Učební texty k státní bakalářské zkoušce
Matematika

študenti MFF

14. května 2018

Vážený študent/čitateľ,

toto je zbierka vypracovaných otázok pre bakalárske skúšky Informatikov. Otázky boli vypracované študentmi MFF počas prípravy na tieto skúšky, a teda zatiaľ neboli overené kvalifikovanými osobami (profesormi/dokotorandmi mff atď.) - preto nie je žiadna záruka ich správnosti alebo úplnosti.

Väčšina textov je vypracovaná v češtine resp. slovenčine, prosíme dodržujte túto konvenciu (a obmedzujte teda používanie napr. anglických textov). Ak nájdete nejakú chybu, nepresnosť alebo neúplnú informáciu - neváhajte kontaktovať administrátora alebo niektorého z prispievateľov, ktorý má write-prístup k svn stromu, s opravou :-) Podobne - ak nájdete v „texte“ veci ako ??? a TODO, znamená to že danú informáciu je potrebné skontrolovať, resp. doplniť...

Texty je možné ďalej používať a šíriť pod licenciou **GNU GFDL** (čo pre všetkých prispievajúcich znamená, že musia súhlasiť so zverejnením svojich úprav podľa tejto licencie).

Veríme, že Vám tieto texty pomôžu k úspešnému zloženiu skúšok.

Hlavní writeři :-) :

- *ajs*
- *andree* – http://andree.matfyz.cz/
- *Hydrant*
- *joshis / Petr Dvořák*
- *kostej*
- *nohis*
- *tuetschek* – http://tuetschek.wz.cz/

Úvodné verzie niektorých textov vznikli prepisom otázok vypracovaných „písomne na papier“, alebo inak ne-TEX-ovsky. Autormi týchto pôvodných verzií sú najmä nasledujúce osoby: *gASK*, *Grafi*, *Kate* (mat-15), *Nytram*, *Oscar*, *Stando*, *xStyler*. Časť je prebratá aj z pôvodných súborkových textov... Všetkým patrí naša/vaša vďaka.

Obsah

1 Čísla

Požadavky

- Vlastnosti přirozených, celých, racionálních, reálných a komplexních čísel
- Posloupnosti a limity
- Cauchyovské posloupnosti

1.1 Reálná čísla

Množinou všech reálných čísel (značíme ji $\mathbb{R}$) budeme rozumět množinu, na níž je definováno sčítání (značíme $x + y$), násobení (značíme $x \cdot y$) a uspořádání (značíme $x \leq y$), která spňují tyto axiomy:

1. (Algebraické operace)
   (a) $\forall x, y, z \in \mathbb{R} : x + (y + z) = (x + y) + z$ *(asociativní zákon pro sčítání)*
   (b) $\forall x, y \in \mathbb{R} : x + y = y + x$ *(komutativní zákon pro sčítání)*
   (c) v $\mathbb{R}$ existuje nulový prvek (značíme ho 0) tak, že $\forall x \in \mathbb{R} : x + 0 = x$
   (d) pro každý $x \in \mathbb{R}$ existuje opačný prvek (značíme ho $-x$) tak, že $x+(-x) = 0$
   (e) $\forall x, y, z \in \mathbb{R} : x \cdot (y \cdot z) = (x \cdot y) \cdot z$ *(asociativní zákon pro násobení)*
   (f) $\forall x, y \in \mathbb{R} : x \cdot y = y \cdot x$ *(komutativní zákon pro násobení)*
   (g) v $\mathbb{R}$ existuje jednotkový prvek (značíme ho 1) tak, že $\forall x \in \mathbb{R} : x \cdot 1 = x$
   (h) pro každý $x \in \mathbb{R}, x \neq 0$ existuje inverzní prvek (značíme ho x^{-1}) tak, že $x \cdot x^{-1} = 1$
   (i) $\forall x, y, z \in \mathbb{R} : (x + y) \cdot z = x \cdot z + y \cdot z$ *(distributivní zákon)*
2. (Uspořádání)
   (a) $\forall x, y, z \in \mathbb{R} : ((x \leq y) \wedge (y \leq z)) \Rightarrow (x \leq z)$ *(tranzitivita)*
   (b) $\forall x, y \in \mathbb{R} : (((x \leq y) \wedge (y \leq x)) \Rightarrow (x = y)$ *(slabá antisymetrie)*
   (c) $\forall x, y \in \mathbb{R} : (x \leq y) \vee (y \leq x)$
   (d) $\forall x, y, z \in \mathbb{R} : (x \leq y) \Rightarrow (x + z \leq y + z)$
   (e) $\forall x, y, z \in \mathbb{R} : (x \leq y) \wedge (0 \leq z) \Rightarrow (x \cdot z \leq y \cdot z)$
3. (Netrivialita)
   (a) $0 \neq 1$
4. (Úplnost)
   Definice *(Axiom suprema)*
   Nechť $M \subset \mathbb{R}$ je neprázdná a shora omezená. Pak existuje číslo $s \in \mathbb{R}$, které má vlastnosti:
   (a) $\forall x \in M : x \leq s$
   (b) $\forall s' \in \mathbb{R}, s' < s \ \exists x \in M : x > s'$

Číslo s z axiomu suprema je jednoznačně určeno, značí se $\sup M$ a říká se mu *supremum množiny* M. Supremum množiny je její nejmenší horní závora (*horní závora* je každý takový prvek, pro který platí bod (a) definice suprema). Největší dolní závoru množiny M (pokud existuje – a dá se dokázat, že existuje, je-li množina zdola omezená) nazýváme *infimem množiny* M a značíme $\inf M$.

Poznámka
Relace „<“ na reálných číslech (a stejně tak na přirozených a racionálních číslech) se definuje takto: $a < b$, právě když $a \leq b$ a zároveň $a \neq b$.

1.2 Přirozená čísla

Definice
Řekneme, že množina $S \subset \mathbb{R}$ je *induktivní*, jestliže platí

- $1 \in S$
- $[x \in S \Rightarrow (x+1) \in S]$

Množinu *přirozených čísel* $\mathbb{N}$ definujeme jako průnik všech induktivních podmnožin $\mathbb{R}$, tedy

$$N := \bigcap \{S; S \subset \mathbb{R}; S \textit{ induktivní}\}$$

Věta *(Induktivnost přirozených čísel)*
Množina $\mathbb{N}$ je induktivní.

Věta *(Vlastnosti přirozených čísel)*
Množina $\mathbb{N}$ má nasledujúcí vlastnosti:

1. $n \in \mathbb{N} \Rightarrow n \geq 1$
2. $n \in \mathbb{N} \backslash \{1\} \Rightarrow \exists m \in \mathbb{N} : n = m + 1$
3. $m, n \in \mathbb{N}, m < n \Rightarrow m + 1 \leq n$
4. každá neprázdná podmnožina $\mathbb{N}$ má nejmenší prvek

Věta *(Archimédova vlastnost reálných čísel)*
Pro každé $x \in \mathbb{R}$ existuje $n \in \mathbb{N}$ takové, že $x < n$

Věta *(Peanove axiómy pre zavedenie prirodzených čísel)*

- Existuje číslo 0 (to neznamená, že nula je prirodzené číslo, v $\mathbb{N}$ roli tejto nuly hraje jednotka).
- Na množine prirodzených čísel je definovaná unárna operácia „nasledovník“, označovaná S.
- Neexistuje žiadne prirodzené číslo, ktorého nasledovníkom je 0.
- Rôzne prirodzené čísla majú rôznych nasledovníkov: $a \neq b \Rightarrow S(a) \neq S(b)$ (t.j. funkcia nasledovníka je prostá).

- Ak číslo 0 spĺňa nejakú vlastnosť a súčasne ju spĺňa každý nasledovník prirodzeného čísla, potom túto vlastnosť spĺňajú všetky prirodzené čísla (*axióm matematickej indukcie*).

Věta *(Konštrukcia prirodzených čísel založená na teórii množín)*
Označme $0 := \{\}$ a definujme $S(a) = a \cup \{a\}$ pre všetky a. Množina prirodzených čísel je potom definovaná ako prienik všetkých množín obsahujúcich 0, ktoré sú uzavreté vzhľadom na funkciu nasledovníka. Predpokladajúc platnost axiómu nekonečnosti, dá sa dokázať, že táto definícia spĺňa Peanove axiómy. *Axióm nekonečnosti* vyzerá takto:

$$\exists \mathbb{N} : \emptyset \in \mathbb{N} \wedge (\forall x : x \in \mathbb{N} \Rightarrow x \cup \{x\} \in \mathbb{N})$$

V „klasickom“ zápise čísel potom každému prirodzenému číslu zodpovedá množina prirodzených čísel menších ako ono samo, takže

- $0 = \{\}$
- $1 = \{0\} = \{\{\}\}$
- $2 = \{0, 1\} = \{0, \{0\}\} = \{\{\}, \{\{\}\}\}$
- $3 = \{0, 1, 2\} = \{0, \{0\}, \{0, \{0\}\}\} = \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}$

$\mathbb{N}$ je uzavretá na sčítanie.

1.3 Celá a racionální čísla

Definice
Kromě symbolů $\mathbb{R}$ a $\mathbb{N}$, které jsme již zavedli, budeme značit symbolem $\mathbb{Z}$ množinu *celých čísel*, tedy

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-n, n \in \mathbb{N}\}$$

a symbolem $\mathbb{Q}$ množinu *racionálních čísel*, tedy

$$\mathbb{Q} = \left\{ \frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N} \right\}$$

$\mathbb{Z}$ je uzavřena na sčítání, odčítání a násobení, $\mathbb{Q}$ je uzavřena na sčítání, odčítání, násobení a dělení nenulovým číslem.

Věta *(Existence celé části)*
Pro každé $x \in \mathbb{R}$ existuje právě jedno číslo $[x] \in \mathbb{Z}$ splňující

$$x - 1 < [x] \leq x$$

Toto číslo nazýváme *celou částí čísla x.*

Věta *(Hustota $\mathbb{Q}$ a $\mathbb{R} \backslash \mathbb{Q}$)*
Nechť $a, b \in \mathbb{R}, a < b$. Pak existují $q \in \mathbb{Q}$ a $r \in \mathbb{R} \backslash \mathbb{Q}$ takové, že

$$a < q < b, \ a < r < b$$

Věta *(o existenci n-té odmocniny)*
Nechť $x \in \mathbb{R}, x \geq 0$ a nechť $n \in \mathbb{N}$. Pak existuje právě jedno $y \in \mathbb{R}, y \geq 0$ takové, že $y^n = x$

1.4 Komplexní čísla

Definice

Komplexním číslem nazveme číslo tvaru $a + bi$, kde $a, b \in \mathbb{R}$ nazýváme **reálnou a imaginární částí** komplexního čísla. Tento tvar komplexního čísla se nazývá **algebraický**. Písmeno i značí **imaginární jednotku**, která se formálně zavádí jako číslo splňující rovnici $i^2 + 1 = 0$ tj. jako $\sqrt{-1}$, která v reálných číslech neexistuje.

Pokud je $b = 0$, je dotyčné číslo reálným číslem, tj. reálná čísla tvoří podmnožinu čísel komplexních. Pokud je $a = 0$, mluvíme o **ryze imaginárním čísle**.

1.4.1 Aritmetika

$$(a + ib) + (c + id) = (a + c) + i(b + d)$$

$$(a + ib) - (c + id) = (a - c) + i(b - d)$$

$$(a + ib) \cdot (c + id) = (ac - bd) + i(ad + bc)$$

$$\frac{a + ib}{c + id} = \frac{(a + ib)(c - id)}{(c + id)(c - id)} = \frac{(ac + bd) + i(bc - ad)}{c^2 + d^2} = \left(\frac{ac + bd}{c^2 + d^2}\right) + i\left(\frac{bc - ad}{c^2 + d^2}\right)$$

Komplexní čísla se zobrazují v **komplexní (Gaussově) rovině** jako body se souřadnicemi $[x, y]$; x je reálná část komplexního čísla, y imaginární část. Na ose x leží reálná čísla, na ose y ryze imaginární čísla.

Pojmem **komplexně sdružené číslo** komplexního čísla $z = a + ib$ se nazývá číslo $\overline{z} = a - ib$

Absolutní hodnotu komplexního čísla $z = a + bi$ lze vyjádřit takto:

$$|z| = \sqrt{a^2 + b^2}$$

Následující vlastnosti platí pro všechna komplexní čísla z a w, není-li uvedeno jinak.

$$\overline{z + w} = \overline{z} + \overline{w}$$

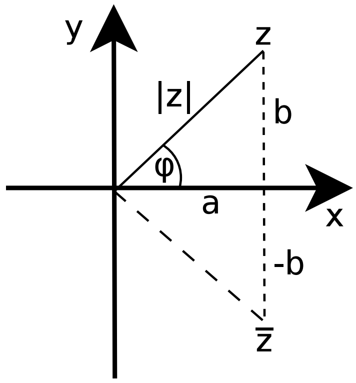
$$\overline{zw} = \overline{z}\ \overline{w}$$

$$\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}, \textit{pro } w \textit{ nenulové}$$

$$\overline{z} = z, \textit{právě když je } z \textit{ reálné číslo}$$

$$|\overline{z}| = |z|$$

$$|z|^2 = z\overline{z}$$



Obrázek 1: Komplexní číslo ve 2D

$$z^{-1} = \frac{\overline{z}}{|z|^2}, \textit{pro z nenulové}$$

Každé komplexní číslo z různé od nuly je možné jednoznačně vyjádřit v **goniometrickém tvaru**. Pokud si v komplexní rovině zvolíme polární souřadnicový systém, vzdálenost čísla z od počátku je právě jeho absolutní hodnota $|z|$ (také nazývaná **modul**) a orientovaný úhel $\varphi = |\sphericalangle JOZ|$ (*argument*), kde J je bod $J[1,0]$, O je počátkem soustavy a Z je obraz komplexního čísla $a + bi$ se souřadnicemi $Z[a,b]$, platí:

$$z = |z|(\cos\varphi + i \cdot \sin\varphi)$$

Argument φ lze vyjádřit ze vztahů: $\cos\varphi = \frac{a}{|z|}$ a $\sin\varphi = \frac{b}{|z|}$

Pro dělení komplexních čísel $z_1 = |z_1| \cdot (\cos\varphi_1 + i \cdot \sin\varphi_1)$ a $z_2 = |z_2| \cdot (\cos\varphi_2 + i \cdot \sin\varphi_2)$ platí následující rovnice:

$$\frac{z_1}{z_2} = \frac{|z_1|}{|z_2|} \cdot [\cos(\varphi_1 - \varphi_2) + i \cdot \sin(\varphi_1 - \varphi_2)]$$

Pro násobení komplexních čísel z_1 a z_2 z předchozího příkladu slouží vzorec:

$$z_1 \cdot z_2 = |z_1| \cdot |z_2| \cdot [\cos(\varphi_1 + \varphi_2) + i \cdot \sin(\varphi_1 + \varphi_2)]$$

Pro **n-tou mocninu komplexní čísla** v goniometrickém tvaru platí tzv. **Moivreova věta**:

$$z^n = |z|^n(\cos n\varphi + i \cdot \sin n\varphi)$$

1.5 Posloupnosti a limity

Definice *(posloupnost)*

Posloupností reálných čísel nazýváme jakékoli zobrazení z množiny $\mathbb{N}$ do množiny $\mathbb{R}$. Posloupnost obvykle značíme symbolem $\{a_n\}_{n=1}^{\infty}$ nebo $\{a_n\}_{n\in\mathbb{N}}$. Pro každé konkrétní $n \in \mathbb{N}$ nazýváme reálné číslo a_n *n-tým členem* posloupnosti $\{a_n\}$.

Definice *(Omezené posloupnosti)*

1. Posloupnost $\{a_n\}$ je *shora omezená*, je-li $\{a_n; n \in \mathbb{N}\}$ shora omezená.
2. Posloupnost $\{a_n\}$ je *zdola omezená*, je-li $\{a_n; n \in \mathbb{N}\}$ zdola omezená.
3. Posloupnost $\{a_n\}$ je *omezená*, je-li zdola omezená a shora omezená.

Definice *(Rostoucí a klesající posloupnosti)*

1. Posloupnost $\{a_n\}$ je *klesající*, jestliže $\forall n \in \mathbb{N} : a_n > a_{n+1}$.
2. Posloupnost $\{a_n\}$ je *rostoucí*, jestliže $\forall n \in \mathbb{N} : a_n < a_{n+1}$.
3. Posloupnost $\{a_n\}$ je *neklesající*, jestliže $\forall n \in \mathbb{N} : a_n \leq a_{n+1}$.
4. Posloupnost $\{a_n\}$ je *nerostoucí*, jestliže $\forall n \in \mathbb{N} : a_n \geq a_{n+1}$.
5. Posloupnost $\{a_n\}$ je *monotónní*, jestliže je nerostoucí nebo neklesající.
6. Posloupnost $\{a_n\}$ je *ryze monotónní*, jestliže je rostoucí nebo klesající.

1.5.1 Vlastní limity

Definice

Nechť $\{a_n\}$ je posloupnost reálných čísel a $A \in \mathbb{R}$. Řekneme, že A je *vlastní limitou posloupnosti* $\{a_n\}$, jestliže

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

značíme

$$\lim_{n \to \infty} a_n = A$$

Dá se jednoduše ukázat, že toto je splněno i pokud máme vždy od n_0 dále zaručeno jen to, že $|a_n - A| < K \cdot \varepsilon$ pro nějaké $K > 0$.

Definice

Jestliže existuje $A \in \mathbb{R}$ tak, že $\lim_{n\to\infty} a_n = A$, pak říkáme, že posloupnost $\{a_n\}$ má *vlastní limitu* nebo že *konverguje* (je *konvergentní*). V opačném případě říkáme, že posloupnost *diverguje*.

Pozorování

Ne každá posloupnost je konvergentní. Například posloupnost 0,1,0,1,0,... nemá vlastní limitu a podobně posloupnost $\{2^n\}$ nemá vlastní limitu.

Příklady

- $\lim_{n\to\infty}(\sqrt{n+1} - \sqrt{n}) = 0$
- $\lim_{n\to\infty} \sqrt[n]{n} = 1$

Věta *(o jednoznačnosti limity posloupnosti)*

Každá posloupnost má nejvýše jednu limitu.

Věta *(o omezenosti konvergentní posloupnosti)*

Každá konvergentní posloupnost je omezená.

Definice

Nechť $\{a_n\}_{n\in\mathbb{N}}$ je posloupnost reálných čísel. Řekneme, že posloupnost $\{b_k\}_{k\in\mathbb{N}}$ je *vybraná* z posloupnosti, neboli že posloupnost $\{b_k\}_{k\in\mathbb{N}}$ je *podposloupností* posloupnosti $\{a_n\}_{n\in\mathbb{N}}$, jestliže existuje rostoucí posloupnost přirozených čísel $\{n_k\}$ taková, že $b_k = a_{n_k}$ pro všechna $k \in \mathbb{N}$.

Věta *(o limitě vybrané posloupnosti)*

Nechť $\{a_n\}_{n\in\mathbb{N}}$ je posloupnost reálných čísel a nechť $\lim_{n\to\infty} a_n = A$. Nechť posloupnost $\{b_k\}_{k\in\mathbb{N}}$ je vybraná z posloupnosti $\{a_n\}_{n\in\mathbb{N}}$. Pak $\lim_{k\to\infty} b_k = A$.

Věta *(o aritmetice limit)*

Nechť $\{a_n\}_{n\in\mathbb{N}}$ a $\{b_n\}_{n\in\mathbb{N}}$ jsou dvě posloupnosti reálných čísel a nechť $\lim_{n\to\infty} a_n = A \in \mathbb{R}$ a $\lim_{n\to\infty} b_n = B \in \mathbb{R}$. Pak platí:

1. $\lim_{n\to\infty}(a_n + b_n) = A + B$
2. $\lim_{n\to\infty}(a_n \cdot b_n) = A \cdot B$
3. je-li $\forall n \in \mathbb{N} : b_n \neq 0$ a $B \neq 0$, pak $\lim_{n\to\infty} \frac{a_n}{b_n} = \frac{A}{B}$

Věta *(o limitě a uspořádání)*

Nechť $\{a_n\}_{n\in\mathbb{N}}$ a $\{b_n\}_{n\in\mathbb{N}}$ jsou dvě posloupnosti reálných čísel a nechť $\lim_{n\to\infty} a_n = A \in \mathbb{R}$ a $\lim_{n\to\infty} b_n = B \in \mathbb{R}$. Pak platí:

1. Jestliže $A < B$, potom $\exists n_0 \in \mathbb{N}\ \forall n > n_0 : a_n < b_n$
2. Jestliže $\exists n_0 \in \mathbb{N}\ \forall n \geq n_0 : a_n \geq b_n$, pak $A \geq B$

Pozor, ostrost nerovností v tomto případě je důležitá.

Věta *(o policajtech)*

Nechť $\{a_n\}_{n\in\mathbb{N}}$, $\{b_n\}_{n\in\mathbb{N}}$ a $\{c_n\}_{n\in\mathbb{N}}$ jsou posloupnosti reálných čísel, splňující

1. $\exists n_0 \in \mathbb{N}\ \forall n > n_0 : a_n \leq c_n \leq b_n$
2. $\lim_{n\to\infty} a_n = \lim b_n = A \in \mathbb{R}$

Pak

$$\lim c_n = A$$

Věta *(o limitě součinu mizející (*$\lim = 0$*) a omezené posloupnosti)*

Nechť $\{a_n\}_{n\in\mathbb{N}}$ a $\{b_n\}_{n\in\mathbb{N}}$ jsou posloupnosti reálných čísel, nechť je $\lim_{n\to\infty} a_n = 0$ a $\{b_n\}$ omezená. Pak

$$\lim_{n\to\infty} (a_n \cdot b_n) = 0$$

1.5.2 Nevlastní limity

Definice

Řekneme, že posloupnost $\{a_n\}$ má *nevlastní limitu* $+\infty$, jestliže:

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

Obdobně řekneme, že posloupnost $\{a_n\}$ má *nevlastní limitu* $-\infty$, jestliže:

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

Má-li posloupnost nevlastní limitu, říkáme o ní, že diverguje, stejně jako v případě, že žádnou limitu nemá.

Poznámka

Všechny možné situace jsou znázorněny na následujícím diagramu:

limita posloupnosti:

- neexistuje
- existuje
  - vlastní
  - nevlastní
    - $-\infty$
    - $+\infty$

Definice

Množinu $\mathbb{R}^* := \mathbb{R} \cup \{+\infty, -\infty\}$ nazýváme *rozšířenou reálnou osou.*

Poznámka

Věty o jednoznačnosti limity, o limitě vybrané posloupnosti, o limitě a uspořádání a o policajtech platí v nezměněné podobě, jestliže připustíme nevlastní limity. Věta o omezenosti konvergentní posloupnosti zrejmě neplatí - neboť je-li $\lim_{n\to\infty} a_n = \infty$ (nebo $-\infty$), pak posloupnost $\{a_n\}$ není omezená. Větu o aritmetice limit pro rozšírenou osu uvedeme zvlášť.

Věta *(o aritmetice limit pro nevlastní limity)*

Nechť $\{a_n\}_{n\in\mathbb{N}}$ a $\{b_n\}_{n\in\mathbb{N}}$ jsou dvě posloupnosti reálných čísel a nechť $\lim_{n\to\infty} a_n = A \in \mathbb{R}^*$ a $\lim_{n\to\infty} b_n = B \in \mathbb{R}^*$. Pak platí:

1. $\lim_{n\to\infty}(a_n + b_n) = A + B$, *pokud je výraz* $A+B$ *definován*
2. $\lim_{n\to\infty}(a_n \cdot b_n) = A \cdot B$, *pokud je výraz* $A \cdot B$ *definován*
3. je-li $\forall n \in \mathbb{N} : b_n \neq 0$ a $B \neq 0$, pak $\lim_{n\to\infty} \frac{a_n}{b_n} = \frac{A}{B}$, *pokud je výraz* $\frac{A}{B}$ *definován*

Definice *(Supremum a infimum na rozšířené reálné ose)*

- Nechť množina $A \subset \mathbb{R}$ je shora neomezená. Pak klademe $\sup A := +\infty$
- Nechť množina $A \subset \mathbb{R}$ je zdola neomezená. Pak klademe $\inf A := -\infty$
- Nechť $A = \emptyset$. Pak klademe $\sup A := -\infty$ a $inf A := +\infty$

Poznámka
Prázdná množina je jediná množina, jejíž supremum je menší než její infimum.

Věta *(o limitě podílu kladné a mizející posloupnosti)*
Nechť $\{a_n\}_{n\in\mathbb{N}}$ a $\{b_n\}_{n\in\mathbb{N}}$ jsou posloupnosti reálných čísel, nechť je $\lim_{n\to\infty} a_n = A \in \mathbb{R}^*, A > 0$ a nechť $\lim_{n\to\infty}\{b_n\} = 0$. Nechť

$$\exists n_0 \in \mathbb{N}\ \forall n \geq n_0, n \in \mathbb{N} : b_n > 0$$

Pak

$$\lim_{n\to\infty} \frac{a_n}{b_n} = +\infty$$

1.5.3 Monotónní posloupnosti

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

Poznámka
Je-li posloupnost neklesající (nerostoucí) a navíc shora (zdola) omezená, pak má vlastní limitu. Je-li posloupnost neklesající (nerostoucí) a navíc shora (zdola) neomezená, pak má limitu $+\infty$ $(-\infty)$.

Definice *(Limes superior a limes inferior)*
Nechť $\{a_n\}_{n\in\mathbb{N}}$ je posloupnost reálných čísel. Je-li $\{a_n\}$ shora omezená, definujeme posloupnost $\{b_n\}_{n\in\mathbb{N}}$ předpisem:

$$b_n := \sup\{a_k; k \geq n\}$$

Je-li $\{a_n\}$ zdola omezená, definujeme posloupnost $\{c_n\}_{n\in\mathbb{N}}$ předpisem:

$$c_n := \inf\{a_k; k \geq n\}$$

V takovém případě definujeme:

$$\limsup\ a_n := \begin{cases} \lim_{n\to\infty} b_n & \textit{jestliže je } \{a_n\} \textit{ shora omezená} \\ \infty & \textit{jestliže je } \{a_n\} \textit{ shora neomezená} \end{cases}$$

Tuto hodnotu nazýváme *limes superior* posloupnosti $\{a_n\}_{n\in\mathbb{N}}$. Obdobně definujeme *limes inferior* posloupnosti $\{a_n\}_{n\in\mathbb{N}}$ předpisem:

$$\liminf\ a_n := \begin{cases} \lim_{n\to\infty} c_n & \textit{jestliže je } \{a_n\} \textit{ zdola omezená} \\ -\infty & \textit{jestliže je } \{a_n\} \textit{ zdola neomezená} \end{cases}$$

Poznámka
Limes superior a limes inferior jsou vždy dobře definované hodnoty a platí

$$\limsup\ a_n \in \mathbb{R}^*, \liminf\ a_n \in \mathbb{R}^*,$$

Na rozdíl od limity, která nemusí existovat, tyto dvě hodnoty existují pro libovolnou posloupnost reálných čísel.

Věta *(o vztahu limity, limes superior a limes inferior)*
Nechť $\{a_n\}_{n\in\mathbb{N}}$ je posloupnost reálných čísel. Potom

$$\lim a_n = A \in \mathbb{R}^*$$

právě tehdy, když

$$\limsup\ a_n = \liminf\ a_n = A \in \mathbb{R}^*$$

Definice
Nechť $\{a_n\}_{n\in\mathbb{N}}$ je posloupnost reálných čísel. Pak $A \in \mathbb{R}^*$ nazveme *hromadnou hodnotou* posloupnosti $\{a_n\}$, jestliže existuje vybraná posloupnost taková $\{a_{n_k}\}$, že $\lim_{k\to\infty} a_{n_k} = A$. Množina všech hromadných hodnot značíme $H(\{a_n\})$

Věta *(o vztahu limes superior, limes inferior a hromadných hodnot)*
Nechť $\{a_n\}_{n\in\mathbb{N}}$ je posloupnost reálných čísel. Potom $H\{(a_n)\} \neq \emptyset$,

$$\limsup\ a_n = \max H(\{a_n\})\ \ a\ \ \liminf\ a_n = \min H(\{a_n\})$$

1.6 Cauchyovské posloupnosti

Tato sekce je vypracovaná podle skript Prof. A. Pultra z matematické analýzy (`http://kam.mff.cuni.cz/~pultr/`)

Definice *(Bolzano-Cauchyova podmínka)*
Řekneme, že posloupnost $\{a_n\}_{n\geq 0}$ je *cauchyovská*, nebo-li že splňuje *Bolzano-Cauchyho podmínku*, pokud pro ní platí:

$$\forall \varepsilon > 0\ \ \exists n_0 \in \mathbb{N} : \forall m, n \in \mathbb{N} : m \geq n_0, n \geq n_0 : |a_n - a_m| < \varepsilon$$

Věta *(Bolzano-Weierstrassova)*
Z každé omezené posloupnosti lze vybrat konvergentní podposloupnost. Jsou-li a_n v kompaktním intervalu $[a, b]$, je limita vybrané posloupnosti v tomto intervalu.

Důkaz
První část dokážeme nalezením takové posloupnosti. Vezmeme $A := \limsup\ a_n$ a definujeme pro každé $k \in \mathbb{N}$ množinu $M_k := \{j \in \mathbb{N} | j > n_{k-1}, a_j \in \langle A - \frac{1}{2^k}, A + \frac{1}{2^k}\rangle\}$ a $n_k := \min M_k$. Potom $\{a_{n_k}\}$ je vybraná posloupnost, která konverguje. Druhá část je přímým důsledkem věty o limitě a uspořádání.

Lemma
Má-li cauchyovská posloupnost konvergentní podposloupnost, je konvergentní.

Důkaz
Nechť $\lim a_{n_k} = x$. Pro $\varepsilon > 0$ zvolme n_0, aby pro $m, n \geq n_0$ platilo $|a_m - a_n| < \frac{\varepsilon}{2}$ a $|a_k - x| < \frac{\varepsilon}{2}$. Protože $k_n \geq n$, platí $|a_n - x| = |a_n - a_{k_n}| + |a_{k_n} - x| < \varepsilon$.

Věta *(Bolzano-Cauchyova)*
Posloupnost $\{a_n\}$ má vlastní limitu, právě když je cauchyovská.

Důkaz

1. Implikace „$\Rightarrow$“ je hned vidět – stačí vzít k ε takové n_0, že $|a_n - x| < \frac{\varepsilon}{2}\ \forall n \geq n_0$. Potom je $|a_n - a_m| = |a_n - x + x - a_m| \leq |a_n - x| + |x - a_m| \leq \varepsilon\ \forall m, n \geq n_0$.
2. Pro druhou implikaci stačí dokázat, že je cauchyovská posloupnost omezená a zbytek dostaneme z předchozího lemmatu a Bolzano-Weierstrassovy věty. Pro $\varepsilon = 1$ existuje n_0 takové, že $a_{n_0} - 1 < a_n < a_{n_0} + 1$ pro každé $n \geq n_0$ (to plyne přímo z podmínky), takže zbývá jen konečný počet členů mimo toto rozmezí (pro $n < n_0$), a ty vždy tvoří omezený systém.

2 Základy diferenciálního počtu

Požadavky

- Reálné funkce jedné reálné proměnné
- Spojitost, limita funkce v bodě (vlastní i nevlastní)
- Některé konkrétní funkce (polynomy, racionální lomené funkce, goniometrické a cyklometrické funkce, logaritmy a exponenciální funkce)
- Derivace: definice a základní pravidla, věty o střední hodnotě, derivace vyšších řádů
- Některé aplikace (průběhy funkcí, Newtonova metoda hledání nulového bodu, Taylorův polynom se zbytkem)

2.1 Reálné funkce jedné reálné proměnné

Definice *(Reálná funkce)*
Reálná funkce jedné proměnné je zobrazení $f : M \to \mathbb{R}$, kde $M \subseteq \mathbb{R}$.
f je na M:

- *rostoucí*: $\forall x, y : x < y \Rightarrow f(x) < f(y)$
- *klesající*: $\forall x, y : x < y \Rightarrow f(x) > f(y)$
- *neklesající*: $\forall x, y : x < y \Rightarrow f(x) \leq f(y)$
- *nerostoucí*: $\forall x, y : x < y \Rightarrow f(x) \geq f(y)$
- *sudá*: $x \in M \Rightarrow -x \in M \wedge f(x) = f(-x), \forall x \in M$
- *lichá*: $x \in M \Rightarrow -x \in M \wedge f(x) = -f(-x), \forall x \in M$
- *periodická* s periodou $p \in \mathbb{R}$: $x \in M \Rightarrow x \pm p \in M \wedge f(x) = f(x+p) = f(x-p), \forall x \in M$

Definice *(Okolí bodu)*
$P(a, \delta) = (a - \delta, a) \cup (a, a + \delta)$ (prstencové okolí)
$P^{+}(a, \delta) = (a, a + \delta)$ (pravé prstencové okolí)
$P^{-}(a, \delta) = (a - \delta, a)$ (levé prstencové okolí)
$B(a, \delta) = (a - \delta, a + \delta) = P(a, \delta) + \{a\}$ (δ-okolí)
Podobně se definuje i levé a pravé δ-okolí bodu a.

