f(a)$.

Věta (jednoznačnost limity) Funkce má v každém bodě nejvýše jednu limitu.

Věta (o aritmetice limit) Nechť $a \in \mathbb{R}^*$ a funkce f a g jsou definované na nějakém redukovaném okolí bodu a a nechť $\lim_{x \rightarrow a} f(x) = A \in \mathbb{R}^*$, $\lim_{x \rightarrow a} g(x) = B \in \mathbb{R}^*$. Pak platí

$$\text{i. } \lim_{x \rightarrow a} (f(x) + g(x)) = A + B,$$

$$\text{ii. } \lim_{x \rightarrow a} f(x)g(x) = AB,$$

$$\text{iii. } \lim_{x \rightarrow a} \frac{f(x)}{g(x)} = \frac{A}{B}, \text{ pokud } B \neq 0,$$

pokud jsou výrazy na pravých stranách definované.

Zde je vhodné znát myšlenku důkazu.

Důsledek Pokud funkce f a g jsou spojité v bodě a , pak i $f \pm g$, fg a f/g (pokud $g(a) \neq 0$) jsou spojité v bodě a .

Definice Řekneme, že funkce je *spojitá na intervalu I* , pokud je spojité ve všech vnitřních bodech intervalu I a spojité zprava/zleva v jeho krajních bodech.

Definice Nechť $f : M \rightarrow \mathbb{R}$, $M \subseteq \mathbb{R}$ a nechť $a \in M$, řekneme že f nabývá v bodě a

- svého *maxima (minima)* na M , jestliže $f(x) \leq f(a) \forall x \in M$ (\geq),
- svého *ostrého maxima (minima)* na M , jestliže $f(x) < f(a) \forall x \in M$ ($>$),
- svého *lokálního maxima (minima)*, pokud $\exists U(a) : f(x) \leq f(a) \forall x \in U(a)$ (\geq),
- svého *ostrého lokálního maxima (minima)*, pokud $\exists U(a) : f(x) < f(a) \forall x \in U(a)$ ($>$).

Věta (spojitost a extrémy) $a, b \in \mathbb{R}$, $a < b$, f spojitá na $\langle a, b \rangle$. Pak funkce f nabývá na intervalu $\langle a, b \rangle$ maxima a minima.

Věta (spojitost a omezenost) Nechť $a, b \in \mathbb{R}$, $a < b$, a f spojitá na $\langle a, b \rangle$. Pak je tam omezená.

Definice Derivací funkce f v bodě x_0 rozumíme limitu

$$\lim_{x \rightarrow x_0} \frac{f(x) - f(x_0)}{x - x_0},$$

pokud tato limita existuje. Značíme $f'(x_0)$.

Alternativně také $\lim_{h \rightarrow 0} \frac{f(x_0 + h) - f(x_0)}{h}$.

Definice Derivaci funkce f v bodě a nazveme *vlastní*, pokud $f'(a) \in \mathbb{R}$ a *ne-vlastní*, pokud $f'(a) = \pm\infty$.

Věta (derivace a spojitost) Má-li funkce f v bodě vlastní derivaci, pak je v něm spojitá.

Věta (aritmetika derivací) Platí

- $(f + g)'(x_0) = f'(x_0) + g'(x_0)$,
- $(fg)'(x_0) = f'(x_0)g(x_0) + f(x_0)g'(x_0)$,
- $\left(\frac{f}{g}\right)'(x_0) = \frac{f'(x_0)g(x_0) - f(x_0)g'(x_0)}{(g(x_0))^2}$, pokud $g(x_0) \neq 0$.

Zde je vhodné znát myšlenku důkazu.

Věta (derivace složené funkce) Nechť má funkce f derivaci v bodě y_0 , nechť je funkce g spojitá v bodě x_0 a má v něm derivaci a nechť $y_0 = g(x_0)$. Pak $(f \circ g)'(x_0) = f'(g(x_0))g'(x_0)$.

Věta (derivace inverzní funkce) Nechť je funkce f spojitá a ryze monotónní na (a, b) , $x_0 \in (a, b)$ a $y_0 = f(x_0)$. Pokud

1. $f'(x_0) \in \mathbb{R}^* \setminus \{0\}$ pak $(f^{-1})'(y_0) = \frac{1}{f'(f^{-1}(y_0))}$,
2. $f'(x_0) = 0$ a f je rostoucí (klesající) v (a, b) , pak $(f^{-1})'(y_0) = \infty (-\infty)$.

1.2.2 Hlubší věty o spojitéch funkčích

Věta (o nabývání mezihodnot) Nechť je funkce f spojitá na intervalu $\langle a,b \rangle$, $-\infty < a < b < \infty$. Nechť $f(a) < f(b)$ a $y \in (f(a), f(b))$. Pak $\exists x \in (a,b) : f(x) = y$. Analogicky pro $f(a) > f(b)$.

Zde je vhodné znát myšlenku důkazu. Na to se mě přímo ptali, ale stačilo jim "sporem přes definici suprema".

Věta (spojitý obraz intervalu) Nechť I je interval a f je spojitá na I . Pak $f(I)$ je také interval.

Věta (o spojitosti inverzní funkce) Nechť f je spojitá rostoucí (klesající) na intervalu I . Pak f^{-1} je spojitá rostoucí (klesající) na $f(I)$.

1.2.3 Věty o střední hodnotě a jejich důsledky

Věta (Rolleova) Nechť $a, b \in \mathbb{R}$, $a < b$ a nechť

- i. $f \in \mathcal{C}(\langle a,b \rangle)$,
- ii. $\exists f'(x) \forall x \in (a,b)$,
- iii. $f(a) = f(b) = 0$.

Pak $\exists \xi \in (a,b) : f'(\xi) = 0$. Zde je vhodné znát důkaz.

Věta (Langrangeova věta o střední hodnotě, Lagrangeova věta o přírůstku funkce) Nechť $a, b \in \mathbb{R}$, $a < b$ a

- i. $f \in \mathcal{C}(\langle a,b \rangle)$,
- ii. $\exists f'(x) \forall x \in (a,b)$.

Pak existuje $\xi \in (a,b)$ takové, že

$$f'(\xi) = \frac{f(b) - f(a)}{b - a}.$$

Zde je vhodné znát důkaz.

Věta (Cauchyova) Nechť $a, b \in \mathbb{R}$, $a < b$, $f, g \in \mathcal{C}(\langle a,b \rangle)$, f a g mají derivaci na (a,b) a v každém bodě je alespoň jedna z nich konečná (tj.

$\min\{f'(x), g'(x)\} \in \mathbb{R}$, $\forall x \in (a,b)$), a nechť $g'(x) \neq 0 \forall x \in (a,b)$. Pak existuje $\xi \in (a,b)$ takové, že

$$\frac{f'(\xi)}{g'(\xi)} = \frac{f(b) - f(a)}{g(b) - g(a)}.$$

Věta (L'Hospital) Nechť $x_0 \in \mathbb{R}^*$, nechť f a g mají vlastní derivace v nějakém redukovaném okolí bodu x_0 a platí alespoň jedna z podmínek

- i. $\lim_{x \rightarrow x_0} f(x) = 0 = \lim_{x \rightarrow x_0} g(x)$,

ii. $\lim_{x \rightarrow x_0} |g(x)| = \infty$.

Pak

$$\lim_{x \rightarrow x_0} \frac{f(x)}{g(x)} = \lim_{x \rightarrow x_0} \frac{f'(x)}{g'(x)},$$

pokud limita na pravé straně existuje.

L'Hospitalova věta je důsledkem Cauchyovy věty o střední hodnoty.

Věta (o derivaci zprava) Nechť je f spojitá zprava v bodě a a nechť $\lim_{x \rightarrow a^+} f'(x) = A \in \mathbb{R}^*$. Pak $f'_+(a) = A$.

Věta o derivaci zprava je důsledkem Lagrangeovy věty o střední hodnotě.

1.2.4 Vztahy monotonie a znaménka derivace

Věta Nechť I je interval, $I \subset \mathbb{R}$, $f \in \mathcal{C}(I)$ a f má na I vlastní derivaci.

- i. Pokud $f'(x) \geq 0 \forall x \in \text{Int}(I)$, pak f je neklesající v I .
- ii. Pokud $f'(x) > 0 \forall x \in \text{Int}(I)$, pak f je rostoucí v I .
- iii. Pokud $f'(x) \leq 0 \forall x \in \text{Int}(I)$, pak f je nerostoucí v I .
- iv. Pokud $f'(x) < 0 \forall x \in \text{Int}(I)$, pak f je klesající v I .

Zde je vhodné znát důkaz.

Důsledek Nechť I je interval a $f'(x) = 0 \forall x \in I$. Pak f je konstantní na I .

1.2.5 Konvexita

Definice Nechť $I \subset \mathbb{R}$ je interval, $f : I \rightarrow \mathbb{R}$ je

- *konvexní* v I , pokud $\forall x, y \in I, \forall \lambda \in (0,1)$ platí $f(\lambda x + (1 - \lambda)y) \leq \lambda f(x) + (1 - \lambda)f(y)$,
- *ryze konvexní* v I , pokud $\forall x, y \in I, \forall \lambda \in (0,1), x \neq y$ platí $f(\lambda x + (1 - \lambda)y) < \lambda f(x) + (1 - \lambda)f(y)$,
- *(ryze) konkávní*, pokud $-f$ je (ryze) konvexní.

Věta (konvexita a jednostranné derivace) Nechť f je konvexní na intervalu $I \subset \mathbb{R}$. Pak existují konečné jednostranné derivace $f'_-(x_0), f'_+(x_0) \forall x_0 \in \text{Int}(I)$ a navíc $f'_-(x_0) \leq f'_+(x_0)$.

Věta (vztah konvexity a spojitosti) Nechť f je konvexní na $(a, b) \subset \mathbb{R}$. Pak $f \in \mathcal{C}((a, b))$.

Otevřenosť intervalu je důležitá. Jedná se o důsledek předchozí věty.

Věta (vztah druhé derivace a konvexity) Nechť f je spojitá na intervalu $I \subset \mathbb{R}$ a nechť má na I spojitu první derivaci. Jestliže $f''(x) \geq 0 \forall x \in I$ pak f

je konvexní.

Definice Nechť f má vlastní derivaci v bodě $x_0 \in \mathbb{R}$. Řekneme, že x_0 je *inflexním bodem* funkce f pokud existuje $\delta > 0$ takové, že platí alespoň jedna z podmínek

1. $\forall x \in P_-(x_0, \delta) : f(x) < f(x_0) + f'(x_0)(x - x_0) \wedge \forall x \in P_+(x_0, \delta) : f(x) > f(x_0) + f'(x_0)(x - x_0),$
2. $\forall x \in P_-(x_0, \delta) : f(x) > f(x_0) + f'(x_0)(x - x_0) \wedge \forall x \in P_+(x_0, \delta) : f(x) < f(x_0) + f'(x_0)(x - x_0).$

Věta (nutná podmínka pro inflexi) Nechť $x_0 \in \mathbb{R}$ a $f''(x_0) \neq 0$. Pak x_0 není inflexním bodem f .

Zde je vhodné znát důkaz.

Věta (postačující podmínka pro inflexi) Nechť f má spojitou první derivaci v $(a, b) \subset \mathbb{R}$, nechť $x_0 \in (a, b)$ a $\exists \delta > 0$ takové, že platí alespoň jedna z podmínek

1. $\forall x \in P_-(x_0, \delta) : f''(x) > 0 \wedge \forall x \in P_+(x_0, \delta) : f''(x_0) < 0,$
2. $\forall x \in P_-(x_0, \delta) : f''(x) < 0 \wedge \forall x \in P_+(x_0, \delta) : f''(x_0) > 0.$

Pak x_0 je inflexní bod.

Zde je vhodné znát důkaz.

1.2.6 Taylorův polynom, Taylorovy řady

Definice Nechť $f, g : \mathbb{R} \rightarrow \mathbb{R}$, $x_0 \in \mathbb{R}^*$. Řekneme, že $f(x) = o(g(x))$ pro $x \rightarrow x_0$, jestliže

$$\lim_{x \rightarrow x_0} \frac{f(x)}{g(x)} = 0.$$

Definice Nechť $f : \mathbb{R} \rightarrow \mathbb{R}$, $x_0 \in \mathbb{R}$. Nechť existuje vlastní $f^{(n)}(x_0) \in \mathbb{R}$, $n \in \mathbb{N}$. Potom polynom

$$T_{n,x_0}^f(x) = \sum_{k=0}^n \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k, \quad \forall x \in \mathbb{R}$$

je *Taylorův polynom funkce f řádu n v bodě a*.

Věta (Peanova) Nechť $n \in \mathbb{N}$, $f : \mathbb{R} \rightarrow \mathbb{R}$, $x_0 \in \mathbb{R}$, $f^{(n)}(x_0) \in \mathbb{R}$. Pak existuje právě jeden polynom P_n stupně nejvýše n takový, že

$$\lim_{x \rightarrow x_0} \frac{f(x) - P_n(x)}{(x - x_0)^n} = 0,$$

tj. $f(x) - P_n(x) = o((x - x_0)^n)$ a to právě polynom $P_n = T_{n,x_0}^f$.

Definice Nechť jsou splněny podmínky definice Taylorova polynomu.

Pak $R_{n+1,x_0}^f(x) := f(x) - T_{n,x_0}^f(x)$ nazýváme *zbytkem* po n -tém členu Taylorova polynomu.

Věta (Taylorova věta o zbytku) Nechť $f, \varphi : \mathbb{R} \rightarrow \mathbb{R}$, $x_0, x \in \mathbb{R}$, $x_0 \neq x$ a nechť J je uzavřený interval s krajními body x a x_0 . Nechť platí

1. $f^{(n+1)}(t) \in \mathbb{R}$, $\forall t \in J$ a
2. $\varphi \in C(J)$, $0 \neq \varphi'(t) \in \mathbb{R}$, $\forall t \in \text{Int}(J)$.

Pak existuje $\xi \in \text{Int}(J)$ takové, že

$$R_{n+1}(x) = \frac{(x - \xi)^n}{n!} \frac{\varphi(x) - \varphi(x_0)}{\varphi'(x_0)} f^{(n+1)}(\xi).$$

Speciálně volbou $\varphi(t) = t$ dostáváme *Cauchyův tvar zbytku*

$$R_{n+1}(x) = \frac{(x - \xi)^n}{n!} (x - x_0) f^{(n+1)}(\xi),$$

a volbou $\varphi(t) = (x - t)^{n+1}$ dostáváme *Lagrangeův tvar zbytku*

$$R_{n+1}(x) = \frac{(x - x_0)^{n+1}}{(n+1)!} f^{(n+1)}(\xi).$$

Zde je vhodné znát důkaz.

Definice Nechť $f : \mathbb{R} \rightarrow \mathbb{R}$, $x_0 \in \mathbb{R}$, nechť f má v x_0 konečné derivace všech řádů. Pak řadu

$$T_{x_0}^f(x) = \sum_{k=0}^{\infty} \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k$$

nazýváme *Taylorovou řadou* funkce f v bodě x_0 . Pokud $x_0 = 0$ pak jde o *MacLaurinovu řadu*.

Věta Platí $T_{x_0}^f = f$ právě tehdy, když $\lim_{n \rightarrow \infty} R_{n+1} = 0$.

Zde je vhodné znát příklady některých Taylorových (MacLaurinových) řad, například pro e^x , $\sin x$, $\cos x$, ...

1.3 Integrální počet funkcí jedné reálné proměnné

1.3.1 Primitivní funkce, určitý integrál

Definice Nechť $a, b \in \mathbb{R}$, $a < b$ a $F, f : (a, b) \rightarrow \mathbb{R}$. Řekneme, že F je *primitivní funkcí* f na (a, b) , jestliže $F'(x) = f(x)$ $\forall x \in (a, b)$.

Věta (primitivní funkce a spojitost) Každá primitivní funkce je spojitá.

Věta (postačující podmínka pro existenci primitivní funkce) Nechť $a, b \in \mathbb{R}$, $a < b$ a $f \in \mathcal{C}((a,b))$. Pak f má na (a,b) primitivní funkci.

Věta (o jednoznačnosti primitivní funkce) Nechť F a G jsou dvě primitivní funkce k f na intervalu (a,b) . Pak existuje konstanta $c \in \mathbb{R}$ taková, že $F(x) = G(x) + c$, $\forall x \in (a,b)$.

Zde je vhodné znát důkaz.

Věta (linearita primitivní funkce) Nechť $a, b \in \mathbb{R}$, $a < b$ a nechť F je primitivní funkce k f na (a,b) a G je primitivní funkce k g na (a,b) a $\alpha, \beta \in \mathbb{R}$. Potom $\alpha f + \beta g$ má na (a,b) primitivní funkce $\alpha F + \beta G$.

Definice Nechť $a, b \in \mathbb{R}$, $a < b$. Končenou posloupnost $\{x_0, \dots, x_n\}$ nazveme *dělením intervalu* $\langle a, b \rangle \subset \mathbb{R}$, pokud $a = x_0 < x_1 < \dots < x_{n-1} < x_n = b$.

Řekneme, že D' je *zjemnění* dělení D , pokud každý bod D je zároveň i bodem D' .

Definice Nechť $a, b \in \mathbb{R}$, $a < b$, $\{x_0, \dots, x_n\}$ dělení $\langle a, b \rangle$ a funkce f definovaná na $\langle a, b \rangle$. Označme

$$m_i = \inf_{x \in (x_{i-1}, x_i)} f(x), \quad M_i = \sup_{x \in (x_{i-1}, x_i)} f(x)$$

a

$$s(f, D) = \sum_{i=1}^n m_i(x_i - x_{i-1}) \leq \sum_{i=1}^n M_i(x_i - x_{i-1}) = S(f, D).$$

$s(f, D)$ nazýváme *dolní součet* a $S(f, D)$ *horní součet* funkce f při dělení D .

Pak definujeme *dolní Riemannův integrál* jako

$$\underline{\int_a^b} f := \sup\{s(D), D \text{ dělení } \langle a, b \rangle\},$$

a *horní Riemannův integrál* jako

$$\overline{\int_a^b} f := \inf\{S(D), D \text{ dělení } \langle a, b \rangle\}.$$

Definice Řekneme, že funkce f má *Riemannův integrál* ($f \in \mathcal{R}(\langle a, b \rangle)$), pokud

$$\underline{\int_a^b} f = \overline{\int_a^b} f,$$

pak tento integrál definujeme jako

$$\int_a^b f = \overline{\int_a^b} f = \underline{\int_a^b} f.$$

Definice Norma dělení D je $\|D\| = \max\{(x_i - x_{i-1}), i = 1, \dots, n\}$.

Věta (o horním a dolním součtu zjemnění) Nechť D' je zjemnění dělení D .

Pak

$$s(f, D) \leq s(f, D') \leq S(f, D') \leq S(f, D).$$

Věta (aproximace horního a dolního Riemannova integrálu) Nechť $a, b \in \mathbb{R}$, $a < b$ a je funkce f omezená na intervalu $\langle a, b \rangle$. Pak $\forall \epsilon > 0 \exists \delta > 0 : \forall D, \|D\| < \delta$ platí

$$\overline{\int_a^b} f \leq S(f, D) < \overline{\int_a^b} f + \epsilon \wedge \underline{\int_a^b} f - \epsilon < s(f, D) \leq \underline{\int_a^b} f.$$

Definice Nechť $a, b \in \mathbb{R}$, $a < b$ a $f, F : (a, b) \rightarrow \mathbb{R}$. Pokud platí $F \in \mathcal{C}((a, b))$ a $F'(x) = f(x) \forall x \in (a, b) \setminus K$, kde K je konečná množina, pak F je *zobecněná primitivní funkce* k f na (a, b) .

Definice Nechť $a, b \in \mathbb{R}$, $a < b$, $f : (a, b) \rightarrow \mathbb{R}$ a F je zobecněná primitivní funkce k f na (a, b) . Pak *Newtonovým integrálem* funkce f od a do b rozumíme

$$\int_a^b f = [F]_a^b := \lim_{x \rightarrow b^-} F(x) - \lim_{x \rightarrow a^+} F(x),$$

má-li tento rozdíl smysl. Má-li funkce f Newtonův integrál značíme $f \in \mathcal{N}((a, b))$.

Věta (vztah Newtonova a Riemannova integrálu) Nechť $a, b \in \mathbb{R}$, $a < b$ a $f : \langle a, b \rangle \rightarrow \mathbb{R}$. Pokud $f \in \mathcal{N}((a, b)) \cap \mathcal{R}(\langle a, b \rangle)$ pak

$$(\mathcal{N}) \int_a^b f = (\mathcal{R}) \int_a^b f.$$

1.3.2 Základní vlastnosti, vztah k primitivní funkci

Věta (vlastnosti Riemannova integrálu) Nechť $a, b \in \mathbb{R}$, $a < b$.

(i.) *Linearita:* Nechť $f, g \in \mathcal{R}(\langle a, b \rangle)$, $\lambda \in \mathbb{R}$. Pak $f+g \in \mathcal{R}(\langle a, b \rangle)$, $\lambda f \in \mathcal{R}(\langle a, b \rangle)$

$$\int_a^b (f+g) = \int_a^b f + \int_a^b g, \quad \int_a^b \lambda f = \lambda \int_a^b f.$$

(ii.) *Monotonie:* Nechť $f, g \in \mathcal{R}(\langle a, b \rangle)$, $f \leq g$ na $\langle a, b \rangle$. Pak

$$\int_a^b f \leq \int_a^b g.$$

(iii.) *Aditivita:* Nechť $c \in (a, b)$ a f definovaná na $\langle a, b \rangle$. Pak

$$f \in \mathcal{R}(\langle a, b \rangle) \Leftrightarrow f \in \mathcal{R}(\langle a, c \rangle) \wedge f \in \mathcal{R}(\langle c, b \rangle),$$

a

$$\int_a^b f = \int_a^c f + \int_c^b f.$$

(iv.) *Absolutní konvergencie*: Nechť $f \in \mathcal{R}(\langle a,b \rangle)$, pak $|f| \in \mathcal{R}(\langle a,b \rangle)$ a platí

$$\left| \int_a^b f \right| \leq \int_a^b |f|. \quad \text{---}$$

Věta (vztah Riemannova integrálu a primitivní funkce) Nechť $a,b \in \mathbb{R}$, $a < b$, $f \in \mathcal{R}(\langle a,b \rangle)$. Pak funkce $F(x) := \int_a^x f$, $\forall x \in \langle a,b \rangle$ je spojitá v $\langle a,b \rangle$ a $F'(x) = f(x)$ pro všechny body spojitosti f .

Věta (o rovnosti integrálů) $a,b \in \mathbb{R}$, $a < b$ a $f \in \mathcal{R}(\langle a,b \rangle)$ a $g : \langle a,b \rangle \rightarrow \mathbb{R}$ taková, že $g = f$ na $\langle a,b \rangle \setminus K$, kde K je konečná množina. Potom

$$\int_a^b g = \int_a^b f.$$

Věta (vlastnosti Newtonova integrálu) Newtonův integrál má vlastnosti *linearity* a *monotonicity* stejné jako Riemannův. Dále

(iii.) *Linearita*: Nechť $a,b \in \mathbb{R}$, $a < b$, $c \in (a,b)$. Pak

$$f \in \mathcal{N}(\langle a,c \rangle), f \in \mathcal{N}(\langle c,b \rangle), f \text{ spojitá v } c \Leftrightarrow f \in \mathcal{N}(\langle a,b \rangle).$$

(iv.) Pokud $|f| \in \mathcal{N}((a,b))$, f spojitá, pak $f \in \mathcal{N}((a,b))$.

Definice Řekneme, že funkce f je *stejnomořně spojitá* na intervalu I , pokud

$$\forall \epsilon > 0 \exists \delta > 0 \forall x,y \in I : |x-y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon.$$

1.3.3 Metody výpočtu

Věta (integrace per partes) Nechť $a,b,\alpha,\beta \in \mathbb{R}$, $a < b$, $\alpha < \beta$, F je primitivní funkce k f na (a,b) a G je primitivní funkce g na (a,b) . Pak na (a,b) platí

$$\int F(x)g(x)dx = F(x)G(x) - \int f(x)G(x)dx.$$

Věta (substituční metody) Nechť $a,b \in \mathbb{R}$, $a < b$ a

(i.) F je primitivní funkce k f na (a,b) a $\varphi : (\alpha,\beta) \rightarrow (a,b)$, $\varphi'(t)$ existuje $\forall t \in (\alpha,\beta)$. Pak

$$\int f(\varphi(t))\varphi'(t)dt = F(\varphi(t)) + c \quad \forall t \in (\alpha,\beta).$$

(ii.) $\varphi : (\alpha, \beta) \xrightarrow{na} (a, b)$, $0 \neq \varphi'(t) \forall t \in (\alpha, \beta)$, $f : (a, b) \rightarrow \mathbb{R}$ a G je primitivní funkce k $f(\varphi(t))\varphi'(t)$ na (a, b) . Pak

$$\int f(x)dx = G(\varphi^{-1}(x)).$$

Zde je vhodné znát důkaz.

Věta (per partes pro Newtonův integrál) Nechť $a, b \in \mathbb{R}$, $a < b$ a F je primitivní funkci k f na (a, b) a G je primitivní funkce k g na (a, b) . Pak

$$\int_a^b Fg = [FG]_a^b - \int_a^b fG.$$

Věta (o střední hodnotě pro integrály I.) Nechť $a, b \in \mathbb{R}$, $a < b$ a $f \in C(\langle a, b \rangle)$, $g \geq 0$ v $\langle a, b \rangle \setminus K$, kde K je konečná. Pak

$$\exists \xi \in \langle a, b \rangle : \int_a^b fg = f(\xi) \int_a^b g,$$

pokud integrály $\int_a^b fg$ a $\int_a^b g$ existují.

Věta (o střední hodnotě pro integrály II.) Nechť $a, b \in \mathbb{R}$, $a < b$ a $f : \langle a, b \rangle \rightarrow \mathbb{R}$ spojitá funkce a $g : \langle a, b \rangle \rightarrow \mathbb{R}$ monotonné a spojitá. Pak

$$\exists \xi \in \langle a, b \rangle : \int_a^b fg = g(a) \int_a^\xi f + g(b) \int_\xi^b f.$$

Tyhle dvě věty nemusí asi být tak důležité, ale věty o středních hodnotách jsou moje favority.

Postup integrace racionální funkce Nechť $Q(x) = \frac{P(x)}{R(x)}$.

1. Pokud $\text{st}P \geq \text{st}Q$ tak částečné dělení polynomů na tvar $P_1 + \frac{P_2}{Q}$.
2. Rozklad Q na součin ireducibilních dvou a trojčlenů.
3. Rozklad na parciální zlomky.
4. Integrace parciálních zlomků.

Detailní přístup je popsáný na webových stránkách Mgr. Kristýny Kuncové. V archivu má cvika z Analýz 1 a 2 a v nich skvělé materiály.

Goniometrické substituce

1. Pokud $R(\sin x, \cos x) = R(-\sin x, -\cos x)$ pak se používá substituce $t = \tan x$, pak

$$dx = \frac{dt}{1+t^2}, \quad \sin^2 x = \frac{t^2}{1+t^2}, \quad \cos^2 x = \frac{1}{1+t^2}, \quad \sin x \cos x = \frac{t}{1+t^2}.$$

2. V jakémkoliv případě lze použít substituci $t = \tan \frac{x}{2}$. Pak

$$dx = \frac{2dt}{1+t^2}, \quad \sin x = \frac{2t}{1+t^2}, \quad \cos x = \frac{1-t^2}{1+t^2}.$$

Věta (Integrální kritérium pro konvergenci řad) Nechť f je spojitá, kladná a nerostoucí na $\langle n_0, \infty \rangle$ a nechť $a_n = f(n) \forall n \in \mathbb{N}, n \geq n_0$. Pak

$$\sum_{n=1}^{\infty} a_n \text{ konverguje} \Leftrightarrow \int_{n_0}^{\infty} f(x) dx < \infty.$$

Tady se ještě hodí vědět: délka křivky, objem rotačního tělesa, Fubiniova věta a Fubini o substituci. Moc zmatený a ugh.

1.3.4 Základní kritéria existence

Věta (existence Riemannova integrálu I.) Nechť $a, b \in \mathbb{R}, a < b$ a $f \in C(\langle a, b \rangle)$. Pak $f \in \mathcal{R}(\langle a, b \rangle)$.

Věta (existence Riemannova integrálu II.) Nechť $a, b \in \mathbb{R}, a < b$ a f monotonní na $\langle a, b \rangle$. Pak $f \in \mathcal{R}(\langle a, b \rangle)$.

Věta (existence Riemannova integrálu III.) Nechť $a, b \in \mathbb{R}, a < b$ a f omezená na $\langle a, b \rangle$. Pak platí

$$\int_a^b f \text{ existuje} \Leftrightarrow \forall \epsilon > 0 \exists D \text{ dělení } \langle a, b \rangle : S(f, D) - s(f, D) < \epsilon.$$

Zde je vhodné znát důkaz.

Věta (existence Newtonova integrálu) Nechť $a, b \in \mathbb{R}, a < b$ a f je spojitá a omezená na (a, b) . Pak $f \in \mathcal{N}((a, b))$.

Věta (srovnávací kritéria pro Newtonův integrál) Nechť $a, b \in \mathbb{R}, a < b$.

(i.) Pokud $0 \leq f \leq g$ na $\langle a, b \rangle$, f spojitá na $\langle a, b \rangle$, pak

$$g \in \mathcal{N}((a, b)) \Rightarrow f \in \mathcal{N}((a, b)).$$

(ii.) Pokud f a g jsou nezáporné spojité na $\langle a, b \rangle$ a platí

$$\lim_{x \rightarrow b^-} \frac{f(x)}{g(x)} = c, \quad c \in (0, \infty).$$

Pak $f \in \mathcal{N}((a, b)) \Leftrightarrow g \in \mathcal{N}((a, b))$.

Věta (Abel-Dirichlet pro Newtonův integrál) Nechť $a, b \in \mathbb{R}, a < b$ a $f : \langle a, b \rangle \rightarrow \mathbb{R}$ je spojitá a F je primitivní funkce k f na $\langle a, b \rangle$, $g : \langle a, b \rangle \rightarrow \mathbb{R}$ monotonné a spojitá. Nechť platí alespoň jedna z následujících podmínek:

(A) $f \in \mathcal{N}((a, b))$ a g je omezená na (a, b) ,

(D) F omezená na (a, b) a $\lim_{x \rightarrow b^-} g(x) = 0$.

Pak $fg \in \mathcal{N}((a, b))$.

1.4 Funkce více proměnných

1.4.1 Diferenciál a parciální derivace

Tahle kapitola je dost zmatená, ale (zatím) se mi nepodařilo to srovnat. You try.

Definice Nechť $f : \mathbb{R}^n \rightarrow \mathbb{R}$, $a \in \mathbb{R}^n$. Parciální derivace f v bodě a podle i -té proměnné je

$$\frac{\partial f}{\partial x_i}(a) = \lim_{t \rightarrow 0} \frac{f(a + te^i) - f(a)}{t}.$$

Definice Nechť $f : \mathbb{R}^n \rightarrow \mathbb{R}$, $a \in \mathbb{R}^n$, $\vec{v} \in \mathbb{R}^n \setminus \{0\}$. Derivací f v bodě a ve směru \vec{v} je

$$D_{\vec{v}} f(a) = \lim_{t \rightarrow 0} \frac{f(a + t\vec{v}) - f(a)}{t}.$$

Definice Nechť $f : \mathbb{R}^n \rightarrow \mathbb{R}$, $a \in \mathbb{R}^n$, $L : \mathbb{R}^n \rightarrow \mathbb{R}$ je lineární zobrazení. Řekneme, že L je totální diferenciál funkce f v bodě a , jestliže

$$\lim_{h \rightarrow 0} \frac{f(a + h) - f(a) - L(h)}{\|h\|} = 0.$$

Věta (o tvaru totálního diferenciálu) Má-li f v bodě a totální diferenciál, pak je v a spojitá, existují v a všechny parciální derivace a platí

$$L(h) = \frac{\partial f}{\partial x_1}(a)h_1 + \dots + \frac{\partial f}{\partial x_n}(a)h_n.$$

Věta (postačující podmínka pro existenci totálního diferenciálu) Nechť $f : \mathbb{R}^n \rightarrow \mathbb{R}$ má v bodě a spojité všechny parciální derivace, pak má v a totální diferenciál.