2.2 Spojitost, limita funkce v bodě (vlastní i nevlastní)

Definice *(Limita)*
Řekneme, že f má v bodě $a \in \mathbb{R}^*$ limitu $A \in \mathbb{R}^*$, jestliže

$$\forall \varepsilon > 0 \ \exists \delta > 0 : \forall x \in P(a, \delta) \Rightarrow f(x) \in B(A, \varepsilon)$$

a značíme $\lim_{x \to a} f(x) = A$

Platí-li tato vlastnost jen pro pravá okolí bodů a a A, mluvíme o *jednostranné limitě zprava* a podobně zleva.

Definice *(Spojitost v bodě)*
Řekneme, že f je spojitá v bodě $a \in \mathbb{R}$, jestliže $\lim_{x \to a} f(x) = f(a)$

Věta *(Heineho věta)*
Nechť $f : M \to \mathbb{R}, M \subseteq \mathbb{R}$. Nechť f je definováno na nějakém prstencovém okolí bodu $a \in \mathbb{R}^*$. Potom následující dvě tvrzení jsou ekvivalentní:

1. $lim_{x \to a} f(x) = A \in \mathbb{R}^*$
2. Pro každou posloupnost $\{x_n\}_{n=1}^{\infty}$ splňující $x_n \in D(f)\ \forall n \in \mathbb{N}$ a $\lim x_n = a, x_n \neq a\ \forall n$ platí $\lim_{n \to \infty} f(x_n) = A$

Heineho věta umožňuje tvrzení, vyslovená o limitách posloupností, převádět na limity funkcí v bodě.

Věta *(Věta o jednoznačnosti limity funkce)*
Funkce f má v každém bodě nejvýše jednu limitu.

Věta *(O lokální omezenosti funkce s vlastní limitou)*
Nechť funkce f má v bodě $a \in \mathbb{R}^*$ vlastní limitu. Potom existuje $\delta > 0$ takové, že f je na $P(a, \delta)$ omezená.

Věta *(Aritmetika limit pro funkce)*
Nechť $\lim_{x \to a} f(x) = A$, $\lim_{x \to a} g(x) = B$, $a \in R^*$. Potom

1. $\lim(f(x) + g(x)) = A + B$, je-li výraz na pravé straně definován.
2. $\lim(f(x)g(x)) = A \cdot B$, je-li výraz na pravé straně definován.
3. $\lim \frac{f(x)}{g(x)} = \frac{A}{B}$, je-li výraz na pravé straně definován.

Věta *(Limita a uspořádání - policajti pro funkce)*

1. Nechť $\lim_{x \to a} f(x) > \lim_{x \to a} g(x)$, $a \in R^*$.
   Potom $\exists P(a, \delta) : f(x) > g(x)\ \forall x \in P(a, \delta)$
2. Nechť $f(x) \leq g(x), \forall x \in P(a, \delta), \delta > 0$ a existují $\lim_{x \to a} f(x)$, $\lim_{x \to a} g(x)$.
   Potom $\lim_{x \to a} f(x) \leq \lim_{x \to a} g(x)$.
3. Nechť $f(x) \leq h(x) \leq g(x), \forall x \in P(a, \delta), \delta > 0$ a $\lim_{x \to a} f(x) = \lim_{x \to a} g(x)$.
   Potom existuje $\lim h(x)$ a $\lim_{x \to a} h(x) = \lim_{x \to a} f(x) = \lim_{x \to a} g(x)$.

Pozor na ostrost nerovností, v tomto případě je velmi důležitá.

Definice *(Jednostranná spojitost funkce v bodě)*

- *funkce f je spojitá v a* $\Leftrightarrow \lim_{x \to a} f(x) = f(a) \Leftrightarrow \forall \varepsilon > 0\ \exists \delta > 0 : f(B(a, \delta)) \subseteq B(f(a), \varepsilon)$
- *funkce f je spojitá v a zprava* $\Leftrightarrow \lim_{x \to a^+} f(x) = f(a) \Leftrightarrow \forall \varepsilon > 0\ \exists \delta > 0 : f(B^+(a, \delta)) \subseteq B(f(a), \varepsilon)$
- *funkce f je spojitá v a zleva* $\Leftrightarrow \lim_{x \to a^-} f(x) = f(a) \Leftrightarrow \forall \varepsilon > 0\ \exists \delta > 0 : f(B^-(a, \delta)) \subseteq B(f(a), \varepsilon)$

Věta *(O limitě složené funkce)*
Nechť $\lim_{x\to a} g(x) = A$, $\lim_{y\to A} f(y) = B$, $a, A, B \in \mathbb{R}^*$. Nechť navíc platí jeden z předpokladů:
(P1) f je spojitá v A *(vnější funkce je spojitá)*
(P2) $\exists\delta > 0 : g(x) \neq A$ pro $\forall x \in P(a, \delta)$ *(vnitřní je „lokálně prostá")*
Potom $\lim_{x\to a}(f \circ g)(x) = B$.

Definice *(Interval)*
Nechť $a, b \in \mathbb{R}^*, a < b$. Pak *otevřeným intervalem* (a, b) nazveme $\{x|a < x < b\}$, *(uzavřeným) intervalem* $\langle a, b\rangle$ (pro $a, b \in \mathbb{R}$) nazveme $I = \{x|a \leq x \leq b\}$. Uzavřený interval se někdy značí i $[a, b]$.

Věta *(Věta o limitě monotónní funkce)*
Nechť je funkce f monotónní na (a, b), $a, b \in \mathbb{R}^*, a < b$. Potom $\exists \lim_{x\to a^+} f(x)$, $\exists \lim_{x\to b^-} f(x)$.

Definice *(Spojitost na intervalu)*
Je-li $\langle a, b\rangle$ interval, pak a nazýváme počátečním bodem, b koncovým bodem a $x \in (a, b)$ vnitřními body.

Řekneme, že f *je spojitá na intervalu* I, jestliže je spojitá zprava ve všech bodech kromě koncového a spojitá zleva ve všech bodech kromě počátečního.

Věta *(O spojitém obrazu intervalu)*
Nechť funkce $f : I \to \mathbb{R}$ je spojitá na intervalu I. Potom $f(I)$ je také interval.

Věta *(Darbouxova o nabývaní mezihodnot)*
Nechť funkce f je spojitá na $\langle a, b\rangle$ a $f(a) < f(b)$, potom $\forall y \in (f(a), f(b))$ existuje $x \in (a, b)$ takové, že $f(x) = y$.

Definice
$f : M \to \mathbb{R}, M \subseteq \mathbb{R}$. f nabývá v bodě $a \in M$:

- *maxima* na M $\Leftrightarrow \forall x \in M : f(x) \leq f(a)$
- *minima* na M $\Leftrightarrow \forall x \in M : f(x) \geq f(a)$
- *ostrého maxima* na M $\Leftrightarrow \forall x \in M \setminus \{a\} : f(x) < f(a)$
- *ostrého minima* na M $\Leftrightarrow \forall x \in M \setminus \{a\} : f(x) > f(a)$
- *lokálního* maxima (minima, ostrého...)$\Leftrightarrow \exists\delta > 0 : f$ nabývá na $M \bigcap B(a, \delta)$ maxima (minima, ...)

Věta *(Vztah spojitosti a extrémů)*
Nechť f je spojitá na $\langle a, b\rangle$. Potom f nabývá na $\langle a, b\rangle$ svého maxima i minima.

Věta *(Vztah spojitosti a omezenosti)*
Spojitá funkce na uzavřeném intervalu $\langle a, b\rangle$ je omezená.

Definice *(prostá funkce, inverzní funkce)*
Funkce f je *prostá*, jestliže $\forall x, y \in D(f) : x \neq y \Rightarrow f(x) \neq f(y)$.

Nechť f je prostá na M, tedy $f : M \to f(M)$. Pak *inverzní funkce* f^{-1} k funkci f je definovaná na $f(M)$ předpisem: $y \in f(M)$, pak $f^{-1}(y) = x \Leftrightarrow y = f(x)$.

Věta *(O inverzní funkci)*
Nechť I je interval a funkce f je definovaná, spojitá a rostoucí (klesající) na I. Potom inverzní funkce f^{-1} je definována, spojitá a rostoucí (klesající) na $f(I)$.

2.3 Některé konkrétní funkce (polynomy, racionální lomené funkce, goniometrické a cyklometrické funkce, logaritmy a exponenciální funkce)

Věta *(Exponenciální funkce)*
Existuje právě jedna reálná funkce **exp**, splňující:

- $\exp(x + z) = \exp(x)\exp(z), \forall x, z \in \mathbb{R}$
- $\exp(x) \geq 1 + x, \forall x \in \mathbb{R}$

Poznámka *(Některé vlastnosti* exp*)*
Platí:

- $\exp 0 = 1$
- $\exp(-x) = \frac{1}{\exp x}$
- $\exp(x) \neq 0 \ \forall x \in \mathbb{R}$
- $\lim_{x\to\infty} \exp x = \infty$, $\lim_{x\to-\infty} \exp x = 0$
- exp je rostoucí na $\mathbb{R}$
- $\lim_{x\to 0} \frac{\exp x - 1}{x} = 1$

Věta *(Vlastnosti* log*)*
Funkce log, definovaná předpisem $\log = \exp^{-1}$ má následující vlastnosti:

- $D(\log) = (0, \infty)$, $\log((0, \infty)) \to \mathbb{R}$
- $\log(x \cdot y) = \log x + \log y, \forall x, y \in (0, \infty)$, $\log(x^n) = n \log x$
- log je spojitá, rostoucí na $(0, \infty)$, $\log 1 = 0$, $\log e = 1$
- $lim_{x\to 0_+} \log x = -\infty$, $lim_{x\to\infty} \log x = \infty$
- $lim_{x\to 1} \frac{\log x}{x-1} = 1$, $lim_{x\to 0} \frac{\log x+1}{x} = 1$

Definice *(obecná mocnina)*
Obecná mocnina $a^b = \exp(b \log a)$ pro $a > 0, b \in \mathbb{R}$. Speciálně pro $a = e : e^x = \exp x$

Věta
Existuje právě jedna reálná funkce s a právě jedna reálná funkce c taková, že:

- $s(x+y) = s(x)c(y) + c(x)s(y)$
- $c(x+y) = c(x)c(y) - s(x)s(y)$
- s je lichá, c sudá
- $s > 0$ *na* $(0,1), s(1) = 0$

Definice
Podle s a c definujeme *Goniometrické funkce*:
$\sin(x) = s(\frac{x}{\pi})$, $\cos(x) = c(\frac{x}{\pi})$, $\mathrm{tg}(x) = \frac{\sin(x)}{\cos(x)}$, $\mathrm{cotg}(x) = \frac{\cos(x)}{\sin(x)}$
Cyklometrické funkce:

- $\arcsin x = y \Leftrightarrow y \in < -\frac{\pi}{2}, \frac{\pi}{2} > \wedge \sin y = x$
- $\arccos x = y \Leftrightarrow y \in < 0, \pi > \wedge \cos y = x$
- $\mathrm{arctg}\ x = y \Leftrightarrow y \in (-\frac{\pi}{2}, \frac{\pi}{2}) \wedge \mathrm{tg}\ y = x$
- $\mathrm{arccotg}\ x = y \Leftrightarrow y \in (0, \pi) \wedge \mathrm{cotg}\ y = x$

a platí

$$\lim_{x\to 0} \frac{\arcsin x}{x} = 1$$
$$\lim_{x\to 0} \frac{\arccos x}{\sqrt{1-x}} = \lim_{x\to 0} \frac{\mathrm{arctg} x}{x} = 1$$

2.4 Derivace: definice a základní pravidla, věty o střední hodnotě, derivace vyšších řádů

Definice
Nechť f je reálná funkce jedné proměnné, $a \in \mathbb{R}$. Derivací funkce f v bodě a nazveme

$$f'(a) = \lim_{h\to 0} \frac{f(a+h) - f(a)}{h}, \text{ pokud existuje}$$

Derivací zprava a zleva rozumíme:

$$f'_+(a) = \lim_{h\to 0_+} \frac{f(a+h) - f(a)}{h},\ f'_-(a) = \lim_{h\to 0_-} \frac{f(a+h) - f(a)}{h}$$

Věta *(Vztah derivace a spojitosti)*
Má-li f v a vlastní derivaci, potom je f v a spojitá.

Věta *(Aritmetika derivací)*
Nechť existují $f'(a)$, $g'(a)$:

1. $(f+g)'(a) = f'(a) + g'(a)$, je-li pravá strana definována
2. je-li g nebo f spojitá v a, pak $(fg)'(a) = f'(a)g(a) + f(a)g'(a)$
3. je-li g spojitá v a, $g(a) \neq 0$, pak $(\frac{f}{g})'(a) = \frac{f'(a)g(a) - f(a)g'(a)}{g^2(a)}$

Věta *(O derivaci složené funkce)*
Nechť funkce f má derivaci v y_0, g má derivaci v x_0, g je spojitá v x_0 a $y_0 = g(x_0)$. Potom $(f \circ g)'(x_0) = f'(y_0) \cdot g'(x_0) = f'(g(x_0)) \cdot g'(x_0)$.

Věta *(O derivaci inverzní funkce)*
Nechť funkce f je na intervalu (a, b) spojitá a ryze monotonní a má v bodě $x_0 \in (a, b)$ derivaci $f'(x_0)$ vlastní a různou od nuly. Potom má funkce f^{-1} derivaci v bodě $y_0 = f(x_0)$ a platí rovnost

$$(f^{-1})'(y_0) = \frac{1}{f'(f^{-1}(y_0))}.$$

Poznámka
Pokud v situaci popsané v právě uvedené větě je $f'(x_0)$ nevlastní, je $(f^{-1})'(y_0) = 0$. Je-li $f'(x_0) = 0$, je $(f^{-1})'(y_0) = +\infty$ (je-li f rostoucí), resp. $= -\infty$ (je-li f klesající).

Věta *(Nutná podmínka lokálního extrému)*
Nechť $M \subseteq \mathbb{R}$, $f : M \to \mathbb{R}$. Nechť f má v $a \in M$ lokální extrém. Pak buď neexistuje $f'(a)$, nebo $f'(a) = 0$.

Věta *(Rolleova věta)*
Nechť f je spojitá na $\langle a, b\rangle$ a nechť existuje $f'(x)$ $\forall x \in (a, b)$. Nechť $f(a) = f(b)$. Potom existuje $\xi \in (a, b) : f'(\xi) = 0$.

Věta *(Lagrangeova o střední hodnotě)*
Nechť f je spojitá na $\langle a, b\rangle$ a nechť existuje $f'(x)$ $\forall x \in (a, b)$. Potom existuje

$$\xi \in (a, b) : f'(\xi) = \frac{f(b) - f(a)}{b - a}$$

Věta *(Cauchyova o střední hodnotě)*
Nechť f a g jsou spojité na $\langle a, b\rangle$, nechť existuje $f'(x)$ $\forall x \in (a, b)$ a nechť existuje $g'(x)$ vlastní a nenulové. Potom existuje

$$\xi \in (a, b) : \frac{f(b) - f(a)}{g(b) - g(a)} = \frac{f'(\xi)}{g'(\xi)}$$

Důkaz
$g(a) \neq g(b)$, neboť jinak by podle Rolleovy věty existovalo $\xi \in (a, b) : g'(\xi) = 0$. Definujeme $H(x) = (f(x) - f(a))(g(b) - g(a)) - (g(x) - g(a))(f(b) - f(a))$. Potom $H(a) = H(b) = 0$, H je spojitá na $\langle a, b\rangle \Rightarrow \exists H' na (a, b)$. Tedy podle Rolleovy věty $\exists \xi : 0 = H'(\xi) = f'(\xi)(g(b) - g(a)) - g'(\xi)(f(b) - f(a))$. Tedy $\frac{f(b)-f(a)}{g(b)-g(a)} = \frac{f'(\xi)}{g'(\xi)}$, neboť $g'(\xi) \neq 0$ a $g(b) - g(a) \neq 0$

□

Věta *(L'Hospitalovo pravidlo)*
Nechť $a \in \mathbb{R}^*$ a funkce f, g jsou definovány na nějakém $P(a,\delta)$, f, g mají v $P(a,\delta)$ vlastní derivaci, $\forall x \in P(a,\delta) : g'(x) \neq 0$ a existuje $\lim_{x\to a} \frac{f'(x)}{g'(x)}$. Nechť platí i jedna z následujících podmínek:

1. $\lim_{x\to a} f(x) = \lim_{x\to a} g(x) = 0$
2. $\lim_{x\to a+} |g(x)| = +\infty$

Potom existuje i $\lim_{x\to a} \frac{f(x)}{g(x)}$ a platí $\lim_{x\to a} \frac{f(x)}{g(x)} = \lim_{x\to a} \frac{f'(x)}{g'(x)}$.

Věta *(O limitě derivací)*
Nechť funkce f je spojitá zprava v $a \in \mathbb{R}$ a nechť existuje $\lim_{x\to a+} f'(x) = A \in \mathbb{R}^*$. Potom $f'_+(a) = A$.

Věta *(Vztah derivace a monotonie)*
Nechť I je nezdegenerovaný interval (tj. nejde o jediný bod) a $Int(I) = \{vnitřní\ body\ I\}$. Nechť f je spojitá na I a existuje f' vlastní na $Int(I)$.:

1. je-li $f' > 0$ na $Int(I)$, pak f je rostoucí na I
2. je-li $f' \geq 0$ na $Int(I)$, pak f je neklesající na I
3. je-li $f' < 0$ na $Int(I)$, pak f je klesající na I
4. je-li $f' \leq 0$ na $Int(I)$, pak f je nerostoucí na I

Definice *(Tečna, inflexe)*
Nechť funkce f má v $a \in \mathbb{R}$ vlastní derivaci. Označíme $T_a = \{[x,y] \in \mathbb{R}^2, y = f(a) + f'(a)(x-a)\}$. Řekneme, že $[x, f(x)] \in \mathbb{R}^2$ leží nad (pod) tečnou T_a, jestliže $f(x) > f(a) + f'(a)(x-a)$ $(f(x) < f(a) + f'(a)(x-a))$.

Nechť f má v $a \in \mathbb{R}$ vlastní derivaci. Řekneme, že f má v a *inflexi*, jestliže $\exists \delta > 0$: buď $\forall x \in (a-\delta, a) : [x, f(x)]$ leží nad $T_a \wedge \forall x \in (a, a+\delta) : [x, f(x)]$ leží pod T_a, nebo opačně.

Věta *(Nutná podmínka existence inflexe)*
Jestliže $f''(a) \neq 0$, pak f nemá v a inflexi.

Věta *(Postačující podmínka existence inflexe)*
Nechť f má spojitou první derivaci na (a,b). Nechť $z \in (a,b)$. Nechť $\forall x \in (a,z) : f''(x) > 0$ a $\forall x \in (z,b) : f''(x) < 0$ (nebo naopak). Pak z je bod inflexe f.

Definice
Řekneme, že funkce f je na intervalu I:

- *konvexní*, jestliže pro každé $x_1, x_2 \in I$ a každé $\lambda \in \langle 0,1 \rangle$ platí $f(\lambda x_1 + (1-\lambda)x_2) \leq \lambda \cdot f(x_1) + (1-\lambda) \cdot f(x_2)$.
- *konkávní*, jestliže pro každé $x_1, x_2 \in I$ a každé $\lambda \in \langle 0,1 \rangle$ platí $f(\lambda x_1 + (1-\lambda)x_2) \geq \lambda \cdot f(x_1) + (1-\lambda) \cdot f(x_2)$.
- *ryze konvexní*, jestliže pro každé $x_1, x_2 \in I, x_1 \neq x_2$ a každé $\lambda \in (0,1)$ platí $f(\lambda x_1 + (1-\lambda)x_2) < \lambda \cdot f(x_1) + (1-\lambda) \cot f(x_2)$.
- *ryze konkávní*, jestliže pro každé $x_1, x_2 \in I, x_1 \neq x_2$ a každé $\lambda \in (0,1)$ platí $f(\lambda x_1 + (1-\lambda)x_2) > \lambda \cdot f(x_1) + (1-\lambda) \cdot f(x_2)$.

Věta
Nechť funkce f je konvexní na I a $a \in Int(I)$. Potom $\exists f'_+(a) \in \mathbb{R}$ a $\exists f'_-(a) \in \mathbb{R}$. Tj. konvexnost implikuje existenci vlastních jednostranných derivací, neznamená to ale, že existuje derivace.

Věta *(Vztah konvexity a spojitosti)*
Nechť f je konvexní na otevřeném intervalu (a, b). Pak f je na (a, b) spojitá.

Věta
Nechť f má spojitou první derivaci na $I = (a, b)$. Potom:

- $f''(x) > 0 \ \forall x \in (a, b)$, pak f je ryze konvexní na (a, b)
- $f''(x) \geq 0 \ \forall x \in (a, b)$, pak f je konvexní na (a, b)
- $f''(x) < 0 \ \forall x \in (a, b)$, pak f je ryze konkávní na (a, b)
- $f''(x) \leq 0 \ \forall x \in (a, b)$, pak f je konkávní na (a, b)

Definice *(Asymptota)*
Funkce f má *asymptotu* $ax + b$ v $+\infty$ $(-\infty)$, jestliže f je definována na nějakém okolí $+\infty(-\infty)$ a platí

$$\lim_{\substack{x \to \infty \\ (x \to -\infty)}} (f(x) - ax - b) = 0$$

Věta *(Výpočet asymptoty)*
Funkce f má v ∞ asymptotu $ax + b$, právě když

$$\lim_{x \to \infty} \frac{f(x)}{x} = a \in \mathbb{R}, \ \lim_{x \to \infty} (f(x) - ax) = b \in \mathbb{R}$$

Analogicky pro $-\infty$.

2.5 Některé aplikace (průběhy funkcí, Newtonova metoda hledání nulového bodu, Taylorův polynom se zbytkem)

Vyšetření průběhu funkce:

1. Určíme definiční obor a obor spojitosti funkce.
2. Zjistíme symetrie: lichost, sudost, periodicita.
3. Dopočítáme limity v „krajních bodech definičního oboru".
4. Spočítáme první derivaci (tam, kde existuje, případně jednostranné derivace), určíme intervaly monotonie a nalezneme lokální a globální extrémy. Určíme obor hodnot.
5. Spočteme druhou derivaci a určíme intervaly, kde funkce f je konvexní nebo konkávní. Určíme inflexní body.
6. Vypočteme asymptoty funkce.
7. Načrtneme graf funkce.

Taylorův polynom se zbytkem

Definice

Nechť f je reálná funkce, $a \in \mathbb{R}$, $n \in \mathbb{N}$ a f má derivace do řádu n. Pak funkci

$$T_n^{f,a}(x) = f(a) + f'(a)(x-a) + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n$$

nazýváme *Taylorovým polynomem funkce f řádu n v bodě a.*

Věta

Nechť f je reálná funkce, $a \in \mathbb{R}$, nechť existuje vlastní $f^{(n)}(a)$. Nechť P je polynom stupně $\leq n$. Pak

$$\lim_{x \to a} \frac{f(x) - P(x)}{(x-a)^n} = 0 \Leftrightarrow P = T_n^{f,a}$$

Věta *(Obecný tvar zbytku)*

Nechť f má vlastní (n+1)-ní derivaci v intervalu $\langle a, x \rangle$, $x > a$. Nechť φ je spojitá funkce na $\langle a, x \rangle$, která má na (a, x) vlastní nenulové derivace. Pak:

$$\exists \xi \in (a, x) : R_n^{f,a}(x) = f(x) - T_n^{f,a}(x) = \frac{1}{n!} . \frac{\varphi(x) - \varphi(a)}{\varphi'(\xi)} . f^{(n+1)}(\xi) . (x - \xi)^n$$

Důkaz

Věta je důsledkem Cauchyho věty o střední hodnotě, aplikované na funkci $F(t) := f(x) - T_n^{f,t}(x)$, definované pro $t \in [a, x]$. (Ošklivou a pracnou) derivací této funkce vyjde, že $F'(t) = -\frac{f^{(n+1)}(t)}{n!}(x-t)^n$ $\forall t \in (a, x)$ a teď použijeme onu Cauchyho větu a dostaneme

$$\frac{-\frac{f^{(n+1)}(\xi)}{n!}(x-\xi)^n}{\varphi'(\xi)} = \frac{F'(\xi)}{\varphi'(\xi)} = \frac{F(x) - F(a)}{\varphi(x) - \varphi(a)} = \frac{0 - R_n^{f,a}(x)}{\varphi(x) - \varphi(a)}$$

což už dává kýžený tvar zbytku.

$\square$

Důsledek

Lagrangeův tvar zbytku: Je-li $\varphi(t) = (x-t)^{n+1}$, dostaneme

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

Cauchyho tvar zbytku: Je-li $\varphi(t) = t$, dostaneme

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

Newtonova metoda hledání nulového bodu

Zdroje:
`http://www.kvd.zcu.cz/cz/materialy/numet/_numet.html#_Toc501178905`,
`http://www.mojeskola.cz/Vyuka/Php/Learning/Derivace/matika_krokem5.php`
:-)

Newtonova metoda je numerická…

Jde o nalezení nulového bodu nějaké funkce, tedy bodu, kde $f(x) = 0$ pro nějakou reálnou funkci f na intervalu $\langle A, B\rangle$.

Jako první aproximaci (x_1) kořene rovnice v intervalu $\langle A, B\rangle$ použijeme střed tohoto intervalu. V něm sestrojíme tečnu a její průsečík s osou x je novou aproximací (x_2) kořene. V tomto bodě sestrojíme opět tečnu atd.

Další, přesnější, novou aproximaci kořene tedy hledáme jako průsečík tečny ve staré aproximaci s osou x.

Máme-li řešit rovnici $f(x) = 0$, pak rovnice tečny ve starém průsečíku (x_n) bude $y - f(x_n) = f'(x_n)(x - x_n)$ Průsečík s osou x získáme vyjádřením x z rovnice: $0 - f(x_n) = f'(x_n)(x - x_n)$ Tedy: $x = x_n - \frac{f(x_n)}{f'(x_n)}$ Tento průsečík bude novou aproximací (x_{n+1}) kořene.

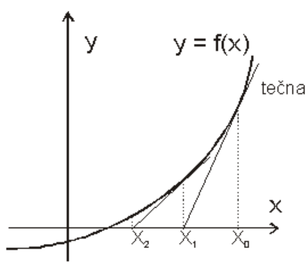
Výsledný vztah pro výpočet nové aproximace tedy zní:

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

Lze očekávat při každé iteraci dojde ke zdvojnásobení počtu platných číslic. Pro odhad chyby lze použít vzorec $chyba \leq \frac{|f(x_i)|}{m}$, kde m je minimum hodnoty první derivace v intervalu od počáteční aproximace ke kořeni. Nevýhodou této metody je ovšem to, že nemusí konvergovat vždy. Také kriterium použitelnosti může značně omezit oblast jejího používání:

- funkce musí být v okolí kořene spojitá
- funkce nesmí mít v okolí kořene nulovou derivaci a musí být splněna podmínka $\left|\frac{f(x)f''(x)}{[f'(x)]^2}\right| \leq m < 1$

Řešení je pro konvexní i konkávní funkce stejné, pouze je zapotřebí jinak volit výchozí bod. U konvexních funkcí je zapotřebí zvolit výchozí bod nad očekávaným kořen a přibližovat se k němu shora. U konkávních funkcí je třeba zvolit výchozí pod kořenem a ke kořenu se přibližovat zdola. Princip Newtonovy metody pro konvexní funkce je znázorněn na následujícím obrázku:



3 Posloupnosti a řady funkcí

Požadavky

- Spojitost za předpokladu stejnoměrné konvergence
- Mocninné řady
- Taylorovy řady
- Fourierovy řady

Táto otázka je vypracovaná hlavne podľa skrípt prof. Kalendu, takže je možné že niektoré vety (napr. od prof. Pultra) budú mať iné znenie. Hlavne časť o Fourierových funkciách vyzerá byť prednášaná odlišne (menej obecne)... ;-(

andree

3.1 Spojitost za předpokladu stejnoměrné konvergence

Definice *(Bodová/stejnoměrná konvergence posloupnosti funkcí)*
Řekneme, že posloupnost funkcí f_n *konverguje bodově k funkci* f *na množině* M (značíme $f_n \to f$), jestliže pro každé $x \in M$ platí $\lim_{n\to\infty} f_n(x) = f(x)$, tj. jestliže

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

Řekneme, že posloupnost f_n *konverguje stejnoměrně k funkci* f *na množině* M (značíme $f_n \rightrightarrows f$), jestliže

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

Řekneme že posloupnost funkcí je *stejnoměrně konvergentní* na M, jestliže konverguje k nějaké funkci na M.

Definice
$\{f_n\}$ *konverguje lokálně stejnoměrně* k funkci f na množině M (značíme $f_n \rightrightarrows^{loc} f$ na M), jestliže pro každé $x \in M$ existuje $\varepsilon > 0$ takové, že $f_n \rightrightarrows f$ na $M \cap (x - \varepsilon, x + \varepsilon)$.

Věta *(Kritérium stejnoměrné konvergence)*
Nechť M je (neprázdná) množina, f funkce definovaná na M a $\{f_n\}_{n=1}^{\infty}$ posloupnost funkcí definovaných na M. Pak $f_n \rightrightarrows f$, právě když:

$$\lim_{n\to\infty} \sup\{|f_n(x) - f(x)|; x \in M\} = 0,$$

tj. existuje $n_0 \in \mathbb{N}$ takové, že pro $n \geq n_0$ je $sup\{|f_n(x) - f(x)|; x \in M\}$ definováno (a konečné) a tato posloupnost má limitu 0.

Věta *(Bolzano-Cauchyho podmínka pro stejnoměrnou konvergenci)*
Nechť M je (neprázdná) množina, $\{f_n\}_{n=1}^{\infty}$ posloupnost funkcí definovaných na M. Pak posloupnost f_n je stejnoměrně konvergentní na M, právě když:

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

Věta *(O záměně limit, Moore-Osgoodova)*

Nechť $a, b \in \mathbb{R}^*, a < b$, f je funkce definovaná na (a, b) a $\{f_n\}_{n=1}^{\infty}$ posloupnost funkcí definovaných na (a, b). Dále nechť $f_n \rightrightarrows f$ na (a, b) a pro každé $n \in \mathbb{N}$ existuje vlastní $\lim_{x \to a+} f_n(x) = c_n$. Pak existují vlastní limity $\lim_{n\to\infty} c_n$ a $\lim_{x\to a+} f(x)$ a platí:

$$\lim_{n\to\infty} c_n = \lim_{x\to a+} f(x)$$

Analogicky v bodě b zleva…

Poznámka

Jiný zápis je, že platí:

$$\lim_{n\to\infty} \lim_{x\to a+} f_n(x) = \lim_{x\to a+} \lim_{n\to\infty} f_n(x)$$

a navíc jsou tyto limity vlastní, pokud pro každé $n \in \mathbb{N}$ existuje vlastní limita $\lim_{x\to a+} f_n(x)$ a posloupnost f_n je stejnoměrně konvergentní na (a, b) pro nějaké $b > a$. Tato věta platí i pro „oboustranné“ limity.

Věta *(Spojitost limitní funkce)*

Nechť $I \subset \mathbb{R}$ je interval, f funkce definovaná na I a $\{f_n\}_{n=1}^{\infty}$ posloupnost funkcí definovaných na I. Jestliže f_n je spojitá na I pro každé $n \in \mathbb{N}$ a $f_n \rightrightarrows^{loc} f$ na I, pak f je spojitá na I.

Věta *(Záměna limity a derivace)*

Nechť $a, b \in \mathbb{R}, a < b$ a $\{f_n\}_{n=1}^{\infty}$ je posloupnost funkcí definovaných na intervalu (a, b), které mají v každém bodě (a, b) vlastní derivaci. Nechť dále platí:

1. Existuje takové $x_0 \in (a, b)$, že posloupnost $\{f_n(x_0)\}$ je konvergentní
2. Posloupnost $\{f_n'\}$ je stejnoměrně konvergentní na (a, b)

Pak posloupnost $\{f_n\}$ je stejnoměrně konvergentní na (a, b), a označíme-li f její limitu, pak funkce f má v každém bodě $x \in (a, b)$ vlastní derivaci a platí $f'(x) = \lim_{n\to\infty} f_n'(x)$.

Definice *(Bodová/stejnoměrná konvergence řady funkcí)*

Řekneme, že řada $\sum_{n=1}^{\infty} u_n$ *konverguje bodově na množině* M, pokud posloupnost jejich částečných součtů je bodově konvergentní na M, tj, pro každé $x \in M$ konverguje řada $\sum_{n=1}^{\infty} u_n(x)$.

Součtem řady $\sum_{n=1}^{\infty} u_n$ nazveme funkci

$$S(x) = \sum_{n=1}^{\infty} u_n(x) = \lim_{n\to\infty} s_n(x),\ x \in M,$$

pokud řada konverguje bodově na M.

Řekneme, že řada $\sum_{n=1}^{\infty} u_n$ *konverguje stejnoměrně na množině* M, pokud posloupnost jejich částečných součtů je stejnoměrně konvergentní na M.

Je-li navíc $M \subset \mathbb{R}$, řekneme, že řada $\sum_{n=1}^{\infty} u_n$ *konverguje lokálně stejnoměrně na množině* M, pokud posloupnost jejich částečných součtů je lokálně stejnoměrně konvergentní.

Věta *(Nutná podmínka stejnoměrné konvergence řady)*
Nechť řada $\sum_{n=1}^{\infty} u_n$ konverguje stejnoměrně na množině M. Pak $u_n \rightrightarrows 0$ na M.