Definice Nechť $f : \mathbb{R}^n \rightarrow \mathbb{R}$, $a \in \mathbb{R}^n$ a f má v a všechny parciální derivace vlastní. Gradient funkce f v bodě a je

$$\nabla f(a) = \left(\frac{\partial f}{\partial x_1}(a), \dots, \frac{\partial f}{\partial x_n}(a) \right).$$

Gradient udává směr největšího růstu funkce.

Věta (o gradientu a derivacích ve směru) Nechť $f : \mathbb{R}^n \rightarrow \mathbb{R}$, $a \in \mathbb{R}^n$. Pak $D_{\vec{v}} f(a) = \langle \nabla f(a), \vec{v} \rangle$.

Definice Nechť F je zobrazení z \mathbb{R}^n do \mathbb{R}^k , $a \in \mathbb{R}^n$ a L je lineární zobrazení z \mathbb{R}^n do \mathbb{R}^k . Pak L je derivací F v a , pokud

$$\lim_{h \rightarrow 0} \frac{\|F(a + h) - F(a) - L(h)\|}{\|h\|} = 0.$$

Pak

$$F'(a) = \left(\frac{\partial F_j}{\partial x_i}(a) \right)_{i,j=1}^{k,n}.$$

Tato matice se nazývá *Jakobiho matici*. Je-li $k = n$ pak determinant této matice nazýváme *Jakobián*.

Věta (aritmetika totálního diferenciálu) Nechť $f, g : \mathbb{R}^n \rightarrow \mathbb{R}$ mají totální diferenciály L_f a L_g v $a \in \mathbb{R}^n$ a nechť $\alpha \in \mathbb{R}$. Pak existují totální diferenciály $L_{f \pm g}(a)$, $L_{fg}(a)$, $L_{\alpha f}(a)$ a $L_{\frac{f}{g}}(a)$ pro $g(a) \neq 0$ a platí vztahy

$$L_{f \pm g}(a) = L_f(a) \pm L_g(a),$$

$$L_{\alpha f}(a) = \alpha L_f(a),$$

$$L_{fg}(a) = L_f(a)g(a) + L_g(a)f(a),$$

$$L_{\frac{f}{g}}(a) = \frac{g(a)L_f(a) - f(a)L_g(a)}{g^2}.$$

Věta (o diferenciálu složeného zobrazení, řetízkové pravidlo): Nechť $f : \mathbb{R}^n \rightarrow \mathbb{R}$, $g_i : \mathbb{R}^s \rightarrow \mathbb{R}$, $i = 1, \dots, n$, $a \in \mathbb{R}^s$, $b \in \mathbb{R}^n$, $b = [g_1(a), \dots, g_n(a)]$ a nechť f má totální diferenciál v b a g_i mají totální diferenciál v a pro všechny $i = 1, \dots, n$. Bud $H(x) = f([g_1(x), \dots, g_n(x)])$. Pak H má v a totální diferenciál a platí

$$L_H(a)(h) = \sum_{i=1}^s \left[\sum_{j=1}^n \frac{\partial f}{\partial y_j}(b) \frac{\partial g_j}{\partial x_i}(a) \right] h_i,$$

speciálně

$$\frac{\partial H}{\partial x_i}(a) = \sum_{j=1}^n \frac{\partial f}{\partial y_j}(b) \frac{\partial g_j}{\partial x_i}(a).$$

Věta (o střední hodnotě) Nechť $f : \mathbb{R}^n \rightarrow \mathbb{R}$ má všechny parciální derivace na úsečce mezi $a, b \in \mathbb{R}^n$. Pak existuje $\xi \in (0, 1)$ takové, že

$$f(b) - f(a) = \sum_{i=1}^n \frac{\partial f}{\partial x_i} \left(a + \xi(b - a) \right) \cdot (b_i - a_i).$$

Definice Nechť $G \subset \mathbb{R}^n$ je otevřená množina a $f : G \rightarrow \mathbb{R}$ má v G všechny parciální derivace a nechť $a \in G$. 2. parciální derivace f jsou

$$\frac{\partial^2 f}{\partial x_i \partial x_j}(a) = \frac{\partial}{\partial x_j} \left(\frac{\partial f}{\partial x_i} \right)(a).$$

Věta (záměnnost parciálních derivací druhého řádu) Nechť $f : \mathbb{R}^n \rightarrow \mathbb{R}$ má v $a \in \mathbb{R}^n$ spojitou parciální derivaci $\frac{\partial^2 f}{\partial x_i \partial x_j}$. Pak tam je spojitá i parciální

derivace $\frac{\partial^2 f}{\partial x_j \partial x_i}$ a tyto dvě se rovnají.

Definice Nechť $f : \mathbb{R}^n \rightarrow \mathbb{R}$, $a \in \mathbb{R}^n$ a nechť $\frac{\partial f}{\partial x_i}$ mají totální diferenciál v bodě a pro všechny $i = 1, \dots, n$. Druhý diferenciál funkce f v bodě a je

$$\sum_{i=1}^n \sum_{j=1}^n \frac{\partial^2 f}{\partial x_i \partial x_j}(a) \cdot h_i \cdot k_j,$$

maticově

$$\left(\frac{\partial^2 f}{\partial x_i \partial x_j}(a) \right)_{i,j=1}^n.$$

Tato matice se nazývá *Hessova matice*.

Definice Nechť $G \subset \mathbb{R}^n$ je otevřená. Množina $C^k(G)$ je množina těch funkcí, které mají spojité parciální derivace k -tého řádu na G .

Věta (postačující podmínka pro existenci druhého diferenciálu) Nechť $G \subset \mathbb{R}^n$ je otevřená a $f \in C^2(G)$. Pak f má na G druhý diferenciál.

1.4.2 Implicitní funkce

Definice *Explicitní vyjádření funkce* je $y = y(x)$ a *implicitní vyjádření funkce* je $F(x,y) = 0$.

Věta (o implicitní funkci) Nechť $k \in \mathbb{N}$, $\Omega \subset \mathbb{R}^{n+1}$ otevřená množina, $F : \Omega \rightarrow \mathbb{R}$, $F = F(x_1, \dots, x_n, y) = F(x, y)$. Nechť $[a, b] = [a_1, \dots, a_n, b] \in \Omega$ a nechť platí

- i. $F(a, b) = 0$,
- ii. $F \in C^k(\Omega)$,
- iii. $\frac{\partial F}{\partial y}(a, b) \neq 0$.

Pak $\exists \delta_1, \delta_2$:

$$(i.) \forall x \in \mathcal{U}(a, \delta_1) \exists! y \in \mathcal{U}(b, \delta_2) : F(x, y) = 0, \text{ tj. } y = y(x),$$

$$(ii.) y \in C^k(\mathcal{U}(a, \delta_1)) \text{ a } \frac{\partial y}{\partial x_i}(x) = \frac{-\frac{\partial F}{\partial x_i}(x, y(x))}{\frac{\partial F}{\partial y}(x, y(x))}, \forall x \in \mathcal{U}(a, \delta_1), i = 1, \dots, n.$$

Věta (o implicitním zobrazení) Nechť $k \in \mathbb{N}$, $\Omega \subset \mathbb{R}^{n+m}$ otevřená množina, $F : \Omega \rightarrow \mathbb{R}^m$, $F = F(x_1, \dots, x_n, y_1, \dots, y_m) = F(x, y)$, nechť $[a, b] = [a_1, \dots, a_n, b_1, \dots, b_m] \in \Omega$ a platí

- i. $F(a, b) = 0$,
- ii. $F \in C^k(\Omega)$,
- iii. $\frac{D(F_1, \dots, F_m)}{D(y_1, \dots, y_m)}(a, b) = \det \left(\frac{\partial F_i}{\partial y_j}(a, b) \right)_{i,j=1}^m \neq 0$.

Pak $\exists \mathcal{U}(a) \subset \mathbb{R}^n$, $\exists \mathcal{U}(b) \subset \mathbb{R}^m$:

$$\forall x \in \mathcal{U}(a) \exists! y \in \mathcal{U}(b) : F(x, y) = 0, \text{ tj. } y = (y_1(x), \dots, y_m(x)) \text{ a } y \in C^k(\mathcal{U}(a)).$$

1.4.3 Volné a vázané extrémy funkcí více proměnných

Definice Nechť $f : \mathbb{R}^n \rightarrow \mathbb{R}$, $a \in \mathbb{R}^n$. Řekneme, že funkce f má v a *globální maximum*, pokud $\forall x \in \mathbb{R}^n : f(a) \geq f(x)$. Řekneme, že funkce f má v bodě a *lokální maximum*, jestliže $\exists \mathcal{U}(a) : f(a) \geq f(x) \forall x \in \mathcal{U}(a)$. Tyto extrémy jsou *volné*.

Analogicky minimum.

Definice Nechť $M \subset \mathbb{R}^n$ a $f : M \rightarrow \mathbb{R}$. Řekneme, že funkce f nabývá v bodě $a \in M$ *maxima vzhledem k M* , pokud $\forall x \in M : f(x) \leq f(a)$. Řekneme, že funkce f má v a *lokální maximum vzhledem k M* , pokud $\exists \mathcal{U}(a) : f(x) \leq f(a) \forall x \in \mathcal{U}(a) \cap M$. Tyto extrémy jsou *vázané*.

Analogicky minimum.

Definice Nechť $G \subset \mathbb{R}^n$ je otevřená a nechť $f : G \rightarrow \mathbb{R}$. Řekneme, že $x_0 \in G$ je *stacionárním bodem* f , jestliže má f v x_0 všechny parciální derivace prvního řádu nulové.

1.4.4 Nutné a postačující podmínky pro volné extrémy, nutné podmínky pro vázané extrémy

Věta (nutná podmínka pro volný extrém) Nechť $G \subset \mathbb{R}^n$ je otevřená, $f : G \rightarrow \mathbb{R}$. Má-li f v bodě $a \in G$ lokální extrém vzhledem k G , pak $\frac{\partial f}{\partial x_j}(a)$ buď neexistuje nebo je nulová pro každé $j = 1, \dots, n$.

Věta (postačující podmínka pro volný extrém) Nechť $G \subset \mathbb{R}^n$ je otevřená, $a \in G$, $f : G \rightarrow \mathbb{R}$, $f \in C^2(G)$ a $\nabla f(a) = 0$.

- i. Jestliže $D^2 f(a)$ je pozitivně definitní, pak a je lokální minimum,
- ii. jestliže $D^2 f(a)$ je negativně definitní, pak a je lokální maximum,
- iii. jestliže $D^2 f(a)$ je indefinitní, pak v a není extrém,

$$\text{kde } D^2 f(a) = \left(\frac{\partial^2 f}{\partial x_i \partial x_j}(a) \right)_{i,j=1}^n.$$

Věta (Lagrangeova o vázaných extrémech) Nechť $G \subset \mathbb{R}^{n+m}$ a $f, g_1, \dots, g_m : G \rightarrow \mathbb{R}$, $f, g_1, \dots, g_m \in C^1(G)$. Nechť $M = \{x \in \mathbb{R}^{n+m} : g_1(x) = 0, \dots, g_m(x) = 0\}$ a nechť $\nabla g_1, \dots, \nabla g_m$ jsou lineárně nezávislé na M . Pokud f má v $a \in M$ lokální extrém vzhledem k M , pak existují $\lambda_1, \dots, \lambda_m \in \mathbb{R}$ takové, že

$$\nabla f(a) + \lambda_1 \nabla g_1(a) + \dots + \lambda_m \nabla g_m(a) = 0.$$

1.5 Obyčejné diferenciální rovnice

1.5.1 Věta o existenci a jednoznačnosti řešení počáteční úlohy

Definice *Obyčejná diferenciální rovnice* je rovnice tvaru $F(x,y,y',\dots,y^{(n)}) = 0$, $n \in \mathbb{N}$, kde F je reálná funkce.

Definice *Řešením diferenciální rovnice* $F(x,y,y',\dots,y^{(n)}) = 0$ rozumíme funkci $y = y(x)$ definovanou v neprázdném intervalu (a,b) takovou, že existuje vlastní $y^{(n)}(x)$ pro všechny $x \in (a,b)$ a platí $F(x,y(x),y'(x),\dots,y^{(n)}(x)) = 0$ na (a,b) .

Definice Řekneme, že diferenciální rovnice je *rozřešená* vzhledem k $y^{(n)}$, pokud je tvaru $y^{(n)} = f(x,y,y',\dots,y^{(n-1)})$.

Definice Řekneme, že (\tilde{y},\tilde{I}) je *rozšířením řešení* (y,I) , pokud je řešením, platí $I \subset \tilde{I}$ a $y = \tilde{y}$ na I .

Definice Řekneme, že (y,I) je *maximální řešení*, pokud neexistuje jeho rozšíření kromě triviálního.

Věta (Peanova) Nechť $\Omega \subset \mathbb{R}^{n+1}$ je otevřená množina, $[x_0,y_0,\dots,y_{n-1}] \in \Omega$ a $f : \Omega \rightarrow \mathbb{R}$ je spojitá funkce. Pak existuje okolí $\mathcal{U}(x_0)$ a funkce y definované na $\mathcal{U}(x_0)$ takové, že $y^{(n)}(x) = f(x,y(x),\dots,y^{(n-1)}(x))$ a splňují $y(x_0) = y_0$, $y'(x_0) = y_1, \dots, y^{(n-1)}(x) = y_{n-1}$.

Definice Nechť $\Omega \subset \mathbb{R}^{n+1}$, $f : \Omega \rightarrow \mathbb{R}$ je *lokálně Lipschitzovská vzhledem k posledním n proměnným*, pokud pro každou otevřenou $U \subset \Omega$ existuje $K > 0$ takové, že

$$\forall [x_0,y], [x_0,\tilde{y}] \subset U : |f(x_0,y) - f(x_0,\tilde{y})| \leq K \|y - \tilde{y}\|_{\mathbb{R}^n},$$

kde y a \tilde{y} jsou n -složkové proměnné.

Věta (Picardova) Nechť $\Omega \subset \mathbb{R}^{n+1}$ je otevřená množina, $[x_0,y_0,\dots,y_{n-1}] \in \Omega$ a $f : \Omega \rightarrow \mathbb{R}$ je spojitá funkce, která je navíc lokálně Lipschitzovská vzhledem k posledním n proměnným. Pak existuje okolí $\mathcal{U}(x_0)$ a funkce y definované na $\mathcal{U}(x_0)$ takové, že $y^{(n)}(x) = f(x,y(x),\dots,y^{(n-1)}(x))$ a splňují $y(x_0) = y_0$, $y'(x_0) = y_1, \dots, y^{(n-1)}(x) = y_{n-1}$. Každá dvě řešení navíc splývají v průniku svých definičních oborů a maximální řešení je určeno jednoznačně.

Věta (Peanova pro $n = 1$) Nechť $\Omega \subset \mathbb{R}^2$, $[x_0,y_0] \in \Omega$, $f : \Omega \rightarrow \mathbb{R}$ je spojitá. Pak existuje $\delta > 0$ a funkce y definované na $\mathcal{U}(x_0,\delta)$ takové, že $y'(x) = f(x,y(x)) \quad \forall x \in \mathcal{U}(x_0,\delta)$ a $y(x_0) = y_0$.

Věta (Picardova pro $n = 1$) Nechť $\Omega \subset \mathbb{R}^2$, $[x_0,y_0] \in \Omega$, $f : \Omega \rightarrow \mathbb{R}$ je spojitá a lokálně Lipschitzovská vzhledem k y . Pak existuje $\delta > 0$ a funkce y definované na $\mathcal{U}(x_0,\delta)$ takové, že $y'(x) = f(x,y(x)) \quad \forall x \in \mathcal{U}(x_0,\delta)$ a $y(x_0) = y_0$. Každá dvě řešení navíc splývají v průniku svých definičních oborů a maximální řešení je určeno

jednoznačně.

Věta (o tvaru řešení) Nechť $I \subset \mathbb{R}$, $x_0 \in I$, $y_0 \in \mathbb{R}$, $y \in C(I)$. Pak y je na I řešením rovnice $y' = f(x,y)$ s podmínkou $y(x_0) = y_0$ právě tehdy, když platí

$$y(x) = y_0 + \int_{x_0}^x f(t,y(t))dt, \quad \forall x \in I.$$

Věta (o lepení řešení) Nechť $a \in \mathbb{R}$, $\delta, \gamma > 0$, $f \in C^2((a-\delta, a+\gamma))$. Budě y_L řešení $y' = f(x,y)$ na $(a-\delta, a)$ a budě y_R řešení $y' = f(x,y)$ na $(a, a+\gamma)$. Pokud platí $\lim_{x \rightarrow a^-} y_L(x) = A = \lim_{x \rightarrow a^+} y_R(x)$, pak

$$y(x) = \begin{cases} y_L(x), & x \in (a-\delta, a), \\ A, & x = a, \\ y_R(x), & x \in (a, a+\delta), \end{cases}$$

je řešením $y' = f(x,y)$ na $(a-\delta, a+\gamma)$.