Věta *(Srovnávací kritérium pro stejnoměrnou konvergenci)*
Nechť M je (neprázdná) množina a $\{u_n\}_{n=1}^{\infty}$, $\{v_n\}_{n=1}^{\infty}$ dvě posloupnosti funkcí definovaných na M, pro které platí $|u_n(x)| \leq v_n(x)$ pro všechna $x \in M$. Jestliže řada $\sum_{n=1}^{\infty} v_n$ konverguje stejnoměrně na M, pak i řada $\sum_{n=1}^{\infty} u_n$ konverguje stejnoměrně na M.

Věta *(Weierstrassovo kritérium)*
Nechť M je (neprázdná) množina, $\{u_n\}_{n=1}^{\infty}$ posloupnost funkcí definovaných na M a $\sum_{n=1}^{\infty} c_n$ konvergentní řada reálných čísel. Pokud pro každé $x \in M$ platí $|u_n(x)| \leq c_n$, pak řada $\sum_{n=1}^{\infty} u_n$ konverguje stejnoměrně na M.

Věta *(Leibnizovo kritérium pro stejnoměrnou konvergenci)*
Nechť M je (neprázdná) množina, $\{u_n\}_{n=1}^{\infty}$ posloupnost funkcí definovaných na M splňujících *obě* podmínky:

1. Pro všechna $x \in M$ a $n \in \mathbb{N}$ je $u_n(x) \geq u_{n+1}(x) \geq 0$
2. $u_n \rightrightarrows 0$ na M

Pak řada $\sum_{n=1}^{\infty} (-1)^n u_n$ konverguje stejnoměrně na M.

Věta *(Dirichletovo a Abelovo kritérium)*
Nechť M je (neprázdná) množina a $\{u_n\}_{n=1}^{\infty}$, $\{v_n\}_{n=1}^{\infty}$ dvě posloupnosti funkcí definovaných na M, přičemž pro každé $x \in M$ a každé $n \in \mathbb{N}$ platí $v_n(x) \geq v_{n+1}(x) \geq 0$. Nechť navíc platí alespoň jedna z podmínek:

1. (Abelovo) Řada $\sum_{n=1}^{\infty} u_n$ konverguje stejnoměrně na M, pro každé pevné x je posloupnost hodnot funkcí $\{v_n(x)\}$ monotónní (klidně pro každé x jinak) a existuje $K \in \mathbb{R}$ takové, že $\forall n \in \mathbb{N}\ \forall x \in M : |v_n(x)| < K$ (tj. $\{v_n\}$ je stejnoměrně omezená na M).

2. (Dirichletovo) Existuje $K \in \mathbb{R}$ takové, že pro všechna $x \in M$ a $n \in \mathbb{N}$ je $|u_1(x) + \cdots + u_n(x)| \leq K$ (tj. posloupnost část. součtů $\{\sum_{i=1}^{n} u_n(x)\}$ je *stejnoměrně omezená* na M) a dále $v_n \rightrightarrows 0$ na M (konverguje stejnoměrně k nulové funkci).

   Pak řada $\sum_{n=1}^{\infty} u_n \cdot v_n$ konverguje stejnoměrně na M.

(*Pozn. autora: Dále platí i věty ekvivalentní větám o záměně limit při posloupnostech...*)

3.2 Mocninné řady

Definice
Nechť $a \in \mathbb{R}$ a $\{c_n\}_{n=0}^{\infty}$ je posloupnost reálných čísel. Nekonečnou řadu funkcí tvaru $\sum_{n=0}^{\infty} c_n(x-a)^n$ nazýváme *mocninnou řadou o středu a*.

Definice

Nechť $\sum_{n=0}^{\infty} c_n(x-a)^n$ je mocninná řada o středu a. Jejím *poloměrem konvergence* rozumíme číslo

$$R = \sup\{r \in \langle 0, +\infty) \,;\, \sum_{n=0}^{\infty} |c_n| r^n \textit{konverguje}\},$$

je-li uvedená množina shora omezená. Není-li shora omezená, klademe $R = +\infty$.

Věta

Nechť $\sum_{n=0}^{\infty} c_n(x-a)^n$ je mocninná řada o středu a a R její poloměr konvergence.

1. Je-li $|x-a| < R$, pak řada $\sum_{n=0}^{\infty} c_n(x-a)^n$ konverguje absolutně;
   Je-li $|x-a| > R$, pak řada $\sum_{n=0}^{\infty} c_n(x-a)^n$ diverguje.
2. Je-li $r \in (0, R)$, pak řada $\sum_{n=0}^{\infty} c_n(x-a)^n$ konverguje stejnoměrně na množině $\overline{B}(a,r) = \{x \in \mathbb{R}; |x-a| \leq r\} = \langle a-r, a+r \rangle$.
3. Řada $\sum_{n=0}^{\infty} c_n(x-a)^n$ konverguje lokálně stejnoměrně na množině $B(a,R) = \{x \in \mathbb{R}; |x-a| < R\}$.

Body 2. a 3. jsou vlastně ekvivalentní. Je-li $R = \infty$, pak řada konverguje lokálně stejnoměrně na celém $\mathbb{R}$.

Poznámka

Množině $B(a,R)$, kde R je poloměr konvergence mocninné řady $\sum_{n=0}^{\infty} c_n(x-a)^n$, se říká *kruh konvergence.*

Věta *(Výpočet poloměru konvergence)*

Nechť $\sum_{n=0}^{\infty} c_n(x-a)^n$ je mocninná řada o středu a a R její poloměr konvergence.

1. Jestliže $L = \limsup_{n\to\infty} \sqrt[n]{|c_n|}$, pak
$$R = \begin{cases} \frac{1}{L}, & L > 0, \\ +\infty, & L = 0 \end{cases}$$
2. Týž vzoreček platí, je-li $L = \limsup_{n\to\infty} \left|\frac{c_{n+1}}{c_n}\right|$

První bod plyne z Cauchyova odmocninového kritéria konvergence řady, druhý z D'Alembertova podílového kritéria. Stejné tvrzení platí i pro limity daných výrazů v případě, že existují.

Věta *(…„jen“ pomocná pro následující)*

Nechť $\sum_{n=0}^{\infty} c_n(x-a)^n$ je mocninná řada o středu a a R její poloměr konvergence. Pak i mocninné řady $\sum_{n=0}^{\infty} n.c_n(x-a)^{n-1}$ a $\sum_{n=0}^{\infty} \frac{c_n}{n+1}(x-a)^{n+1}$ mají poloměr konvergence R.

Věta *(Derivace a integrace mocninné řady)*

Nechť $\sum_{n=0}^{\infty} c_n(x-a)^n$ je mocninná řada o středu a a $R > 0$ její poloměr konvergence. Definujme funkci $f(x) = \sum_{n=0}^{\infty} c_n(x-a)^n, x \in B(a,R)$. Pak platí:

1. Funkce f je spojitá na $B(a,R)$.
2. Funkce f má v každém bodě $x \in B(a,R)$ vlastní derivaci a platí $f'(x) = \sum_{n=0}^{\infty} n \cdot c_n(x-a)^{n-1}$.
3. Funkce $F(x) = \sum_{n=0}^{\infty} \frac{c_n}{n+1}(x-a)^{n+1}$ je primitivní funkcí k f na $B(a,R)$.

3.3 Taylorovy řady

Definice

Nechť funkce f má v bodě a derivace všech řádů. Pak řadu $\sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n$ nazýváme *Taylorovou řadou funkce f o středu a v bodě x.*

Poznámka

Nechť funkce f má v bodě a derivace všech řádů a $x \in \mathbb{R}$. Pak funkce f je v bodě x součtem své Taylorovy řady o středu a, právě když $\lim_{n\to\infty}(f(x) - T_n^a(x)) = 0$.

Věta

Nechť $x > a$ a funkce f má v každém bodě intervalu $\langle a, x\rangle$ derivace všech řádů. Jestliže platí podmínka

- existuje $C \in \mathbb{R}$ takové, že pro každé $t \in (a, x)$ a každé $n \in \mathbb{N}$ je $|f^{(n)}(t)| \leq C$,

pak funkce f je v bodě x součtem své Taylorovy řady o středu a. Analogicky pro případ $x < a$.

Věta

Nechť $\sum_{n=0}^{\infty} c_n(x-a)^n$ je mocninná řada o středu a a $R > 0$ její poloměr konvergence. Definujme funkci $f(x) = \sum_{n=0}^{\infty} c_n(x-a)^n$, $x \in B(a, R)$. Pak řada

$$\sum_{n=0}^{\infty} c_n(x-a)^n$$

je *Taylorovou řadou funkce f* o středu a, tj. pro každé $n \in \mathbb{N} \cup \{0\}$ platí $c_n = \frac{f^{(n)}(a)}{n!}$.

Význam Taylorových řad:

- aproximace funkcí – příklady (Taylorovy řady elementárních funkcí):

$$\forall x \in \mathbb{R} : \exp x = \sum_{k=0}^{\infty} \frac{1}{k!} x^k$$

$$\forall x \in \mathbb{R} : \sin x = \sum_{k=0}^{\infty} \frac{(-1)^{k-1}}{(2k-1)!} x^{2k-1} \qquad \ldots$$

- zjednodušení důkazů – příklad (Důkaz binomické věty):

  Rozvineme funkci $f(x) = (1+x)^\alpha$ v okolí nuly. Indukcí lze ověřit, že $f^{(k)}(x) = \alpha(\alpha-1)\cdot \cdots \cdot(\alpha-k+1)\cdot(1+x)^{\alpha-k}$. Taylorova řada funkce $f(x) = (1+x)^\alpha$ konverguje na $(-1, 1)$ a je rovna hodnotě $(1+x)^\alpha$:

$$(1+x)^\alpha = \sum_{k=0}^{\infty} \frac{\alpha(\alpha-1)\cdot\cdots\cdot(\alpha-k+1)}{k!} x^k = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k$$

  a to dává binomickou větu.

3.4 Fourierovy řady

3.4.1 Obecné Fourierovy řady

Definice

Nechť $\{\varphi_n\}_{n=1}^{\infty}$ je posloupnost komplexních funkcí na $\langle a, b\rangle$, z nichž žádná není konstantně nulová. Řekneme, že tato posloupnost tvoří *ortogonální (krátce OG) systém na* $\langle a, b\rangle$, jestliže pro každá dvě různá $m, n \in \mathbb{N}$ platí:

$$\int_a^b \varphi_m \overline{\varphi_n} = 0$$

Pokud navíc

$$\int_a^b |\varphi_n|^2 = 1$$

pro všechna $n \in \mathbb{N}$, říkáme, že jde o *ortonormální systém.*

Poznámka

Příklady OG systémů:

- Systém tvořený funkcemi $\exp \frac{2k\pi i x}{p}, k \in \mathbb{Z}$ je OG na intervalu $\langle a, a+p\rangle$ pro každé $a \in \mathbb{R}$
- Systém tvořený funkcemi $1, \cos \frac{2k\pi x}{p}, \sin \frac{2k\pi x}{p}, k \in \mathbb{N}$ je OG na intervalu $\langle a, a+p\rangle$ pro každé $a \in \mathbb{R}$

Věta

Nechť $\{\varphi_n\}_{n=1}^{\infty}$ je posloupnost komplexních funkcí na $\langle a, b\rangle$, $\{a_n\}_{n=0}^{\infty}$ je posloupnost komplexních čísel. Jestliže

$$f(x) = \sum_{n=1}^{\infty} a_n \varphi_n(x),\ x \in \langle a, b\rangle\,,$$

a uvedená řada konverguje stejnoměrně na $\langle a, b\rangle$, pak pro každé $n \in \mathbb{N}$ platí

$$a_n = \frac{\int_a^b f\overline{\varphi_n}}{\int_a^b |\varphi_n|^2}.$$

Definice *(po částech spojitá funkce)*

Řekneme, že funkce f je *po částech spojitá na* $\langle a, b\rangle$, jestliže existuje $D = \{x_i\}_{j=0}^{N}$ dělení intervalu $\langle a, b\rangle$ takové, že pro každé $j \in \{1, \ldots, N\}$ je funkce f spojitá na intervalu (x_{j-1}, x_j) a v krajních bodech tohoto intervalu má vlastní jednostranné limity.

Definice

Nechť $\{\varphi_n\}_{n=1}^{\infty}$ je OG systém na $\langle a,b\rangle$ a funkce f je po částech spojitá na $\langle a,b\rangle$. Pro $n\in\mathbb{N}$ položme

$$a_n=\frac{\int_a^b f\overline{\varphi_n}}{\int_a^b|\varphi_n|^2}.$$

Tato čísla nazýváme *Fourierovými koeficienty funkce f vzhledem k OG systému $\{\varphi_n\}_{n=1}^{\infty}$ na $\langle a,b\rangle$* a řadu

$$\sum_{n=1}^{\infty}a_n\varphi_n$$

nazýváme *Fourierovou řadou f vzhledem k OG systému $\{\varphi_n\}_{n=1}^{\infty}$ na $\langle a,b\rangle$*.

3.4.2 Trigonometriké Fourierovy řady

Definice *(po částech spojitá periodická funkce)*

Buď funkce f periodická s periodou $p>0$. Řekneme, že je *po částech spojitá*, je-li po částech spojitá na intervalu $\langle 0,p\rangle$.

Poznámka

Nechť f je p-periodická funkce a $a,b\in\mathbb{R}$.

1. Pak f je počástech spojitá na $\langle a,a+p\rangle$, právě když je po částech spojitá na $\langle b,b+p\rangle$.
2. $\int_a^{a+p}f=\int_b^{b+p}f$, pokud alespoň jeden z těchto integrálů existuje.

Definice

Nechť funkce f je p-periodická po částech spojitá funkce. Jejími *trigonometrickými Fourierovými koeficienty* rozumíme čísla

$$a_n=\frac{2}{p}\int_0^p f(x)\cos\frac{2\pi nx}{p}dx,\ n\in\mathbb{N}\cup\{0\}$$

$$b_n=\frac{2}{p}\int_0^p f(x)\sin\frac{2\pi nx}{p}dx,\ n\in\mathbb{N}$$

Definice

Trigonometrickou Fourierovou řadou funkce f pak rozumíme řadu

$$\frac{a_0}{2}+\sum_{n=1}^{\infty}\left(a_n\cos\frac{2\pi nx}{p}+b_n\sin\frac{2\pi nx}{p}\right)$$

Poznámka *(Besselova nerovnost)*

Besselova nerovnost pro trigonometrické Fourierovy řady má tvar

$$\frac{|a_0|^2}{4}p + \sum_{n=1}^{\infty}(|a_n|^2 + |b_n|^2)\frac{p}{2} \leq \int_0^p |f|^2.$$

Podobná nerovnost platí i pro obecné Fourierovy řady.

(Riemann-Lebesgue) důsledkem této nerovnosti je fakt, že $\lim a_n = \lim b_n = 0$.

Věta *(Persevalova rovnost)*

Pro trigonometrické Fourierovy řady platí v Besselově nerovnosti rovnost. Pro funkce s periodou 2π potom platí:

$$\frac{1}{\pi}\int_{-\pi}^{\pi} |f|^2 = \frac{|a_0|^2}{2} + \sum_{n=1}^{\infty}(|a_n|^2 + |b_n|^2) \text{ \textit{(jedna z variant zápisu)}}$$

Poznámka

Nechť f je p-periodická po částech spojitá funkce taková, že všechny její trigonometrické Fourierovy koeficienty jsou nulové. Pak $f(x) = 0$ pro všechna $x \in \langle 0, p\rangle$ s výjimkou konečně mnoha bodů.

Věta *(Symetrie funkce a Trigonometrické Fourierovy koeficienty)*

Nechť f je p-periodická po částech spojitá funkce, $a_n, n \in \mathbb{N} \cup \{0\}$ a $b_n, n \in \mathbb{N}$, její trigonometrické Fourierovy koeficienty. Pak platí

1. Pro všechna $n \in \mathbb{N} \cup \{0\}$ je $a_n = 0$, právě když $f(-x) = -f(x)$ pro všechna $x \in \langle 0, p\rangle$ s výjimkou konečně mnoha bodů.
2. Pro všechna $n \in \mathbb{N}$ je $b_n = 0$, právě když $f(-x) = f(x)$ pro všechna $x \in \langle 0, p\rangle$ s výjimkou konečně mnoha bodů.

Definice

Nechť f je p-periodická po částech spojitá funkce. Řekneme, že f je *po částech hladká*, jestliže f' je po částech spojitá.

Věta *(O konvergenci Fourierových řad)*

Nechť f je po částech hladká p-periodická funkce. Pak platí:

1. Trigonometrická Fourierova řada funkce f konverguje bodově na $\mathbb{R}$ a její součet v bodě $x \in \mathbb{R}$ je $\frac{1}{2}\left(\lim_{t\to x-} f(t) + \lim_{t\to x+} f(t)\right)$
2. Je-li f navíc spojitá na intervalu (a, b), pak její trigonometrická Fourierova řada konverguje lokálně stejnoměrně na (a, b) a její součet je $f(x)$ pro každé $x \in (a, b)$.
3. Je-li navíc spojitá na $\mathbb{R}$, pak její trigonometrická Fourierova řada konverguje stejnoměrně na $\mathbb{R}$ a její součet je $f(x)$ pro každé $x \in \mathbb{R}$.

4 Integrál

Požadavky

- Primitivní funkce, metody výpočtu
- Určitý (Riemannův) integrál, užití určitého integrálu
- Vícerozměrný integrál a Fubiniho věta

4.1 Primitivní funkce, metody výpočtu

Definice

Nechť funkce f je definována na otevřeném intervalu I. Řekneme, že funkce F je *primitivní funkce k* f *na* I, jestliže pro každé $x \in I$ existuje $F'(x)$ a platí $F'(x) = f(x)$.

Věta *(Tvar primitivní funkce)*

Nechť F a G jsou dvě primitivní funkce k funkci f na otevřeném intervalu I. Pak existuje $c \in \mathbb{R}$ tak, že $F(x) = G(x) + c$ pro každé $x \in I$.

Věta *(Linearita primitivní funkce)*

Nechť f má na otevřeném intervalu I primitivní funkci F, funkce g má na na I primitivní funkci G a $\alpha, \beta \in \mathbb{R}$. Potom funkce $\alpha F + \beta G$ je primitivní funkcí k $\alpha f + \beta g$ na I.

Poznámka

Předchozí tvrzení často zapisujeme (pokud alespoň jedno z čísel α, β je různé od nuly)

$$\int (\alpha f(x) + \beta g(x))\mathrm{d}x = \alpha \int f(x)\mathrm{d}x + \beta \int g(x)\mathrm{d}x.$$

Věta *(Spojitost a existence primitivní funkce)*

Nechť f je spojitá funkce na otevřeném intervalu I. Pak f má na I primitivní funkci.

Věta *(O substituci)*

1. Nechť F je primitivní funkce k f na (a, b). Nechť φ je funkce definována na (α, β) s hodnotami v intervalu (a, b), která má v každém bodě $t \in (\alpha, \beta)$ vlastní derivaci. Pak
$$\int f(\varphi(t))\varphi'(t)dt = F(\varphi(t)) + C \ na \ (\alpha, \beta)$$
2. Nechť funkce φ má v každém bodě intervalu (α, β) nenulovou vlastní derivaci a $\varphi((\alpha, \beta)) = (a, b)$. Nechť funkce f je definována na intervalu (a, b) a platí
$$\int f(\varphi(t))\varphi'(t)dt = G(t) + C \ na \ (\alpha, \beta)$$
Pak
$$\int f(x)\mathrm{d}x = G(\varphi^{-1}(x)) + C \ na \ (a, b)$$

Věta *(Integrace per partes)*
Nechť I je otevřený interval a funkce f a g jsou spojité na I. Nechť F je primitivní funkce k f na I a G je primitivní funkce ke g na I. Pak platí

$$\int g(x)F(x)\mathrm{d}x = G(x)F(x) - \int G(x)f(x)\mathrm{d}x \text{ na } I$$

(*Poznámka autora*: $\int u'v = uv - \int uv'$)

4.1.1 Postup integrace racionální funkce

Věta *(Dělení polynomu)*
Nechť P a Q jsou polynomy s reálnými koeficienty, přičemž Q není identicky roven nule. Pak existují (jednoznačně určené) polynomy R a S takové, že stupeň S je menší než stupeň Q a pro všechna $x \in \mathbb{R}$ platí $P(x) = R(x)Q(x) + S(x)$.

Věta *(Základní věta algebry)*
Nechť $P(x) = a_n x^n + \cdots + a_1 x + a_0$ je polynom stupně n s reálnými koeficienty. Pak existují čísla $x_1, \ldots, x_n \in \mathbb{C}$ taková, že

$$P(x) = a_n(x - x_1)\ldots(x - x_n),\ x \in \mathbb{R}$$

Věta *(O kořenech polynomu)*
Nechť P je polynom s reálnými koeficienty a $z \in \mathbb{C}$ je kořen P násobnosti $k \in \mathbb{N}$. Pak i $\overline{z}$ je kořen P násobnosti k.

Věta *(O rozkladu polynomu)*
Nechť $P(x) = a_n x^n + \cdots + a_1 x + a_0$ je polynom stupně n s reálnými koeficienty. Pak existují reálná čísla $x_1, \ldots, x_k, \alpha_1, \ldots, \alpha_l, \beta_1, \ldots, \beta_l$ a přirozená čísla $p_1, \ldots, p_k, q_1, \ldots, q_l$ taková, že:

1. $P(x) = a_n(x - x_1)^{p_1} \ldots (x - x_k)^{p_k}(x^2 + \alpha_1 x + \beta_1)^{q_1} \ldots (x^2 + \alpha_l x + \beta_l)^{q_l}$,
2. žádné dva z mnohočlenů $x-x_1, x-x_2, \ldots, x-x_k, x^2+\alpha_1 x+\beta_1, \ldots, x^2+\alpha_l x+\beta_l$ nemají společný kořen,
3. mnohočleny $x^2 + \alpha_1 x + \beta_1, \ldots, x^2 + \alpha_l x + \beta_l$ nemají žádný reálný kořen.

Věta *(O rozkladu na parciální zlomky)*
Nechť P, Q jsou polynomy s reálnými koeficienty takové, že

1. stupeň P je ostře menší než stupeň Q,
2. $Q(x) = a_n(x - x_1)^{p_1} \ldots (x - x_k)^{p_k}(x^2 + \alpha_1 x + \beta_1)^{q_1} \ldots (x^2 + \alpha_l x + \beta_l)^{q_l}$,
3. $a_n, x_1, \ldots, x_k, \alpha_1, \ldots, \alpha_l, \beta_1, \ldots, \beta_l \in \mathbb{R}, a_n \neq 0$
4. $p_1, \ldots, p_k, q_1, \ldots, q_l \in \mathbb{N}$
5. žádné dva z mnohočlenů $x-x_1, x-x_2, \ldots, x-x_k, x^2+\alpha_1 x+\beta_1, \ldots, x^2+\alpha_l x+\beta_l$ nemají společný kořen
6. mnohočleny $x^2 + \alpha_1 x + \beta_1, \ldots, x^2 + \alpha_l x + \beta_l$ nemají reálný kořen

Pak existují jednoznačně určená čísla $A_1^1, \ldots, A_{p_1}^1, \ldots, A_1^k, \ldots, A_{p_k}^k$, $B_1^1, C_1^1, \ldots, B_{q_1}^1, C_{q_1}^1, \ldots, B_1^l, C_1^l, \ldots, B_{q_l}^l, C_{q_l}^l$ taková, že platí

$$\begin{aligned}\frac{P(x)}{Q(x)} = & \frac{A_1^1}{(x-x_1)^{p_1}} + \cdots + \frac{A_{p_1}^1}{(x-x_1)} + \cdots + \frac{A_1^k}{(x-x_k)^{p_k}} + \cdots + \frac{A_{p_k}^k}{(x-x_k)} \\ & + \frac{B_1^1 x + C_1^1}{(x^2+\alpha_1 x+\beta_1)^{q_1}} + \cdots + \frac{B_{q_1}^1 x + C_{q_1}^1}{x^2+\alpha_1 x+\beta_1} + \ldots \\ & + \frac{B_1^l x + C_1^l}{(x^2+\alpha_l x+\beta_l)^{q_l}} + \cdots + \frac{B_{q_l}^l x + C_{q_l}^l}{x^2+\alpha_l x+\beta_l}.\end{aligned}$$

Postup integrace racionální funkce $\frac{P(x)}{Q(x)}$ je:

1. Vydělíme polynomy P a Q - najdeme polynomy R a S takové, že
$$\frac{P(x)}{Q(x)} = R(x) + \frac{S(x)}{Q(x)}$$
a stupeň S je menší než stupeň Q.
2. Najdeme rozklad polynomu Q ve tvaru uvedeném ve *větě o rozkladu polynomu.*
3. Najdeme rozklad $\frac{S}{Q}$ na parciální zlomky ve tvaru uvedeném ve *větě o rozkladu na parciální zlomky.*
4. Najdeme primitivní funkce ke všem parciálním zlomkům.

4.2 Určitý (Riemannův) integrál, užití určitého integrálu

Definice

Konečnou posloupnost $D = \{x_j\}_{j=0}^n$ nazýváme *dělením intervalu* $\langle a, b\rangle$, jestliže platí
$$a = x_0 < x_1 < \cdots < x_n = b$$

Body $x_0, \ldots, x_n$ nazýváme dělícími body. *Normou dělení* D rozumíme číslo
$$v(D) = \max\{x_j - x_{j-1}; j = 1, \ldots, n\}.$$

Řekneme, že dělení D' intervalu $\langle a, b\rangle$ je *zjemněním dělení* D intervalu $\langle a, b\rangle$, jestliže každý dělící bod D je i dělícím bodem D'.

Definice

Nechť f je omezená funkce definovaná na intervalu $\langle a, b\rangle$ a $D = \{x_j\}_{j=0}^n$ je dělení $\langle a, b\rangle$. Označme

$$S(f, D) = \sum_{j=1}^n M_j(x_j - x_{j-1}),\ \textit{kde } M_j = \sup\{f(x); x \in \langle x_{j-1}, x_j\rangle\}$$

$$s(f, D) = \sum_{j=1}^n m_j(x_j - x_{j-1}),\ \textit{kde } m_j = \inf\{f(x); x \in \langle x_{j-1}, x_j\rangle\}$$

Poznámka
Nechť f je omezená funkce definovaná na intervalu $\langle a, b\rangle$.

1. Pro každé dělaní D intervalu $\langle a, b\rangle$. platí $s(f, D) \leq S(f, D)$.
2. Je-li D_1 zjemněním D_2, pak $s(f, D_1) \geq s(f, D_2)$ a $S(f, D_1) \leq S(f, D_2)$
3. Jsou-li D_1 a D_2 dělení intervalu $\langle a, b\rangle$, pak $s(f, D_1) \leq S(f, D_2)$.

Definice
Nechť f je omezená funkce definovaná na intervalu $\langle a, b\rangle$.

1. Označme
$$\overline{\int_a^b} f = \inf\{S(f, D); D \textit{ je dělením intervalu } \langle a, b\rangle\}$$
(tzv. horní *Riemannův integrál funkce* f přes $\langle a, b\rangle$),
$$\underline{\int_a^b} f = \sup\{s(f, D); D \textit{ je dělením intervalu } \langle a, b\rangle\}$$
(tzv. dolní *Riemannův integrál funkce* f přes $\langle a, b\rangle$)
2. Řekneme, že funkce f má *Riemannův integrál přes* $\langle a, b\rangle$, pokud $\overline{\int_a^b} f = \underline{\int_a^b} f$.
Hodnota tohoto integrálu je pak rovna $\overline{\int_a^b f}$ a značíme ji $\int_a^b f$.
Pokud $a > b$, definujeme $\int_a^b f = -\int_b^a f$, v případě, že $a = b$, definujeme $\int_a^b = 0$.

Věta *(Kritérium existence Riemannova integrálu)*
Nechť $a < b$ a f je funkce omezená na $\langle a, b\rangle$. Pak $\int_a^b f$ existuje, právě když pro každé $\varepsilon > 0$ existuje dělení D intervalu $\langle a, b\rangle$ takové, že $S(f, D) - s(f, D) < \varepsilon$

Věta *(Monotonie a linearita Riemannova integrálu)*
Nechť $a, b \in \mathbb{R}, a < b$ a funkce f, g mají Riemannův integrál přes interval $\langle a, b\rangle$. Pak platí:

1. Jestliže pro každé $x \in \langle a, b\rangle$ je $f(x) \leq g(x)$, pak $\int_a^b f \ \leq \int_a^b g$
2. $\int_a^b (f + g) = \int_a^b f + \int_a^b g$
3. $\int_a^b cf = c \int_a^b f$ pro každé $c \in \mathbb{R}$

Věta *(Spojitost a Riemannovská integrovatelnost)*
Nechť $a, b \in \mathbb{R}, a < b$ a funkce f je spojitá na intervalu $\langle a, b\rangle$. Pak existuje $\int_a^b f$.
Poznámka
Platí dokonce: Pokud je f omezená na $\langle a, b\rangle$ a je spojitá ve všech bodech intervalu $\langle a, b\rangle$ s výjimkou konečně mnoha, pak existuje $\int_a^b f$.

Věta *(Monotonie a Riemannovská integrovatelnost)*
Je li f omezená a monotónní na uzavřeném intervalu, pak je Riemannovsky integrovatelná.

Věta *(Vlastnosti $\int$)*
Nechť $a, b \in \mathbb{R}, a < b$ a funkce f je omezená na intervalu $\langle a, b\rangle$. Pak platí

1. Jestliže existuje $\int_a^b f$, pak pro každý interval $\langle c, d\rangle \subset \langle a, b\rangle$ existuje $\int_c^d f$.
2. Je-li $c \in (a, b)$, pak $\int_a^b f = \int_a^c f + \int_c^b f$, má-li alespoň jedna strana smysl (*aditivita Riemannova integrálu jako funkce intervalu*)

Věta *(Riemannův integrál jako primitivní funkce)*
Nechť $a, b \in \mathbb{R}, a < b$ a funkce f je omezená na intervalu $\langle a, b\rangle$. Pro $x \in \langle a, b\rangle$ položme $F(x) = \overline{\int_a^x} f$. Potom platí:

1. Funkce F je spojitá na $\langle a, b\rangle$
2. Je-li $x_0 \in (a, b)$ a funkce f je v bodě x_0 spojitá, pak $F'(x_0) = f(x_0)$.

Stejná tvrzení platí i pro funkci $G(x) = \underline{\int_a^x} f$

Poznámka
Pro Riemannovy integrály lze použít i metodu per partes nebo pravidlo substituce.

Věta *(Základní věta analýzy)*
Nechť $a, b \in \mathbb{R}, a < b$ a funkce f je spojitá na intervalu $\langle a, b\rangle$. Nechť F je primitivní funkce k f na intervalu (a, b). Pak existují vlastní limity $\lim_{x\to a+} F(x)$ a $\lim_{x\to b-} F(x)$ a platí:

$$\int_a^b f = (\lim_{x\to b-} F(x)) - (\lim_{x\to a+} F(x))$$

Definice *(Newtonův integrál)*
Nechť funkce f je definována na intervalu (a, b) a F je primitivní funkce k f na (a, b). *Newtonovým integrálem* funkce f přes interval (a, b) nazýváme číslo

$$(N) \int_a^b f = (\lim_{x\to b-} F(x)) - (\lim_{x\to a+} F(x))$$

pokud obě limity na pravé straně existují a jsou vlastní.

Poznámka *(Vztah Riemannova a Newtonova integrálu)*
Je-li funkce f spojitá na intervalu $\langle a, b\rangle$, pak platí:

$$(N) \int_a^b f(x)\mathrm{d}x = (R) \int_a^b f(x)\mathrm{d}x$$

Množiny funkcí integrovatelných newtonovsky a riemannovsky jsou neporovnatelné.

4.2.1 Užití určitého integrálu

Obsahy rovinných útvarů…
Věta *(Délka křivky)*
Nechť f má na (a,b) spojitou derivaci. Délka křivky v $\mathbb{R}^2$, vyznačené průběhem funkce f z $[a; f(a)]$ do $[b; f(b)]$ potom je dána předpisem:

$$L(f) = \int_a^b \sqrt{1 + (f'(x))^2} \mathrm{d}x.$$

Věta *(Objem rotačního tělesa)*
Nechť f je definována na $\langle a, b\rangle$ a $f > 0$. Objem tělesa vzniknutého rotací křivky je $V = \pi \int_a^b f(x)^2 \mathrm{d}x$

Věta *(Integrální kritérium konvergence řad)*
Nechť f je spojitá, nezáporná a nerostoucí na $\langle n_0 - 1, \infty)$, kde $n_0 \in \mathbb{N}$. Potom

$$\sum_{n=1}^{\infty} f(n) \textit{ konverguje} \Leftrightarrow (N) \int_{n_0}^{\infty} f(t)dt < \infty$$

4.3 Vícerozměrný integrál a Fubiniho věta

Definice
(Kompaktním) *intervalem* v n-rozměrném euklidovském prostoru E_n rozumíme součin

$$J = \langle a_1, b_1\rangle \times \cdots \times \langle a_n, b_n\rangle$$

kde $\langle a_i, b_i\rangle$ jsou kompaktní intervaly v $\mathbb{R}$.

Definice

- *Rozdělením* D takového intervalu J rozumíme n-tici $D_1, \ldots, D_n$, kde D_i je rozdělení intervalu $\langle a_i, b_i\rangle$.
- Rozdělení $D = (D_1, \ldots, D_n)$ je *zjemněním* $D' = (D'_1, \ldots, D'_n)$ jestliže D_i zjemňuje D'_i.

Pozorování
Každé dvě rozdělení mají společné zjemnění.

Definice
Člen rozdělení $D = (D_1, \ldots, D_n)$ je kterýkoliv interval $K = \langle t_{1,i_1}, t_{1,i_1+1}\rangle \times \cdots \times \langle t_{n,i_n}, t_{n,i_n+1}\rangle$, kde $D_k : t_{k0} < \cdots < t_{k,r(k)}$, $0 \le i_j \le r(j)$. Množina všech členů rozdělení D bude označována $|D|$.

Definice
Objem intervalu $J = \langle a_1, b_1\rangle \times \cdots \times \langle a_n, b_n\rangle$ je číslo

$$\mathrm{vol}\, J = (b_1 - a_1).(b_2 - a_2)\dots(b_n - a_n)$$

Definice
Buď f omezená funkce na intervalu J, buď D rozdělení J. *Dolní (resp. horní) sumou* funkce f v rozdělení D rozumíme číslo

$$s(f, D) = \sum_{K \in |D|} m_K \cdot \mathrm{vol}\, K \ \ \textit{resp.}\ \ S(f, D) = \sum_{K \in |D|} M_K \cdot \mathrm{vol}\, K,$$

kde m_K je infimum a M_k supremum funkce f na intervalu K.

Pozorování
Pro libovolná dvě rozdělení D a D' platí $s(f, D) \leq S(f, D')$

Definice
Dolní a horní Riemannův integrál definujeme jako

$$\underline{\int}_J f = \sup_D s(f, D), \quad \overline{\int}_J f = \inf_D S(f, D)$$

a při rovnosti těchto hodnot mluvíme o Riemannově integrálu a píšeme prostě

$$\int_J f \ \ \textit{nebo} \ \int_J f(x_1, \dots, x_n)\mathrm{d}x_1 \dots x_n, \quad \int_J f(\overrightarrow{x})d\overrightarrow{x}.$$

Věta
Pro vícerozměrný Riemannův integrál platí (podobně jako pro jednorozměrný případ) že f je Riemannovsky integrovatelná, právě když ke každému $\varepsilon > 0$ existuje rozdělení D takové, že

$$S(f, D) - s(f, D) < \varepsilon$$

Platí i věta, že spojitá funkce na intervalu J je Riemannovsky integrovatelná.

Věta *(Vlastnosti Riemannova vícerozměrného integrálu)*
Platí:

1. $|\int_J f| \leq \int_J |f|$ (existují-li příslušné integrály)
2. Buďte f, g Riemannovsky integrovatelné funkce na J, buď $f \leq g$. Potom $\int_J f \leq \int_J g$.
3. Speciálně, je-li $f(\overrightarrow{x}) \leq C$ pro nějakou konstantu C, platí $\int_J f \leq C \cdot \mathrm{vol}\, J$

Věta *(Fubiniova)*

Buďte $J' \subseteq E^n, J'' \subseteq E^m$ intervaly, $J = J' \times J''$, buď f spojitá funkce definovaná na J. Potom

$$\int_J f(\overrightarrow{x}, \overrightarrow{y}) d\overrightarrow{x}\overrightarrow{y} = \int_{J'} \left(\int_{J''} f(\overrightarrow{x}, \overrightarrow{y}) d\overrightarrow{y} \right) d\overrightarrow{x} = \int_{J''} \left(\int_{J'} f(\overrightarrow{x}, \overrightarrow{y}) d\overrightarrow{x} \right) d\overrightarrow{y}$$

(Inými slovami: Hodnota „integrálu“ cez celý interval je rovná hodnote po integrovaní postupne cez (jednotlivé) „rozmery“ - pričom je možné integrovať v ľubovoľnom poradí.)

Definice *(Parciální derivace)*

Parciální derivace funkce f v bodě $a \in \mathbb{R}^n$ podle proměnné x_i se definuje následovně:

$$\frac{\partial f}{\partial x_i}(a) = \lim_{h \to 0} \frac{f(a_1, \ldots, a_{i-1}, a_i + h, a_{i+1}, \ldots, a_n) - f(a_1, \ldots, a_n)}{h}$$

Definice *(Jacobiho matice, jakobián)*

Jacobiho matice funkce $\overrightarrow{f} : D \to \mathbb{R}^n$ v bodě $a \in D$, kde D je otevřená množina v $\mathbb{R}^m$ a $f_1, f_2, \ldots f_n$ jsou souřadnicové funkce f, je dána předpisem:

$$\left(\frac{\partial f_i}{\partial x_j}(a) \right)_{i,j=1}^{n,m} = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_m} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_m} \end{pmatrix}$$

Táto čtvercová matice se obvykle značí $\frac{D(f_1,\ldots,f_n)}{D(x_1,\ldots,x_n)}$ – a je-li $m = n$, její determinant se nazývá *Jakobián* (a značí se rovnako???).

Definice *(Regulární zobrazení)*

Nechť $U \subseteq \mathbb{R}^n$ je otevřená množina, $\overrightarrow{f} : U \to \mathbb{R}^n$ má spojité parciální derivace. *Zobrazení $\overrightarrow{f}$ je regulární*, je-li jakobián

$$\frac{D(f_1, \ldots, f_n)}{D(x_1, \ldots, x_n)}(\overrightarrow{x}) \neq 0, \ \forall \overrightarrow{x} \in U$$

Věta *(O substituci)*

Nechť $\varphi : U \subseteq \mathbb{R}^n \to \mathbb{R}^n$ je regulární zobrazení, A je uzavřená množina v $\mathbb{R}^n$, $A \subseteq U$ na které existuje $\int_{\varphi(A)} f(\overrightarrow{x}) d\overrightarrow{x}$. Potom platí:

$$\int_A f(\overrightarrow{\varphi}(\overrightarrow{t})) \frac{D(\overrightarrow{\varphi})}{D(\overrightarrow{t})} d\overrightarrow{t} = \int_{\varphi(A)} f(\overrightarrow{x}) d\overrightarrow{x}$$

5 Základy teorie funkcí více proměnných

Požadavky

- Parciální derivace a totální diferenciál
- Věty o střední hodnotě
- Extrémy funkcí více proměnných
- Věta o implicitních funkcích

5.1 Parciální derivace a totální diferenciál

Definice *(Parciální derivace)*
Nechť $f : \mathbb{R}^n \to \mathbb{R}$, $t \in \mathbb{R}$, $X = [x_1, \ldots, x_n], X \in \mathbb{R}^n$. Potom *parciální derivací funkce f podle i-té složky v bodě X* nazveme limitu

$$\frac{\partial f}{\partial x_i}(X) = \lim_{t \to 0} \frac{f(x_1, \ldots, x_i + t, \ldots, x_n) - f(x_1, \ldots, x_n)}{t}$$

pokud tato limita existuje a je vlastní.

Definice *(Derivace ve směru vektoru)*
Nechť $f : \mathbb{R}^n \to \mathbb{R}$, $v \in \mathbb{R}^n \setminus \{0^n\}$, $X = [x_1, \ldots, x_n], X \in \mathbb{R}^n$. Potom *derivací funkce f ve směru vektoru v* nazveme limitu

$$D_v f(X) = \lim_{t \to 0} \frac{f(X + t \cdot v) - f(X)}{t}$$

pokud tato limita existuje a je vlastní.

Definice *(Gradient)*
Nechť $f : \mathbb{R}^n \to \mathbb{R}$, $X = [x_1, \ldots, x_n], X \in \mathbb{R}^n$ a nechť existují všechny parciální derivace funkce f v bodě X a jsou vlastní. Pak vektor $\nabla f(X) = [\frac{\partial f}{\partial x_1}(X), \ldots, \frac{\partial f}{\partial x_n}(X)]$ nazýváme *gradientem funkce f v bodě X.*

Definice *(Totální diferenciál)*
Nechť $f : \mathbb{R}^n \to \mathbb{R}$, $X = [x_1, \ldots, x_n], X \in \mathbb{R}^n$ a nechť $v \in \mathbb{R}^n$. Existuje-li lineární zobrazení $Df(X)(v)$ takové, že platí:

$$\lim_{\|h\| \to 0} \frac{f(X + h) - f(X) - Df(X)(h)}{\|h\|} = 0$$

potom toto zobrazení nazýváme *totální diferenciál funkce f v bodě X.*

Definice *(Parciální derivace druhého řádu)*
Nechť $M \subseteq \mathbb{R}^n$ otevřená, a nechť má funkce f parciální derivaci $\frac{\partial f}{\partial x_i}$. Pak pro $a \in M$ definujeme *parciální derivaci druhého řádu (podle i-té a j-té složky)* jako $\frac{\partial^2 f}{\partial x_i \partial x_j}(a) = \frac{\partial}{\partial x_j}(\frac{\partial f}{\partial x_i}(a))$.

Definice *(Druhý diferenciál)*

Nechť $f : \mathbb{R}^n \to \mathbb{R}$ a $a \in \mathbb{R}^n$. Řekneme, že f má v bodě a *druhý diferenciál*, pokud každá parciální derivace f má v bodě a totální diferenciál. Druhý diferenciál je bilineární zobrazení $D^2 f(a) : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ a má tedy následující tvar:

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

Použijeme-li analogii gradientu pro první diferenciál, můžeme říct, že druhý diferenciál je reprezentován maticí:

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

Definice *(Klasifikace bilineárních forem)*

Nechť $F : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ je bilineární forma.

- F se nazývá *pozitivně definitní*, pokud $\exists \varepsilon > 0$ tak, že $F(h,h) \geq \varepsilon \|h\|^2$, $\forall h \in \mathbb{R}^n$.
- F se *nazývá negativně definitní*, pokud je $-F$ pozitivně definitní.
- F se nazývá *indefinitní*, pokud $F(g,g) < 0$ a $F(h,h) > 0$ pro nějaké $g, h \in \mathbb{R}^n$.

Poznámka

Při určování toho, zda je bilineární forma pozitivně definitní, negativně definitní, nebo indefinitní nám může pomoci tzv. Sylvestrovo kritérium, které tvrdí následující:

- jsou-li všechny hlavní subdeterminanty matice reprezentující bilineární formu F kladné, potom je F pozitivně definitní.
- jestliže je první hlavní subdeterminant této matice záporný a poté alterují znaménka, je forma negativně definitní.
- nenastává-li ani jedna z předchozích dvou možností a všechny hlavní subdeterminanty jsou nenulové, je F indefinitní.

Pakliže nenastane žádná z výše uvedených možností, Sylvestrovo kritérium nám nepomůže a je nutno o typu bilineární formy rozhodovat jiným způsobem (např. pomocí vlastních čísel).

Věta *(Tvar totálního diferenciálu)*

Nechť $f : \mathbb{R}^n \to \mathbb{R}$ má v bodě $a \in \mathbb{R}^n$ totální diferenciál. Potom:

- pro $\forall v \in \mathbb{R}^n \setminus \{0^n\}$ existuje $D_v f(a)$ vlastní a platí $D_v f(a) = Df(a)(v)$.
- existují všechny parciální derivace a pro $\forall v \in \mathbb{R}^n : Df(a)(v) = \sum_{i=0}^{n} \frac{\partial f}{\partial x_i}(a) \cdot v_i$ (neboli $Df(a)(h) = \langle \nabla f(a), h \rangle$).
- f je spojitá v a.

Věta *(Aritmetika totálního diferenciálu)*
Nechť $f, g : \mathbb{R}^n \to \mathbb{R}$ mají v bodě $a \in \mathbb{R}^n$ totální diferenciál. Nechť $\alpha \in \mathbb{R}$. Potom existují totální diferenciály $D(f+g)(a)$, $D(\alpha f)(a)$, $D(f \cdot g)(a)$. Pokud navíc $g(a) \neq 0$ existuje i $D(f \div g)(a)$. Navíc platí:

- $D(f+g)(a) = Df(a) + Dg(a)$
- $D(\alpha f)(a) = \alpha Df(a)$
- $D(f \cdot g)(a) = g(a)Df(a) + f(a)Dg(a)$.
- $D(f \div g)(a) = \frac{g(a)Df(a) - f(a)Dg(a)}{g^2(a)}$.

Věta *(Diferenciál složeného zobrazení)*
Mějme funkci $f : \mathbb{R}^n \to \mathbb{R}$ a n funkcí $g_j : \mathbb{R}^m \to \mathbb{R}$. Nechť $a \in \mathbb{R}^m$ a $b \in \mathbb{R}^n$ a $b_j = g_j(a)$. Nechť existují $Df(a)$ a $Dg_i(a), i = 1 \dots n$. Definujeme-li zobrazení $H : \mathbb{R}^m \to \mathbb{R}$ předpisem $H(x) = f(g_1(x), \dots, g_n(x))$, potom H má v bodě a totální diferenciál a pro $h \in \mathbb{R}^m$ platí

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

Z čehož plyne tzv. *řetízkové pravidlo*, tj.:

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

Věta *(Postačující podmínka pro existenci totálního diferenciálu)*
Nechť $f : \mathbb{R}^n \to \mathbb{R}$ má v bodě $a \in \mathbb{R}^n$ spojité všechny parciální derivace. Potom má f v bodě a totální diferenciál.

Věta *(Postačující podmínka pro existenci druhého diferenciálu)*
Nechť $M \subseteq \mathbb{R}^n$ je otevřená a f má spojité parciální derivace druhého řádu na M. Potom f má v každém bodě z M druhý diferenciál.

Věta *(Záměnnost parciálních derivací druhého řádu)*
Mějme funkci $f : \mathbb{R}^n \to \mathbb{R}$. Nechť f má spojitou parciální derivaci $\frac{\partial^2 f}{\partial x_i \partial x_j}(a)$. Potom existuje i $\frac{\partial^2 f}{\partial x_j \partial x_i}(a)$ a obě tyto parciální derivace druhého řádu se rovnají.

Důsledek
Důsledkem dvou právě uvedených vět je fakt, že matice, která reprezentuje druhý diferenciál funkce f v bodě a (tedy hovoříme o situaci, kdy f má v bodě a druhý diferenciál), je symetrická.

5.2 Věty o střední hodnotě

Věta *(O střední hodnotě pro funkce více proměnných)*
Nechť $f : \mathbb{R}^n \to \mathbb{R}$ a $a, b \in \mathbb{R}^n$. Nechť f má všechny parciální derivace spojité v každém bodě úsečky (a, b). Potom $\exists \xi \in (0, 1)$ takové, že

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

Důkaz
Plyne z Lagrangeovy věty o střední hodnotě pro funkci $F : [0, 1] \to \mathbb{R}$ definovanou předpisem $F(t) = f(a + t(b - a))$ a řetízkového pravidla.

5.3 Věta o implicitních funkcích

Věta *(O implicitní funkci (pro obecné křivky v R^2))*
Nechť $F([x, y]) : \mathbb{R}^2 \to \mathbb{R}$ má spojité parciální derivace. Mějme dva body $x_0, y_0 \in \mathbb{R}$ takové, že $F([x_0, y_0]) = 0$. Nechť navíc $\frac{\partial F}{\partial y}([x_0, y_0]) \neq 0$. Potom exisuje okolí U bodu x_0 a okolí V bodu y_0 tak, že pro $\forall x \in U$ existuje právě jedno $y \in V$ takové, že $F([x, y]) = 0$. Označíme-li takto definovanou (implicitní) funkci jako $y = \varphi(x)$, potom φ je diferencovatelná na U a platí:

$$\frac{\partial \varphi}{\partial x}(x) = -\frac{\frac{\partial F}{\partial x}([x, \varphi(x)])}{\frac{\partial F}{\partial y}([x, \varphi(x)])}$$

Věta *(Věta o implicitní funkci (případ v R^{n+1}))*
Nechť $F : G \to \mathbb{R}$, kde $G \subseteq \mathbb{R}^{n+1}$ je otevřená množina. Uvažujme body $x_0 \in \mathbb{R}^n$, $y_0 \in \mathbb{R}$ takové, že $[x_0, y_0] \in G$ a $F([x_0, y_0]) = 0$. Nechť F má spojité parciální derivace a nechť navíc $\frac{\partial F}{\partial y}([x_0, y_0]) \neq 0$. Potom existuje okolí $U \subseteq \mathbb{R}^n$ bodu x_0 a okolí $V \subseteq \mathbb{R}$ bodu y_0 takové, že pro $\forall x \in U$ existuje právě jedno $y \in V$ takové, že $F([x, y]) = 0$. Navíc, označíme-li $y = \varphi(x)$, potom φ má spojité parciální derivace na U a platí:

$$\frac{\partial \varphi}{\partial x_i}(x) = -\frac{\frac{\partial F}{\partial x_i}([x, \varphi(x)])}{\frac{\partial F}{\partial y}([x, \varphi(x)])}$$

Poznámka
Na tomto místě uvedeme malou, ale pro nás důležitou poznámku z algebry. Mějme bod $a \in \mathbb{R}^n$ a funkce $F_j, j = 1 \ldots n$, $F_j : \mathbb{R}^n \to \mathbb{R}$, které mají všechny své parciální derivace. Potom determinant

$$JF_{j=1}^{n}(a) = \left| \frac{\partial(F_1, \ldots, F_n)}{\partial(x_1, \ldots, x_n)} \right| = \det \left(\frac{\partial F_i}{\partial x_j}(a) \right)_{i=1, j=1}^{n,n} \tag{2}$$

nazveme Jakobiánem funkcí F_j (v bodě a) vzhledem k proměnným $x_1, \ldots, x_n$. Pojem Jakobián lze ekvivalentně zavést i pomocí vektorových funkcí. To zde však nebudeme potřebovat.

Věta *(O implicitních funkcích (případ v R^{n+m}))*
Nechť $F_j : G \to \mathbb{R}, j = 1 \dots m$, kde $G \subseteq \mathbb{R}^{n+m}$ je otevřená množina. Uvažujme body $x_0 \in \mathbb{R}^n$, $y_0 \in \mathbb{R}^m$ takové, že $[x_0, y_0] \in G$ a $F_j([x_0, y_0]) = 0$ pro všechny $j = 1 \dots m$. Nechť každá funkce F_j má spojité parciální derivace a nechť navíc $JF_{j=1}^m([x_0, y_0]) \neq 0$. Potom existuje okolí $U \subseteq \mathbb{R}^n$ bodu x_0 a okolí $V \subseteq \mathbb{R}^m$ bodu y_0 takové, že pro $\forall x \in U$ existuje právě jedno $y \in V$ takové, že $F_j([x, y]) = 0, j = 1 \dots m$. Navíc, označíme-li $y_j = \varphi_j(x), j = 1 \dots m$, potom φ_j má spojité parciální derivace na U a platí:

$$\frac{\partial \varphi_i}{\partial x_j}(x) = -\frac{\left|\frac{\partial(F_1,\dots,F_m)}{\partial(y_1,\dots,y_{i-1},x_j,y_{i+1},\dots,y_m)}\right|}{\left|\frac{\partial(F_1,\dots,F_m)}{\partial(y_1,\dots,y_m)}\right|}$$

Věta *(O inverzních funkcích)*
Důsledkem věty o implicitních funkcích je následující věta: Nechť $f : U \to \mathbb{R}^m$, kde $U \subseteq \mathbb{R}^m$ je okolí bodu x_0, je zobrazení se spojitými parciálními derivacemi, které má v x_0 nenulový jakobián. Potom existují okolí $U_1 \subseteq U$ a $V \subseteq \mathbb{R}^m$ bodů x_0 a $y_0 = f(x_0)$ taková, že $f : U_1 \to V$ je bijekce, inverzní zobrazení $f^{-1} : V \to U_1$ má spojité parciální derivace a pro každé $x \in U_1$ v bodě $y = f(x) \in V$ máme

$$Df^{-1}(y) = (Df(x))^{-1}$$

Jacobiho matice zobrazení f^{-1} v bodě y je tedy inverzní k Jacobiho matici zobrazení f v bodě x.

5.4 Extrémy funkcí více proměnných

Definice *(Extrémy funkce)*
Nechť $f : \mathbb{R}^n \to \mathbb{R}$, $\overline{X} \in \mathbb{R}^n$, $M \subseteq \mathbb{R}^n$. Řekneme, že bod $\overline{X}$ je bodem *maxima funkce f na množině M*, pokud $\forall X \in M : f(\overline{X}) \geq f(X)$. Analogicky definujeme *minimum funkce f na množině M*.

Definice *(Lokální extrémy funkce)*
Nechť $f : \mathbb{R}^n \to \mathbb{R}$, $\overline{X} \in \mathbb{R}^n$, $M \subseteq \mathbb{R}^n$. Řekneme, že bod $\overline{X}$ je bodem ***lokálního*** *maxima funkce f na M*, pokud $\exists \delta > 0$ tak, že $\forall X \in M \cap B(\overline{X}, \delta) : f(\overline{X}) \geq f(X)$. Analogicky definujeme ***lokální*** *minimum funkce f na množině M*.

Definice *(Stacionární bod)*
Nechť $M \subseteq \mathbb{R}^n$ otevřená, $f : M \to \mathbb{R}$, $\overline{X} \in M$. Řekneme, že bod $\overline{X}$ je *stacionárním bodem funkce f*, pokud existují všechny parciální derivace funkce f v bodě $\overline{X}$ a jsou nulové.

Věta *(Nutná podmínka existence lokálního extrému)*
Pokud $a \in \mathbb{R}^n$ je bodem lokálního extrému funkce $F : \mathbb{R}^n \to \mathbb{R}$ a v a existují všechny parciální derivace funkce F, potom jsou tyto nulové.

Věta *(Postačující podmínka pro existenci lokálního extrému)*
Nechť $G \subseteq \mathbb{R}^n$ je otevřená množina a $a \in G$. Nechť $F : G \to \mathbb{R}$ má spojité parciální derivace druhého řádu. Jestliže $Df(a) = 0$, potom platí:

- je-li $D^2 f(a)$ pozitivně definitní, potom a je bodem lokálního minima
- je-li $D^2 f(a)$ negativně definitní, potom a je bodem lokálního maxima
- je-li $D^2 f(a)$ indefinitní, potom v bodě a není lokální extrém

Věta *(O vázaných extrémech (Lagrangeovy multiplikátory))*
Nechť $G \subseteq \mathbb{R}^n$ je otevřená. Mějme funkce $F, g_1, \dots g_m,\ m < n$, které mají spojité parciální derivace. Zadefinujme množinu M společných nulových bodů funkcí g_i, $i = 1 \dots m$, tedy:

$$M = \{x \in \mathbb{R}^n : g_1(x) = \dots = g_m(x) = 0\}$$

Je-li bod $a = [a_1, \dots, a_n]$ bodem lokálního extrému funkce F na M a platí-li, že vektory $\nabla g_1(a), \dots, \nabla g_m(a)$ jsou lineárně nezávislé, potom existují tzv. Lagrangeovy multiplikátory $\lambda_1, \dots, \lambda_m$ takové, že:

$$DF(a) + \lambda_1 Dg_1(a) + \dots + \lambda_m Dg_m(a) = 0$$

neboli

$$\frac{\partial F}{\partial x_i}(a) = \sum_{k=1}^{m} \lambda_k \frac{\partial g_k}{\partial x_i}(a),\ i = 1, \dots, n$$

6 Metrické prostory

Požadavky

- Definice metrického prostoru, příklady.
- Spojitost a stejnoměrná spojitost.
- Kompaktní prostory a jejich vlastnosti, úplné prostory.

Při přepracovávání a rozšiřování této otázky jsem použil skripta Prof. A. Pultra z matematické analýzy
(`http://kam.mff.cuni.cz/~pultr/ma.ps`)

– Tuetschek

6.1 Definice metrického prostoru, příklady

Metrický prostor, metrika

Definice *(Metrický prostor)*
Metrický prostor je dvojice (M, d), kde M je množina a $d : M \times M \to \mathbb{R}$ je zobrazení, zvané *metrika*, splňující tři axiomy:

1. $d(x, y) = 0 \Leftrightarrow x = y$
2. $d(x, y) = d(y, x)$ *(symetrie)*
3. $d(x, y) \leq d(x, z) + d(z, y)$ *(trojúhelníková nerovnost)*

Metrické prostory jsou abstrakcí jevu vzdálenosti. Z axiomů 1. a 3. vyplývá nezápornost hodnot metriky (která se ale většinou explicitně uvádí jako součást prvního axiomu). Prvky metrického prostoru nazveme *body*.

Příklady metrik

Nechť $M = \mathbb{R}^n$ a $p \geq 1$ je reálné číslo. Na M definujeme metriky
(kde $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$)

$$d_p(x, y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{1/p}$$

Potom:

1. Pro $p = 1, n = 1$ dostáváme metriku $|x - y|$.
2. Pro $p = 2, n \geq 2$ dostáváme euklidovskou metriku

$$d_2(x, y) = \| x - y \| = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2}$$

3. Pro $p = 1, n \geq 2$ dostáváme tzv. pošťáckou metriku a pro $p \to \infty$ maximovou metriku

$$d_1(x, y) = \max_{1 \leq i \leq n} |x_i - y_i|$$

Buď X libovolná množina. $F(X)$ označme množinu všech omezených funkcí $f : X \to \mathbb{R}$ a definujme funkci d předpisem

$$d(f, g) = \sup_{x \in X} |f(x) - g(x)|$$

Pak $(F(X), d)$ je metrický prostor (s tzv. supremovou metrikou).

Úplně triviální příklad metriky dostaneme, když na nějaké množině X položíme $d(x, y) = 1$ pro $x \neq y$ a $d(x, x) = 0$.

Definícia *(euklidovský priestor)*
Euklidovským priestorom rozumieme metrický priestor $(\mathbb{R}^n, d_2)$, kde d_2 je funkcia daná predpisom $d_2(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$.

Otevřené a uzavřené množiny

Definícia *(otvorená a uzavretá guľa)*
Nech (M, d) je metrický priestor, $x \in M, r > 0$, potom

- **otvorenou guľou** (r-*okolím*) so stredom x a polomerom r nazveme množinu

$$B(x, r) = \{y \in M | d(x, y) < r\}$$

- **uzavretou guľou** (r-*okolím*) so stredom x a polomerom r nazveme množinu

$$\overline{B}(x, r) = \{y \in M | d(x, y) \leq r\}$$

Definícia *(otvorená a uzavretá množina)*
Nech (M, d) je metrický priestor, $G \subseteq M$, potom

- G je **otvorená** v M, ak

$$\forall x \in G \; \exists r > \; 0 : \; B(x, r) \subseteq G$$

  (tj. množina G je okolím každého svojho bodu)
- G je **uzavretá** v M, ak jej doplnok $M \setminus G$ je otvorený v M.

Otvorená guľa je otvorená množina v každom metrickom priestore. Podobné tvrdenie platí aj pre uzavretú guľu.

Veta *(vlastnosti otvorených množín)*
Nech (M, d) je metrický priestor, potom platí

1. $\emptyset$, M sú otvorené v M
2. konečný prienik otvorených množín je otvorená množina v M
3. ľubovoľne veľké zjednotenie otvorených množín je otvorená množina v M

Veta *(vlastnosti uzavretých množín)*
Nech (M,d) je metrický priestor, potom platí

1. $\emptyset$, M sú uzavreté v M
2. ľubovoľný prienik uzavretých množín je uzavretá množina v M
3. konečné zjednotenie uzavretých množín je uzavretá množina v M

Definícia *(uzáver)*
Uzáverom množiny A v metrickom priestore (M,d) nazývame množinu

$$\overline{A} = \bigcap_{\forall F} \{F | F \text{ uzavretá}, A \subseteq F \subseteq M\}$$

Definícia *(vnútro)*
Vnútrom množiny A v metrickom priestore (M,d) nazývame množinu

$$\text{int}A = A^0 = \bigcup_{\forall F} \{F | F \subset A, F \text{ otvorená}\}$$

Definice *(Vzdálenost bodu od množiny)*
V metrickém prostoru (X,ρ) buď $A \subset X$ množina a $x \in (X,\rho)$ bod. *Vzdálenost bodu x od množiny A* je číslo $\rho(x,A) = \inf\{\rho(x,y) | y \in A\}$.

Veta *(vlastnosti uzáveru)*
Nech (M,d) je metrický priestor a A, B množiny v nem, potom platí:

1. $\overline{\emptyset} = \emptyset$, $\overline{M} = M$
2. $A \subset B \Rightarrow \overline{A} \subset \overline{B}$
3. $\overline{\overline{A}} = \overline{A}$
4. $\overline{A \cup B} = \overline{A} \cup \overline{B}$
5. charakteristika uzáveru: $\overline{A} = \{x \in M | d(x,A) = 0\}$
6. $\overline{A}$ je najmenšia uzavretá množina obsahujúci A, preto A je uzavretá práve keď $\overline{A} = A$.

Posloupnost bodů

Definice *(Konvergence posloupnosti bodů)*
Řekneme, že posloupnost bodů $(x_n)_{n\geq 0}$ nějakého metrického prostoru (X,ρ) *konverguje k bodu x* ($x_n \to x$), nebo že $x = \lim_{n\geq 0} x_n$, jestliže

$$\forall \varepsilon > 0 \; \exists n_0 : n \geq n_0 \;\Rightarrow\; \rho(x_n, x) < \varepsilon$$

Poznámka *(vlastnosti konvergence)*
Nechť je dán metrický prostor (X, ρ) a v něm posloupnost bodů $(x_n)_{n\geq 0}$. Potom platí:

1. Jestliže pro nějaký bod $y \in X$ platí $\exists n_0 \in \mathbb{N} : \forall n \geq n_0 : x_n = y$, pak $x_n \to y$
2. Nechť $x_n \to y_1$ a zároveň $x_n \to y_2$. Potom $y_1 = y_2$.
3. Vybraná posloupnost z konvergentní posloupnosti konverguje ke stejnému bodu.

Poznámka *(Ekvivalentní definice uzavřené množiny)*
Množina $M \subset (X, \rho)$ je uzavřená, jestliže každá posloupnost bodů $(x_n)_{n\geq 0}$, která v M leží a konverguje, v M má také svou limitu.

6.2 Spojitost a stejnoměrná spojitost

Spojitá a stejnoměrně spojitá zobrazení

Definice *(Spojité zobrazení)*
Pro metrické prostory (X, ρ) a (Y, σ) je zobrazení $f : X \to Y$ *spojité v bodě* $x \in X$, jestliže

$$\forall \varepsilon > 0\ \exists \delta > 0 : \rho(x, y) < \delta \ \Rightarrow\ \sigma(f(x), f(y)) < \varepsilon$$

Zobrazení f je *spojité*, pokud je spojité v každém bodě $x \in X$.

Věta *(Vlastnosti spojitosti)*
Nechť je dáno zobrazení $f : X \to Y$ mezi dvěma metrickými prostory (X, ρ), (Y, σ). Pak jsou následující tvrzení ekvivalentní:

1. f je spojité
2. pro každou konvergentní posloupnost $(x_n)_{n\geq 0}$ v X platí $f(\lim x_n) = \lim f(x_n)$
3. pro každé x a každé okolí U bodu $f(x)$ existuje okolí V bodu x takové, že $f[V] \subseteq U$
4. obrazy otevřených množin z Y zobrazením $f^{-1}(U)$ jsou v X otevřené
5. obrazy uzavřených množin z Y zobrazením $f^{-1}(U)$ jsou v X uzavřené
6. pro každou $M \subseteq X$ platí $f[\overline{M}] \subseteq \overline{f[M]}$

Definice *(Stejnoměrně spojité zobrazení)*
Řekneme, že zobrazení$f : (X, \rho) \to (Y, \sigma)$ je *stejnoměrně spojité*, jestliže

$$\forall \varepsilon > 0\ \exists \delta > 0 \text{ takové, že } \forall (x, y) \text{ platí } \rho(x, y) < \delta \ \Rightarrow\ \sigma(f(x), f(y)) < \varepsilon$$

Věta *(Skládání zobrazení)*
Složení dvou spojitých (nebo stejnoměrně spojitých) zobrazení je spojité (resp. stejnoměrně spojité).

Definice *(homeomorfismus)*

Existuje-li ke (stejnoměrně) spojitému zobrazení $f : (X, \rho) \to (Y, \sigma)$ inverzní (stejnoměrně) spojité zobrazení f^{-1}, řekneme, že f je *(stejnoměrný) homeomorfismus* a prostory X a Y jsou *(stejnoměrně) homeomorfní.* Pokud je takové f identické zobrazení z (X, ρ_1) do (X, ρ_2), říkáme, že metriky ρ_1 a ρ_2 jsou *(stejnoměrně) ekvivalentní* (jiná definice ekvivalentních metrik je, že dvě metriky jsou ekvivalentní, jestliže mají metrické prostory (X, ρ_1) a (X, ρ_2) tytéž otevřené množiny).

Věta *(aritmetika zobrazení)*

Jsou-li f, g spojité funkce $(X, \rho) \to \mathbb{R}$ (kde (X, ρ) je metrický prostor) a $\alpha \in \mathbb{R}$, potom i funkce $f + g$, $\alpha \cdot f$, $f \cdot g$ a $\frac{f}{g}$ (má-li tato smysl) jsou spojité. Platí i pro spojitost zobrazení v nějakém bodě $x_0 \in X$.

Důkaz

Důkaz této věty je vlastně stejný jako důkaz věty o aritmetice limit pro reálné funkce (jen pracujeme se zobrazeními na metrických prostorech).

Definice *(Stejnoměrná konvergence posloupnosti zobrazení)*

Řekneme, že posloupnost $(f_n)_{n\geq 0}$ zobrazení z (X, ρ) do (Y, σ) *konverguje stejnoměrně* k zobrazení $f : X \to Y$ ($f_n \rightrightarrows f$), jestliže

$$\forall \varepsilon > 0\ \exists n_0 : \forall n \geq n_0\ \forall x \in X\ \sigma(f_n(x), f(x)) < \varepsilon$$

Věta *(spojitost limitního zobrazení)*

Jsou-li f_n spojité a $f_n \rightrightarrows f$, pak je i f spojité.