1.5.2 Jednoduché rovnice prvního řádu a lineární rovnice vyššího řádu s konstantními koeficienty

Věta (existence a jednoznačnost pro separované proměnné) Nechť $(a,b) \subset \mathbb{R}$, $(c,d) \subset \mathbb{R}$, $f \in C((a,b))$, $g \in C((c,d))$, $g \neq 0$ v (c,d) . Nechť $x_0 \in (a,b)$, $y_0 \in (c,d)$. Pak existuje právě jedno y řešení rovnice $y'(x) = f(x)g(y)$ splňující podmítku $y(x_0) = y_0$, definičním oborem je maximální otevřený interval $I \subset (a,b)$ splňující $G(y(x)) = F(x) + k$, kde $k \in \mathbb{R}$ je konstanta a

$$F(x) = \int_{x_0}^x f(t)dt, \quad G(y) = \int_{y_0}^y \frac{1}{g(t)}dt.$$

Řešení je pak tvaru $y(x) = (G^{-1} \circ F)(x)$, $\forall x \in I$.

Definice Úloha ve tvaru z předchozí věty se nazývá *diferenciální rovnice se separovanými proměnnými*.

Věta (metoda integračního faktoru) Nechť $(a,b) \subset \mathbb{R}$, $p, q \in C((a,b))$, P primitivní funkce k p na (a,b) splňující $P(x_0) = 0$, kde $x_0 \in (a,b)$. Nechť $y_0 \in \mathbb{R}$. Pak existuje právě jedno maximální řešení rovnice $y' + py = q$ splňující $y(x_0) = y_0$ a splňuje

$$y(x)e^{P(x)} = \int_{x_0}^x q(t)e^{P(t)}dt + y_0.$$

Definice Rovnice tvaru $y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_0y = q(x)$, kde $a_0, \dots, a_{n-1} \in \mathbb{R}$, $(a,b) \subset \mathbb{R}$ a $q \in C((a,b))$ se nazývá *lineární diferenciální rovnice n-tého řádu s konstantními koeficienty*. Příslušná *homogenní rovnice* je rovnice tvaru $y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_0y = 0$.

Definice Bázi všech maximálních řešení homogenní rovnice nazýváme *fundamentální systém* rovnice.

Definice Polynom $P(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_0$ nazýváme *charakteristický polynom* rovnice.

Věta (o fundamentálním systému) Nechť $\lambda_1, \dots, \lambda_s, s \in \mathbb{N}$ jsou všechny různé reálné kořeny charakteristického polynomu rovnice s násobnostmi r_1, \dots, r_s a nechť $\alpha_1 + i\beta_1, \dots, \alpha_l + i\beta_l, l \in \mathbb{N}$ jsou všechny různé komplexní kořeny s násobnostmi q_1, \dots, q_l . Pak funkce

$$\begin{aligned} & e^{\lambda_1 x}, xe^{\lambda_1 x}, \dots, x^{r_1-1}e^{\lambda_1 x}, \\ & e^{\lambda_2 x}, xe^{\lambda_2 x}, \dots, x^{r_2-1}e^{\lambda_2 x}, \\ & \quad \dots \\ & e^{\lambda_s x}, xe^{\lambda_s x}, \dots, x^{r_s-1}e^{\lambda_s x}, \\ & e^{\alpha_1 x} \cos \beta_1 x, xe^{\alpha_1 x} \cos \beta_1 x, \dots, x^{q_1-1}e^{\alpha_1 x} \cos \beta_1 x, \\ & e^{\alpha_1 x} \sin \beta_1 x, xe^{\alpha_1 x} \sin \beta_1 x, \dots, x^{q_1-1}e^{\alpha_1 x} \sin \beta_1 x, \\ & e^{\alpha_2 x} \cos \beta_2 x, xe^{\alpha_2 x} \cos \beta_2 x, \dots, x^{q_2-1}e^{\alpha_2 x} \cos \beta_2 x, \\ & e^{\alpha_2 x} \sin \beta_2 x, xe^{\alpha_2 x} \sin \beta_2 x, \dots, x^{q_2-1}e^{\alpha_2 x} \sin \beta_2 x, \\ & \quad \dots \\ & e^{\alpha_l x} \cos \beta_l x, xe^{\alpha_l x} \cos \beta_l x, \dots, x^{q_l-1}e^{\alpha_l x} \cos \beta_l x, \\ & e^{\alpha_l x} \sin \beta_l x, xe^{\alpha_l x} \sin \beta_l x, \dots, x^{q_l-1}e^{\alpha_l x} \sin \beta_l x, \end{aligned}$$

tvoří fundamentální systém homogenní rovnice.

Věta (řešení rovnice se specifickou pravou stranou) Nechť $\alpha + i\beta, \alpha, \beta \in \mathbb{R}$ je k -násobný kořen charakteristického polynomu. Pak rovnice

$$y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_0y = Q_1(x)e^{\alpha x} \cos \beta x + Q_2(x)e^{\alpha x} \sin \beta x,$$

kde Q_1, Q_2 jsou polynomy má řešení tvaru

$$y(x) = x^k P_1(x)e^{\alpha x} \cos \beta x + x^k P_2(x)e^{\alpha x} \sin \beta x, x \in \mathbb{R},$$

kde P_1 a P_2 jsou vhodné polynomy stupně $\leq \max\{\text{st}Q_1, \text{st}Q_2\}$.

Věta (o řešení homogenní rovnice) Maximální řešení homogenní rovnice jsou definována na celém \mathbb{R} a tvoří podprostor dimenze n prostoru $C^n(\mathbb{R})$.

Věta (variace konstant) Nechť $(a,b) \subset \mathbb{R}$, $a_0, \dots, a_{n-1} \in \mathbb{R}$, $q : (a,b) \rightarrow \mathbb{R}$ je funkce spojitá na (a,b) . Nechť funkce y_1, \dots, y_n tvoří fundamentální systém homogenní rovnice. Nechť jsou funkce c'_1, \dots, c'_n řešením soustavy

$$\begin{aligned} c'_1(x)y_1(x) + \dots + c'_n(x)y_n(x) &= 0 \\ c'_1(x)y'_1(x) + \dots + c'_n(x)y'_n(x) &= 0 \\ & \quad \dots \\ c'_1(x)y_1^{(n-2)}(x) + \dots + c'_n(x)y_n^{(n-2)}(x) &= 0 \\ c'_1(x)y_1^{(n-1)}(x) + \dots + c'_n(x)y_n^{(n-1)}(x) &= q(x), \end{aligned}$$

a c_i je primitivní funkcií k c'_i na (a,b) pro $i = 1, \dots, n$. Pak

$$Y(x) = \sum_{i=1}^n c_i(x)y_i(x)$$

je řešením rovnice $y_{(n)} + a_{n-1}y^{(n-1)} + \dots + a_0y = q(x)$ na (a,b) .

2. Algebra

Algebru nesnáším a učit se jí mě vůbec nebavilo. Některá téma jsem si zpracovala divně a tak je tu vynechám. Je to třeba metoda nejmenších čtverců, pseudo-inverze, nebo rozklady matic. Konkrétně rozklady matic jsou pěkná nuda. Taky důkazy jsem si vybírala náhodně a nechci to tak doporučovat. Co já vím, tak u determinantů se na ně ptali (naštěstí ne mě). Have fun.

2.1 Matice a determinanty, soustavy lineárních rovnic

2.1.1 Základní pojmy a operace s maticemi a jejich vlastnosti

Definice *Vektor* je uspořádaná n -tice reálných čísel.

Předpokládám, že sčítání, odčítání vektorů a opačný vektor definovat nemusím.

Definice *Soustavou lineárních rovnic* rozumíme soustavu tvaru

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1$$

$$a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2$$

⋮

$$a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n = b_n,$$

kde $a_{11}, \dots, a_{nn}, b_1, \dots, b_n$ jsou konstanty.

Definice *Ekvivalentní úprava* je taková úprava, která nemění množinu všech řešení.

Definice *Matrice* je obdélníkové schéma s reálnými (komplexními) čísly.

Opět nebudu definovat součet matic, násobení skalárem, nulovou matice, diagonálu, čtvercovou matici, diagonální matici ani jednotkovou matici.

Definice *Transponovaná matice* k matici $\mathbb{A} = (a_{ij})_{m \times n}$ je $\mathbb{A}^T = (b_{ji})_{n \times m}$, kde $b_{ji} = a_{ij}$.

Věta (vlastnosti operací s maticemi) Necht $\mathbb{A}, \mathbb{B}, \mathbb{C}$ jsou stejnědimenzionální matice, \mathbb{O} je nulová matice a s, t jsou reálné konstanty. Pak

- $(\mathbb{A} + \mathbb{B}) + \mathbb{C} = \mathbb{A} + (\mathbb{B} + \mathbb{C}),$
- $\mathbb{A} + \mathbb{O} = \mathbb{A},$
- $\mathbb{A} + (-\mathbb{A}) = \mathbb{O},$

- $\mathbb{A} + \mathbb{B} = \mathbb{B} + \mathbb{A}$,
- $s(t\mathbb{A}) = (st)\mathbb{A}$,
- $(s+t)\mathbb{A} = s\mathbb{A} + t\mathbb{A}$,
- $s(\mathbb{A} + \mathbb{B}) = s\mathbb{A} + s\mathbb{B}$,
- $(\mathbb{A}^T)^T = \mathbb{A}$,
- $(\mathbb{A} + \mathbb{B})^T = \mathbb{A}^T + \mathbb{B}^T$,
- $(s\mathbb{A})^T = s\mathbb{A}^T$.

Definice Součin matice $\mathbb{A} = (\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_n)$, kde $\mathbf{a}_1, \dots, \mathbf{a}_n$ jsou vektory, s vektorem $\mathbf{b} = (b_1, b_2, \dots, b_n)^T$ je

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

Definice Součin dvou matic \mathbb{A} typu $m \times n$ a $\mathbb{B} = (\mathbf{b}_1|\dots|\mathbf{b}_p)$ typu $n \times p$ je matice

$$\mathbb{A}\mathbb{B} = (\mathbb{A}\mathbf{b}_1|\mathbb{A}\mathbf{b}_2|\dots|\mathbb{A}\mathbf{b}_p).$$

Součin matic je definovaný pouze pro matice vhodných typů, pro jiné definován není.

Tvrzení (o prvku na místě ij) Prvek na místě (i,j) v součinu matic \mathbb{A} a \mathbb{B} je

$$a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj} = \sum_{k=1}^n a_{ik}b_{kj} = a_i^T b_j.$$

Věta (vlastnosti násobení matic) Nechť $\mathbb{A}, \mathbb{B}, \mathbb{C}, \mathbb{D}$ a \mathbb{E} jsou matice vhodného typu a \mathbb{I} jsou jednotkové matice. Pak platí

- násobení matic není komutativní,
- $(\mathbb{A} + \mathbb{B})\mathbb{C} = \mathbb{A}\mathbb{C} + \mathbb{B}\mathbb{C}$,
- $\mathbb{C}(\mathbb{D} + \mathbb{E}) = \mathbb{C}\mathbb{D} + \mathbb{C}\mathbb{E}$,
- $(\mathbb{B}\mathbb{C})\mathbb{D} = \mathbb{B}(\mathbb{C}\mathbb{D})$,
- $s(\mathbb{A}\mathbb{B}) = (s\mathbb{A})\mathbb{B} = \mathbb{A}(s\mathbb{B})$,
- $(\mathbb{A}\mathbb{B})^T = \mathbb{B}^T\mathbb{A}^T$,
- $\mathbb{I}_m\mathbb{A} = \mathbb{A} = \mathbb{A}\mathbb{I}_n$.

Dál je dobré vědět, co je permutační matice, horní a dolní trojúhelníková matice. Součin těchto stejných dvou dá vždy takovou.

Definice Matice \mathbb{A} je *invertovatelná*, pokud je čtvercová a existuje matice \mathbb{X} taková, že $\mathbb{A}\mathbb{X} = \mathbb{X}\mathbb{A} = \mathbb{I}_n$. Pak matici \mathbb{X} značíme \mathbb{A}^{-1} a nazýváme *inverzem* k matici \mathbb{A} .

Věta (o invertovatelnosti a regularitě) Každá invertovatelná matice je regulární.

Ano, regularita ještě nebyla "zavedená", ale tohle je podle mě fajn vědět už tady.

Věta (o jednoznačnosti inverzu) Nechť \mathbb{A} je čtvercová matice a nechť \mathbb{X} a \mathbb{Y} jsou čtvercové matice takové, že platí $\mathbb{Y}\mathbb{A} = \mathbb{I}_n$ a $\mathbb{A}\mathbb{X} = \mathbb{I}_n$, pak $\mathbb{X} = \mathbb{Y}$.

Věta (vlastnosti inverzu) Nechť \mathbb{A}, \mathbb{B} jsou regulární, pak platí

- matice \mathbb{A}^{-1} je regulární a platí $(\mathbb{A}^{-1})^{-1} = \mathbb{A}$,
- matice \mathbb{A}^T je regulární a platí $(\mathbb{A}^T)^{-1} = (\mathbb{A}^{-1})^T$,
- matice $t\mathbb{A}$ je regulární a platí $(t\mathbb{A})^{-1} = t^{-1}\mathbb{A}^{-1}$,
- matice $\mathbb{A}\mathbb{B}$ je regulární a platí $(AB)^{-1} = A^{-1}B^{-1}$.

2.1.2 Hodnost matice

Definice *Hodnost matice* je počet nenulových řádků v matici v odstupňovaném tvaru. Značíme $\text{rank}(\mathbb{A})$.

Odstupňovaný tvar v pozdějších kapitolách. Fakt nevím proč je to seřazený takhle.

Definice *Hodnost matice* je dimenze řádkového a sloupcového prostoru matice.

Věta (o hodnosti matice) Platí $\text{rank}(\mathbb{A}) = \text{rank}(\mathbb{A}^T) \leq m, n$. Hodnost se nemění elementárními řádkovými úpravami.

Věta (o hodnosti součinu) platí $\text{rank}(\mathbb{A}\mathbb{B}) \leq \text{rank}(\mathbb{A}), \text{rank}(\mathbb{A}\mathbb{B}) \leq \text{rank}(\mathbb{B})$. Pokud je matice \mathbb{R} regulární, pak platí $\text{rank}(\mathbb{R}\mathbb{A}) = \text{rank}(\mathbb{A}\mathbb{R}) = \text{rank}(\mathbb{A})$.

Věta (o hodnosti čtvercové matice) Matice \mathbb{A} je regulární matice typu $n \times n$ právě tehdy, když $\text{rank}(\mathbb{A}) = n$.

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

2.1.3 Soustavy lineárních rovnic, Gaussova eliminace, podmínky řešitelnosti

Definice Lineární rovnice je rovnice tvaru $a_1x_1 + \dots + a_nx_n = b$, kde a_1, \dots, a_n, b jsou dané konstanty a x_1, \dots, x_n jsou neznámé.

Definice Soustavou lineárních rovnic rozumíme soustavu tvaru

$$\begin{array}{lcl} a_{11}x_1 + \dots + a_{1n}x_n & = & b_1 \\ \vdots & & \vdots \quad \vdots \\ a_{n1}x_1 + \dots + a_{nn}x_n & = & b_n \end{array},$$

kde $a_{11}, \dots, a_{nn}, b_1, \dots, b_n$ jsou dané konstanty a x_1, \dots, x_n jsou neznámé.

Definice Ekvivalentní úpravy jsou takové úpravy, které nemění množinu všech řešení. Symbol je pro ekvivalentní úpravy je \sim .

Definice Elementární úpravy nazýváme prohození dvou řádků, vynásobení řádku konstantou $t \neq 0$ a přičtení s -násobku jednoho řádku k jinému řádku.

Věta (o elementárních úpravách) Elementární úpravy jsou ekvivalentní.