Podprostor metrického prostoru

Definice *(Podprostor)*

Pro metrický prostor (X, ρ) a množinu $X_1 \subset X$ vezmeme funkci $\rho_1 : X_1 \times X_1 \to \mathbb{R}$ danou předpisem $\rho_1(x, y) = \rho(x, y)\ \forall x, y \in X_1$. Pak (X_1, ρ_1) je *podprostor* metrického prostoru (X, ρ) (indukovaný podmnožinou X_1).

Poznámka

Zobrazení vložení $j : (X_1, \rho) \to (X, \rho)$, $j(x) = x\ \forall x \in X_1$ je stejnoměrně spojité.

Věta *(Vlastnosti podprostorů)*

Buď Y podprostor metrického prostoru X. Potom platí:

1. o okolí bodů: $B_Y(x, \varepsilon) = B_X(x, \varepsilon) \cap Y$
2. U je otevřená množina v Y, právě když existuje otevřená mn. V v X taková, že $U = V \cap Y$ (to samé platí i pro uzavřené množiny)
3. o uzávěru množiny: $\overline{A}^Y = \overline{A}^X \cap Y$

Věta *(Podprostor zachovává spojitost)*

Pro $f : (X, \rho) \to (Y, \sigma)$ (stejnoměrně) spojité zobrazení a $X_1 \subseteq X$, $Y_1 \subseteq Y$ takové, že $f[X_1] \subseteq Y_1$ je $f_1 : X_1 \to Y_1$ definované předpisem $f_1(x) = f(x)\ \forall x \in X_1$ (stejnoměrně) spojité.

6.3 Kompaktní prostory a jejich vlastnosti, úplné prostory

Kompaktní metrické prostory

Definice *(Kompaktní prostor)*
Řekneme, že metrický prostor je *kompaktní*, jestliže v něm lze z každé posloupnosti bodů vybrat konvergentní podposloupnost.

Příklady

- Každý konečný prostor je kompaktní.
- Každý omezený uzavřený interval je kompaktní.

Věta *(Uzavřenost kompaktního podprostoru)*
Každý kompaktní podprostor Y libovolného metrického prostoru X je uzavřený. Je-li X kompaktní, je každý jeho uzavřený podprostor taky kompaktní.
Důkaz
Obě tvrzení se dokážou z definice uzavřených množin – všechny konvergentní posloupnosti v nich mají svou limitu.

Definice *(omezená podmnožina)*
Podmnožina M metrického prostoru (X, ρ) je *omezená*, pokud existuje konečné K takové, že

$$x, y \in M \;\Rightarrow\; \rho(x, y) < K$$

Věta *(Omezený euklidovský podprostor)*

1. Podprostor X euklidovského prostoru dimenze n ($\mathbb{E}_n$) je kompaktní, právě když je uzavřený a omezený.
2. Kompaktní podprostor $X \subseteq \mathbb{R}$ ($\equiv \mathbb{E}_1$) má největší a nejmenší prvek.

Věta *(Spojitá zobrazení a kompaktní množiny)*
Buď $f : (X, \rho) \to (Y, \sigma)$ spojité zobrazení a X kompaktní metrický prostor. Potom platí:

1. Zobrazení f je stejnoměrně spojité.
2. $f[X]$ je kompaktní podmnožina Y.
3. Je-li f navíc prosté, je f stejnoměrný homeomorfismus.

Důsledek
Z bodu 2. předchozího tvrzení a 1. před-předchozího plyne, že spojitá reálná funkce nabývá na kompaktním prostoru minima i maxima.

Úplné prostory

Definice *(Cauchyovská posloupnost bodů)*
Posloupnost $(x_n)_{n\geq 0}$ bodů z metrického prostoru (X, ρ) budiž *cauchyovská*, jestliže

$$\forall \varepsilon > 0 \; \exists n_0 : m, n \geq n_0 \;\Rightarrow\; \rho(x_m, x_n) < \varepsilon$$

Poznámka
Je-li posloupnost $\{x_n\}$ konvergentní, pak je cauchyovská. Obrácená implikace obecně neplatí.

Definice *(Úplný prostor)*
Prostor je *úplný*, pokud v něm každá cauchyovská posloupnost konverguje.

Věta *(O podposloupnosti)*
Pokud má cauchyovská posloupnost nějakou konvergentní podposloupnost, pak konverguje sama.

Příklady

- $\mathbb{R}$ je úplný prostor (díky Bolzano-Cauchyho podmínce)
- Každý kompaktní prostor je úplný (podle předchozí věty)
- $\mathbb{E}_n$ je úplný prostor (bez důkazu; vyžaduje součiny prostorů)

Věta *(Zachování úplnosti)*
Stejnoměrný homeomorfismus zachovává úplnost (protože stejnoměrně spojité zobrazení zachovává cauchyovské posloupnosti).
Poznámka
Používá se zejména při nahrazování metriky metrikou s ní stejnoměrně ekvivalentní. Tvrzení pro „obyčejnou“ spojitost neplatí.

Věta *(O úplném podprostoru)*
Podprostor Y úplného prostoru X je úplný, právě když je Y v X uzavřená množina.

Věta o pevném bodě

Definice *(kontrahující zobrazení)*
Zobrazení $f : (X, \rho) \to (Y, \sigma)$ mezi dvěma metrickými prostory nazveme *kontrahující*, pokud existuje číslo q, $0 < q < 1$ takové, že

$$\forall x, y \in X : \sigma(f(x), f(y)) \leq q \cdot \rho(x, y)$$

Takové zobrazení je jistě stejnoměrně spojité.

Definice *(pevný bod, posloupnost iterací)*
Pevný bod zobrazení $f : X \to X$ z nějaké množiny do sebe sama je takový bod $x \in X$, že $f(x) = x$. *Posloupnost iterací* zobrazení $f : X \to X$ je taková posloupnost $(x_n)_{n \geq 0}$, pro kterou platí $x_i = f(x_{i-1})$ $\forall i \geq 1$ (a x_0 je libovolný *startovací bod* iterací).

Věta *(Pickardova-Banachova o pevném bodě)*
Každé kontrahující zobrazení f úplného metrického prostoru (M, d) do sebe má právě jeden pevný bod. Navíc každá posloupnost iterací $(x_n)_{n \geq 0}$ tohoto zobrazení konverguje k tomuto pevnému bodu.

7 Diferenciální rovnice

Požadavky

- Soustavy lineárních diferenciálních rovnic prvního řádu
- lineární rovnice n-tého řádu s konstantními koeficienty
- Jejich řešení a speciální vlastnosti.

Vypracováno podle textu Dr. M. Klazara pro Matematickou analýzu III
`http://kam.mff.cuni.cz/~klazar/vseMAIII.pdf`

7.1 Obyčejné diferenciální rovnice

Definice *(Diferenciální rovnice)*
Diferenciální rovnice je (neformálně) rovnicový popis relací mezi hodnotami derivací nějakých neznámých funkcí. Rozlišují se dva druhy diferenciálních rovnic (přičemž my se omezíme na první z nich, a ještě speciálnější):

- *Obyčejné diferenciální rovnice* - takové rovnice, kde vystupují pouze derivace funkcí jedné proměnné
- *Parciální diferenciální rovnice* - v nich se objevují parciální derivace funkcí více proměnných.

Definice *(Obecný tvar obyčejné diferenciální rovnice)*
Obyčejná diferenciální rovnice v obecném tvaru pro neznámou funkci $y = y(x)$ vypadá následovně:

$$F(x, y, y', y'', \dots, y^{(n)}) = 0$$

(a F je nějaká funkce $n+2$ proměnných.) Nejvyšší řád derivace, která se v rovnici vyskytuje, označujeme jako *řád rovnice*.

Definice *(Lineární diferenciální rovnice)*
Speciálním případem obyčejných diferenciálních rovnic jsou rovnice *lineární*. Jsou to všechny rovnice, které se dají zapsat ve tvaru:

$$a_n(x)y^{(n)} + a_{n-1}(x)y^{(n-1)} + \cdots + a_1(x)y' + a_0(x)y = b(x)$$

Funkce $a_i(x)$ a $b(x)$ jsou zadané a $y = y(x)$ je neznámá. $b(x)$ se označuje jako *pravá strana* rovnice. Je-li funkce $b(x)$ identicky nulová, mluvíme o takové rovnici jako o *homogenní*.

Definice *(Algebraické diferenciální rovnice)*
Pokud je $F(x, y, y', \dots, y^{(n)}) = 0$ (obyčejná) diferenciální rovnice a F je nějaký polynom, mluvíme o této rovnici jako o *algebraické*. Lineární diferenciální rovnice jsou speciálním případem algebraických.

Definice *(Řešení diferenciální rovnice)*
Řešením diferenciální rovnice $F(x, y, y', \dots, y^{(n)}) = 0$ rozumíme dvojici (y, I), kde $I \subseteq \mathbb{R}$ je otevřený interval a $y : I \to \mathbb{R}$ je na I n-krát diferencovatelná funkce, pro níž v každém bodě a intervalu I platí $F(a, y(a), y'(a), y^{(n)}(a)) = 0$.

7.2 Řešení některých speciálních typů obyčejných diferenciálních rovnic

TODO

- Metoda integračního faktoru (pro 1 lin. rovnici)
- Variace konstant (pro 1 lin. rovnici)
- Separované proměnné
- Exaktní rovnice

7.3 Soustavy lineárních diferenciálních rovnic

Definice *(Soustava lineárních diferenciálních rovnic 1. řádu)*
Diferenciální rovnice 1. řádu jsou takové, ve kterých se vyskytují maximálně první derivace. Soustavou lineárních diferenciálních rovnic prvního řádu rozumíme soustavu rovnic

$$y_i' = a_{i,1}y_1 + \cdots + a_{i,n}y_n + b_i \quad 1 \leq i \leq n$$

a y_i je n neznámých funkcí, $a_{i,j} = a_{i,j}(x)$ a $b_i = b_i(x)$ jsou zadané funkce (celkem je jich $n^2 + n$) na otevřeném intervalu $I \subseteq \mathbb{R}$.
Maticově lze totéž vyjádřit jako:

$$y' = Ay + b$$

Poznámka *(Převod jedné rovnice n-tého řádu na soustavu prvního řádu)*
Je zřejmé, že funkce $y = y(x)$ je na otevřeném intervalu I řešením rovnice

$$F(x, y, y', y'', \ldots, y^{(n)}) = 0$$

, právě když jsou funkce $y, y_1, y_2, \ldots, y_n$ řešením soustavy

$$\begin{aligned} y_1 &= y' \\ y_2 &= y_1' \\ &\vdots \\ y_n &= y_{n-1}' \\ F(x, y, y_1, \ldots, y_n) &= 0 \end{aligned}$$

Lineární diferenciální rovnice n-tého řádu je pak ekvivalentní soustavě lin. rovnic 1. řádu:

$$\begin{aligned} y_1 &= y' \\ &\vdots \\ y_n &= y_{n-1}' \\ y_n + a_{n-1}y_{n-1} + \cdots + a_0 y + b &= 0 \end{aligned}$$

Věta *(O jednoznačném řešení soustavy lineárních diferenciálních rovnic)*
Nechť $a_{i,j}, b_i : I \to \mathbb{R}$ jsou spojité funkce definované na I pro $i \in \{1, \dots, n\}$. Potom soustava lineárních diferenciálních rovnic 1. řádu

$$y'(x) = Ay(x) + b$$

s počátečními podmínkami $y(\alpha) = \beta$ (kde $\alpha \in I$, $\beta \in \mathbb{R}^n$) má na I jednoznačné řešení, tj. existuje právě jedna matice funkcí $y_1, \dots, y_n$ se spojitými derivacemi (neboli z množiny $\mathcal{C}^1(I)$), která splňuje

$$y_i(\alpha) = \beta_i,\ y_i'(x) = \sum_{j=1}^{n} a_{i,j}(x) y_j(x) + b_i(x)$$

pro každé $i \in \{1, 2, \dots, n\}$ a každé $x \in I$.

Důsledek
Pokud se dvě řešení soustavy lineárních diferenciálních rovnic prvního řádu shodují v jednom bodě intervalu I, pak se shodují na celém I.

Definice *(Množiny řešení homogenní a nehomogenní soustavy)*
Pro soustavy lineárních dif. rovnic prvního řádu definujeme:

- $H = \{y \in \mathcal{C}^1(I)^n | y' = Ay\ \forall a \in I\}$ jako množinu řešení homogenní soustavy,
- $M = \{y \in \mathcal{C}^1(I)^n | y' = Ay + b\ \forall a \in I\}$ jako množinu řešení nehomogenní soustavy.

Věta *(O množinách řešení)*
Pro nějakou lineární dif. rovnici prvního řádu je H z přechozí definice vektorový podprostor prostoru $\mathcal{C}^1(I)^n$ o dimenzi n. M je afinní podprostor $\mathcal{C}^1(I)^n$ dimenze n a platí $\forall y \in M : M = y + H = \{y + z | z \in H\}$.

Definice *(Fundamentální systém řešení)*
Každou bázi prostoru $H = \{y \in \mathcal{C}^1(I)^n | y' = Ay\ \forall a \in I\}$ nazveme *fundamentálním systémem řešení.*

Definice *(Wronskián)*
Wronského determinant neboli *wronskián* n-tice funkcí $f_1, \dots, f_n$ (kde $f_i : I \to \mathbb{R}^n$ a $I \subset \mathbb{R}^n$) je funkce $W : I \to \mathbb{R}$ definovaná předpisem:

$$W(x) = W_{f_1,\dots,f_n} = \det \begin{pmatrix} f_{1,1} & f_{1,2} & \cdots & f_{1,n} \\ f_{2,1} & f_{2,2} & \cdots & f_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ f_{n,1} & f_{n,2} & \cdots & f_{n,n} \end{pmatrix}$$

Tato matice funkcí se někdy označuje jako *fundamentální matice.*

Věta *(Wronskián a fundamentání systém řešení)*
V případě, že funkce $f_1, \dots, f_n$ jsou řešením homogenní soustavy lin. diferenciálních rovnic prvního řádu $(f_i)' = Af_i$ $1 \leq i \leq n$, platí:

$$f_1, \dots, f_n \text{ jsou lineárně závislé, právě když } W(x) = 0\ \forall x \in I.$$

A wronskián je nulový ve všech bodech intervalu I, právě když je nulový pro jedno $x \in I$. To znamená, že pokud $f_1, \dots, f_n$ má na I v nějakém bodě nulový wronskián, pak není fundamentálním systémem řešení rovnice $(f_i)' = Af_i$ $1 \leq i \leq n$, v opačném případě však ano.

Věta *(O variaci konstant pro soustavu lin. diferenciálních rovnic 1. řádu)*
Nechť $I \subseteq \mathbb{R}^n$ je otevřený interval, $A : I \to \mathbb{R}^{n \times n}$, $b : I \to \mathbb{R}^n$ spojité maticové funkce a $y^1, \dots, y^n$ (kde $y^i : I \to \mathbb{R}\ \forall i$) je fundamentální systém řešení homogenní soustavy rovnic $y' = Ay$. Nechť $x_0 \in I$ a $y^0 \in \mathbb{R}^n$ jsou dané počáteční podmínky a $Y = Y(x)$ je matice funkcí fundamentálního systému řešení – fundamentální matice (jejíž determinant by byl wronskián).

Pak vektorová funkce $z : I \to \mathbb{R}^n$ daná předpisem

$$z(x) = Y(x)(\int_{x_0}^{x} Y(t)^{-1} b(t) \mathrm{d}t + Y(x_0)^{-1} y_0)$$

je řešením nehomogenní soustavy $y' = Ay + b$ a splňuje počáteční podmínku $z(x_0) = y^0$.

Poznámka
Variace konstant nám dovoluje získat řešení soustavy pro nějakou konkrétní pravou stranu rovnic, známe-li fundamentální systém řešení.

7.4 Lineární diferenciální rovnice s konstantními koeficienty

Definice *(Lineární rovnice s konstantními koeficienty)*
Rovnici $R(y)$ tvaru

$$a_n y^{(n)} + \cdots + a_1 y' + a_0 y = 0$$

pro $a_i \in \mathbb{R}\ \forall i$ konstanty, a_n nenulové a $y = y(x)$ neznámou funkci nazveme *lineární diferenciální rovnicí řádu n s konstantními koeficienty.* Definiční interval I je zde $I = \mathbb{R}$.

Definice *(Charakteristický polynom)*
Charakteristickým polynomem lineární diferenciální rovnice s konstantními koeficienty rozumíme

$$p(x) = a_n x^n + \cdots + a_1 x + a_0.$$

Podle základní věty algebry má množinu kořenů $K(p) = \{\lambda \in \mathbb{C} | p(\lambda) = 0\}$, jejichž násobnost označíme $n(\lambda) \in \mathbb{N}$.

Definice *(Množiny $\mathcal{F}(R,\mathbb{C})$ a $\mathcal{F}(R,\mathbb{R})$)*
Pro lineární dif. rovnici $R(y)$ definujeme množiny

$$\begin{aligned}
\mathcal{F}(R,\mathbb{C}) &= \{x^k \cdot \mathrm{e}^{\lambda x} | \lambda \in K(p), 0 \leq k \leq n(\lambda)\} \text{ a} \\
\mathcal{F}(R,\mathbb{R}) &= \{x^k \cdot \mathrm{e}^{\lambda x} | \lambda \in K(p) \cap \mathbb{R}, 0 \leq k \leq n(\lambda)\} \\
&\quad \cup \{x^k \mathrm{e}^{\lambda x} \sin(\mu x) | \lambda + \mu i \in K(p), \lambda, \mu \in \mathbb{R}, \mu \geq 0, 0 \leq k \leq n(\lambda + \mu i)\} \\
&\quad \cup \{x^k \mathrm{e}^{\lambda x} \cos(\mu x) | \lambda + \mu i \in K(p), \lambda, \mu \in \mathbb{R}, \mu \geq 0, 0 \leq k \leq n(\lambda + \mu i)\}
\end{aligned}$$

kde i značí imaginární jednotku komplexních čísel.

Věta *(O řešení rovnic s konstatními koeficienty)*
Každá funkce z $\mathcal{F}(R,\mathbb{C})$ i každá funkce z $\mathcal{F}(R,\mathbb{R})$ je řešením rovnice $R(y) = 0$.

Věta *(O lineární nezávislosti kořenů)*
Funkce z $\mathcal{F}(R,\mathbb{R})$ jsou lineárně nezávislé.

TODO: doplnit – podle rozsahu souborkových textů???

8 Algebra

Požadavky

- Grupa, okruh, těleso – definice a příklady
- Podgrupa, normální podgrupa, faktorgrupa, ideál
- Homomorfismy grup
- Dělitelnost a ireducibilní rozklady polynomů
- Rozklady polynomů na kořenové činitele pro polynom s reálnými, racionálními, komplexními koeficienty.
- Násobnost kořenů a jejich souvislost s derivacemi mnohočlenu

8.1 Grupa, okruh, těleso – definice a příklady

Definice *(algebra)*
Pro množinu A je zobrazení $\alpha : A^n \to A$, kde $n \in \{0, 1, ...\}$ *n-ární operace* (n je *arita*). Jsou-li $\alpha_i, i \in I$ operace arity Ω_i na množině A, pak $(A, \alpha_i | i \in I)$ je *algebra.*

Definice *(grupoid)*
Algebra s 1 binární operací je *grupoid.* V něm je $e \in G : e \cdot g = g \cdot e = g \ \forall g \in G$ *neutrální prvek.* Algebra s jednou asociativní binární operací a neutrálním prvkem vzhledem k ní je *monoid.* Nechť je dán monoid s neutrálním prvkem $(M, \cdot, e)$ a nějakým prvek $m \in M$. Potom řekneme, že prvek $m^{-1} \in M$ je *inverzní* k prvku m, pokud $m \cdot m^{-1} = m^{-1} \cdot m = e$. Prvek je *invertibilní*, pokud má nějaký inverzní prvek.

Poznámka
Každý grupoid obsahuje nejvýš 1 neutrální prvek. V libovolném monoidu platí, že pokud $(a \cdot b = e)$ & $(b \cdot c = e)$, pak $a = c$ (tj. inverzní prvek zleva a zprava musí být ten samý). Každý inverzní prvek je sám invertibilní.

Definice *(grupa)*
Algebra $(G, \cdot, ^{-1}, e)$ je *grupa*, pokud je $(G, \cdot, e)$ monoid a $^{-1}$ je operace inv. prvku (tedy unární operace, která každému prvku přiřadí prvek k němu inverzní). Grupa G je *komutativní (abelovská)*, pokud je operace „$\cdot$“ komutativní.

Příklady
Příklady grup:

- Množina $\mathbb{R}$ s operací sčítání, inverzním prvkem $-x$ a neutrálním prvkem 0
- Množina $\mathbb{R}_+$ (kladných reálných čísel, tedy bez nuly, protože k té bychom inverzní prvek nenašli) s operací násobení, inverzním prvkem x^{-1} a neutrálním prvkem 1
- Množina $\mathbb{Z}_n = \{0, \ldots, n-1\}$ pro n libovolné přirozené číslo; s operací sčítání modulo n, inverzním prvkem $(-x)$ modulo n a neutrálním prvkem 0
- Množina polynomů stupně $\leq n$ se sčítáním, opačným polynomem (s opačnými koeficienty) a neutrálním prvkem 0

- Množina všech permutací prvků $(1, \dots, n)$ s operací skládání permutací, opačnou permutací (takovou, že její složení s původní dává identitu) a neutrálním prvkem **id** (na rozdíl od všech předchozích pro permutace délky větší než 3 není abelovská)
- Množina regulárních matic $n \times n$ s operací maticového násobení, inverzními maticemi a jednotkovou maticí (taktéž není obecně abelovská)

Definice *(okruh)*

Nechť $(R, +, \cdot, -, 0, 1)$ je algebra taková, že $(R, +, -, 0)$ tvoří komutativní grupu, $(R, \cdot, 1)$ je monoid a platí $a(b+c) = ab + ac$ a $(a+b)c = ac + bc\ \forall a, b, c \in R$ (tedy distributivita sčítání vzhledem k násobení). Pak je $(R, +, \cdot, -, 0, 1)$ *okruh.*

Příklady

Příklady okruhů:

- Množina $\mathbb{Z}$ s operacemi sčítání a násobení, inverzem vůči sčítání – unárním minus a neutrálními prvky 0 a 1.
- Množina všech lineárních zobrazení na $\mathbb{R}^n$ s operacemi sčítání a skládání, „opačným“ zobrazením (kde $(-f)(x) = -(f(x))$), nulovým zobrazením a identitou (pro obecná zobrazení toto nefunguje, neplatí distributivita)

Poznámka *(Vlastnosti okruhů)*

V okruhu $(R, +, \cdot, -, 0, 1)$ pro každé 2 prvky $a, b \in R$ platí:

1. $0 \cdot a = a \cdot 0 = 0$
2. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$
4. $|R| > 1 \ \Leftrightarrow\ 0 \neq 1$

Definice *(těleso)*

Těleso je okruh $(F, +, -, \cdot, 0, 1)$, pro který navíc platí, že pro každé $x \in F$ kromě nuly existuje $y \in F$ takové, že $x \cdot y = y \cdot x = 1$, tj. pro všechny prvky kromě nuly existuje inverzní prvek vůči operaci „$\cdot$“ – „x^{-1}“. Navíc v F musí platit, že $0 \neq 1$ (vyloučení triviálních okruhů).

Komutativní těleso je takové těleso, ve kterém je operace „$\cdot$“ komutativní.

Příklady

Příklady těles:

- Tělesa $\mathbb{C}$ a $\mathbb{R}$
- Racionální čísla $\mathbb{Q} = \{\frac{a}{b}\ |a, b \in \mathbb{Z}, b \neq 0\}$
- $\mathbb{Z}_{p^n} = \{0, \dots, p^n - 1\}$, kde p je prvočíslo a n přirozené číslo – tzv. *Gallois field*, pro dané p a n existuje vždy až na isomorfismus (přejmenování prvků) jen jedno.

Všechna uvedená tělesa jsou komutativní. Obecně všechna konečná tělesa jsou komutativní (Wedderburnova věta).

8.2 Podgrupa, normální podgrupa, faktorgrupa, ideál

Definice *(podalgebra)*

Množina B je *uzavřená* na operaci α, když $\forall b_1, \ldots b_n \in B$ platí $\alpha(b_1, ...b_n) \in B$. Pro algebru $(A, \alpha_i | i \in I)$ je množina $B \subseteq A$ spolu s operacemi α_i *podalgebra* A, je-li množina B uzavřená na operaci α_i $\forall i \in I$.

Definice *(podgrupa)*

Podalgebra grupy je *podgrupa* (tj. jde o podmnožinu pův. množiny prvků, uzavřenou na „$\cdot$“ a „$^{-1}$“, spolu s původními operacemi). Podgrupa H grupy G je *normální*, pokud pro každé $g \in G$ (z původní množiny!) a pro každé $h \in H$ platí, že $g^{-1} \cdot h \cdot g \in H$ (někdy se píše zkráceně $G^{-1}HG \subseteq H$).

Poznámka *(Vlastnosti podgrup)*

Průnik podgrup $G \cap H$ je opět podgrupa. To určitě neplatí o sjednocení $G \cup H$ (to je podgrupou jen pokud je $G \subset H$ nebo $H \subset G$). Každá podmnožina grupy má nějakou nejmenší podgrupu, která ji obsahuje – to je *podgrupa generovaná* touto *množinou.* Podgrupa (i grupa) generovaná jedním prvkem se nazývá *cyklická.* Každá podgrupa cyklické grupy je také cyklická.

Podgrupy každé grupy společně s průnikem jako infimem a podgrupou generovanou sjednocením jako supremem tvoří úplný svaz (algebru se dvěma operacemi se speciálními vlastnostmi, supremem a infimem, definovanými pro všechny její podmnožiny). Úplný svaz se stejnými operacemi tvoří také normální podgrupy (jde o podsvaz prvního).

Příklady

Příklady podgrup:

- G a $\{e\}$ jsou vždy normální podgrupy grupy $(G, \cdot, ^{-1}, e)$.
- Množina $Z(G) = \{z \in G | gz = zg \ \forall g \in G\}$ je normální podgrupou G („*centrum grupy*“).
- $\mathbb{Z}_8$ má dvě netriviální podgrupy – $\{0, 4\}$ a $\{0, 2, 4, 6\}$ (je sama cyklická, takže obě jsou cyklické), plus samozřejmě triviální $\mathbb{Z}_8$ a $\{0\}$.

Definice

Pro grupu G a její podgrupu H se relace rmod_H definuje předpisem : $(a, b) \in \mathrm{rmod}_H \equiv ab^{-1} \in H$. Symetricky se definuje relace lmod_H $((a, b) \in \mathrm{lmod}_H \equiv a^{-1}b \in H)$. Tyto relace jsou ekvivalence. *Index podgrupy v grupě* je $[G : H] = |G/\mathrm{rmod}_H| = |G/\mathrm{lmod}_H|$ (počet tříd ekvivalence podle rmod_H nebo lmod_H).

Věta *(Lagrangeova)*

Pro grupu G a její podgrupu H platí: $|G| = [G : H] \cdot |H|$. Z toho plyne, že velikost podgrupy dělí velikost konečné grupy.

Definice *(faktorgrupa)*

Pro grupu $(G, \cdot, ^{-1}, e)$ a nějakou její normální podgrupu N je *faktorgrupa* $G/N = \{gn | g \in G, n \in N\}$. Běžně se definuje jako množina všech levých rozkladových tříd podle nějaké normální podgrupy (kde levá *rozkladová třída* podle podgrupy je $gH = \{gh | h \in H\}$). Faktorgrupa cyklické nebo abelovské grupy je také cyklická, resp. abelovská.

Příklady

Příklady faktorgrup:

- Pro grupu celých čísel $\mathbb{Z}$ a její normální podgrupu sudých celých čísel $2\mathbb{Z}$ je $\mathbb{Z}/2\mathbb{Z}$ faktorgrupou, isomorfní s grupou $\{0, 1\}$. Podobně to platí pro libovolné $n\mathbb{Z}$, kde n je přirozené.
- $\mathbb{R}/\mathbb{Z}$ je faktorgrupa grupy $\mathbb{R}$ (rozkladové třídy jsou tvaru $a + \mathbb{Z}$, kde a je reálné číslo v intervalu $\langle 0, 1)$.
- Faktorová grupa $\mathbb{Z}_4/\{0, 2\}$ je isomorfní se $\mathbb{Z}_2$.

Definice *(kongruence)*

Obecně v algebrách je *relace ρ slučitelná s operací α* arity n, pokud $a_1, \dots a_n, b_1, \dots b_n$: $(a_i, b_i) \in \rho\ \forall i$ implikuje $(\alpha(a_1, \dots a_n), \alpha(b_1, \dots b_n)) \in \rho$. *Kongruence* je každá ekvivalence slučitelná se všemi operacemi algebry.

Poznámka

Faktorgrupa je vlastně grupa, v níž jsou jednotlivé prvky třídy ekvivalence na původní grupě podle nějaké kongruence (levé rozkladové třídy tvoří kongruence).

Definice *(ideál)*

Nechť $(R, +, \cdot, -, 0, 1)$ je okruh a $I \subseteq R$. Pak I je *pravý ideál*, pokud $I \leq (R, +, -, 0)$ (tzn. I je podgrupou grupy R; je i normální, protože grupa R je z definice okruhu komutativní) a pro každé $i \in I$ a $r \in R$ platí $i \cdot r \in I$. *Levý ideál* se definuje stejně, jen poslední podmínka zní $r \cdot i \in I$. Každý levý i pravý ideál I je podle této definice uzavřený na násobení.

I je *ideál*, pokud je pravý a zároveň levý ideál. Ideál je *netriviální (vlastní)*, pokud $I \neq R$ a $I \neq \{0\}$.

Příklady

Příklady ideálů:

- $\{0\}$ a R jsou (nevlastní, triviální) ideály v každém okruhu R
- Sudá celá čísla tvoří ideál v okruhu $\mathbb{Z}$, podobně to platí pro $n\mathbb{Z}$, kde n je přirozené.
- Množina polynomů dělitelných $x^2 + 1$ je ideálem v okruhu všech polynomů s 1 proměnnou a reálnými koeficienty
- Množina matic $n \times n$ s nulovým posledním sloupcem vpravo je levý ideál v okruhu všech matic $n \times n$, není to ale pravý ideál (podobně s řádky a opačnými ideály)

Poznámka *(Vlastnosti ideálů)*
Průnik (levých, pravých) ideálů tvoří opět (levý, pravý) ideál. *Ideál generovaný podmnožinou* X okruhu R je průnik všech ideálů v R, které X obsahují. Všechny ideály nad nějakým okruhem s průniky a ideály generovanými sjednocením tvoří úplný svaz.

I je *maximální ideál*, pokud je netriviální a žádný jiný netriviální ideál není jeho nevlastní nadmnožinou. *Prvoideál* P v okruhu R je takový ideál, že pro každé $a, b \in R$, pokud je $ab \in P$, potom musí být $a \in P$ nebo $b \in P$. Prvoideály mají v některých ohledech podobné vlastnosti jako prvočísla.

Je-li ideál vlastní, pak neobsahuje 1. Každý ideál je neprázdný, protože jako podgrupa $(R, +, -, 0)$ musí obsahovat 0.

8.3 Homomorfismy grup

Obecná tvrzení o homomorfismech algeber (platí i pro grupy)

Definice *(homomorfismus)*
O zobrazení $f : A \to B$ řekneme, že je *slučitelné* s operací α, pokud pro každé $a_1, \dots a_n \in A$ platí $f(\alpha_{(A)}(a_1, ...a_n)) = \alpha_{(B)}(f(a_1), ...f(a_n))$. Pro algebry stejného typu (se stejným počtem operací stejné arity) je zobrazení $f : A \to B$ *homomorfismus*, pokud je slučitelné se všemi jejich operacemi.

Bijektivní homomorfismus se nazývá *isomorfismus*, algebry stejného typu jsou *isomorfní*, existuje-li mezi nimi aspoň 1 isomorfismus.

Poznámka *(Vlastnosti homomorfismů)*
Složení homomorfismů je homomorfismus. Je-li f bijekce a homomorfismus, je f^{-1} taky homomorfismus.

Definice *(přirozená projekce, jádro zobrazení)*
Přirozená projekce množiny A podle kongruence ρ je $\pi_\rho : A \to A/\rho$, kde $\pi_\rho(a) = [a]_\rho$. Pro zobrazení $f : A \to B$ se *jádro zobrazení* definuje jako relace $\ker f$ předpisem $(a_1, a_2) \in \ker f \equiv^{def} f(a_1) = f(a_2)$.

Poznámka *(homomorfismy a kongruence)*
Pro každou kongruenci ρ na libovolné algebře A je přirozená projekce $\pi_\rho : A \to A/\rho$ homomorfismus.

Věta *(O homomorfismu)*
Nechť $f : A \to B$ je homomorfismus algeber stejného typu a ρ kongruence na A. Potom:

1. existuje homomorfismus $g : A/\rho \to B$ takový, že $f = g\pi_\rho$ právě když $\rho \subseteq \ker f$,
2. g je navíc isomorfismus, právě když f je na (surjekce) a $\rho = \ker f$.

Věta *(Věty o isomorfismu)*

1. Nechť $f : A \to B$ je homomorfismus algeber stejného typu, pak $f(A)$ je podalgebra B a $^A/_{\ker f}$ je isomorfní algebře $f(A)$.
2. Nechť $\rho \subseteq \eta$ jsou dvě kongruence na algebře A. Pak algebra $^{(A/\rho)}/_{(\eta/\rho)}$ je isomorfní algebře $^A/_\eta$.

Homomorfismy grup

Věta *(O homomorfismu grup)*
Je-li zobrazení $f : G \to H$, kde G, H jsou grupy, slučitelné s bin. operací, pak je homomorfismus. (Důkaz: nejdřív dokázat slučitelnost s „e" a pak „$^{-1}$", oboje přímo z definice grupy.)

Definice *(mocnina prvku)*
V grupě lze definovat g^n (kde $n \in \mathbb{Z}$) jako:

- $g^0 = 1$,
- $g^{n+1} = g \cdot g^n \quad (n > 0)$,
- $g^n = (g^{-1})^{-n} \quad (n < 0)$.

Mocninná podgrupa grupy G je potom cyklická podgrupa – pro nějaký prvek $g \in G$ jde o množinu $\{\dots, g^{-1}, g^0, g, g^2, \dots\}$.

Poznámka *(O mocnině prvku)*
Je-li zobrazení $\varphi : \mathbb{Z} \to G$ definováno předpisem $\varphi_g(n) = g^n$ (tj. jde o mocniny prvku g), kde $g \in (G, \cdot, ^{-1}, 1)$, pak je φ grupový homomorfismus $(\mathbb{Z}, +, -, 0)$ a $(G, \cdot, ^{-1}, 1)$.

Poznámka *(Vlastnosti cyklických grup)*
Nechť grupa $(G, \cdot, ^{-1}, 1)$ je cyklická. Potom platí:

1. Je-li G nekonečná, pak $G \simeq (\mathbb{Z}, +, -, 0)$ (je isomorfní s celými čísly).
2. Je-li $n = |G|$ konečné, pak $(G, \cdot, ^{-1}, 1) \simeq (\mathbb{Z}_n, +, -, 0)$ (je isomorfní s grupou zbytkových tříd odpovídající velikosti).

8.4 Dělitelnost a ireducibilní rozklady polynomů

Zdroje následujících sekcí: texty J. Žemličky k přednášce Algebra II
`http://www.karlin.mff.cuni.cz/~zemlicka/cvic6-7/algi.htm`
a skripta R. El Bashira k přednášce Algebra I a II pro matematiky
`http://www.karlin.mff.cuni.cz/~bashir/`

Největší společný dělitel

Definice *(Komutativní monoid s krácením)*
Monoid $(S, \cdot, 1)$ je *komutativní monoid s krácením*, pokud operace „$\cdot$" je komutativní a navíc splňuje

$$\forall a, b, c \in S : a \cdot c = b \cdot c \;\Rightarrow\; a = b$$

Definice *(Dělení, asociovanost)*
O prvcích a, b nějakého komutativního monoidu s krácením S řekneme, že *a dělí b* ($a|b$, b je dělitelné a), pokud existuje takové $c \in S$, že $b = a \cdot c$. Řekneme, že *a je asociován s b* ($a||b$), jestliže $a|b$ a zároveň $b|a$.

Definice *(Obor integrity)*
Obor integrity je takový komutativní okruh $(R, +, \cdot, -, 0, 1)$, ve kterém platí, že $a \cdot b = 0$ implikuje $a = 0$ nebo $b = 0$.

Příklady

1. $(\mathbb{Z}, +, \cdot, -, 0, 1)$ je obor integrity.
2. Pro každý obor integrity $(R, +, \cdot, -, 0, 1)$ je $(R \setminus \{0\}, \cdot, 1)$ komutativní monoid s krácením („multiplikativní monoid").

Poznámka *(Vlastnosti „||")*
V komutativním monoidu s krácením $(S, \cdot, 1)$ platí pro $a, b \in S$, že $a||b$, právě když existuje invertibilní prvek u z S takový, že $a = b \cdot u$. Relace „$||$" tvoří kongruenci na S a faktoralgebra $(S/||, \cdot, [1]_{||})$ podle této kongruence je také komutativní monoid s krácením (relace „$|$" na něm tvoří uspořádání).

Definice *(Největší společný dělitel)*
Mějme komutativní monoid s krácením $(S, \cdot, 1)$ a v něm prvky $a_1, \ldots, a_n$. Prvek c nazveme největším společným dělitelem prvků $a_1, \ldots, a_n$, pokud $c|a_i$ pro všechna $i \in \{1, \ldots, n\}$ a zároveň libovolný prvek $d \in S$, který dělí všechna a_i dělí i c. Píšeme $\mathbf{NSD}(a_1, \ldots, a_n) = c$.

Stejně se definuje největší společný dělitel pro obory integrity (bereme obor integrity $(R, +, \cdot, -, 1, 0)$ jako komutativní monoid s krácením $(R \setminus \{0\}, \cdot, 1)$).

Definice *(Ireducibilní prvek, prvočinitelé)*
Prvek c komutativního monoidu s krácením $(S, \cdot, 1)$ nazveme *ireducibilním*, pokud c není invertibilní a zároveň $c = a \cdot b$ pro nějaké $a, b \in S$ vždy implikuje $c||a$ nebo $c||b$. Prvek c nazveme *prvočinitelem*, pokud není invertibilní a zároveň $c|a \cdot b$ pro $a, b \in S$ vždy implikuje $c|a$ nebo $c|b$.

Na oborech integrity se prvočinitelé a ireducibilní prvky definují stejně.

Věta *(Vlastnosti* **NSD***)*
V komutativním monoidu s krácením $(S, \cdot, 1)$ pro prvky a, b, c, d, e platí:

1. $d = \mathbf{NSD}(a, b)$ & $e = \mathbf{NSD}(a \cdot c, b \cdot c) \;\Rightarrow\; (d \cdot c)||e$.
2. $1 = \mathbf{NSD}(a, b)$ & $a|(b \cdot c)$ & $\mathbf{NSD}(a \cdot c, b \cdot c)$ existuje $\;\Rightarrow\; a|c$.

Věta *(Vlastnosti prvočinitelů)*
V komutativním monoidu s krácením je každý prvočinitel ireducibilní. Pokud navíc pro každé dva jeho prvky existuje největší společný dělitel, je každý ireducibilní prvek prvočinitelem.

Polynomy

Definice *(Okruh polynomů)*
Nad okruhem $(R, +, \cdot, -, 0, 1)$ a monoidem $(M, \cdot, e)$ definujme okruh $(R[M], +, \cdot, -, 0, 1)$, kde:

- $R[M] = \{p : M \to R | \{m | p(m) \neq 0\}$ je konečné $\}$
- prvek $p \in R[M]$ se dá zapsat jako $p = \sum_{m \in M} (p(m).m)$
- operace „+" je definována jako: $p + q = \sum_{m \in M} ((p(m) + q(m)).m)$
- „·" je definováno následovně: $p \cdot q = \sum_{m \in M} ((\sum_{r \cdot s = m} p(r) \cdot q(s)).m)$
- další operace:
  - $-p = \sum_{m \in M} (-p(m)) \cdot m$,
  - $0 = \sum_{m \in M} 0.m$,
  - $1 = (1 \cdot e) + \sum_{m \in M \setminus \{e\}} 0.m$.

Pro okruh $(R, +, \cdot, -, 0, 1)$ a monoid $(\mathbb{N}_0, +, 0)$ nezáporných celých čísel se sčítáním nazveme $R[\mathbb{N}_0]$ (označme $R[x]$) *okruh polynomů jedné neznámé*. Jeho prvky potom nazveme *polynomy* a budeme je zapisovat ve tvaru $p = \sum_{n \in \mathbb{N}_0} p(n).x^n$.

Poznámka
$R[x]$ nad okruhem R je obor integrity, právě když R je obor integrity.

Definice *(Stupeň polynomu)*
Pro polynom p v okruhu $R[x]$ nad $(R, +, \cdot, -, 0, 1)$ definujeme *stupeň polynomu* (deg p, st p) následovně:

$$\deg p = \begin{cases} \text{největší } n \in \mathbb{N}_0 : p(n) \neq 0, \text{ je-li } p \neq 0 \\ -1, \text{ je-li } p = 0 \end{cases}$$

Poznámka *(Vlastnosti* deg p*)*
V okruhu $R[x]$ nad $(R, +, \cdot, -, 0, 1)$ platí pro $p, r \in R[x]$:

- $\deg -p = \deg p$
- $\deg (p + q) = \max(\deg p, \deg q)$
- Je-li $p \neq 0, q \neq 0$, pak $\deg (p \cdot q) \leq \deg p + \deg q$ (na oborech integrity platí rovnost)

Věta *(Dělení polynomů se zbytkem)*
Nechť jsou na oboru integrity $(R[x], +, \cdot, -, 0, 1)$ (nad oborem integrity R) dány prvky $a, b \in R[x]$. Nechť navíc $m = \deg b \geq 0$ a b_m je invertibilní v R. Potom existují jednoznačně určené polynomy $q, r \in R[x]$ takové, že $a = b \cdot q + r$ a $\deg r < \deg b$.

Poznámka
Polynom q je *podíl* polynomů a a b, polynom r je *zbytek* při dělení.

Největší společný dělitel

Definice *(Eukleidovský obor integrity)*
Obor integrity $(R, +, \cdot, -, 0, 1)$ je *eukleidovský*, jestliže existuje zobrazení $\nu : R \to \mathbb{N}_0 \cup \{-1\}$ (*eukleidovská funkce*), které pro každé $a, b \in R$ splňuje:

1. Jestliže $a|b$ a $b \neq 0$, pak $\nu(a) \leq \nu(b)$
2. Pokud $b \neq 0$, existují $q, r \in R$ taková, že $a = b \cdot q + r$ a $\nu(r) < \nu(b)$

Poznámka
Je-li $(T, +, \cdot, -, 0, 1)$ nějaké komutativní těleso, pak $T[x]$ je eukleidovským oborem integrity s eukleidovskou funkcí danou stupněm polynomů. Příkladem eukleidovského oboru integrity jsou např. i celá čísla (se sčítáním, násobením, unárním minus, jedničkou a nulou), kde eukleidovská funkce je funkce absolutní hodnoty prvku.

Algoritmus *(Eukleidův algoritmus)*
Na eukleidovském okruhu R s eukleidovskou funkcí ν pro dva prvky $a_0, a_1 \in R \backslash \{0\}$ najdeme největší společný dělitel následujícím postupem:

- Je-li $i \geq 1$ a $a_i \not| \, a_{i-1}$, vezmeme $a_{i+1} \in R$ takové, že $a_{i-1} = a_i \cdot q_i + a_{i+1}$ pro nějaké q_i a $\nu(a_{i+1}) < \nu(a_i)$. i zvýšíme o 1 a pokračujeme další iterací.
- Je-li $i \geq 1$ a $a_i | a_{i-1}$, potom $a_i = \mathbf{NSD}(a_0, a_1)$ a výpočet končí.

Dá se dokázat, že se výpočet zastaví a kroky jsou dobře definované (lze nalézt a_{i+1} a q_i), tedy libovolné dva polynomy mají největšího společného dělitele.

Poznámka
Největší společný dělitel je v polynomech $R[x]$ určen až na asociovanost ($||$) jednoznačně. Pro asociované polynomy p, q vždy platí, že $\deg p = \deg q$ a $p = r \cdot q$ pro nějaké $r \in R$.

8.5 Rozklady polynomů na kořenové činitele

Rozklady polynomů

Poznámka *(Ireducibilní polynomy)*
Polynom je ireducibilní, pokud není součinem dvou polynomů nižších stupňů a jeho stupeň je větší nebo roven jedné. Všechny polynomy stupně 1 jsou ireducibilní. Jedinými děliteli ireducibilního polynomu jsou asociované polynomy a nenulové skaláry (tj. polynomy stupně 0).

Věta *(Rozklad polynomu)*
Každý polynom stupně alespoň 1 má až na asociovanost jednoznačný rozklad na součin ireducibilních polynomů.
Důkaz existence: indukcí podle deg p – najdeme vždy dělitel p nejmenšího možného kladného stupně, vydělíme a pokračujeme, dokud nedostaneme polynom, který nemá dělitel kladného stupně menšího než je jeho vlastní.

Definice *(Dosazování do polynomů)*
Nechť $(S, +, \cdot, -, 0, 1)$ je okruh, R jeho podokruh ($R \subset S$) a nechť $\alpha \in S$. Potom zobrazení $j_\alpha : R[x] \to S$, dané předpisem $j_\alpha(\sum_{n \in \mathbb{N}_0} a_n . x^n) = \sum_{n \in \mathbb{N}_0} a_n \cdot \alpha^n$ je okruhový homomorfismus. Nazývá se *dosazovací homomorfismus.*

Poznámka *(Dosazovaní a* deg p*)*
Pro obor integrity $R[x]$ nad oborem integrity $(R, +, \cdot, -, 0, 1)$ je polynom $p[x]$ invertibilní, právě když deg $p = 0$ a $j_0(p) = p(0)$ je invertibilní na R.

Definice *(Kořen polynomu)*
Pro okruh $(S, +, \cdot, -, 0, 1)$ a jeho podokruh R je *kořen polynomu* $p \in R[x]$ takové $\alpha \in S$, že $j_\alpha(p) = p(\alpha) = 0$ (při dosazení α se polynom p zobrazí na 0).

Definice *(Kořenový činitel, rozklad)*
Je-li $a = c \cdot p_1^{k_1} \cdot \ldots p_n^{k_n}$ rozklad polynomu $p \in R[x]$ na ireducibilní polynomy, potom *kořenovým činitelem* polynomu p nazveme takové p_i, které je ve tvaru $x - \alpha$ (tedy stupně 1 s koeficienty 1 a α). Řekneme, že polynom $p \in R[x]$ se *rozkládá na kořenové činitele* v $R[x]$, jestliže existuje takový jeho rozklad na ireducibilní polynomy, že všechny p_i jsou kořenové činitele. Potom nazveme k_i *násobnostmi kořenů.*

Věta *(kořen a kořenový činitel)*
Na oboru integrity $R[x]$ nad oborem integrity R je $\alpha \in R$ kořenem polynomu $p \in R[x], p \neq 0$, právě když $(x - \alpha)|p$.

Komplexní, reálné a racionální polynomy

Definice *(Algebraicky uzavřené těleso)*
Nechť T je těleso a S jeho nadtěleso. Prvek $a \in S$ je *algebraický* nad T, pokud existuje nějaký nenulový polynom z $T[x]$, jehož je a kořenem. Pokud žádný takový polynom neexistuje, nazývá se prvek *transcendentní.* Těleso T je *algebraicky uzavřené*, pokud všechny nad ním algebraické prvky jsou i jeho prvky (jsou v něm obsaženy).

Poznámka

Každý polynom v okruhu polynomů o jedné neznámé nad algebraicky uzavřeným tělesem se rozkládá na kořenové činitele.

Věta *(Základní věta algebry)*

Těleso $\mathbb{C}$ komplexních čísel je algebraicky uzavřené.

Důsledek

Proto má každý polynom $p(x) \in \mathbb{C}[x]$ stupně alespoň 1 v $\mathbb{C}[x]$ rozklad tvaru $p(x) = a(x-\beta_1)^{k_1} \cdot \dots \cdot (x-\beta_s)^{k_s}$, kde $\sum_{i=1}^{s} k_i = n$ a β_i jsou navzájem různá.

Věta *(Komplexně sdružené kořeny v $\mathbb{C}$)*

Má-li polynom p nad $\mathbb{C}[x]$ s reálnými koeficienty ($a_i \in \mathbb{R}$) kořen $\alpha \in \mathbb{C}$, pak je jeho kořenem i $\overline{\alpha}$, tedy číslo komplexně sdružené s α.

Důsledek

Polynom $p(x) \in \mathbb{R}[x]$ stupně alespoň 1 má v $\mathbb{R}[x]$ rozklad tvaru

$$p(x) = a(x-\alpha_1)^{k_1} \cdot \ldots (x-\alpha_r)^{k_r} \cdot (x^2 - a_1 x + b_1)^{l_1} \cdot \ldots (x^2 - a_s x + b_s)^{l_s}$$

a polynomy $x^2 + a_j x + b_j$, kde $j \in \{1, \dots s\}$ mají za kořeny dvojice komplexně sdružených čísel (která nejsou čistě reálná). Navíc $\deg p = k_1 + \dots + k_r + 2(l_1 + \dots + l_s)$.

Důsledek

Každý polynom v $\mathbb{R}[x]$ lichého stupně má alespoň jeden reálný kořen.

Věta *(Ireducibilní polynomy v $\mathbb{Q}$)*

V $\mathbb{Q}[x]$ existují ireducibilní polynomy libovolného stupně většího nebo rovného jedné (tj. ne vždy existuje rozklad na kořenové činitele, ani rozklad na polynomy stupně max. 2 jako v reálných číslech).

8.6 Násobnost kořenů a jejich souvislost s derivacemi mnohočlenu

Věta *(o počtu kořenů)*

Každý nenulový polynom $p \in R[x]$, kde $R[x]$ je okruh polynomů nad oborem integrity $(R, +, \cdot, -, 0, 1)$, má nejvýše $\deg p$ kořenů (plyne z vlastností $\deg p$).

Definice *(vícenásobný kořen)*

Pro komutativní okruh $(R, +, \cdot, -, 0, 1)$ a polynom $p \in R[x]$ je $\alpha \in R$ *vícenásobný kořen*, pokud polynom $(x-\alpha)(x-\alpha)$ dělí p.

Definice *(Derivace polynomu)*

Pro polynom $p = \sum_{i \geq 0} a_i x^i$ z okruhu polynomů $R[x]$ nad komutativním okruhem $(R, +, \cdot, -, 0, 1)$ definujeme *derivaci* (p', $p' \in R[x]$) předpisem

$$p' = \sum_{i \geq 0} (i+1) a_{i+1} x^i$$

Poznámka *(Vlastnosti derivace)*
Pro okruh $(R, +, \cdot, -, 0, 1)$, prvek $\alpha \in R$ a polynomy $p, q \in R[x]$ platí:

- $(p + q)' = p' + q'$
- $(\alpha p)' = \alpha p'$
- $(p \cdot q)' = p' \cdot q + p \cdot q'$

Věta *(derivace a vícenásobný kořen)*
Nad oborem integrity $(R, +, \cdot, -, 0, 1)$ buď $p \in R[x]$ polynom. Je-li $\alpha \in R$ jeho kořen, pak α je vícenásobný kořen, právě když je α kořenem p'.

Definice *(Charakteristika oboru integrity)*
Pro obor integrity $(R, +, \cdot, -, 0, 1)$ definujeme *charakteristiku oboru integrity* jako

- 0 (nebo někdy ∞), pokud cyklická podgrupa grupy $(R, +, 0)$ generovaná prvkem 1 je nekonečná.
- p, pokud cyklická pogrupa grupy $(R, +, 0)$ generovaná jedničkou má konečný řád p.

Věta *(derivace snižuje stupeň polynomu)*
Nad oborem integrity charakteristiky 0 $(R, +, \cdot, -, 0, 1)$ buď p polynom ($p \in R[x]$) stupně $n > 0$. Potom p' je polynom stupně $n - 1$.

Věta *(derivace a násobný kořen)*
Nad tělesem charakteristiky 0 $(T, +, \cdot, -, 0, 1)$ buď p polynom ($p \in T[x]$) stupně alespoň 1. Potom prvek $\alpha \in U$, kde U je nějaké nadtěleso T, je k-násobným kořenem p, právě když platí obě následující podmínky:

- $p(\alpha) = j_\alpha(p) = 0,\ p'(\alpha) = 0,\ \ldots\ p^{(k-1)}(\alpha) = 0$
- $p^{(k)}(\alpha) \neq 0$

Věta *(derivace a největší společný dělitel)*
Mějme těleso $(T, +, \cdot, -, 0, 1)$ charakteristiky 0 a nad ním něm polynom $p \in T[x]$ stupně alespoň 1. Potom platí:

- Pokud $\mathbf{NSD}(p, p') = 1$, pak p nemá žádný vícenásobný kořen.
- Každý k-násobný kořen p je $(k - n)$-násobným kořenem n-té derivace p.
- Polynom $q \in R[T]$ takový, že $q \cdot \mathbf{NSD}(p, p') = p$ má stejné kořeny jako p, ale jednoduché.

Věta
Nechť $(R, +, \cdot, -, 0, 1)$ je obor integrity a jeho charakteristika nedělí přir. číslo n. Potom polynomy $x^n - 1$ a $x^{n+1} - x$ v $R[x]$ nemají vícenásobný kořen.

9 Vektorové priestory

Požiadavky

- Základné vlastnosti vektorových priestorov, podpriestorov generovania, lineárna závislost a nezávislosť.
- Veta o výmene
- Konečne generované vektorové priestory, báza.
- Lineárne zobrazenie.

Ako zdroj pre vypracovanie otázky boli použité vlastné poznámky z prednášok Lineárna algebra Jiřího Fialu a suborkové texty.

9.1 Definície

Definícia

Nech $(T, +, \cdot)$ je teleso a V je množina (jej prvky nazývame *vektory*) s binárnou operáciou $+$ a $\cdot : T \times V \to V$ je zobrazenie, potom $(V, +, \cdot)$ sa nazýva **vektorový prostor** nad telesom T ak je splnených nasledujúcich 8 axiomov.

(SA) $\forall u, v, w \in V : \quad (u + v) + w = u + (v + w)$ *(asociativita súčtu)*
(SK) $\forall u, v \in V : \quad u + v = v + u$ *(komutativita súčtu)*
(S0) $\exists \mathbf{0} \in V : \quad u + \mathbf{0} = \mathbf{0} + u = u$ *(neutrálný prvok súčtu)*
(SI) $\forall u \in V \, \exists -u \in V : \quad u + (-u) = \mathbf{0}$ *(inverzný prvok súčtu)*
(NA) $\forall a, b \in T \, \forall u \in V : \quad (a \cdot b) \cdot u = a \cdot (b \cdot u)$ *(asociativita súčinu)*
(N1) $\forall u \in V : \quad 1 \cdot u = u$ kde $1 \in T$ je jednotkový prvok telesa T
(D1) $\forall a, b \in T \, \forall u \in V : \quad (a + b) \cdot u = a \cdot u + b \cdot u$ *(distributivita)*
(D2) $\forall a \in T \, \forall u, v \in V : \quad a \cdot (u + v) = a \cdot u + a \cdot v$ *(distributivita)*

Príklady

- $\{\mathbf{0}\}$ … triviálny vektorový priestor
- T^n aritmetický vektorový priestor dimenzie n nad telesom T. Ide o usporiadané n-tice, kde $+$ je definované predpisom

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

  a násobenie predpisom

$$\alpha(x_1, \ldots, x_n) = (\alpha x_1, \ldots, \alpha x_n)$$

- Z každého telesa T je možné vybudovať vektorový priestor rovnakej veľkosti $V = T^1$
- $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_p$, …, $\mathbb{R}^2$, $\mathbb{Q}^2$, …
- Matice typu $m \times n$ nad T (pre konkrétne m, n)
- Polynomy nad T (napríklad obmedzeného stupňa)

9.2 Vlastnosti vektorových priestorov

Pozorovanie

1. $\mathbf{0}$, $-u$ sú určené jednoznačne.
2. $\forall a \in T\ \forall u \in V: \quad a \cdot \mathbf{0} = 0 \cdot u = \mathbf{0}$
3. $\forall a \in T\ \forall u \in V: \quad a \cdot u = \mathbf{0} \ \Rightarrow\ a = 0 \ \vee\ u = \mathbf{0}$.

Definícia

Nech $(V, +, \cdot)$ je vektorový priestor nad telesom T a $U \subseteq V, U \neq \emptyset$ taká, že

- $\forall u, v \in U: \quad u + v \in U$ *(uzavretosť na súčet)*
- $\forall u \in U\ \forall a \in T: \quad a \cdot u \in U$ *(uzavretosť na súčin)*

potom $(U, +, \cdot)$ nazývame **podpriestorom** V.

Pozorovanie

Podpriestor je tiež vektorový priestor.

Veta

Prienik ľubovolného systému podpriestorov je podpriestor.

Definícia *(Lineárny obal, množina generátorov)*

Nech V je vektorový priestor nad telesom T a X je podmnožina V, potom

$$\mathcal{L}(X) = \bigcap \{U | X \subseteq U, U \,\text{je podpriestor}\, V\}$$

je podpriestor V generovaný X nazývaný **lineárny obal** X. Množina X sa potom nazýva *systém generátorov* podpriestoru $\mathcal{L}(X)$.

Keď $\mathcal{L}(X) = V$, potom X je systém generátorov vektorového priestoru V.

Definice

Spojení dvou podprostorů je podprostor

$$W_1 \oplus W_2 = \mathcal{L}(W_1 \cup W_2)$$

Veta

Lineárny obal $\mathcal{L}(X)$ obsahuje všetky lineárne kombinácie vektorov z X.

$$\mathcal{L}(X) = \{w \big| w = \sum_{i=1}^{n} a_i u_i, n \geq 0, n\, konečné, \forall i:\ a_i \in T, u_i \in X\}$$

Špeciálne v prípade, že $X = \emptyset$ a teda $n = 0$, platí $\mathcal{L}(X) = \{0\}$.

Definícia

Nech V je vektorový priestor nad telesom T, potom n-tica vektorov $v_1, \dots, v_n \in V$ je **lineárne nezávislá**, ak rovnica

$$a_1 v_1 + a_2 v_2 + \dots + a_n v_n = \mathbf{0}$$

má iba triviálne riešenie $a_i = 0$ pre všetky $i \in \{1, 2, \dots, n\}$

Nekonečná množina vektorov je lineárne nezávislá, ak každá jej konečná podmnožina je lineárne nezávislá.

Pozorovanie

X je lineárne nezávislá práve keď $\forall u \in X : u \notin \mathcal{L}(X \setminus \{u\})$

Věta

1. Obsahuje-li systém $x_1, \dots, x_n$ nulový vektor, je závislý.
2. Obsahuje-li systém $x_1, \dots, x_n$ dva stejné vektory, je závislý.
3. Pro libovolná reálná čísla $\beta_2, \dots, \beta_n$ je systém $x_1, \dots, x_n$ lineárně závislý, právě když je systém $x_1 + \sum_{i=2}^{n} \beta_i x_i, x_2, \dots, x_n$ lineárně závislý. *(Inak povedané, ak pričítame k jednému vektoru ľubovolnú lineárnu kombináciu ostatných vektorov, nezmeníme tým ich lineárnu závislosť.)*

Věta

1. Podsystém lineárně nezávislého systému je lineárně nezávislý.
2. Nadsystém systému generátorů je systém generátorů.

Definícia

Nech V je vektorový priestor. Množina $X \subseteq V$ sa nazýva **báza** vektorového priestoru V ak

- je lineárne nezávislá
- $\mathcal{L}(X) = V$

(Inak povedané, báza je lineárne nezávislý systém generátorov.)

Veta

Každý prvok vektorového priestoru možem vyjadriť ako lineárnu kombináciu prvkov jeho báze a toto vyjadrenie je jednoznačné.

Definícia

Vyjadrenie vektoru $u \in V$ vzhladom k báze X sa nazýva **vektor súradníc**. Značí sa $[u]_X$.

$(x_1, \dots, x_n) = X$ je báza V, $u \in V : u = a_1 x_1 + a_2 x_2 + \dots + a_n x_n$

$[u]_X = (a_1, \dots, a_n)$

9.3 Veta o výmene

Lemma *(o výmene)*

Nech $v_1, v_2, \dots, v_n$ je systém generátorov priestoru V a pre $u \in V$ platí $u = a_1v_1 + a_2v_2 + \cdots + a_nv_n$, potom platí

$$\forall i: \; a_i \neq 0 \Rightarrow \mathcal{L}(v_1, v_2, \dots, v_{i-1}, u, v_{i+1}, \dots, v_n) = V$$

(Inak povedané, vektor bázy ktorý sa "podielal" na vytvorení vektoru u, možme s u zameniť.)

Dôkaz

Pre ľubovolné $w \in V$, môžme písať $w = b_1v_1 + b_2v_2 + \dots b_nv_n$. Do tohoto vyjadrenia miesto v_i dosadíme vyjadrenie v_i z rovnice $u = a_1v_1 + a_2v_2 + \cdots + a_nv_n$, čím dostaneme vyjadrenie ľubovolného w pomocou $v_1, v_2, \dots, v_{i-1}, u, v_{i+1}, \dots, v_n$, z čoho výplýva, že tieto vektory sú tiež systém generátorov.

Veta *(Steinitzova o výmene)*

Nech V je vektorový priestor, $X \subseteq V$ je lineárne nezávislá a $Y \subseteq V$je konečný systém generátorov. Potom existuje $Z \subseteq V$ také, že

- $|Z| = |Y|$
- $\mathcal{L}(Z) = V$
- $Z \setminus X \subseteq Y$
- $X \subseteq Z$

(V krátkosti povedané - každý nezávislý systém vektorov X je možné, pridaním vektorov zo systému generátorov Y, rozšíriť na systém generátorov V.)

Dôkaz

Ak $X \subseteq Y$ sme hotoví a $Z = Y$. Inak vezmeme Y a postupne do neho začneme pridávať prvky z $X \setminus Y$. Pri každom pridaní, podľa lemmy o výmene, jeden prvok z tejto množiny odstránime. Po poslednej iterácii získame hľadané Z.

(Pri každej iterácií vyhadzujeme jeden prvok, ktorý nepatrí do X, pretože X je lineárne nezávislá.)

Dôsledok

Ak má V konečnú bázu, majú všetky bázy rovnakú veľkosť.

Dôsledok

Ak má V konečnú bázu, potom môžme každú lineárne nezávislú množinu X doplniť na bázu.

Definícia

Veľkosť bázy konečne generovaného priestoru V sa nazýva **dimenzia** priestoru V. Značíme $\dim(V)$.

Věta

Buďte W_1, W_2 konečně generované podprostory vektorového prostoru V. Potom

$$\dim W_1 + \dim W_2 = \dim(W_1 \cap W_2) + \dim(W_1 \oplus W_2)$$

9.4 Lineárne zobrazenie

Definice *(lineární zobrazení)*
Mějme vektorové prostory V, W. Řekneme, že zobrazení $f : V \to W$ je **lineární**, jestliže pro libovolná $x, y \in V$ a $a, b \in T$ platí

$$f(a \cdot x + b \cdot y) = a \cdot f(x) + b \cdot f(y)$$

Definice *(lineární operátor)*
Lineární zobrazení $f : V \to V$ se nazývá *lineární operátor.*

Příklady

1. Identické zobrazení V na V (to je příklad lineárního operátoru).
2. Buď α pevné reálné číslo. Zobrazení $V \to V$ dané předpisem $x \to \alpha x$.
3. Derivace je lineární zobrazení z množiny reálných spojitých funkcí $C_1(J)$ do množiny reálných funkcí $F(J)$.
4. V $\mathbb{R}^2$ jsou lineární zobrazení např. zrcadlení $(x, y) \mapsto (-x, y)$ nebo zkosení $(x, y) \mapsto (x + y, y)$.

Definice *(Hodnost lineárního zobrazení)*
Pro lineární zobrazení $f : U \to V$ mezi dvěma vekt. prostory definujeme *jádro zobrazení* (Ker f) jako množinu Ker $f = f^{-1}[\{0\}]$. *Obraz* zobrazení f (Im f) je množina Im $f = f[U]$. Jako *hodnost zobrazení* f označíme číslo dim(Ker f).

Věta *(Základní vlastnosti lineárního zobrazení)*
Nechť $f : V \to W$ je lineární zobrazení. Potom platí:

1. $f(\mathbf{0}_V) = \mathbf{0}_W$
2. Im f je podprostor prostoru W
3. Ker (f) je podprostor prostoru V
4. f je prosté, právě když Ker $(f) = \{0\}$
5. je-li $\dim V = \dim W$ a je-li zobrazení f prosté, potom je f bijekce a inversní zobrazení $f^{-1} : W \to V$ je opět lineární.

Věta *(O dimenzi obrazu a jádra)*
Pro $f : U \to V$ mezi dvěma vektorovými prostory konečné dimenze platí:

$$\dim(\text{Ker } f) + \dim(\text{Im } f) = \dim(U)$$

Věta *(Báze určuje lineární zobrazení)*
Mějme dány vektorové prostory V, W a bázi $B = b_1, \ldots, b_n$ prostoru V. Potom pro každé lineární zobrazení $f : B \to W$ existuje právě jedno lineární zobrazení $g : V \to W$ takové, že $f(b_i) = g(b_i)\ \forall i \in \{1, \ldots, n\}$.

Jiná formulace: Pro libovolné vektory $y_1, \ldots, y_n \in W$ existuje právě jedno lineární zobrazení $g : V \to W$ takové, že $g(b_i) = y_i\ \forall i \in \{1, \ldots, n\}$.

Definice *(Isomorfismus)*

Lineární zobrazení se nazývá *isomorfismus*, existuje-li k němu inversní lineární zobrazení. Pokud existuje isomorfismus $V \to W$, říkáme, že prostory V a W jsou *isomorfní.*

Věta

Je-li lineární zobrazení bijektivní, je to isomorfismus.

Věta *(Isomorfismus vekt. prostorů nad $\mathbb{T}$)*

Každý n-dimensionální vektorový prostor nad tělesem $\mathbb{T}$ je isomorfní vekt. prostoru $\mathbb{T}^n$ (tj. jehož prvky jsou uspořádané n-tice prvků z $\mathbb{T}$).

Věta *(Další vlastnosti lin. zobrazení)*

1. Je-li lineární zobrazení prosté, zachovává lineární nezávislost.
2. Je-li na (surjekce), zachovává vlastnost „být systémem generátorů“.