Definice Rozšířená matice soustavy z definice je matice

$$\left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n1} & \dots & a_{nn} & b_n \end{array} \right).$$

Je-li $b = 0$, pak jde o homogenní soustavu.

Definice Matice v odstupňovaném tvaru je matice typu $m \times n$ taková, která splňuje následující: existuje $r \in \{0, 1, \dots, m\}$ takové, že řádky $r+1, \dots, m$ jsou nulové a pro indexy sloupců s prvním nenulovým číslem platí $k_1 < k_2 < \dots < k_r$.

Gaussova eliminace je proces pro převod matice do odstupňovaného tvaru pomocí ekvivalentních úprav. Eliminace jednoho sloupce funguje následujícím způsobem:

1. Najdeme první nenulový sloupec s indexem k_1 . Pokud nenulový sloupec neexistuje, pak je matice nulová a tím pádem v odstupňovaném tvaru.
2. Pokud $a_{1k_1} = 0$, pak prohodíme první řádek s libovolným řádkem i , kde $a_{ik_1} \neq 0$. Výběr specifického řádku závisí na implementaci.
3. Pro každé $i = 2, 3, \dots, m$ přičteme $\left(-\frac{a_{ik_1}}{a_{1k_1}}\right)$ -násobek prvního řádku k i -tému řádku.
4. Postup dále opakujeme s maticí bez prvního řádku.

Věta (o Gaussově eliminaci) Gaussova eliminace vždy převede matici do odstupňovaného tvaru.

Definice *Hodnost matice* je počet nenulových řádků po Gaussově eliminaci.

Definice *Bázové sloupce* jsou sloupce s indexy k_1, \dots, k_r .

Věta (řešitelnost) Po použití Gaussovy eliminace na rozšířenou matici soustavy $(\mathbb{A}|b)$. Pokud b bude bázový sloupec, tak nastává situace $0x_1 + \dots + 0x_n = d_r$ a soustava nemá řešení. V opačném případě řešení mám.

Způsob pro nalezení je *zpětná substituce*. Nechť P jsou nebázové sloupce. Pak $x_p, p \in P$ jsou *volné proměnné*, neboli *parametry*. Platí, že každá volba hodnot volných proměnných dává právě jedno řešení. Množina řešení pak vypadá následovně

$$\{u + \sum_{p \in P} t_p v_p : t_p \in \mathbb{R} \ \forall p \in P\}.$$

Věta (řešitelnost) Soustava je řešitelná právě tehdy, když b je lineární kombinací sloupců z \mathbb{A} .

Věta (Frobeniova) Soustava je řešitelná právě tehdy, když $\text{rank}(\mathbb{A}) = \text{rank}(\mathbb{A}|b)$.

Věta (o všech řešeních) Nechť $u = (x_1, \dots, x_n)$ je řešení soustavy $\mathbb{A}x = b$ a $W_{\mathbb{A}}$ je množina všech řešení homogenní soustavy. Pak $u + W_{\mathbb{A}}$ je množina všech řešení soustavy.

2.1.4 Determinanty a metody jejich výpočtu

Definice *Permutací* množiny X je bijekce $X \rightarrow X$. Symbolem S_X je množina všech permutací na X .

Věta (vlastnosti permutace)

- i. $\pi \in S_X \Rightarrow \pi^{-1} \in S_X$,
- ii. $\pi, \rho \in S_X \Rightarrow \pi \circ \rho \in S_X$.

Definice Zápis permutace na množině $X = (s_1, \dots, s_n)$ je tvaru

$$\begin{pmatrix} s_1 & s_2 & \dots & s_n \\ t_1 & t_2 & \dots & t_n \end{pmatrix}.$$

V případě na množině $X = (1, 2, \dots, n)$ tedy

$$\begin{pmatrix} 1 & 2 & \dots & n \\ t_1 & t_2 & \dots & t_n \end{pmatrix},$$

tj. $\pi(i) = t_i$.

Definice Cyklus délky k je permutace splňující $\pi(x_1) = x_2, \pi(x_2) = x_3, \dots, \pi(x_k) = x_1$ a $\pi(y) = y, \forall y \notin \{x_1, \dots, x_k\}$. Permutaci tvořenou jedním cyklem značíme následovně $\pi = (x_1 x_2 \dots x_k)$.

Definice Dva cykly jsou *nezávislé*, pokud množiny prvků v cyklech jsou disjunktní.

Definice Transpozice je cyklus délky dva.

Věta (rozklad permutace) Každou permutaci lze zapsat jako složení nezávislých cyklů. Tento zápis je jednoznačný až na pořadí cyklů a nazývá se *cyklický*.

Věta (o transpozicích) Každá permutace je složení transpozic.

Zápis složením transpozic se dá zapsat různými způsoby, ale jeho parita (sudost/lichost počtu transpozic v zápisu).

Definice Znaménko permutace se značí $\text{sgn}\pi$ a je definováno jako 1, pokud je permutace *sudá*, tedy má sudý počet transpozic, a jako -1, pokud je permutace *lichá*, tedy má lichý počet transpozic.

Věta (výpočet znaménka permutace) Nechť pro permutaci π platí $\pi = \pi_1 \pi_2 \dots \pi_m$ rozklad na cykly s délkami k_1, k_2, \dots, k_m . Pak $\text{sgn}(\pi) = \prod_{i=1}^m (-1)^{(k_i-1)}$.

Věta (výpočet znaménka permutace II.) Platí

- i. $\text{sgn}(\text{id})=1$,
- ii. $\text{sgn}(\pi^{-1})=\text{sgn}(\pi)$,
- iii. $\text{sgn}(\pi\rho)=\text{sgn}(\pi)\text{sgn}(\rho)$.

Definice Determinant matice \mathbb{A} je definován následovně

$$\det \mathbb{A} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \sum_{\pi \in S_n} \text{sgn}(\pi) a_{1r_1} a_{2r_2} \dots a_{nr_n},$$

kde

$$\pi = \begin{pmatrix} 1 & \dots & n \\ r_1 & \dots & r_n \end{pmatrix}.$$

Věta (výpočet determinantu) Platí

- i. pro horní trojúhelníkovou matici je determinant součin prvků na diagonále,
- ii. $\det(\mathbb{A}^T)=\det(\mathbb{A})$,
- iii. $\det(v_1|v_2|\dots|v_i+u|\dots|v_n) = \det(v_1|v_2|\dots|v_i|\dots|v_n) + \det(v_1|v_2|\dots|u|\dots|v_n)$,
- iv. $\det(v_1|v_2|\dots|t \times v_i|\dots|v_n) = t \times \det(v_1|v_2|\dots|v_i|\dots|v_n)$,

v. Pokud matice \mathbb{B} vznikne permutací π sloupců matice \mathbb{A} , pak
 $\det(\mathbb{B}) = \det(\mathbb{A})\text{sgn}(\pi)$.

Věta (o regularitě) Matice \mathbb{A} je regulární právě tehdy, když má nenulový determinant.

Definice Minor matice \mathbb{A} typu $m \times n$ je determinant matice vzniklé z matice \mathbb{A} výběrem k sloupců a k řádků.

Věta (o determinantu součinu) Nechť pro matice \mathbb{A} a \mathbb{B} existuje jejich součin. Pak platí $\det(\mathbb{A}\mathbb{B}) = \det(\mathbb{A})\det(\mathbb{B})$.

Věta (o determinantu inverzu) Nechť je matice \mathbb{A} invertibilní. Pak platí $\det(\mathbb{A}^{-1}) = \det(\mathbb{A})^{-1}$.

Věta (Cramérovo pravidlo) Nechť je matice \mathbb{A} regulární a $\mathbb{A}x = b$. Pak vektor x lze vypočítat jako

$$x_j = \frac{\det \mathbb{A}_j}{\det \mathbb{A}},$$

kde \mathbb{A}_j je matice \mathbb{A} , která má místo j -tého sloupce vektor b .

Definice Nechť \mathbb{A} je čtvercová matice řádu n , a a_{ij} je její prvek. *Algebraický doplněk* matice \mathbb{A} prvku a_{ij} je prvek

$$\mathbb{A}_{ij} = (-1)^{i+j} \det(\mathbb{M}_{ij}),$$

kde \mathbb{M}_{ij} je matice \mathbb{A} bez i -tého řádku a j -tého sloupce.

Věta (rozvoj podle sloupce) Nechť je matice \mathbb{A} čtvercová řádu n . Pak platí

$$\det \mathbb{A} = \sum_{i=1}^n a_{ij} \mathbb{A}_{ij}.$$

S použitím transpozice se dá odvodit i pravidlo pro rozvoj podle řádku:

$$\det \mathbb{A} = \sum_{j=1}^n a_{ij} \mathbb{A}_{ij}.$$

Věta (o falešném rozvoji) Platí $\sum_{i=1}^n a_{ij} \mathbb{A}_{ik} = 0$, když $j \neq k$.

Definice *Adjungovaná matice* k matici \mathbb{A} je matice $\text{adj}(\mathbb{A})$ která má na místě (i,j) prvek \mathbb{A}_{ji} .

Věta (o adjungované matici) Platí $\text{adj}(\mathbb{A}) \cdot \mathbb{A} = \mathbb{A} \cdot \text{adj}(\mathbb{A}) = \det(\mathbb{A}) \mathbb{I}_n$, tj. pro regulární matici \mathbb{A} platí

$$\mathbb{A}^{-1} = \frac{\text{adj} \mathbb{A}}{\det \mathbb{A}}.$$

2.2 Vektorové prostory

2.2.1 Pojem vektorového prostoru, lineární nezávislost, lineární obal, báze a dimenze

Definice *Těleso* je množina prvků T s operacemi sčítání $+ : T \times T \rightarrow T$ a násobení $\cdot : T \times T \rightarrow T$ splňující:

- $a + b \in T, a \cdot b \in T, \forall a,b \in T,$
- *asociativita*: $(a + b) + c = a + (b + c), (a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a,b,c \in T,$
- *komutativita*: $a + b = b + a, a \cdot b = b \cdot a, \forall a,b \in T,$
- *existence nulového prvku*: $\exists 0 \in T : a + 0 = a,$
- *existence jednotkového prvku*: $\exists 1 \in T : 1 \cdot a = a,$
- *existence opačného prvku*: $\forall a \in T \exists (-a) \in T : a + (-a) = 0,$
- *existence inverzu*: $\forall a \in T \exists a^{-1} \in T : a \cdot a^{-1} = 1,$
- *distributivita*: $(a + b) \cdot c = ac + bc, c \cdot (a + b) = ca + cb.$

Definice *Vektorový prostor nad T* je neprázdná množina V se sčítáním $+ : V \times V \rightarrow V$ a násobením skalárem $\cdot : T \times V \rightarrow V$, splňující

- *komutativita*: $u + v = v + u, \forall u,v \in V,$
- *asociativita*: $u + (v + w) = (u + v) + w, \forall u,v,w \in V,$
- *existence nulového prvku*: $\exists \mathbb{0} \in V : 0 \cdot u = \mathbb{0},$
- $r(u + v) = ru + rv, \forall r \in T, \forall u,v \in V,$
- $(r + s)u = ru + su, \forall r,s \in T, \forall u \in V,$
- $r(su) = (rs)u, \forall r,s \in T, \forall u \in V,$
- $1 \cdot u = u.$

Prvky T nazýváme *skaláry*, prvky V nazýváme *vektory*.

Definice Nechť V je vektorový prostor nad tělesem T a $X \subseteq V$. *Lineárním obalem* množiny X rozumíme

$\langle X \rangle = \{t_1v_1 + \dots + t_kv_k; k \in \mathbb{N}_0, v_1, \dots, v_k \in X, t_1, \dots, t_k \in T\}$, tj. lineární kombinace všech prvků množiny X .

Tvrzení (o lineárním obalu) Nechť V je vektorový prostor nad tělesem T a $X \subseteq V$, pak $\langle X \rangle$ je podprostor V .

Definice Nechť V je vektorový prostor nad tělesem T a $X \subseteq V$. Pokud $\langle X \rangle = V$, pak X nazveme *množinou generátorů* prostoru V .

Definice Sloupcový (řádkový) prostor matice je lineární obal jejích sloupců (řádků), značíme $\text{Im}(\mathbb{A})$, resp. $\text{Im}(\mathbb{A}^T)$.

Věta (o sloupcových (řádkových) prostorech) Nechť \mathbb{A} je matice typu $m \times n$ a \mathbb{R} je matice typu $m \times m$ regulární. Pak $\text{Im}(\mathbb{R}\mathbb{A}) = \langle \mathbb{R}a_1, \mathbb{R}a_2, \dots, \mathbb{R}a_n \rangle$. Platí, že elementární sloupcové (řádkové) úpravy nemění sloupcový (řádkový) prostor.

Definice Řekneme, že posloupnost prvků z V je *lineárně závislá*, pokud pro nějaké i platí, že v_i je lineární kombinací $v_1, v_2, \dots, v_{i-1}, v_{i+1}, \dots, v_n$. V opačném případě řekneme, že je *lineárně nezávislá*.

Věta (o nezávislosti) Platí, že posloupnost $\{v_1, \dots, v_n\}$ je lineárně nezávislá právě tehdy, když 0 lze vyjádřit pouze jako $0 \cdot v_1 + 0 \cdot v_2 + \dots + 0 \cdot v_n$.

Tvrzení (o nezávislosti sloupců matice) Sloupce matice jsou nezávislé, pokud jádro matice je 0 , tedy $\mathbb{A}x = 0$ má právě jedno řešení, tj. $x = 0$.

Tvrzení (nezávislost a elementární úpravy) Elementární řádkové i sloupcové úpravy nemění nezávislost řádků i sloupců matice.

Definice Báze vektorového prostoru V je posloupnost (v_1, \dots, v_n) , která je lineárně nezávislá a pro kterou platí $\langle v_1, \dots, v_n \rangle = V$.

Věta (o bázi) Platí

- báze je minimální posloupnost generátorů,
- z každé množiny generátorů prostoru lze vybrat bázi,
- každý konečně generovaný prostor má bázi.

Definice Dimenze konečně generovaného prostoru V je počet prvků jeho báze.

Věta (o bázi) Maximální lineárně nezávislá posloupnost ve vektorovém prostoru je báze.

Věta (o prostoru dimenze n) Každá množina generátorů prostoru dimenze n má alespoň n prvků a každá n -prvková lineárně nezávislá posloupnost je báze.

Definice Nechť $B = (v_1, \dots, v_n)$ báze V , $w \in V$. Souřadnice w vzhledem k B jsou prvky (a_1, \dots, a_n) takové, že $w = a_1v_1 + a_2v_2 + \dots + a_nv_n$, značíme $[w]_B$.

Vlastnosti souřadnic Platí

- $[u + w]_B = [u]_B + [w]_B$,
- $[tu]_B = t[u]_B$.

Definice Matici přechodu mezi bázemi $B = (v_1, \dots, v_n)$ a $C = (w_1, \dots, w_l)$ je

$$[id]_C^B = ([v_1]_C, [v_2]_C, \dots, [v_n]_C).$$

Věta (o přechodu mezi bázemi) Platí $[x]_C = [id]_C^B[x]_B$.

2.2.2 Steinitzova věta o výměně

Věta (Steinitzova o výměně) Nechť $N = (v_1, \dots, v_k)$ je lineárně nezávislá posloupnost prvků lineárního prostoru V nad tělesem T a nechť $G = (w_1, \dots, w_l)$ generuje V . Pak $k \leq l$ a při vhodném uspořádání $G' = (w'_1, \dots, w'_l)$ posloupnosti G platí, že $(v_1, \dots, v_k, w'_{k+1}, \dots, w'_l)$ generuje V .

Zde je vhodné znát celý důkaz. Není nijak složitý, ale nechce se mi psát. Je ve skriptech z LA.

Důsledek I. Každé dvě báze mají stejný počet prvků.

Důsledek II. Každou lineárně nezávislou posloupnost lze doplnit na bázi prvky z libovolné množiny generátorů.

Důsledek III. Maximální posloupnost lineárně nezávislých prvků v konečně generovaném prostoru je bází.

2.2.3 Podprostory a jejich dimenze

Definice Řekneme, že U je podprostor lineárního prostoru V , pokud $U \subseteq V$ a je uzavřená na operace sčítání a násobení skalárem. Značíme $U \leq V$.

Věta (o jádru matice) Pro libovolnou matici typu $m \times n$ nad tělesem T platí, že její jádro je podprostor T^n .

Věta (o lineárním obalu) Nechť $X \subseteq V$, pak $\langle X \rangle$ je podprostor V .

Věta (o řádkovém a sloupcovém prostoru matice) Pro libovolnou matici typu $m \times n$ nad tělesem T platí, že její řádkový a sloupcový prostor jsou podprostory T^n , resp. T^m .

Definice Sloupec matice nazveme bázový, pokud není lineární kombinací předchozích sloupců.

Věta (o bázový sloupcích) Bázové sloupce matice tvoří bázi sloupcového prostoru matice.

Věta (o dimenzi řádkového a sloupcového prostoru) Platí $\dim(\text{Im } A) = \dim(\text{Im } A^T)$.

Definice Hodnost matic je dimenze jejího řádkového (nebo sloupcového) prostoru.

Věta (průnik podprostorů) Nechť I je indexová množina a $V_i, i \in I$ jsou podprostory lineárního prostoru V , pak i

$$\bigcap_{i \in I} V_i$$

je podprostor V .

Definice Nechť I je indexová množina a $V_i, i \in I$ jsou podprostory lineárního prostoru V . Pak jejich součet definujeme jako

$$\sum_{i \in I} V_i = \langle \bigcup_{i \in I} V_i \rangle.$$

Věta (o dimenzi součtu a průniku) Pro U, V podprostory lineárního prostoru W platí

$$\dim(U) + \dim(V) = \dim(U \cap V) + \dim(U \cup V).$$

Věta (o dimenzi podprostoru) Nechť U je podprostor V , pak $\dim(U) \leq \dim(V)$.

2.2.4 Skalární součin, ortogonalizační proces, ortonormální báze

Definice Nechť $v = (v_1, \dots, v_n)$ a $u = (u_1, \dots, u_n)$ jsou vektory nad \mathbb{R} . Standardní skalární součin je $u \cdot v = u_1 v_1 + \dots + u_n v_n$.

Definice Eukleidovská norma (délka) vektoru u je $\|u\| = \sqrt{u \cdot u}$.

Definice Úhel mezi vektory u a v je číslo α definované jako

$$u \cdot v = \|u\| \cdot \|v\| \cdot \cos \alpha.$$

Dva vektory jsou kolmé, pokud $u \cdot v = 0$.

Věta (vlastnosti skalárního součinu nad \mathbb{R}) Nechť u, v, w jsou vektory nad \mathbb{R} a t je skalár. Platí

- $u \cdot v = v \cdot u$,
- $u \cdot (tv) = t(u \cdot v)$,
- $u \cdot (v + w) = u \cdot v + u \cdot w$,
- $u \cdot u \geq 0$ a $u \cdot u = 0 \Leftrightarrow u = 0$.

Definice Nechť $v = (v_1, \dots, v_n)$ a $u = (u_1, \dots, u_n)$ jsou vektory nad \mathbb{C} . Standardní skalární součin je $u \cdot v = \bar{u}_1 v_1 + \dots + \bar{u}_n v_n$.

Definice Hermitovsky sdružená matice k matici $\mathbb{A} = (a_{ij})_{m \times n}$ je matice $\mathbb{A}^* = (b_{ji})_{n \times m}$, kde $b_{ji} = \overline{a_{ij}}$.

Věta (vlastnosti skalárního součinu nad \mathbb{C}) Nechť u, v, w jsou vektory nad \mathbb{C} a t je skalár. Platí

- $u \cdot v = \overline{v \cdot u}$,
- $u \cdot (tv) = t(u \cdot v)$,
- $u \cdot (v + w) = u \cdot v + u \cdot w$,
- $u \cdot u \geq 0$, $\in \mathbb{R}$ a $u \cdot u = 0 \Leftrightarrow u = 0$.

Definice Nechť V je vektorový prostor nad \mathbb{R} nebo \mathbb{C} . Obecný skalární součin definujeme jako zobrazení $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{R}$ nebo \mathbb{C} , splňující

- i. $\langle u, v \rangle = \overline{\langle v, u \rangle}$,
- ii. $\langle u, tv \rangle = t\langle u, v \rangle$,
- iii. $\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle$,
- iv. $\langle u, u \rangle \geq 0$ a $\langle u, u \rangle = 0 \Leftrightarrow u = 0$.

Definice Hermitovská matice je taková komplexní matice, která splňuje $\mathbb{A}^* = \mathbb{A}$.

Definice Pozitivně definitní matice je taková matice \mathbb{A} , která splňuje $u^* \mathbb{A} u \geq 0$ a $u^* \mathbb{A} u = 0 \Leftrightarrow u = 0$.

Věta (o skalárním součinu daném maticí) Nechť $\mathbb{A} \in \mathbb{R}^{n \times n}$, resp. $\mathbb{C}^{n \times n}$. Pak $\langle u, v \rangle = u^* \mathbb{A} v$ je skalární součin právě tehdy, když je \mathbb{A} hermitovská, pozitivně definitní.

Definice Obecná norma je definovaná jako $\|u\| = \sqrt{\langle u, u \rangle}$. Řekneme, že vektor je jednotkový, pokud platí $\|u\| = 1$.

Věta (vlastnosti normy) Nechť u, v jsou vektory a t je skalár. Pak platí

- i. $\|u\| \geq 0$ a $\|u\| = 0 \Leftrightarrow u = 0$,
- ii. $\|tu\| = |t|\|u\|$,
- iii. rovnoběžníkové pravidlo $\|u + v\|^2 + \|u - v\|^2 = 2(\|u\|^2 + \|v\|^2)$.

Věta (Cauchyho-Schwartzova nerovnost) Nechť u, v jsou vektory. Platí

$$|\langle u, v \rangle| \leq \|u\| \cdot \|v\|.$$

Rovnost platí právě tehdy, když jsou vektory u a v lineárně závislé.

Věta (Trovjúhelníková nerovnost) Nechť u, v jsou vektory. Pak platí

$$\|u + v\| \leq \|u\| + \|v\|.$$

Definice Úhel mezi vektory u a v je číslo $\alpha \in (0, \pi)$ splňující

$$\cos \alpha = \frac{\langle u, v \rangle}{\|u\| \cdot \|v\|}.$$

Věta (cosinová) Nechť u, v jsou vektory a α úhel mezi nimi. Pak platí

$$\|u - v\|^2 = \|u\|^2 + \|v\|^2 - 2\|u\| \cdot \|v\| \cos \alpha.$$

Definice Řekneme, že vektory u a v jsou *kolmé*, pokud platí $\langle u, v \rangle = 0$.

Definice Řekneme, že množina vektorů M je *ortogonální*, pokud každé dva její prvky jsou na sebe kolmé.

Definice Řekneme, že množina vektorů M je *ortonormální*, pokud je ortogonální a tvořena jednotkovými vektory.

Věta (o ortogonální posloupnosti) Každá ortogonální posloupnost je lineárně nezávislá.

Věta (o kanonické bázi) Kanonická báze je ortonormální.

Věta (Pythagorova) Pokud jsou u, v kolmé vektory, pak $\|u + v\|^2 = \|u\|^2 + \|v\|^2$.

Věta (souřadnice vzhledem k ortonormální bázi) Nechť $B = (v_1, \dots, v_n)$ je ortonormální báze lineárního prostoru V a $u \in V$. Pak platí

$$u = \langle v_1, u \rangle v_1 + \dots + \langle v_n, u \rangle v_n.$$

Věta (skalární součin a ortonormální báze) Nechť B je ortonormální báze vektorového prostoru V a $u, v \in V$. Pak platí $\langle u, v \rangle = [u]_B^* [v]_B$.

Gramova - Schmidtova ortogonalizace je proces který z libovolné lineárně nezávislé posloupnosti vektorů udělá ortonormální posloupnost generující stejný prostor. Vstupem je lineárně nezávislá posloupnost $\{v_1, \dots, v_n\}$. Algoritmus postupuje ve třech krocích:

1. $u_1 = \frac{v_1}{\|v_1\|},$
2. $u'_i = v_i - \langle u_1, v_i \rangle u_1 - \dots - \langle u_{i-1}, v_i \rangle u_{i-1},$
3. $u_i = \frac{u'_i}{\|u'_i\|}.$

$\forall i \in \{2, \dots, n\}$. Výstupem je ortonormální posloupnost $\{u_1, \dots, u_n\}$ taková, že $\langle v_1, \dots, v_n \rangle = \langle u_1, \dots, u_n \rangle$.

Věta (o Gramově-Schmidtově ortogonalizaci) Převede tímto způsobem každou lineárně nezávislou posloupnost.

Důsledek V každém konečně dimenzionálním prostoru se skalárním součinem existuje ortonormální báze.

2.2.5 Ortogonální projekce, metoda nejmenších čtverců a pseudoinverze

Definice Nechť V je vektorový prostor se skalárním součinem, $v \in V$ a W je podprostor V . Prvek $w \in W$ nazýváme *ortogonální projekce* vektoru v na podprostor W , jestliže $(v - w) \perp W$.

Věta (o approximaci) Je-li W podprostor V , $v \in V$ a w je ortogonální projekce v na W , pak $\forall u \in W, u \neq w$ platí $\|u - w\| < \|v - u\|$, tedy ortogonální projekce je určena jednoznačně.

Zde je jednoduchý důkaz, dobré vědět.

Věta (o projekci a bázi) Nechť V je vektorový prostor, $v \in V$ a W je konečně generovaný podprostor V s ortonormální bází $B = (u_1, \dots, u_k)^T$. Pak prvek

$$w = \langle u_1, v \rangle u_1 + \langle u_2, v \rangle u_2 + \dots + \langle u_k, v \rangle u_k$$

je ortogonální projekcí v na W .

Důsledek Pro ortogonální bázi to je

$$w = \frac{\langle u_1, v \rangle}{\|u_1\|^2} u_1 + \frac{\langle u_2, v \rangle}{\|u_2\|^2} u_2 + \dots + \frac{\langle u_k, v \rangle}{\|u_k\|^2} u_k.$$

Definice Nechť $\mathbb{A} \in \mathbb{C}^{n \times m}$ a $b \in \mathbb{C}^n$. *Problém nejmenších čtverců* (LS) je úloha určení $x \in \mathbb{C}^m$ takového, které minimalizuje $\|f\|_E$ za podmínky $\mathbb{A}x = b + f$.

Téma *metody nejmenších čtverců a pseudoinverze* nemám zpracované dobře a rozhodně se tím nebudu chlubit. Takže si to udělejte sami. Love.

2.2.6 Diagonalizace a ortogonální diagonalizace

Věta (mocnění diagonální matice) $[diag(a_1, \dots, a_k)]^n = diag(a_1^n, \dots, a_k^n)$.

Definice Matice $A \in T^{n \times n}$ je *diagonalizovatelná*, má-li vůči nějaké bázi diagonální matici.

Věta (o diagonalizovatelnosti matice) Matice A je diagonalizovatelná právě tehdy, když existuje báze prostoru T^n tvořena vlastními vektory matice A .

Definice Matice X a Y téhož rádu nad týmž tělesem se nazývají *podobné*, existuje-li regulární matice R taková, že $Y = R^{-1}XR$.

Věta (diagonalizovatelnost a podobnost) Čtvercová matice je diagonalizovatelná právě tehdy, když je podobná nějaké diagonální matici.

Věta (diagonalizovatelnost a vlastní čísla) Nechť matice A rádu n má n navzájem různých vlastních čísel. Pak je diagonalizovatelná.

Věta (o diagonalizovatelnosti a násobnosti) Buď A čtvercová matice rádu n nad T . Pak následující je ekvivalentní

- i. A diagonalizovatelná,
- ii. A má n vlastních čísel včetně algebraických násobností a geometrická násobnost každého vlastního čísla je rovna algebraické.

Definice Řekneme, že reálná (komplexní) čtvercová matice A je *ortogonálně (unitárně) diagonalizovatelná*, existuje-li ortonormální báze B prostoru \mathbb{R}^n (\mathbb{C}^n), že $[f_A]_B^B$ je diagonální.

Definice Matice X a Y jsou *ortogonálně (unitárně) podobné*, existuje-li ortogonální (unitární) matice U taková, že $Y = U^{-1}XU$ ($Y = U^*XU$).

Věta (o ortogonální diagonalizovatelnosti) Nechť A je čtvercová matice nad \mathbb{R} (\mathbb{C}). Pak následující je ekvivalentní

- i. A je ortogonálně (unitárně) diagonalizovatelná,
- ii. \mathbb{R}^n (\mathbb{C}^n) má ortonormální bázi tvořenou vlastními vektory matice A ,
- iii. A je ortogonálně (unitárně) podobná diagonální matici.

Věta (o ortogonální diagonalizovatelnosti II.) A čtvercová nad \mathbb{R} (\mathbb{C}). Pak následující je ekvivalentní

- i. A ortogonálně (unitárně) diagonalizovatelná,
- ii. A má

- n vlastních čísel včetně algebraických násobností,
- geometrická násobnost každého vlastního čísla je rovna algebraické,
- pro každá dvě různá vlastní čísla λ_i a λ_j platí $M_{\lambda_i} \perp M_{\lambda_j}$.

Definice A je *normální*, pokud $A^*A = AA^*$.

Věta (spektrální věta pro normální matice) Nechť A je čtvercová komplexní matice. Pak následující je ekvivalentní

- (i) A je unitárně diagonalizovatelná,
- (ii) A je normální.

Věta (spektrální věta pro hermitovské matice) Nechť A je čtvercová komplexní matice. Pak následující je ekvivalentní

- (i) A je unitárně diagonalizovatelná a všechna její vlastní čísla jsou reálná,
- (ii) A je hermitovská.

Věta (spektrální věta pro symetrické matice) Nechť A je čtvercová reálná matice. Pak následující je ekvivalentní

- (i) A je ortogonálně diagonalizovatelná,
- (ii) A je symetrická.

Věta (spektrální věta pro pozitivně (semi) definitní matice) Nechť A je čtvercová komplexní matice. Pak následující je ekvivalentní

- (i) A je unitárně diagonalizovatelná a všechna její vlastní čísla jsou reálná kladná (nezáporná),
- (ii) A je pozitivně (semi) definitní.

Věta (o hermitovské a pozitivně definitní matici) Nechť je matice A hermitovská (symetrická). Pak je pozitivně (semi) definitní právě tehdy, když má všechna vlastní čísla kladná (nezáporná).

Věta (spektrální věta pro unitární matice) Nechť A je čtvercová komplexní matice. Pak následující je ekvivalentní

- (i) A je unitárně diagonalizovatelná a pro všechna vlastní čísla platí $|\lambda| = 1$,
- (ii) A je unitární.

2.2.7 Různé typy rozkladů matic

Tahle kapitola je obecně dost nahovno a vůbec mě nebavila. Takže tyhle poznámky nejsou **vůbec** dobrý, ale za účelem kompletnosti to sem dám taky. Určitě se doporučuji tohle učit úplně odjinud a třeba si to sem k tomu dopsat. Nebo to zapálit.

Jordanův rozklad

- Jde o jisté zobecnění diagonalizovatelnosti.
- $A = RDR^{-1}$, R regulární matice, D blokově diagonální matice s Jordanova-vými buňkami

$$\begin{bmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ 0 & 0 & \lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \lambda \end{bmatrix},$$

D se nazývá *Jordanova matice*.

- λ_i v Jordanových blocích jsou vlastní čísla matice A .
- Jednomu vlastnímu číslu může patřit více bloků = geometrická násobnost vlastního čísla.
- Součet dimenzí těchto bloků je algebraická násobnost.
- Rozklad je jednoznačný až na pořadí buněk.
- Jordanův rozklad není stabilní.
- Vektory se hledají pomocí tzv. Jordanových řetízků

$$(A - \lambda I) v_1 = 0, \quad (A - \lambda I) v_2 = v_1, \dots$$

a pak se umístí do matice R .

L-U rozklad

- Pouze pro čtvercové regulární matice.
- L-U rozklad není jednoznačný.
- Pokud se při Gaussově eliminaci nemusí prohazovat řádky, pak $A = LU$, L je dolní trojúhelníková matice s jedničkami na diagonále, U horní trojúhelníková matice s nenulovými čísly na diagonále. Jedná se o zápis Gaussovy eliminace - každý její krok je přenásobení maticí zleva a ty dohromady dají matici L .
- Pokud je při Gaussově eliminaci potřeba prohazovat řádky, pak $PA = LU$, kde P je permutační matice.