Věta *(Skládání lineárních zobrazeni)*

Nechť $f : U \to V$, $g : V \to W$ jsou lineární zobrazení. Potom složené zobrazení $g \circ f : U \to W$ definované předpisem

$$(g \circ f)(x) = g(f(x)) \text{ pro } x \in U$$

je rovněž lineárním zobrazením.

Věta *(Sčítání a násobky lin. zobrazení)*

Nechť f, g jsou lineární zobrazení z vekt. prostoru V do W, α skalár. Potom zobrazení $f + g : V \to W$ a $\alpha f : V \to W$ definovaná předpisem

$$(f + g)(x) = f(x) + g(x),\ x \in V$$

$$(\alpha f)(x) = \alpha f(x),\ x \in V$$

jsou lineární zobrazení V do W.

Věta *(Množina lineárních zobrazení je vekt. prostor)*

Množina lineárních zobrazení prostoru V do prostoru W s operacemi sčítání a násobení skalárem, definovanými v předchozí větě, tvoří vektorový prostor, který značíme $L(V, W)$.

Věta

Nechť $\dim V = n$ a $\dim W = m$. Potom prostor $L(V, W)$ je isomorfní prostoru $\mathbb{R}^{m \times n}$. V důsledku toho je

$$\dim L(V, W) = mn$$

10 Skalární součin

Požadavky

- Vlastnosti v reálném i komplexním případě
- Norma
- Cauchy-Schwarzova nerovnost
- Kolmost
- Ortogonální doplněk a jeho vlastnosti

10.1 Vlastnosti v reálném i komplexním případě

Definice

Nechť V je vektorový prostor nad $\mathbb{C}$. Potom zobrazení (funkce) z kartézského součinu $V \times V \to \mathbb{C}$, které dvojici vektorů x a y přiradí číslo $\langle x, y \rangle$ se nazývá *skalární součin*, pokud splňuje následující axiomy (pro všechny $x, x', y \in V$ a $\alpha, \beta \in \mathbb{C}$):

1. $\langle x, x \rangle \geq 0, \ \langle x, x \rangle = 0 \Leftrightarrow x = 0$ *(positivní definitnost)*
2. $\langle \alpha x + \beta x', y \rangle = \alpha \langle x, y \rangle + \beta \langle x', y \rangle$ *(bilinearita)*
   (a) $\langle \alpha x, y \rangle = \alpha \langle x, y \rangle$
   (b) $\langle x + x', y \rangle = \langle x, y \rangle + \langle x', y \rangle$
3. $\langle x, y \rangle = \overline{\langle y, x \rangle}$ *(symetrie - komplexně sdružené)*
   Poznámka
   Pro V' nad $\mathbb{R}$ a vektory $\forall x, y \in V'$: $\langle x, y \rangle = \langle y, x \rangle$

Skalární součin značíme: $\langle x, y \rangle$, $\langle x | y \rangle$, $x.y$ ...

Pozorování

- $\langle x, x \rangle = \overline{\langle x, x \rangle}$, tedy je nutně reálné ($\in \mathbb{R}$) i pro skalární součiny nad $\mathbb{C}$
- $\langle x, \alpha y \rangle = \overline{\langle \alpha y, x \rangle} = \overline{\alpha}.\overline{\langle y, x \rangle} = \overline{\alpha}. \langle x, y \rangle$
- Skalární součin může nabývat záporných hodnot

Definice

Ekvivalentní definice: *Skalární součin* je pozitivně definitní (1) bilineární forma (2). V $\mathbb{R}$ navíc symetrická (3). V $\mathbb{C}$ navíc forma, jejíž matice je hermitovská (3).

Příklady

- „Standardní“ skalární součin pro $\mathbb{C}^n, \mathbb{R}^n$:

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i \overline{y_i}$$

- Jiný součin v $\mathbb{R}^n$ definovaný pomocí regulární matice A řádu n

$$\langle x, y\rangle = x^T A^T A y \qquad (\textit{pozorování: } \langle x, x\rangle = x^T A^T A x = \sum_{i=1}^{n} (Ax)_i^2)$$

- Skalární součin ve vektorovém prostoru $C[a, b]$ (integrovatelných funkcí na intervalu $[a, b]$):

$$\langle f, g\rangle = \int_a^b f(x)g(x)dx$$

10.2 Norma

Definice *(Norma)*
Norma na vektorovém prostoru V (nad $\mathbb{R}$ nebo nad $\mathbb{C}$) je zobrazení $V \to \mathbb{R}$, které přiradí vektoru $x \in V$ číslo $\|x\|$ a splňuje axiomy:

1. $\forall x \in V : \|x\| \geq 0, \|x\| = 0 \Leftrightarrow x = 0$
2. $\forall x \in V, \forall \alpha \in \mathbb{C}(\mathbb{R}) : \|\alpha x\| = |\alpha|.\|x\|$
3. $\forall x, y \in V : \|x\| \geq 0, \|x + y\| \leq \|x\| + \|y\|$ *(trojúhelníková nerovnost)*

Norma $\|x\|$ má význam „délky“ vektoru x.

Definice *(Normovaný vekt. prostor)*
Vektorový prostor s nějakou normou nazýváme *normovaný.*

Příklady

- Norma určená skalárním součinem

$$\|x\| = \sqrt{\langle x, x\rangle}$$

Důkaz
(1), (2) plyne z axiomů skalárního součinu, (3):

$$\begin{aligned}
\langle x, y\rangle^2 \leq \langle x, x\rangle \langle y, y\rangle \Rightarrow \quad & \langle x, y\rangle \leq \sqrt{\langle x, x\rangle \langle y, y\rangle} \\
\Leftrightarrow \quad & \langle x, x\rangle + \langle y, y\rangle + 2\langle x, y\rangle \leq (\sqrt{\langle x, x\rangle} + \sqrt{\langle y, y\rangle})^2 \\
\Leftrightarrow \quad & \langle x + y, x + y\rangle \leq (\sqrt{\langle x, x\rangle} + \sqrt{\langle y, y\rangle})^2 \\
\Leftrightarrow \quad & \|x + y\| \leq \|x\| + \|y\|
\end{aligned}$$

Kde první nerovnost je důsledek Cauchy-Swarzovy nerovnosti…
Ze standardního skalárního součinu na $\mathbb{R}^n$ dostaneme euklidovskou normu (tj. „délku“ vektoru podle Pythagorovy věty) a euklidovskou vzdálenost (vzdálenost bodů u a v je $\|u - v\|$). Každý vektorový prostor se skalárním součinem $\langle ., .\rangle$ je normovaným vektorovým prostorem ($\|x\| = \sqrt{\langle x, x\rangle}$), tedy i metrickým prostorem ($d(x, y) = \|x - y\|$) a tedy i topologickým prostorem.

- L_1 norma na $\mathbb{R}^n$:

$$\|x\| = \sum_{i=1}^{n} |x_i|$$

- L_2 norma na $\mathbb{C}^n$ - Euklidovská norma:

$$\|x\| = \sqrt{\sum_{i=1}^{n} x_i \overline{x_i}}$$

- L_p norma na $\mathbb{R}^n$:

$$\|x\| = \sqrt[p]{\sum_{i=1}^{n} |x_i|^p}$$

- L_∞ norma (stejně jako L_1 norma neodpovídá žádnému skalárnímu součinu):

$$\|x\| = \max_{i=1,\ldots,n} (|x_i|)$$

- Norma v prostoru integrovatelných funkcí na intervalu $[a, b]$ - $C[a, b]$

$$\|f(x)\| = \int_a^b f^2(x)dx$$

10.3 Cauchy-Schwarzova nerovnost

Věta *(Cauchyho-Schwarzova nerovnost)*
Nechť V je prostor se skalárním součinem nad $\mathbb{C}$ a $\|x\|$ je norma odvozená ze skalárního součinu. Potom platí:

$$|\langle x, y\rangle| \leq \|x\| \cdot \|y\| \qquad (\forall x, y \in V)$$

Důkaz
Pro $x = 0$ nebo $y = 0$ máme $0 \ \leq 0$.

Pro libovolné $\alpha \in \mathbb{C}$ platí $\|x + \alpha y\|^2 \geq 0$ (platí i bez $()^2$)

$$\begin{aligned} \|x + \alpha y\|^2 &= \langle x + \alpha y, x + \alpha y\rangle = \langle x, x + \alpha y\rangle + \alpha \langle y, x + \alpha y\rangle = \\ &= \langle x, x\rangle + \overline{\alpha} \langle x, y\rangle + \alpha \langle y, x\rangle + \alpha\overline{\alpha} \langle y, y\rangle \end{aligned}$$

Zvolíme $\alpha = \frac{-\langle x,y\rangle}{\langle y,y\rangle}$ *(tím se eliminují $\overline{\alpha} \langle x, y\rangle$ a $\alpha\overline{\alpha} \langle y, y\rangle$)*

Po dosazení:

$$\begin{aligned} 0 &\leq \langle x, x\rangle + \alpha \langle y, x\rangle \\ 0 &\leq \langle x, x\rangle - \frac{\langle x, y\rangle}{\langle y, y\rangle} \langle y, x\rangle \\ \langle x, y\rangle . \langle y, x\rangle &\leq \langle x, x\rangle . \langle y, y\rangle \\ |\langle x, y\rangle|^2 &\leq \|x\|^2 . \|y\|^2 \end{aligned}$$

...a po odmocnění

$$|\langle x, y\rangle| \leq \|x\| . \|y\|$$

Druhý možný důkaz
Nadefinujeme proměnnou $t \in \mathbb{R}$ a zavedeme funkci

$$p(t) := \langle u + t \cdot v, u + t \cdot v \rangle = ||u + tv||^2$$

Víme: $p(t) \geq 0 \, \forall t \in \mathbb{R}$ (z axiomu 1 skal. součinu). Z linearity plyne, že $\langle u + tv, u + tv \rangle = \langle u, u + tv \rangle + t \langle v, u + tv \rangle = \langle u, u \rangle + t \langle u, v \rangle + t \langle v, u \rangle + t^2 \langle v, v \rangle = ||u||^2 + 2t \langle u, v \rangle + t^2 ||v||^2$. Tj. dostáváme $p(t)$ jako kvadratickou funkci proměnné t:

$$p(t) = t^2 ||v||^2 + 2t \langle u, v \rangle + ||u||^2$$

Protože $p(t)$ má nezáporné hodnoty na celém $\mathbb{R}$, musí mít tato rovnice max. jedno řešení, tj. diskriminant při počítání kořenů nesmí být kladný:

$$D = b^2 - 4ac = 4 \langle u, v \rangle^2 - 4||u||^2||v||^2 \leq 0$$

Po vydělení čtyřmi a odmocnění dostáváme:

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

Důsledek
Platnost trojúhelníkové nerovnosti pro normy odvozené od skalárního součinu – tj. normy odvozené od skalárního součinu splňují všechny axiomy normy.

Důsledek
Nechť $x = (x_1, x_2, \ldots, x_n)^T$, $y = (1, 1, \ldots, 1)^T$ jsou dva vektory, pak pro standardní skalární součin platí

$$\begin{aligned} | \langle x, y \rangle | &= \sum_{i=1}^{n} x_i \cdot 1 \\ \|x\| &= \sqrt{\sum_{i=1}^{n} x_i^2} \\ \|y\| &= \sqrt{n} \end{aligned}$$

po dosazení do Cauchy-Schwarzovy nerovnosti okamžitě dostaneme nerovnost mezi aritmetickým a kvadratickým průměrem

$$\frac{1}{n} \sum_{i=1}^{n} x_i \leq \sqrt{\frac{1}{n} \sum_{i=1}^{n} x_i^2}$$

Důsledek
Ve vektorových prostorech nad $\mathbb{R}$ a $\mathbb{C}$ lze definovat *úhel*, svíraný dvěma vektory:

$$\cos \varphi = \frac{\langle u, v \rangle}{\|u\| \; \|v\|}$$

a Cauchyho-Schwarzova nerovnost zaručuje, že $|\cos \varphi| \leq 1$.

Důsledek
Z takto definovaného úhlu mezi dvěma vektory plyne i *kosinová věta*:

$$\|u - v\|^2 = \|u\|^2 + \|v\|^2 - 2\|u\| \, \|v\| \cos \varphi$$

10.4 Kolmost

Definice *(kolmé vektory)*
Vektory x a y z prostoru se skalárním součinem jsou vzájemně *kolmé* (*ortogonální*), pokud $\langle x, y \rangle = 0$, značíme $x \perp y$.

Definice *(ortogonální a ortonormální systém)*
Soustava (systém) vektorů $v_1, \dots, v_n$ se nazývá *ortogonální*, jestliže $\langle v_i, v_j \rangle = 0$ ($v_i \perp v_j$) pro $\forall i \neq j$ (tj. všechny její vektory jsou navzájem kolmé).
Platí-li ještě navíc $\|v_i\| = 1$ pro $\forall i = 1, \dots, n$, jedná se o soustavu *ortonormální* (vektory jsou kolmé a navíc mají jednotkovou normu).

Pozorování
Každý systém nenulových vzájemně kolmých vektorů (tj. i ortonormální nebo ortogonální) je lineárně nezávislý.

Důsledek
Jestliže ortogonální systém generuje celý vektorový prostor, je jeho bází.

Algoritmus *(Gram-Schmidtova ortogonalizace)*
Tento algoritmus zajišťuje převedení libovolné báze $(v_1, \dots, v_n)$ vektorového prostoru V na ekvivalentní ortogonální bázi $(w_1, \dots, w_n)$. Ortonormalizace báze už po jeho proběhnutí znamená jen vynásobení každého w_i číslem $\frac{1}{\|w_i\|}$. Jeho průběh:

1. Zvolme $w_1 := v_1$.
2. Pro i postupně od 1 do n opakujme:
   Najdi $w_i = v_i - a_{i,1}w_1 - a_{i,2}w_2 - \cdots - a_{i,i-1}w_{i-1}$ tak, aby pro $\forall j \in \{1, \dots, i\}$ platilo:
   $$w_i \perp w_j$$
   Dá se ukázat že koeficienty $a_{i,j}$ jsou tvaru
   $$a_{i,j} = \frac{\langle v_i, w_j \rangle}{\|w_j\|^2}$$
3. Po n iteracích dostaneme $w_1, \dots, w_n$ jako ortogonální bázi prostoru V.

Alternativní postup - Gram-Schmidtova normalizace:

1. Dány: $x_1, \dots, x_m \in V$ lineárně nezávislé.

2. Pro $k = 1, \ldots, m$ proveď:

$$y_k := x_k - \sum_{j=1}^{k-1} \langle x_k, z_j \rangle \, z_j$$

$$z_k := \frac{1}{\|y_k\|} y_k$$

3. Ukonči: $z_1, \ldots, z_m$ je ortonormální systém ve V a $\mathcal{L}(z_1, \ldots, z_m) = \mathcal{L}(x_1, \ldots, x_m)$

Důsledek
Buď $(v_1, \ldots, v_n)$ báze vekt. prostoru se skal. součinem. Potom existuje ortonormální báze $(w_1, \ldots, w_n)$, kdy pro každé $k \in \{1, \ldots, n\}$ je $\mathcal{L}(v_1, \ldots, v_k) = \mathcal{L}(w_1, \ldots, w_k)$. Díky tomu se každý ortogonální systém vektorů v konečnědimensionálním vekt. prostoru se skalárním součinem dá rozšířit na ortogonální bázi (to můžeme díky Gram-Schmidtově ortogonalizaci a Steinitzově větě o výměně).

Věta *(Fourierovy koeficienty)*
Máme-li danou nějakou ortonormální bázi $B = b_1, \ldots, b_n$ vektorového prostoru V, pak pro každé $x \in V$ platí:

$$x = \sum_{i=1}^{n} \langle x, b_i \rangle \, b_i$$

a souřadnice $\langle x, b_i \rangle$ nazveme *Fourierovy koeficienty* vektoru x.

Poznámka
Fourierovy řady jsou souřadnice funkcí ve vektorovém prostoru spojitých funkcí na $[-\pi, \pi]$ se skalárním součinem $\langle f, g \rangle = \int_{-\pi}^{\pi} f(x)g(x)\mathrm{d}x$

10.5 Ortogonální doplněk a jeho vlastnosti

Definice
Nechť V je množina vektorů ve vektorovém prostoru W se skalárním součinem. *Ortogonálním doplňkem* V (značíme $V^\perp$) rozumíme množinu

$$V^\perp = \{v \in W; \forall x \in V : \langle v, x \rangle = 0\}$$

Lemma *(Vlastnosti)*
Nechť V je podprostor prostoru W konečné dimenze. Potom platí:

1. $V^\perp$ je podprostor W
2. $\dim(V^\perp) = \dim(W) - \dim(V)$
3. $(V^\perp)^\perp = V$ *(z rozšiřitelnosti ortogonální báze)*
4. $V \cap V^\perp = \{0\}, \quad V \oplus V^\perp = W$
   (operace $\oplus$ je spojení dvou podprostorů…$\mathcal{L}(V \cup V^\perp)$)

5. U, V podprostory W. Je-li $U \subseteq V$, pak $U^\perp \supseteq V^\perp$
   $(x \in V^\perp \Leftrightarrow x \perp y \in V \Rightarrow x \perp u \in U \Leftrightarrow x \in U^\perp)$
6. $(U \cap V)^\perp = U^\perp \oplus V^\perp$
7. $(U \oplus V)^\perp = U^\perp \cap V^\perp$

Definice *(Ortogonální projekce)*
Ortogonální projekce vekt. prostoru V na podprostor $U \subset V$ je zobrazení, které každému vektoru $v \in V$ přiřadí vektor $u \in U$ tak, že

$$\|v - u\| = \min\{\|v - w\|, w \in U\}$$

tedy vektor $u \in U$, který má ze všech vektorů z U nejmenší vzdálenost od v. Ten se pak nazývá *ortogonální projekcí* vektoru v.

11 Řešení soustav lineárních rovnic

Požadavky

- Lineární množiny ve vektorovém prostoru, jejich geometrická interpretace
- Řešení soustavy rovnic je lineární množina
- Frobeniova věta
- Řešení soustavy úpravou matice
- Souvislost soustavy řešení s ortogonálním doplňkem

Pojem „lineární množina“ moc používaný není, proto se držím výrazu „afinní podprostor“. Vypracováno s použitím poznámek a syllabu z lineární algebry Prof. Matouška a textu Doc. M. Čadka z MU Brno k lineární algebře (`ftp://ftp.math.muni.cz/pub/math/people/Cadek/lectures/linearni_algebra/LA2.pdf`)

11.1 Lineární množiny ve vektorovém prostoru

Definice *(lineární množina / afinní podprostor)*
Podmnožina vektorového prostoru V, která je buď prázdná, nebo tvaru

$$\mathbf{x} + U = \{\mathbf{x} + \mathbf{u} | \mathbf{u} \in U\}$$

kde $\mathbf{x} \in V$ a $U \subset V$ je nějaký podprostor V, se nazývá *afinní podprostor*, *lineární množina* nebo *lineál.*

Poznámka *(Nejednoznačnost určení afinního podprostoru)*
Jeden afinní podprostor je možné určit více způsoby, např. pro vektorový prostor V s vektorem $\mathbf{v}$ a jeho podprostorem U dávají $\mathbf{v} + U$ a $2\mathbf{v} + U$ stejný afinní podprostor.

Věta *(Afinní podprostor určuje vekt. prostor)*
Mějme nějaký afinní podprostor F ve vektorovém prostoru V. Je-li dáno:

$$F = U + \mathbf{x}$$
$$F = U' + \mathbf{x}'$$

pak jistě $U = U'$.
Důkaz
Označíme $\tilde{U} = \{\mathbf{y} - \mathbf{z} | y, z \in F\}$ a dokážeme, že $\tilde{U} = U$ i $\tilde{U} = U'$.

Věta *(Lin. zobrazení určuje afinní podprostor)*
Budiž dáno lineární zobrazení $f : U \to V$ mezi nějakými dvěma vekt. prostory. Pro libovolné $b \in f[U]$ potom platí:

$$f^{-1}(\mathbf{b}) = \{\mathbf{u} \in U | f(\mathbf{u}) = \mathbf{b}\} = \{\mathbf{x}_0 + \text{Ker } f\}$$

kde x_0 je libovolný vektor z množiny $f^{-1}(\mathbf{b})$ a Ker f je jádro zobrazení f (tj. Ker $f = f^{-1}(\mathbf{0})$).

Důkaz
Plyne z faktu, že Ker f je vektorový podprostor U a z linearity f.

11.2 Geometrická interpretace

Definice *(dimenze afinního podprostoru, nadroviny)*
Dimenzi afinního podprostoru $\mathbf{x}+U$, kde $U \subseteq V$ je vektorový podprostor nějakého vekt. prostoru V, definujeme jako $\dim(U)$.

Jednodimensionání afinní podprostor se nazývá *přímka*, dvoudimensionální *rovina*, $n-1$-dimensionální afinní podprostor n-dimensionálního prostoru se jmenuje *nadrovina.*

Poznámka
Totéž platí pro afinní podprostory v $n-$rozměrném eukleidovském geometrickém prostoru – takže např. roviny nebo přímky v trojrozměrném eukleidovském prostoru jsou afinní podprostory.

Definice *(Afinní kombinace bodů)*
$\mathbf{a}, \mathbf{b}$ buďte dva body (vektory) ve vektorovém prostoru V nad tělesem T. Potom pro $\alpha, \beta \in T$ lineární kombinace

$$\alpha\mathbf{a} + \beta\mathbf{b},\ \alpha + \beta = 1_T$$

určující nadrovinu se nazývá *afinní kombinace bodů.* Afinní kombinace několika bodů $\mathbf{a}_1, \ldots, \mathbf{a}_k$ jsou pro $\alpha_i \in T$ body

$$\sum_{i=1}^{k} \alpha_i\mathbf{a}_i,\ \sum_{i=1}^{k} \alpha_i = 1_T$$

Věta *(Geometrické vyjádření afinního podprostoru)*
V afinním podprostoru F nějakého vekt. prostoru V leží s každými k body $\mathbf{f}_1 \ldots \mathbf{f}_k \in F$ i jejich afinní kombinace. Naopak každá množina F ve vekt. prostoru V, v níž pro každé dva body leží i jejich afinní kombinace, je afinní podprostor.
Důkaz
$F = \{U + \mathbf{x}\}$ pro nějaký podprostor $U \subset V$. Potom

$$\forall i \in \{1, \ldots, k\} : \mathbf{f}_i = \mathbf{x} + \mathbf{u}_i$$

pro nějaké $\mathbf{u}_i \in U$. Platí:

$$\sum_{i=1}^{k}(\mathbf{x} + \mathbf{u}_i)\alpha_i = \sum_{i=1}^{k} \alpha_i\mathbf{x} + \sum_{i=1}^{k} \alpha_i\mathbf{u}_i = 1 \cdot \mathbf{x} + \sum_{i=1}^{k} \alpha_i\mathbf{u}_i \in F$$

Opačně zvolme $\mathbf{u} \in F$, potom $F = \mathbf{u} + \{\mathbf{v} - \mathbf{u}, \mathbf{v} \in F\}$ a stačí dokazát, že $U = \{\mathbf{v} - \mathbf{u}, \mathbf{v} \in F\}$ je podprostor V (uzavřenost na skalární násobky a součty).

11.3 Řešení soustavy rovnic je lineární množina

Definice *(Maticový zápis soustavy rovnic)*
Uvažujme soustavu m lineárních rovnic o n neznámých ve tvaru:

$$\begin{array}{ccccccc} a_{1,1}x_1 & +a_{1,2}x_2 & +\dots & +a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 & +a_{2,2}x_2 & +\dots & +a_{2,n}x_n & = & b_2 \\ \vdots & & & \vdots & & \vdots \\ a_{m,1}x_1 & +a_{m,2}x_2 & +\dots & +a_{m,n}x_n & = & b_m \end{array}$$

Takovou soustavu lze zapsat jako

$$A\mathbf{x} = \mathbf{b}$$

kde

- A je *matice soustavy* typu $m \times n$ (s m řádky a n sloupci), kde na souřadnicích $[i, j]$ je koeficient $a_{i,j}$,
- $\mathbf{b}$ je sloupcový vektor pravých stran (matice typu $m \times 1$) a
- $\mathbf{x}$ je sloupcový vektor neznámých (matice typu $n \times 1$)

Maticový součin $A\mathbf{x} = \mathbf{b}$ zřejmě dává stejný výsledek jako explicitní zápis soustavy.

Věta *(Řešení soustavy rovnic je afinní podprostor)*
Pro soustavu lineárních rovnic $A\mathbf{x} = \mathbf{b}$, kde A je matice typu $m \times n$, $\mathbf{b}$ je vektor „pravých stran“ a $\mathbf{x}$ vektor neznámých, platí, že množina jejích řešení je

a) prázdná
b) tvaru $\{\mathbf{x}_0 + L\}$, kde $\mathbf{x}_0$ je jedno z řešení soustavy $A\mathbf{x} = \mathbf{b}$ a L je množina všech řešení *homogenní* soustavy $A\mathbf{x} = 0$.

Důkaz
Je-li F množina řešení rovnic $A\mathbf{x} = \mathbf{b}$ neprázdná, potom platí:

1. řádky matice A generují nějaký podprostor L, $\forall \mathbf{u} \in L : A\mathbf{u} = 0$.
2. jestliže pro nějaké $\mathbf{l}$ platí $A\mathbf{l} = 0$ (tedy $\mathbf{l} \in L$) a mám nějaké $\mathbf{x}_0$, pro které platí $A\mathbf{x}_0 = \mathbf{b}$, potom z distributivity násobení matic plyne $A(\mathbf{x}_0 + \mathbf{l}) = \mathbf{b}$.

Věta *(Afinní podprostor lze popsat soustavou rovnic)*
Opačné tvrzení platí také – každý afinní podprostor lze popsat soustavou lineárních rovnic.
Důkaz
Ve vekt. prostoru V mějme afinní podprostor $F = \{U + \mathbf{v}\}$, kde $U \subseteq V$ je podprostor V a $\mathbf{x} \in V$. $\mathbf{u}_1, \dots, \mathbf{u}_k$ buď báze U. Potom každé $\mathbf{x} \in F$ vyhovuje soustavě rovnic

$$\begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_k \end{pmatrix} \mathbf{x} = \mathbf{v}$$

Důsledek
Je-li dána soustava rovnic $A\mathbf{x} = \mathbf{b}$, kde matice A má n řádků, potom jí určený afinní podprostor má dimenzi $n - \text{rank}(A)$.

Věta *((neprázdný) průnik afinních podprostorů je afinní podprostor)*
Mějme dány afinní podprostory $F_1 = \{U_1 + \mathbf{x}_1\}$ a $F_2 = \{U_2 + \mathbf{x}_2\}$ pro nějaké podprostory U_1, U_2 vektorového prostoru V. Pokud $F_1 \cap F_2 \neq \emptyset$, potom $F_1 \cap F_2$ je afinní podprostor V.
Důkaz
Plyne z předchozích vět o vztahu afinních podprostorů a soustav rovnic – vezmeme rovnicové popisy F_1 a F_2 a složíme je pod sebe, tím dostaneme rovnicový popis dalšího afinního podprostoru (pokud daná soustava rovnic má řešení, tedy průnik je neprázdný).

Příklad
Např. průnik přímky a roviny v $\mathbb{R}^3$ – jeden bod – je afinní podprostor :-).

11.4 Frobeniova věta

Věta *(Frobeniova)*
Soustava lineárních rovnic $A\mathbf{x} = \mathbf{b}$ (kde A je matice s n sloupci) má alespoň jedno řešení, právě když platí
$$\text{rank}(A) = \text{rank}((A\ \mathbf{b}))$$
kde $(A\ \mathbf{b})$ představuje tzv. *rozšířenou matici soustavy*, tj. matici A s „přilepeným" vektorem pravých stran $\mathbf{b}$ v posledním sloupci.
Důkaz
n-tice skalárů $\alpha_1, \ldots, \alpha_n$ je řešením soustavy $A\mathbf{x} = \mathbf{b}$, jinak zapsáno $A_1\alpha_1 + \cdots + A_n\alpha_n = \mathbf{b}$, právě když sloupec $\mathbf{b}$ je lineární kombinací sloupců $A_i, i \in \{1, \ldots, n\}$, tedy $\mathbf{b} \in \mathcal{L}(A_1, \ldots, A_n)$. To znamená, že $\mathcal{L}(A_1, \ldots, A_n, \mathbf{b}) = \mathcal{L}(A_1, \ldots, A_n)$ a tedy
$$\text{rank}(A) = \dim(\mathcal{L}(A_1, \ldots, A_n)) = \dim(\mathcal{L}(A_1, \ldots, A_n, \mathbf{b})) = \text{rank}((A\ \mathbf{b}))$$

11.5 Řešení soustavy úpravou matice

Definice *(Elementární operace)*
Následující tři operace nazýváme *elementárními operacemi* s maticí A (všechny jsou ekvivalentní vynásobení vhodnou regulární maticí zleva):

1. vynásobení i-tého řádku číslem $\alpha \neq 0$
(zapsáno formou maticového násobení $A' = (I + (\alpha - 1)e_i e_i^T)A$)
2. vynásobení i-tého řádku číslem α a přičtení k j-tému řádku, $j \neq i$
(maticový zápis $A' = (I + \alpha e_j e_i^T)A$)
3. výměna i-tého a j-tého řádku, $i \neq j$ (je možné „složit" z předcházejících dvou)
(maticový zápis $A' = (I + (e_i - e_j)(e_j - e_i)^T)A$)

Věta *(O elementárních operacích)*
Elementární operace na rozšířené matici $(A\ \mathbf{b})$ soustavy rovnic $A\mathbf{x} = \mathbf{b}$ nemění množinu řešení soustavy.

Důkaz
Důkaz stačí pro operace 1. a 2., protože třetí je jejich kombinací. Pro úpravy:

1. Po úpravě jsou všechny rovnice (řádky matice) až na i-tou nezměněné, tedy každé $\mathbf{x}$ řešení původní soustavy je splňuje. Pro upravený řádek platí

$$\alpha(a_{i,1}x_1 + \cdots + a_{i,n}x_n) = \alpha \cdot b_i$$

   což je zřejmě také splněno. Podobně se dokáže, že každé $\mathbf{x}$ řešení upravené matice splňuje i všechny rovnice původní.
2. Všechny řádky až na j-tý jsou nezměněné a pro j-tý řádek platí:

$$\alpha(a_{i,1}x_1 + \cdots + a_{i,n}x_n) + (a_{j,1}x_1 + \cdots + a_{j,n}x_n) = \alpha b_i + b_j$$

   a to je také splněno. Opačná implikace se dokáže podobně.

Definice *(Odstupňovaný tvar matice)*
Řekneme, že matice A typu $m \times n$ je v (řádkově) *odstupňovaném tvaru*, jestliže jsou splněny následující podmínky:

1. existuje $r : 0 \leq r \leq m$ takové, že řádky $1, \ldots, r$ jsou nenulové a $r + 1, \ldots, m$ nulové
2. pro $j(i) = \min\{j | a_{i,j} \neq 0\}$ platí $j(1) \leq j(2) \leq \cdots \leq j(r)$

Algoritmus *(Řešení soustavy lin. rovnic)*
Soustavu lineárních rovnic $A\mathbf{x} = \mathbf{b}$ lze řešit následovně

1. Sestavit rozšířenou matici soustavy
2. Převést pomocí elementárních úprav matici do odstupňovaného tvaru
3. Pomocí zpětné substituce popsat všechna řešení

Algoritmus *(Gaussova eliminace)*
Gaussova eliminace je algoritmus pro úpravu dané matice A na odstupňovaný tvar elementárními řádkovými úpravami. Postup:

1. Utřídíme řádky podle délek úseků počátečních nul vzestupně
2. Najdeme-li dva řádky se stejně dlouhým úsekem poč. nul $(j(i) = j(i + 1))$, potom k $i + 1$-tému řádku přičteme $-\frac{a_{i+1,j(i)}}{a_{i,j(i)}}$-násobek i-tého řádku
3. Kroky 1. – 2. opakujeme, dokud existují dva řádky se stejně dlouhým úsekem poč. nul.

Je zaručeno, že algoritmus skončí, protože s každým cyklem roste součet délek počátečních úseků nul všech řádků minimálně o 1 a ten je omezený číslem $m \times n$. Složitost algoritmu je $O(m \cdot n^2)$.

Algoritmus *(Zpětná substituce)*
Buď E rozšířená matice soustavy $A\mathbf{x} = \mathbf{b}$ v odstupňovaném tvaru (získaná pomocí elementárních úprav). Pokud počáteční úsek nul na nějakém řádku má délku n (tedy nenulové číslo je jen ve sloupci pravých stran), soustava nemá řešení. Jinak nazveme *bázové proměnné* ty, v jejichž sloupci je v nějakém řádku první nenulové číslo $(x_{j(1)}, \ldots, x_{j(m)})$, ostatní nazveme *volné*. Existuje potom jednoznačné přiřazení hodnot bázovým proměnným tak, že dohromady tvoří řešení soustavy. Každé řešení je navíc možné získat touto metodou.

Postup:
Indukcí podle $i = r, r-1, \ldots, 2, 1$. Nechť $x_{j(i)}$ je i-tá bázová proměnná a hodnoty proměnných x_k pro $k > j(i)$ jsou dané (buď jsou volné, nebo využívám ind. předpoklad). Potom po dosazení do i-té rovnice získám

$$0x_1 + \cdots + 0x_{j(i)-1} + a_{i,j(i)}x_{j(i)} + \cdots + a_{i,j(n)}x_n = b_i$$

tedy jednu rovnici o 1 neznámé, která má jednoznačné řešení. Libovolné řešení této soustavy $x_1, \ldots, x_n$ lze získat touto metodou – stačí nastavit volné proměnné podle něj a bázové vyjdou správně, protože jejich hodnota je určena jednoznačně. Navíc které proměnné jsou volné a které jsou bázové je také určeno jednoznačně – jinak vždy najdu různé množiny řešení (což je pro stejnou soustavu rovnic nesmysl).