QR rozklad

- Pro obecnou komplexní matici.
- Je dražší, ale stabilnější, než L-U rozklad.
- Je jednoznačný.
- Jedná se o maticový zápis Gram-Schmidtovy ortogonalizace.
- $A = QR$, kde Q je ortonormální matice a R je dolní trojúhelníková matice.
- Postup je Gram-Schmidtův ortogonalizační proces na sloupce matice A dá sloupce matice $Q = (u_1, \dots, u_k)$

$$R = \begin{bmatrix} ||u'_1|| & \langle u_1, v_2 \rangle & \dots & \langle u_1, v_k \rangle \\ 0 & ||u'_2|| & \dots & \langle u_2, v_k \rangle \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & ||u'_k|| \end{bmatrix}.$$

- Obecně se ho dá docílit pomocí Givensových rotací či Householderových reflexí.

Spektrální rozklad

- Pro A normální, hermitovskou pozitivně definitní, s vlastními čísly $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_r = 0$ a $\lambda_{r+1} = \dots = \lambda_n = 0$.
- $A = UDU^*$, U je unitární a D je diagonální.
- U je složená z vlastních vektorů matice A .
- D má vlastní čísla matice A na diagonále.
- Užitečný rozklad pro inverz, $A^{-1} = U^*D^{-1}U$.

Singulární rozklad

- Pro obecnou komplexní matici.
- Platí A^*A i AA^* jsou Hermitovské pozitivně definitní, mají stejná vlastní čísla a když v_j je vlastní vektor A^*A , pak $Av_j/\sqrt{\lambda_j}$ je vlastní vektor matice AA^* $\forall j = 1, \dots, r$.
- u_{r+1}, \dots, u_n pak najdeme jako libovolnou ortonormální bázi ortogonálního doplňku.
- Singulární čísla $\sigma_j = \sqrt{\lambda_j}$, pak platí $Av_j = \sigma_j u_j \quad \forall j = 1, \dots, r$, pak $AV = U\Sigma$, tj. $A = U\Sigma V^*$, kde U, V jsou unitární a

$$\Sigma = \begin{bmatrix} \Sigma_r & \mathbb{O} \\ \mathbb{O} & \mathbb{O} \end{bmatrix}.$$

- Mooreova-Penroseova pseudoinverze: $A^+ = V\Sigma^+U^*$, kde

$$\Sigma^+ = \begin{bmatrix} \Sigma_r^{-1} & \mathbb{O} \\ \mathbb{O} & \mathbb{O} \end{bmatrix},$$

a tedy $A^+ = (A^*A^{-1})A^*$, $A^+ = (A^*)(AA^*)^{-1}$.

Choleského rozklad

- Jedná se o speciální případ L-U rozkladu.
- Pro $A \in \mathbb{C}^{n \times n}$ je hermitovská pozitivně definitní.
- $A = LL^*$, L horní trojúhelníková.

Schurův rozklad

- Pro obecnou čtvercovou matici.
- $A = URU^*$, U unitární, R horní trojúhelníková s vlastními čísly matice A na diagonále.

2.3 Lineární a bilineární formy

2.3.1 Lineární, bilineární a kvadratické formy, matice lineárních zobrazení, vlastní čísla lineárních zobrazení a matic, charakteristický polynom

Definice Zobrazení $f : V \rightarrow W$ se nazývá *lineární*, pokud splňuje $f(u) + f(v) = f(u + v)$ a $f(tu) = tf(u) \forall u, v \in V, \forall t \in T$.

Věta (zobrazení určené maticí) Zobrazení určené maticí A , $f_A(x) := Ax$, je lineární.

Definice Nechť $f : V \rightarrow W$ je lineární zobrazení, $B = (v_1, \dots, v_n)$ je báze prostoru V a C je báze W . Pak *matice f vzhledem k B a C* je

$$[f]_C^B = ([f(v_1)]_C | [f(v_2)]_C | \dots | [f(v_n)]_C).$$

Věta (o matici zobrazení) Platí $[f(x)]_C = [f]_C^B[x]_B$.

Věta (skládání lineárních zobrazení) Nechť U, V, W jsou vektorové prostory nad T , $f : U \rightarrow V$ a $g : V \rightarrow W$ jsou lineární, pak $gf : U \rightarrow W$ je lineární. Pokud navíc B je báze U , C je báze V a D je báze W , pak

$$[gf]_D^B = [g]_D^C [f]_C^B.$$

Věta (inverz lineárního zobrazení) Nechť $f : U \rightarrow V$ je vzájemně jednoznačné lineární zobrazení, pak $f^{-1} : V \rightarrow U$ je také lineární zobrazení a $[f^{-1}]_B^C = ([f]_C^B)^{-1}$.

Věta (o matici zobrazení a matici přechodů bází) Platí

$$[f]_B^B = ([id]_C^B)^{-1} \cdot [f]_C^C \cdot [id]_C^B.$$

Definice Nechť V je vektorový prostor nad tělesem T . Lineární zobrazení f nazveme *lineární forma*, je-li $f : V \rightarrow T$. *Jádrem* f jsou ty $x \in V$ že $f(x) = 0$ a *obraz* je $\{f(x), x \in V\}$.

Věta (o jádru a obraze) Nechť $f : V \rightarrow W$ je lineární zobrazení, B je báze U a C je báze V . Pak

$$[\text{Ker } f]_B = \text{Ker } [f]_C^B, [\text{Im } f]_C = \text{Im } [f]_C^B.$$

Definice Nechť f je lineární forma na V a B je báze V . Pak *matici f vzhledem k bázi B* je

$$[f]^B = (f(v_1), \dots, f(v_n)).$$

Definice *Bilineární forma* je zobrazení $f : V \times V \rightarrow T$ lineární v obou složkách. Pro bilineární formu f definujeme *kvadratickou formu* tvořenou f , $f_2 : V \rightarrow T$, $f_2(v) = f(v, v)$.

Definice Nechť $B = (v_1, \dots, v_n)$ je báze vektorového prostoru V nad tělesem T a nechť f je bilineární forma na V . *Maticí f vzhledem k B* je čtvercová matice rádu n kde na (i, j) místo je $f(v_i, v_j)$. Tuto matici značíme $[f]_B$.

Tvrzení (o matici bilineární formy) Platí $f(x, y) = [x]_B^T [f]_B [y]_B$.

Definice Řekneme, že bilineární forma f je *symetrická*, pokud $f(x, y) = f(y, x)$ a *antisymetrická*, pokud $f(x, y) = -f(y, x)$.

Věta (o (anti)symetrické formě) f je (anti)symetrická právě tehdy, když $[f]_B$ je (anti)symetrická matice.

Věta (o rozkladu bilineární formy) Nechť T je těleso charakteristiky různé od dvou. Pak existuje jednoznačný rozklad $f = f_s + f_a$, kde

$$f_s(x, y) = \frac{1}{2} (f(x, y) + f(y, x)), \quad f_a(x, y) = \frac{1}{2} (f(x, y) - f(y, x)).$$

Věta (součin matic a skládání zobrazení): Nechť $f_A : T^n \rightarrow T^m$ a $f_B : T^p \rightarrow T^n$. Pak $f_A f_B : T^p \rightarrow T^m$ a platí $f_A f_B = f_{AB}$.

Definice Nechť $f : V \rightarrow V$ je lineární operátor. Pak řekneme, že $\lambda \in T$ je *vlastní číslo* f , pokud existuje vektor $x \neq 0$ takový, že $f(x) = \lambda x$. Takové x nazýváme *vlastní vektor* f příslušný λ . Stejná definice platí i pro matice.

Věta (o vlastním čísle 0) Operátor f má vlastní číslo 0 právě tehdy, když f není prostý. Matice A má vlastní číslo 0 právě tehdy, když A je singulární.

Věta (o vlastních číslech a vektorech) Platí λ je vlastní číslo f právě tehdy, když $(f - \lambda \text{id})$ není prostý. Je-li λ vlastní číslo, pak množina M_λ všech vlastních vektorů je podprostor V a $M_\lambda = \text{Ker}(f - \lambda \text{id})$. To samé platí pro matice (místo "není prostý" je "singulární").

Věta (o vlastním číslu a determinantu) Nechť A je čtvercová řádu n nad tělesem T . Pak $\lambda \in T$ je vlastním číslem matice A právě tehdy, když $\det(A - \lambda I_n) = 0$. Nechť f je lineární operátor na konečně generovaném prostoru V dimenze n nad tělesem T a B je báze V . Pak $\lambda \in T$ je vlastním číslem operátoru f právě tehdy, když λ je vlastním číslem matice $[f]_B^B$.

Definice Charakteristický polynom matice A je $p_A(\lambda) = \det(A - \lambda I_n)$

Věta (charakteristický polynom podobných matic) Dvě podobné matice mají stejný charakteristický polynom.

Definice Charakteristický polynom operátoru f je $p_f(\lambda) = \det([f]_B^B - \lambda I_n)$

Definice Algebraická násobnost vlastního čísla je jeho násobnost jakožto kořene charakteristického polynomu.

Věta (o počtu vlastních čísel) Každá matice/operátor nad tělesem dimenze n má nejvýše n vlastních čísel včetně algebraických násobností.

2.3.2 Polární báze a zákon setrvačnosti pro kvadratické formy

Tato kapitola se zabývá pouze symetrickými bilineárními formami - ty jsou vzájemně jednoznačné s kvadratickými.

Definice Nechť f je symetrická bilineární forma na vektorovém prostoru V , $x, y \in V$. Řekneme, že x a y jsou *f-ortogonální*, pokud $f(x,y) = 0$. Řekneme, že báze $B = (v_1, \dots, v_n)$ prostoru V je *f-ortogonální*, pokud $f(v_i, v_j) = 0, \forall i \neq j$, tedy matice f vzhledem k B , $[f]_B$ je diagonální.

Definice Hodnota bilineární formy f je hodnota její matice k libovolné bázi.

Definice Polární báze vzhledem k f je libovolná f -ortogonální báze.

V téhle kapitole je vhodné vědět, jak dostat f -ortogonální bázi - tj. symetrické úpravy a tak.

Věta (o existenci polární báze) Každá symetrická bilineární forma f na konečně generovaném prostoru nad tělesem charakteristiky různé od dvou, má polární bázi.

Věta (zákon setrvačnosti kvadratických forem) Nechť f je symetrická bilineární forma na reálném vektorovém prostoru V dimenze n a C, C' jsou báze V takové, že

$$[f]_C = \text{diag}(\underbrace{1, \dots, 1}_k, \underbrace{-1, \dots, -1}_t, \underbrace{0, \dots, 0}_m)$$

$$[f]_{C'} = \text{diag}(\underbrace{1, \dots, 1}_{k'}, \underbrace{-1, \dots, -1}_{t'}, \underbrace{0, \dots, 0}_{m'})$$

Pak $k = k'$, $t = t'$ a $m = m'$.

Definice Čísla k , t a m z minulé věty nazveme *pozitivní index setrvačnosti* formy f , *negativní index* formy f a *nulita* formy f , značíme $n_+(f)$, $n_-(f)$ a $n_0(f)$. Uspořádanou trojici $(n_0(f), n_+(f), n_-(f))$ nazveme *signatura* formy f .

Definice Řekneme, že symetrická bilineární forma na reálném vektorovém prostoru je *pozitivně definitní* právě tehdy, je-li $f_2(x) > 0 \forall x \neq 0 \in V$.

Věta (o signatuře a pozitivní definitnosti) f pozitivně definitní právě tehdy, když $n_+(f) = n$.

Věta (o ortonormální diagonalizaci) Nechť V je reálný vektorový prostor dimenze n se skalárním součinem \langle , \rangle a f symetrická bilineární forma na V . Pak existuje báze B prostoru V , která je f -ortogonální a zároveň ortonormální vzhledem k \langle , \rangle .

2.3.3 Matice jednoduchých geometrických zobrazení

- otočení v \mathbb{R}^2 o úhel α :

$$\begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix}.$$

- osová symetrie vzhledem k ose x v \mathbb{R}^2 :

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

- symetrie vzhledem k přímce procházející středem, uzavírající úhel s osou x:

$$\begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{bmatrix} = \begin{bmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{bmatrix}.$$

- ortogonální projekce na osu x:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

- ortogonální projekce na přímku procházející středem, uzavírající úhel α s osou x:

$$\begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{bmatrix} = \begin{bmatrix} \cos^2 \alpha & \sin \alpha \cos \alpha \\ \sin \alpha \cos \alpha & \sin^2 \alpha \end{bmatrix}.$$

- Givensova rotace: otočení o úhel α vůči e_i, e_j

$$G_{ij}(\alpha) = \begin{bmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \dots & \cos \alpha & \dots & -\sin \alpha & \dots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \dots & \sin \alpha & \dots & \cos \alpha & \dots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{bmatrix}.$$

- Householderova reflexe: zrcadlení podle nadroviny dimenze $n - 1$ pomocí jejího normálového vektoru q , $\|q\| = 1$. Platí

$$x = (x - x_q) + x_q, \quad x_q = (qq^T)x,$$

pak zrcadlový je

$$y = (x - x_q) - x_q = (\mathbb{I} - 2qq^T)x.$$

Tedy

$$H(q) = (\mathbb{I} - 2qq^T).$$

2.4 Základy teorie grup a komutativních okruhů

2.4.1 Základní vlastnosti grup

Definice Grupa je algebra (množina s operacemi) $G = (G, *, ', e)$ typu (2,1,0) splňující $\forall a, b, c \in G$

- (1) $a * (b * c) = (a * b) * c$,
- (2) $\exists!e : a * e = e * a = a$,
- (3) $\exists!a' : a * a' = a' * a = e$,

tj. e je jednotka a a' inverzní prvek k prvku a . Grupa je *Abelovská*, pokud navíc $\forall a, b \in G : a * b = b * a$.

Definice Nechť G je grupa, pak $H \subseteq G$ je podgrupa, když $\forall a, b \in H$ je $a' \in H$, $a * b \in H$ a $e \in H$. Pak $H = (H, *|_H, '|_H, e)$. Podgrupy se dělí na *vlastní* a *nevlastní*. Nevlastní jsou podgrupy G a e , vlastní jsou všechny ostatní.

Definice Grupa je

- *aditivní*, pokud je tvaru $T = (T, +, -, 0)$,
- *multiplikativní*, pokud je tvaru $T^* = (T \setminus \{0\}, *, ^{-1}, 1)$,

pro libovolné těleso T .

Definice Cyklické grupy jsou $\mathbb{Z}_n = (\{0, 1, \dots, n-1\}, +_{\text{mod } n}, -_{\text{mod } n}, 0)$. Pak multiplikativní grupa \mathbb{Z}_n^* má právě prvky nesoudělné s $n \in \{1, \dots, n-1\}$.

Definice Definujeme grupy

- Symetrická grupa je grupa $S_X = (\{\pi : \pi \text{ permutace na } X\}, \circ, ^{-1}, id)$ s podgrupami
 - alternující podgrupa A_n všech sudých permutací,
 - dihedrální podgrupa D_{2n} všech symetrií pravidelného n -úhelníku.
- Maticová grupa je grupa $GL_n(T) = \{(A : A \in T^{n \times n} \text{ regulární}), \cdot, ^{-1}, \mathbb{I}\}$ s podgrupami
 - $SL_n(T)$ podgrupa matic s determinantem rovným 1,
 - $O_n(T)$ podgrupa ortogonálních matic.

Věta (vlastnosti operací v grupě)

- $a * c = b * c \vee c * a = c * b \Rightarrow a = b$,
- $a * u = a \vee u * a = a \Rightarrow u = e$,
- $a * u = e \vee u * a = e \Rightarrow u = a'$,
- $(a')' = a$,
- $(a * b)' = b' * a'$.

Definice Nejmenší podgrupa G obsahující množinu $X \subset G$ je $\langle X \rangle_G$.

Věta (o lineárním obalu)

$\langle X \rangle_G = \{(k_1 \times x_1) * \dots * (k_n \times x_n); n \in \mathbb{N}, x_1, \dots, x_n \in X, k_1, \dots, k_n \in \mathbb{Z}\}$, kde \times je mocnění v multiplikativní grupě a násobení v aditivní grupě.

Definice $G = (G, *, ', e)$, $H = (H, \cdot, ^{-1}, 1)$ pak $\varphi : G \rightarrow H$ je *homomorfismus*, pokud

- $\varphi(a * b) = \varphi(a) \cdot \varphi(b)$,
- $\varphi(a') = \varphi(a)^{-1}$,

- $\varphi(e) = 1$.

Pokud je navíc bijekce, tak se nazývá *izomorfismus*.

Definice *Jádro homomorfismu je $\text{Ker}\varphi = \{a \in G : \varphi(a) = 1\}$, obraz homomorfismu je $\text{Im}\varphi = \{b \in H : b = \varphi(a)\}$.*

Věta (o homomorfismu) Platí

- i. φ je homomorfismus $\Leftrightarrow \varphi(a * b) = \varphi(a) \cdot \varphi(b)$,
- ii. $\text{Ker}\varphi$ je podgrupa G , $\text{Im}\varphi$ je podgrupa H ,
- iii. φ je prostý homomorfismus $\Leftrightarrow \text{Ker}\varphi = \{e\}$.

Definice *Direktní součin grup $G_i = (G_i, *_i, e_i)$ je $G_1 \times \cdots \times G_n = (G_1 \times \cdots \times G_n, *, ', e)$, kde $(a_1, \dots, a_n) * (b_1, \dots, b_n) = (a_1 *_1 b_1, \dots, a_n *_n b_n)$ a podobně se všemi operacemi.*

Věta (o rozkladu \mathbb{Z}_M) Nechť $M = m_1 \cdot \dots \cdot m_n$, kde m_1, \dots, m_n jsou po dvou nesoudělná. Pak $\mathbb{Z}_M \simeq \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$.
Zde je vhodné znát důkaz.

Věta (Cayleyova a lineární reprezentace grup) Každá konečná grupa je izomorfní nějaké podgrupě některé symetrické (obecné lineární) grupy.

Definice *Řád grupy* je počet prvků G , značíme $|G|$, *řád prvku a v G* je počet prvků $\langle a \rangle_G$, značíme $\text{ord}(a)$.

Věta (o řádu prvku) $\text{ord}(a) =$ nejmenší přirozené n takové, že $n \times a = e$, pokud takové neexistuje, tak inf, tj. v aditivní grupě $na = 0$ a v multiplikativní grupě $a^n = 1$. Platí, že $\text{ord}(a)$ dělí $|G|$ a pokud je $\varphi : G \rightarrow H$ izomorfismus, pak $\text{ord}(a) = \text{ord}(\varphi(a))$.

Definice *Cyklická grupa* je grupa, která je generovaná jedním prvkem.

Věta (izomorfismus cyklických grup) Nechť je G cyklická. Pokud je G nekonečná, pak je izomorfní grupě \mathbb{Z} . Pokud je G konečná, pak existuje n takové, že G je izomorfní grupě \mathbb{Z}_n .

Věta (o podgrupách cyklických grup) Podgrupy cyklických grup jsou také cyklické.

Věta (o \mathbb{Z}_p^*) Grupa \mathbb{Z}_p^* je cyklická pro p prvočíslo a pak je tato grupa izomorfní grupě \mathbb{Z}_{p-1} .

Věta (o symetrické grupě) Platí

- i. řád permutace π v grupě S_X je nejmenší společný násobek délek cyklů,

ii. S_n je generovaná všemi transpozicemi, A_n je generovaná všemi trojcykly.

Definice $a, b \in G$ jsou *konjugované*, pokud $\exists c \in G$ takové, že $a = c \cdot b \cdot c^{-1}$.

Věta (o konjugovaných permutacích) Dvě permutace jsou konjugované právě tehdy, když mají stejný počet cyklů každé délky.

Definice Nechť $G = (G, \cdot, ^{-1}, 1)$ a H podgrupa G . Pak definujeme

- levý rozklad grupy G podle H je $\{aH : a \in G\}$,
- levé rozkladové třídy jsou $aH = \{ah : h \in H\}$,
- levá transverzála obsahuje z každé levé rozkladové třídy právě jeden prvek.

Pravý rozklad, pravé rozkladové třídy a pravou transverzálu definujeme analogicky.

Věta (o rozkladových třídách) $\forall a \in G$ platí $|aH| = |Ha| = |H|$.

Věta (o rozkladech) Levý i pravý rozklad grupy mají stejný počet prvků.

Definice Index podgrupy H v G je $[G : H] = |\{aH : a \in G\}| = |\{Ha : a \in G\}|$.

Věta (Lagrangeova) Nechť G je grupa a H je její podgrupa. Pak $|G| = |H|[G : H]$.

Věta (o velikosti podgrupy) Nechť G je konečná grupa a H její podgrupa. Pak $|H|$ dělí $|G|$.

2.4.2 Působení grupy na množině

Definice Působení grupy G na množinu X je homeomorfismus $\pi : G \rightarrow S_X$. Hodnotu $\pi(g)$ na prvku x budeme značit $g(x)$.

Věta (základní vlastnosti působení) Platí $\pi(1) = id$, tj. $1(x) = x$, g^{-1} je inverzní ke g a $(g \cdot h)(x) = g(h(x))$.

Tuhle "větu" jsem si teď přečetla ze svých poznámek a vůbec jí nerozumím, ale nechťela jsem ji vynechat. Takže here u go, enjoy.

Definice Definujeme relaci *tranzitivity* $x \sim y$ pokud existuje $g \in G$ takové, že $g(x) = y$. Tato relace je ekvivalence a bloky ekvivalence nazýváme *orbity*, $[x] = \{y \in X : x \sim y\}$.

Definice Řekneme, že x je *pevný bod* permutace π , pokud $\pi(x) = x$.

Definice Množina všech pevných bodů $\pi(g)$ je $X_g = \{x \in X : g(x) = x\}$.

Definice Stabilizátor prvku $x \in X$ je $G_x = \{g \in G : g(x) = x\}$.

Věta (o G_x) G_x je podgrupa grupy G .

Věta (o velikosti G) $\forall x \in X$ platí $|G| = |G_x| \cdot |[x]|$.

Definice $X|_{\sim}$ je množina všech bloků ekvivalence, tj. $|X|_{\sim}|$ je počet orbit působení.

Věta (Burnsideova) Nechť G a X jsou konečné, pak

$$|X|_{\sim}| = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g|.$$

2.4.3 Dělitelnost v Eukleidovských oborech, rozšířený Eukleidův algoritmus, existence a jednoznačnost ireducelibilních rozkladů

Věta (o dělitelnosti) Nechť $a = q \cdot b + r$. Pak q je celočíselný podíl a r je zbytek po dělení. Řekneme, že b dělí a , pokud $\exists q$ takové, že $a = b \cdot q$, píšeme $b|a$.

Věta (o NSD a NSN) Platí

$$\text{NSN}(a,b) = \frac{a \cdot b}{\text{NSD}(a,b)}.$$

Věta (Bézoutova rovnost) $\forall a,b \exists u,v : \text{NSD}(a,b) = u \cdot a + v \cdot b$, pak u,v se nazývají *bézoutovy koeficienty*.

Definice Definujeme kongruenci $a \equiv b \pmod{m}$ pokud dávají stejný zbytek po dělení m , tj. $m|(a - b)$.

Definice Eulerova funkce $\varphi(n) =$ počet čísel z $\{1, \dots, n-1\}$ nesoudělných s n .

Věta (Eulerova funkce a prvočíselný rozklad) Nechť $n = p_1^{k_1} \cdot \dots \cdot p_m^{k_m}$, pak $\varphi(n) = p_1^{k_1-1}(p_1 - 1) \cdot \dots \cdot p_m^{k_m-1}(p_m - 1)$.

Věta (Eulerova) Nechť a, m jsou nesoudělná, pak $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Věta (Čínská věta o zbytcích) Nechť m_1, \dots, m_n jsou nesoudělná, $M = m_1 \cdot \dots \cdot m_n$. Pak $\forall u_1, \dots, u_n \exists! x \in \{0, \dots, M-1\}$ takové, že

$$x \equiv u_1 \pmod{m_1} \dots x \equiv u_n \pmod{m_n}.$$

Definice Komutativní okruh s jednotkou je $(R, +, -, \cdot, 0, 1)$, pokud platí:

- $(a + b) + c = a + (b + c)$,

- $a + b = b + a$,
- $a + 0 = a$,
- $a + (-a) = 0$,
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
- $a \cdot b = b \cdot a$,
- $a \cdot 1 = a$,
- $a \cdot (b + c) = a \cdot b + a \cdot c$.

Pokud navíc $a, b \neq 0 \Rightarrow a \cdot b \neq 0$, tak se jedná o *obor integrity*.

Pokud navíc $\forall a \neq 0 \exists b : a \cdot b = 1$, tak se jedná o *těleso*.

Definice Řekneme, že a dělí b v R , pokud $\exists c \in R$ takové, že $b = a \cdot c$.

Definice Řekneme, že a a b jsou *asociované*, pokud $a|b \wedge b|a$.

Definice Řekneme, že a je *invertibilní*, pokud $a||1$, tj. $\exists b : a \cdot b = 1$. Pak b značíme a^{-1} .

Definice Řekneme, že c je *největší společný dělitel* a a b ($c = \text{NSD}(a,b)$), pokud $c|a$ a $c|b$ a pokud pro každé d takové, že $d|a \wedge d|b$ platí $d|c$.

Definice Řekneme, že a a b jsou *nesoudělná*, pokud $\text{NSD}(a,b) = 1$.

Definice Řekneme, že a je *ireducibilní*, pokud je neinvertibilní a nemá vlastní dělitele.

Definice Obor integrity nazveme *Gaussovský*, pokud má každý neinvertibilní nenulový prvek jednoznačný rozklad na ireducibilní činitele.

Věta (Gaussovské obory a NSD) V Gaussovských oborech existuje pro každou dvojici prvků největší společný dělitel.

Definice Eukleidovská norma na R je zobrazení $\nu : R \rightarrow \mathbb{N} \cup \{0\}$ takové, že

- $\nu(0) = 0$,
- Pokud $a|b$, pak $\nu(a) \leq \nu(b)$,
- $\forall a, b \in R, b \neq 0, \exists q, r : a = bq + r$ a $\nu(r) < \nu(b)$.

Řekneme, že obor integrity R je *Eukleidovský*, pokud na něm existuje eukleidovská norma.

Tvrzení V Eukleidovských oborech platí Bézoutova rovnost.

Euklidův algoritmus:

Vstup: $a, b \in R$, $\nu(a) \geq \nu(b)$,

Výstup: $\text{NSD}(a, b)$ a $u, v \in R : \text{NSD}(a, b) = u \cdot a + v \cdot b$.

- $a_0 = a$, $u_0 = 1$, $v_0 = 0$,
- $a_1 = b$, $u_1 = 0$, $v_1 = 1$.
- Najdeme $r, q : a_{i-1} = a_i \cdot q + r$, $\nu(r) < \nu(a_i)$,
- položíme $a_{i+1} = r$, $u_{i+1} = u_{i-1} - u_i \cdot q$, $v_{i+1} = v_{i-1} - v_i \cdot q$.
- Pokud $a_{i+1} = 0$, pak výsledkem jsou a_i, u_i, v_i .

Věta (Euklidův algoritmus) Euklidův algoritmus funguje a vždy dospěje ke správnému výsledku.

Definice Ideál R je $I \subseteq R$ takový, že pro libovolné $a, b \in I$, $u \in R$ platí

- i. $-a \in I$,
- ii. $a + b \in I$,
- iii. $a \cdot u \in I$.

Definice Hlavní ideál R je $aR = \{ar, r \in R\} = \{u \in R : a|u\}$.

Věta (Eukleidovské obory a ideály) Každý ideál v Eukleidovském oboru je hlavní ideál.

2.4.4 Kořenová a rozkladová nadtělesa, minimální polynom a stupeň rozšíření těles

Definice Charakteristika tělesa je nejmenší číslo n takové, že $\underbrace{1 + \dots + 1}_n = 0$. Pokud takové n neexistuje, tak je charakteristika 0.

Definice Rozšíření tělesa T je libovolné nadtěleso $S \supseteq T$.

Definice Nejmenší podtěleso nazýváme prvotěleso.

Věta (o prvotělesu) je izomorfní buď \mathbb{Q} nebo \mathbb{Z}_p .

Definice Nechť I je ideál okruhu R . Definujeme relaci ekvivalence $a \sim b \Leftrightarrow a - b \in I$ a bloky ekvivalence $[a] = a + I$ s operacemi

- $[a + b] = [a] + [b]$,

- $-[a] = [-a]$,
- $[a \cdot b] = [a] \cdot [b]$.

Pak $R|_I = (\{[a], a \in R\}, +, -, \cdot, [0])$ je faktorokruh.

Ideál I je maximální, pokud neexistuje ideál J splňující $I \subset J \subset R$.

Věta (konstrukce faktorokruhů) Nechť R je komutativní okruh s jednotkou a I jeho maximální ideál, pak faktorokruh $R|_I$ je těleso.

Definice Bud $T \subseteq S$ rozšíření těles a $a_1, \dots, a_n \in S$, pak $T[a_1, \dots, a_n]$ je nejmenší podokruh S obsahující T a a_1, \dots, a_n ; a $T(a_1, \dots, a_n)$ je nejmenší podtěleso S obsahující T a a_1, \dots, a_n .

Definice Na rozšíření $S \supseteq T$ se dá nahlížet jako na vektorový prostor nad T s násobením $T \times S \rightarrow S$. To se značí S_T a jeho dimenze je stupeň rozšíření $[S : T] = \dim S_T$.

Definice Nechť $S \supseteq T$ je rozšíření těles a $a \in S$. Pak a je algebraický, existuje-li nenulový polynom z $T[x]$, kde a je kořenem. Pokud prvek a není algebraický, pak je transcendentní. Je-li každý prvek rozšíření S algebraický, pak se jedná o algebraické rozšíření.

Věta (o rozšířeních konečného stupně) Rozšíření konečného stupně jsou algebraická.

Definice Nechť $S \supseteq T$ je rozšíření a $a \in S$ je algebraický prvek nad T . Minimální polynom prvku a nad T je polynom $m_{a,T} \in T[x]$ splňující

- i. $m_{a,T}(a) = 0$,
- ii. a je kořen $f \in T[x]$ pak $m_{a,T}|f$.

Věta (o $m_{a,T}$) Polynom $m_{a,T}$ je v $T[x]$ ireducibilní.

Věta (o stupni rozšíření) Nechť $S \supseteq T$ je rozšíření, $a \in S$ je algebraický nad T . Pak

$$[T(a) : T] = \deg m_{a,T}.$$

Tvrzení Stupeň $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = \deg(x^n - p) = n$.

Věta (o rozšíření rozšíření) Nechť $U \supseteq S \supseteq T$ jsou rozšíření, pak

$$[U : T] = [U : S] \cdot [S : T].$$

Definice Řekneme, že $S \supseteq T$ je *kořenové nadtěleso* polynomu $f \in T[x]$, pokud má f v S kořen a $S = T(a)$.

Věta (o kořenových nadtělesech) Nechť T je těleso a $f \in T[x]$ polynom stupně ≥ 1 . Pak

- i. existuje kořenové nadtěleso k polynomu f ,
- ii. je-li f irreducibilní v $T[x]$, pak jsou každá dvě kořenová nadtělesa T -izomorfní.

Definice Řekneme, že $S \supseteq T$ je *rozkladové nadtěleso* polynomu $f \in T[x]$, pokud se f v $S[x]$ rozkládá na lineární činitele, tj. $f|||(x - a_1) \cdot \dots \cdot (x - a_n)$ pro $a_1, \dots, a_n \in S$ a navíc $S = T(a_1, \dots, a_n)$.

Věta (o rozkladových tělesech) Nechť T je těleso, $f \in T[x]$ je polynom stupně ≥ 1 . Pak

- i. existuje rozkladové nadtěleso f ,
- ii. každá dvě rozkladová nadtělesa f jsou T -izomorfní.

Definice Řekneme, že těleso T je *algebraicky uzavřené*, má-li v něm každý polynom z $T[x]$ kořen.

Věta (o algebraicky uzavřených tělesech) Algebraicky uzavřená tělesa nemohou být konečná.

Definice Řekneme, že $S \supseteq T$ je *algebraický uzávěr* T , je-li S algebraicky uzavřené a je algebraickým rozšířením tělesa T .

Věta (o algebraickém uzávěru) Ke každému tělesu T existuje algebraický uzávěr a každé dva algebraické uzávěry jsou T -izomorfní.