Algoritmus *(Gauss-Jordanova eliminace)*
Gauss-Jordanova eliminace je varianta Gaussovy eliminace, která převádí matici na tzv. *redukovaný odstupňovaný tvar*, to je takový tvar, kde v každém sloupci, příslušejícím nějaké bázové proměnné, je pouze jedno nenulové číslo. Zpětná substituce je pak jednodušší, ale je třeba více aritmetických operací (asymptoticky jsou však algoritmy stejné)
TODO: zkontrolovat & doplnit podrobněji

Poznámka
S řešením soustav rovnic Gaussovou metodou nastává problem při strojových výpočtech – i malá zaokrouhlovací chyba může způsobit velmi radikální změnu množiny řešení (takové matice soustav se nazývají *špatně podmíněné*).

11.6 Souvislost soustavy řešení s ortogonálním doplňkem

Definice *(Ortogonální doplněk)*
Ve vektorovém prostoru V se skaláním součinem definujeme *ortogonální doplněk* množiny $M \subseteq V$ jako

$$M^{\perp} = \{\mathbf{v} \in V : \langle \mathbf{v}, \mathbf{x} \rangle = 0 \ \forall \mathbf{x} \in M\}$$

Věta *(Množina řešení homogenní soustavy je ortog. doplněk řádků její matice)* Mějme dánu homogenní soustavu lineárních rovnic $A\mathbf{x} = \mathbf{0}$ potom její množina řešení je ortogonální doplněk množiny jejích řádků

$$\{\mathbf{x}|A\mathbf{x} = \mathbf{0}\} = \{A_1, A_2, \dots, A_n\}^{\perp}$$

přičemž uvažujeme standardní skalární součin $\langle \mathbf{x}, \mathbf{y} \rangle = x_1y_1 + \cdots + x_ny_n$.

TODO: tady je toho dost málo (ač je to všechno co jsme kdy probírali), ještě něco sem doplnit ???

12 Matice

Požadavky

- Matice a jejich hodnost
- Operace s maticemi a jejich vlastnosti
- Inversní matice
- Regulární matice, různé charakteristiky
- Matice a lineární zobrazení, resp. změny souřadných soustav

12.1 Matice a jejich hodnost

Definice

Obdélníkové schéma sestavené z reálných čísel

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

nazýváme (reálnou) maticí typu $m \times n$. Prvek a_{ij} se nazývá ij-tý *koeficient* matice A. Množinu všech reálných matic typu $m \times n$ značíme $\mathbb{R}^{m \times n}$. Je-li $m = n$, říkáme, že matice je čtvercová řádu n.

Podobně definujeme množinu komplexních matic typu $m \times n$ a značíme ji $\mathbb{C}^{m \times n}$, lze takto definovat množinu matic nad libovolným tělesem.

Definice *(Jednotková matice)*

Čtvercová matice řádu n tvaru

$$I = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

se nazývá *jednotková matice*.

Definice *(Nulová matice)*

Čtvercovou matici A typu $m \times n$, pro kterou $a_{i,j} = 0 \; \forall i \in \{1, \dots, m\}, \forall j \in \{1, \dots, n\}$ nazveme *nulová matice* a označíme $\mathbf{0}$.

Definice *(Prostory související s maticí)*

Buď A matice typu $m \times n$ nad tělesem $\mathbb{K}$. Potom jsou s ní spojené tyto vektorové prostory:

- *sloupcový prostor, též sloupcový modul* – podprostor $\mathbb{K}^m$ generovaný sloupci A
- *řádkový prostor, též řádkový modul* – podprostor $\mathbb{K}^n$ generovaný řádky A

- *jádro matice* (Ker A) – podprostor $\mathbb{K}^n$ generovaný všemi řešeními soustavy $Ax = 0$

Je zřejmé, že elementární maticové úpravy nemění ani řádkový prostor, ani jádro.

Definice *(Hodnost matice)*
Hodnost matice A je maximální počet lineárně nezávislých sloupců matice A (jako vektorů), značíme ji rank(A). Hodnost matice je rovna dimenzi sloupcového prostoru (to je ekvivalentní definice).

Věta *(O hodnosti matice)*
Pro libovolnou matici A typu $m \times n$ je dimenze jejího sloupcového prostoru rovna dimenzi řádkového prostoru. Tedy hodnost matice je rovna i dimenzi řádkového prostoru a platí

$$\text{rank}(A) \leq \min\{m, n\}$$

Důkaz
Pro horní trojúhelníkové matice je tato skutečnost zřejmá, dokazuje se, že Gaussova eliminace (tj. elementární maticové úpravy – násobení vhodnou regulární maticí zleva) nemění hodnost sloupcového prostoru (při operacích s řádky).

Věta *(O dimenzích maticových prostorů)*
Pro matici A s n sloupci platí:

$$\dim(\text{Ker } A) + \text{rank}(A) = n$$

Poznámka
Po provedení *Gaussovy eliminace* na matici A ($\Rightarrow A^R$) je hodnost matice A rovna počtu nenulových řádků matice A^R.

Definice *(Regulární matice)*
Čtvercová matice A se nazývá *regulární*, jestliže soustava

$$Ax = 0$$

má jediné řešení $x = 0$ (tzv. *triviální*).

V opačném případě se nazývá *singulární* (tj. platí $Ax = 0$ pro nějaký vektor $x \neq 0$).

12.2 Operace s maticemi a jejich vlastnosti

Součet a násobení skalárem

Definice *(Sčítání)*
Nechť A, B jsou matice typu $m \times n$. Potom jejich *součtem* $A+B$ nazýváme matici typu $m \times n$ s koeficienty

$$(A+B)_{ij} = A_{ij} + B_{ij}$$

pro $i = 1, \dots, m; j = 1, \dots, n$. Jsou-li A, B různých typů, potom součet $A + B$ není definován.

Definice *(Násobení skalárem)*
Nechť A, B jsou matice typu $m \times n$ a α skalár. Potom $\alpha \cdot A$ je matice typu $m \times n$ s koeficienty

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

pro $i = 1, \dots, m; j = 1, \dots, n$. Nikdy nepíšeme $A \cdot \alpha$.

Lemma *(Vlastnosti součtu matic a násobení matic skalárem)*
Nechť A, B, C jsou matice typu $m \times n$ a α, β skaláry. Potom platí:

1. $A + B = B + A$ *(komutativita)*
2. $(A + B) + C = A + (B + C)$ *(asociativita)*
3. $A + \mathbf{0} = A$ *(existence nulového prvku)*
4. $A + (-1)A = \mathbf{0}$ *(existence opačného prvku)*
5. $\alpha(\beta A) = (\alpha\beta)A$
6. $1 \cdot A = A$
7. $\alpha(A + B) = \alpha A + \alpha B$ *(distributivita)*
8. $(\alpha + \beta)A = \alpha A + \beta A$ *(distributivita)*

Tedy prostor matic typu $m \times n$ odpovídá vektorovému prostoru.

Násobení

Definice *(Maticové násobení)*
Je-li A matice typu $m \times p$ a B matice typu $p \times n$, potom $A \cdot B$ je matice typu $m \times n$ definaná předpisem

$$(A \cdot B)_{ij} = \sum_{k=1}^{p} A_{ik} B_{kj}$$

pro $i = 1, \dots, m; j = 1, \dots, n$.

Lemma *(Vlastnosti součinu matic)*
Nechť A, B, C jsou matice, α skalár. Potom

1. Jestliže součin $(AB)C$ je definován, potom i součin $A(BC)$ je definován a platí $(AB)C = A(BC)$.
2. Jestliže $A(B + C)$ je definován, potom i $AB + AC$ je definován a platí $A(B + C) = AB + AC$.

3. Jestliže $(A+B)C$ je definován, potom i $AC+BC$ je definován a platí $(A+B)C = AC+BC$.
4. Je-li AB definován, je $\alpha(AB) = (\alpha A)B = A(\alpha B)$
5. Je-li A typu $m \times n$, potom $I_m A = A I_n = A$.

Násobení matic není komutativní - tj. obecně neplatí $AB = BA$.

Věta *(O hodnosti součinu matic)*
Pro matici A typu $m \times p$ a matici B typu $p \times n$ platí:

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

Důkaz
Řádkový prostor AB je určitě podprostorem řádkového prostoru matice B a sloupcový prostor AB podprostorem sloupcového prostoru matice A.

Transpozice

Definice
Pro matici $A \in \mathbb{R}^{m \times n}$ definujeme *transponovanou matici* $A^T \in \mathbb{R}^{n \times m}$ předpisem

$$(A^T)_{ji} = A_{ij} \, (i = 1, \ldots, m; j = 1, \ldots, n)$$

Lemma *(Vlastnosti transpozice)*

1. $(A^T)^T = A$
2. jsou-li A, B stejného typu, je $(A+B)^T = A^T + B^T$
3. $(\alpha A)^T = \alpha A^T$, pro každé $\alpha \in \mathbb{R}$
4. je-li AB definován, je i $B^T A^T$ definován a platí $(AB)^T = B^T A^T$.

Definice *(Symetrická matice)*
Matice A se nazývá *symetrická* jestliže $A^T = A$.

Věta
Pro každou matici $A \in \mathbb{R}^{m \times n}$ je $A^T A$ symetrická.

Věta
Pro každou matici $A \in \mathbb{R}^{m \times n}$ platí $\operatorname{rank}(A^T) = \operatorname{rank}(A)$.

12.3 Inversní matice

Věta

Ke každé regulární matici $A \in \mathbb{R}^{n\times n}$ existuje právě jedna matice $A^{-1} \in \mathbb{R}^{n\times n}$ s vlastností

$$AA^{-1} = A^{-1}A = I$$

Naopak, existuje-li k $A \in \mathbb{R}^{n\times n}$ matice A^{-1} s touto vlastností, potom je A regulární.

Definice

Matici A^{-1} s touto vlastností nazýváme *inversní maticí* k matici A.

Poznámka

Inverzní matici mají tedy právě regulární matice.

Důsledek

Je-li A regulární, je i A^{-1} regulární.

Věta *(Inversní matice je oboustranně inversní)*

Jestliže pro $A, X \in \mathbb{R}^{n\times n}$ platí $XA = I$, potom A je regulární a $X = A^{-1}$. Analogicky, jestliže $AX = I$, potom A je regulární a $X = A^{-1}$.

Věta

Je-li $A \in \mathbb{R}^{n\times n}$ regulární, potom pro každé $b \in \mathbb{R}^n$ je jediné řešení soustavy $Ax = b$ dáno vzorcem $x = A^{-1}b$.

Věta *(Výpočet inversní matice)*

Pro čtvercovou matici A řádu n nechť je matice $(A\ I)$ (tj. zřetězení sloupců matice A a jednotkové matice I řádu n) převedena Gauss-Jordanovou eliminací na tvar $(I\ X)$. Potom platí:

$$X = A^{-1}$$

Jestliže Gauss-Jordanova eliminace není proveditelná až do konce, potom A je singulární a nemá inversní matici.

Důkaz

Víme, že Gauss-Jordanova eliminace je vlastně opakované násobení regulárními maticemi zleva. Součin všech těchto matic označme Q. Označme $H_{*,j}$ j-tý sloupec nějaké (obecné) matice. Potom pro $j \in \{1, \dots, n\}$ platí: $(I\ X)_{*,j} = I_{*,j} = Q(A\ I)_{*,j} = (QA)_{*,j}$, tedy $QA = I$, dále platí $(I\ X)_{*,n+j} = X_{*,j} = (QI)_{*,n+j} = Q_{*,j}$, takže $Q = X$ a tedy $AX = I$.

Věta *(Vlastnosti inversní matice)*

Nechť $A, B \in \mathbb{R}^{n\times n}$ jsou regulární matice. Potom platí:

1. $(A^{-1})^{-1} = A$
2. $(A^T)^{-1} = (A^{-1})^T$
3. $(\alpha A)^{-1} = \frac{1}{\alpha}A^{-1}$ *pro* $\alpha \neq 0$
4. $(AB)^{-1} = B^{-1}A^{-1}$

12.4 Regulární matice, různé charakteristiky

Věta *(Násobení regulární maticí a hodnost)*
Pro čtvercovou regulární matici R řádu m a matici A typu $m \times n$ platí:

$$\operatorname{rank}(RA) = \operatorname{rank}(A)$$

Důkaz
Nerovnost „$\leq$“ plyne přímo z věty o hodnosti součinu matic použité pro RA, opačná nerovnost z téže věty, použité na matici $R^{-1} \cdot (RA) = A$.

Věta *(Násobení regulárních matic)*
Jsou-li $A_1, A_2, \ldots, A_q \in \mathbb{R}^{n \times n}$ regulární, $q \geq 1$, potom $A_1 A_2 \ldots A_q$ je regulární.

Důkaz
Plyne přímo z předchozí věty.

Poznámka *(Podmínky regularity)*
Čtvercová $A \in \mathbb{R}^{n \times n}$ je regulární matice, právě když:

- Její řádky jsou lineárně nezávislé
- Její sloupce jsou lineárně nezávislé
- Její hodnost je právě n
- A^T je regulární
- A^{-1} je regulární

Další charakteristiky regulárních matic:

- Matice A je regulární právě když je determinant nenulový.
- Právě když po provedení Gaussovy-Jordanovy eliminace dostaneme jednotkovou matici.
- Právě když lze napsat jako součin matic $E_k \times \cdots \times E_2 \times E_1 \times I_n$, kde I_n je jednotková matice a $E_1 \times E_k$ jsou elementární matice (odpovídají elementárním řádkovým úpravám, které matici A převádí na redukovaný, řádkově odstupňovaný tvar).

12.5 Matice a lineární zobrazení, resp. změny souřadných soustav

Definice
Nechť V, W jsou vektorové prostory nad stejným tělesem (R nebo C). Zobrazení $f : V \to W$ nazýváme *lineárním zobrazením* jestliže

1. $f(x + y) = f(x) + f(y)$ pro každé $x, y \in V$
2. $f(\alpha \cdot x) = \alpha \cdot f(x)$ pro každé $x \in V$ a každý skalár α.

Definice *(Souřadnicový vektor)*

Nechť $\mathbb{B} = (x_1, \ldots, x_n)$ je báze V. Každý vektor $x \in V$ lze potom vyjádřit právě jedním způsobem jako lineární kombinaci vektorů báze $\mathbb{B}$. Potom aritmetický vektor

$$[x]_{\mathbb{B}} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

nazýváme *souřadnicovým vektorem* vektoru x v bázi $\mathbb{B}$ (a $n = \dim V$ a souřadnicový vektor *závisí na výběru báze*).

Definice *(Matice lineárního zobrazení)*

Nechť $\mathbb{B} = \{x_1, \ldots, x_n\}$ je báze vektorového prostoru V, $\mathbb{B}' = \{y_1, \ldots, y_m\}$ je báze vekt. prostrou W a nechť $f : V \to W$ je lineární zobrazení. Potom pro každé $j = 1, \ldots, n$ lze $f(x_j)$ zapsat právě jedním způsobem ve tvaru

$$f(x_j) = \sum_{i=1}^{m} \alpha_{ij} y_j.$$

Matice $A = (\alpha_{ij}) \in \mathbb{R}^{m \times n}$ se nazývá maticí lineárního zobrazení f vzhledem k bázím $\mathbb{B}, \mathbb{B}'$ a značí se

$$[f]_{\mathbb{B}\mathbb{B}'}.$$

Pozorování

$[f]_{\mathbb{B}\mathbb{B}'}$. je matice sestavená ze sloupců

$$([f(x_1)]_{\mathbb{B}'}, \ldots, [f(x_n)]_{\mathbb{B}'}),$$

které jsou souřadnicovými vektory vektorů $f(x_1), \ldots, f(x_n)$ v bázi $\mathbb{B}'$.

Věta

Nechť $\mathbb{B}$ je báze V, $\mathbb{B}'$ je báze W, a nechť $f : V \to W$ je lineární zobrazení. Potom pro každé $x \in V$ platí

$$[f(x)]_{\mathbb{B}'} = [f]_{\mathbb{B}\mathbb{B}'}.[x]_{\mathbb{B}},$$

kde napravo stojí maticový součin.

Věta *(Složené zobrazení a maticový součin)*

Nechť $f : U \to V$, $g : V \to W$ jsou lineární zobrazení a nechť $\mathbb{B}, \mathbb{B}', \mathbb{B}''$ jsou báze U, V, W. Potom platí

$$[g \circ f]_{\mathbb{B}\mathbb{B}''} = [g]_{\mathbb{B}'\mathbb{B}''}[f]_{\mathbb{B}\mathbb{B}'}$$

kde napravo stojí maticový součin.

Věta *(Matice inversního zobrazení)*

Je-li $f : V \to W$ isomorfismus, potom inversní zobrazení $f^{-1} : W \to V$ je rovněž isomorfismus a vzhledem k libovolným bázím $\mathbb{B}, \mathbb{B}'$ prostorů V, W platí:

$$[f^{-1}]_{\mathbb{B}'\mathbb{B}} = [f]^{-1}_{\mathbb{B}\mathbb{B}'}$$

Věta *(Změna souřadnic vektoru při změně báze)*
Nechť jsou dány dvě báze $\mathbb{B}, \mathbb{B}'$ vektorového prostoru V. Potom pro každé $x \in V$ platí:

$$[x]_{\mathbb{B}'} = [\mathrm{id}_V]_{\mathbb{B}\mathbb{B}'}.[x]_{\mathbb{B}}$$

Matice $[\mathrm{id}_V]_{\mathbb{B}\mathbb{B}'}$ se nazývá *maticí přechodu* od báze $\mathbb{B}$ k bázi $\mathbb{B}'$.

Poznámka
Předchozí vzorec vyžaduje znalost hodnot vektorů staré báze $\mathbb{B}$ v nové bází $\mathbb{B}'$. Typická situace ale je, že máme jen starou bázi $\mathbb{B}$ a pomocí ní vyjádříme novou bázi $\mathbb{B}'$. V tom případě můžeme použít vzorec

$$[x]_{\mathbb{B}'} = [\mathrm{id}_V]^{-1}_{\mathbb{B}'\mathbb{B}}[x]_{\mathbb{B}}$$

13 Determinanty

Požadavky

- Definice a základní vlastnosti determinantu
- Úpravy determinantů, výpočet
- Geometrický smysl determinantu
- Minory a inversní matice
- Cramerovo pravidlo.

13.1 Definice a základní vlastnosti determinantu

Neformálně

V lineární algebře je *determinant* zobrazení, které přiřadí každé čtvercové matici A skalár $\det A$.

Determinantem čtvercové matice řádu n nazýváme součet všech součinů n prvků této matice takových, že v žádném z uvedených součinů se nevyskytují dva prvky z téhož řádku ani z téhož sloupce. Každý součin přitom násobíme čísly r a s, kde r představuje znaménko permutace příslušného pořadí prvních indexů a s znaménko permutace příslušného pořadí druhých indexů.

Definice *(permutace, znaménko)*

Permutace je libovolná bijekce $\sigma : X \to X$. Množina *inversí* nějaké permutace σ je $I(\sigma) = \{(i, j) : i < j \ \& \ \sigma(i) > \sigma(j)\}$. Znaménko permutace $\mathrm{sgn}(\sigma)$ se pak definuje jako $\mathrm{sgn}(\sigma) = (-1)^{|I(\sigma)|}$. Nejjednodušší permutace – záměna dvou prvků – se pak nazývá *transpozice.* Ta má vždy znaménko -1 a libovolná permutace je složením nějakých transpozic. Množinu všech permutací na množině $\{1, \ldots, n\}$ značíme S_n.

Poznámka

Pro skládání permutací platí $\mathrm{sgn}(p \circ q) = \mathrm{sgn}(p)\mathrm{sgn}(q)$. Pro inversní permutaci (inversní zobrazení) platí $\mathrm{sgn}(p) = \mathrm{sgn}(p^{-1})$.

Definice *(determinant)*

Nechť $A = (a_{i,j})_{i,j=1}^{n}$ je čtvercová matice řádu n. Determinant je definovaný pomocí *Leibnizova vzorce*:

$$\det A = \sum_{\sigma \in S_n} sgn(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

Poznámka

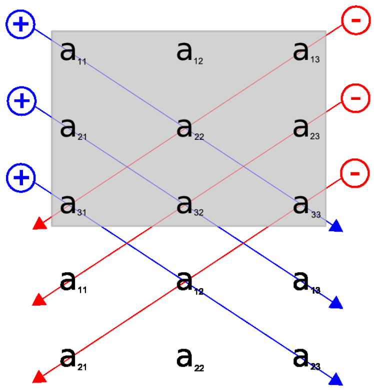
Suma se počítá přes všechny permutace σ čísel $\{1,2,\ldots,n\}$, takže tento vzorec obsahuje $n!$ (faktoriál) sčítanců, což jej s růstem n rychle činí prakticky nepoužitelným pro výpočet. V praxi se proto používají jiné způsoby výpočtu.

Poznámka

Konkrétně, pro matici řádu n, kde:

- $n = 1$: $\det A = a_{1,1}$
- $n = 2$: $\det A = a_{1,1}a_{2,2} - a_{2,1}a_{1,2}$
- $n = 3$: $\det A = a_{1,1}a_{2,2}a_{3,3} + a_{1,3}a_{2,1}a_{3,2} + a_{1,2}a_{2,3}a_{3,1} - a_{1,3}a_{2,2}a_{3,1} - a_{1,1}a_{2,3}a_{3,2} - a_{1,2}a_{2,1}a_{3,3}$

Mnemotechnická pomůcka sloužící k zapamatování postupu výpočtu determinantu třetího řádu se nazývá *Sarrusovo pravidlo*:



Poznámka

Obecný vzorec lze také vyjádřit pomocí Levi-Civitova symbolu $\epsilon_{j_1 j_2 \cdots j_n}$ jako

$$\det A = \sum_{j_1, j_2, \ldots, j_n} \epsilon_{j_1 j_2 \cdots j_n} a_{1,j_1} a_{2,j_2} \ldots a_{n,j_n} = \sum_{j_1, j_2, \ldots, j_n} \epsilon_{j_1 j_2 \cdots j_n} a_{j_1,1} a_{j_2,2} \ldots a_{j_n,n}$$

Vlastnosti determinantu

Věta *(O determinantu transponované matice)*

Pro čtvercovou matici A řádu n platí:

$$\det A = \det A^T$$

Důkaz

Plyne z faktu že $\operatorname{sgn}(p) = \operatorname{sgn}(p^{-1})$:

$$\det(A^T) = \sum_{p \in S_n} \operatorname{sgn}(p) \prod_{i=1}^{n} (A^T)_{i,p(i)} =$$

$$= \sum_{p \in S_n} \operatorname{sgn}(p) \prod_{i=1}^{n} a_{p(i),i} = \sum_{p^{-1} \in S_n} \operatorname{sgn}(p^{-1}) \prod_{i=1}^{n} a_{i,p^{-1}(i)} = \det(A)$$

Věta *(Přerovnání matice)*

Přerovnání řádků nebo sloupců podle permutace p nezmění determinant vůbec, pokud $\operatorname{sgn}(p) = 1$ a změní jen jeho znaménko, pokud $\operatorname{sgn}(p) = -1$.

Důkaz

A buď původní matice a B přerovnaná:

$$\det(B) = \sum_{p \in S_n} \operatorname{sgn}(p) \prod_{i=1}^{n} (B)_{i,p(i)} = \sum_{p \in S_n} \operatorname{sgn}(p) \prod_{i=1}^{n} (A)_{i,q^{-1}(p(i))} =$$

$$= \operatorname{sgn}(q) \sum_{p \in S_n} \operatorname{sgn}(q)\operatorname{sgn}(p) \prod_{i=1}^{n} (A)_{i,q^{-1}(p(i))} = \operatorname{sgn}(q) \sum_{p \in S_n} \operatorname{sgn}(h) \prod_{i=1}^{n} (A)_{i,h(i)} =$$

$$= \operatorname{sgn}(q) \det(A)$$

Důsledek

Má-li matice dva shodné sloupce nebo řádky, má automaticky nulový determinant (přehozením právě těch dvou řádků nebo sloupců vzniknou shodné matice se stejným determinantem, ale má se změnit znaménko).

Věta *(Determinant jako lineární funkce)*

Determinant matice A je lineární funkcí každého jejího řádku i každého sloupce, tj. platí

1.
$$\det \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ b_{i,1} & \dots & b_{i,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix} + \det \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ c_{i,1} & \dots & c_{i,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix} = \det \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ b_{i,1} + c_{i,1} & \dots & b_{i,n} + c_{i,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix}$$

2.
$$\det \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ \kappa a_{i,n} & \dots & \kappa a_{i,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix} = \kappa \det(A)$$

Důkaz

První část plyne z distributivity sčítání vzhledem k násobení – každý člen sumy (produkt prvků) obsahuje jeden prvek typu $b_{i,p(i)} + c_{i,p(i)}$ pro nějakou permutaci a ten je možné rozepsat. Druhá část se dokáže podobně díky komutativitě násobení – prvek κ je také obsažen v každém členu sumy právě jednou, takže je ho možné „vytknout“.

Věta *(Determinant součinu matic)*
Nechť A a B jsou čtvercové matice stejného řádu n nad tělesem T. Potom platí:

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

Důkaz
Je-li jedna z matic singulární, je jejich součin singulární a tedy má nulový determinant; stejně jako je nulový součin determinantů původních matic. Jsou-li obě matice regulární, lze A rozložit na nějaký součin $E_1 \cdot E_2 \cdot \dots \cdot E_k$ elementárních matic. Potom

$$\begin{aligned}\det(AB) &= \det(E_1 E_2 \dots E_k B) = \det(E_1) \cdot \det(E_2 \dots E_k B) \\ &= \det(E_1) \det(E_2) \dots \det(E_k) \det(B) = \det(A) \det(B)\end{aligned}$$

protože víme, jakým způsobem elementární úpravy (ekvivalent elementárních matic ve vzorci) mění determinant.

Důsledek
Čtvercová matice je regulární, právě když má nenulový determinant.

13.2 Úpravy determinantů, výpočet

Gaussova eliminace
Gaussova metoda spočívá v provedení takových úprav matice, které nemění hodnotu determinantu, ale zjednoduší výpočet jeho hodnoty. Cílem prováděných úprav je získat trojúhelníkovou matici $\mathbf{A}$ (kde pro $i > j$ je $a_{i,j} = 0$), neboť pro trojúhelníkové matice platí

$$\det A = a_{1,1} a_{2,2} \dots a_{n,n}$$

tzn. determinant je roven součinu prvků hlavní diagonály matice.
Při úpravách matice pro výpočet determinantu postupujeme podle těchto pravidel:

- Pokud $\mathbf{B}$ vznikne z $\mathbf{A}$ výměnnou dvou řádku nebo sloupců potom $\det B = -\det A$
- Pokud $\mathbf{B}$ vznikne z $\mathbf{A}$ vynásobením řádku nebo sloupce skalárem c, potom $\det B = c. \det A$
- Pokud $\mathbf{B}$ vznikne z $\mathbf{A}$ přičtením násobku jednoho řádku k jinému, nebo přidáním násobku sloupce k jinému sloupci potom $\det B = \det A$

Opakovaným použitím uvedených pravidel převedeme matici na trojúhelníkovou a pro tu poté snadno spočteme determinant.

13.3 Geometrický smysl determinantu

Matice řádu 2

Absolutní hodnotu determinantu matice řádu 2

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

lze interpretovat jako obsah rovnoběžníku s vrcholy v bodech $(0,0)$, (a,c), (b,d) a $(a+b, c+d)$. Znaménko determinantu určuje vzájemnou orientaci vektorů (a,c), (b,d). $\det A$ je kladný, pokud úhel mezi vektory (a,c), (b,d) měřený v kladném směru (tedy proti směru hodinových ručiček) menší než π, a záporný, pokud je tento úhel větší než π.

Matice řádu 3

Podobný geometrický význam jako pro matici řádu 2 najdeme i pro matice $B = (b_{i,j})$ řádu 3. Řádkové vektory

$$b_1 = (b_{1,1}, b_{1,2}, b_{1,3}), b_2 = (b_{2,1}, b_{2,2}, b_{2,3}), b_3 = (b_{3,1}, b_{3,2}, b_{3,3})$$

určují v třídimenzionálním prostoru rovnoběžnostěn, jehož objem je roven $|\det B|$. Pokud je $\det B$ kladný, tak je posloupnost vektorů b_1, b_2, b_3 pravotočivá, a levotočivá, pokud je $\det B$ záporný.

Matice vyšších řádů

I v reálných prostorech vyšších řádů lze determinant chápat jako objem obecného n-rozměrného rovnoběžnostěnu, případně jako pravotočivost, respektive levotočivost posloupnosti $b_1, b_2, \ldots, b_n$.

Definice *(Pravotočivá a levotočivá soustava prostorových kartézských souřadnic)*

Představte si, že v místě, kde stojíte, je počátek prostorové kartézské soustavy. Osa x nechť směřuje přímo vpřed (směrem, kterým se díváte), osa y nechť směřuje vlevo a osa z nechť směřuje vzhůru. Taková soustava se nazývá *pravotočivá souřadná soustava.*

Zaměníme-li osy x a y, získáme *souřadnou soustavu levotočivou.* Obvykle se pracuje s pravotočivou souřadnou soustavou.

Mnemotechnická pomůcka: Soustava souřadnic je pravotočivá pokud při naznačení kladného směru osy z zdviženým palcem pravé ruky naznačují ostatní prsty směr od kladného směru osy x ke kladnému směru osy y.

13.4 Minory a inversní matice

Definice *(Minor)*

Mějme čtvercovou matici A_{ij}, kterou získáme z matice A odstraněním i-tého řádku a j-tého sloupce. Determinant matice A_{ij}, tzn. $\det A_{ij}$ nazýváme *subdeterminantem* (též *minorem*) příslušným k prvku $a_{i,j}$ matice A.

Výpočet determinantu rozvojem podle řádků (sloupců)

Algebraický doplněk lze použít k výpočtu determinantu n-tého řádu. Pro libovolné (pevně dané) i lze determinant matice A vyjádřit pomocí algebraických doplňků jako

$$\det(A) = \sum_{j=1}^{n} a_{i,j} \cdot (-1)^{i+j} \det(A_{ij})$$

Tento postup je označován jako *rozvoj (rozklad) determinantu podle i-tého řádku.* Ekvivalentně lze determinant vyjádřit *rozvojem (rozkladem) podle j-tého sloupce.* Číslo $(-1)^{i+j} \det(A_{ij})$ se někdy nazývá *kofaktorem* nebo *algebraickým doplňkem.*

Definice *(Adjungovaná matice)*

Pro čtvercovou matici A definujeme *adjungovanou matici* adj A předpisem

$$(\text{adj } A)_{i,j} = (-1)^{i+j} \cdot \det(A_{ji})$$

kde A_{ji} jsou minory matice A (s vynechaným j-tým řádkem a i-tým sloupcem – pozor na obrácené pořadí indexů!). Prvky adjungované matice jsou vlastně algebraické doplňky v transponované matici A^T.

Definice *(Inversní matice)*

Pro čtvercovou matici A řádu n definujeme inverzní matici A^{-1} předpisem

$$A.A^{-1} = A^{-1}.A = I_n$$

kde I_n je jednotková matice. Inversní matici lze sestrojit pouze pro regulární matici.

Věta *(Výpočet inversní matice podle minorů)*

Pro každou regulární matici A nad tělesem T platí:

$$A^{-1} = \frac{1}{\det A} \cdot (\text{adj } A)$$

$$A^{-1}_{i,j} = (-1)^{i+j} \frac{\det(A_{ji})}{\det A}$$

Důkaz

Z maticového součinu $A \cdot \text{adj } A$:

1. i-tý řádek $A \times i$-tý sloupec adj A (obs. determinanty minorů odp. i-tému řádku) dá dohromady $\det A$ (z rozvoje determinantu podle řádku)
2. j-tý řádek $A \times i$-tý sloupec adj A dá dohromady 0, protože jde o stejný princip pro matici, kde i-tý řádek je nahrazen j-tým (2 stejné řádky)

Potom $A \cdot \text{adj } A = \det A \cdot I_n$ a to už dává $\frac{1}{\det A}\text{adj } A = A^{-1}$.

13.5 Cramerovo pravidlo

Cramerovo pravidlo je metoda umožňující nalezení řešení soustavy lineárních algebraických rovnic.

Postup

Mějme soustavu lineárních rovnic, která obsahuje stejný počet neznámých jako je počet rovnic. Označme matici soustavy A. Dále označme A_i jako matici, kterou získáme z matice A, nahradíme-li v ní i-tý sloupec sloupcem pravých stran soustavy rovnic.

Pokud zapíšeme matice soustavy a vektor pravých stran jako

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

pak má tvar

$$A_i = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1,i-1} & b_1 & a_{1,i+1} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2,i-1} & b_2 & a_{2,i+1} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{m,i-1} & b_m & a_{m,i+1} & \dots & a_{mn} \end{pmatrix}$$

Pokud je determinant matice soustavy nenulový, $\det A \neq 0$, tzn. matice je regulární, pak má soustava právě jedno řešení, pro které platí

$$x_i = \frac{\det A_i}{\det A}$$

pro $i = 1, 2, \dots, n$.

Důkaz

Pro soustavu $Ax = b$ – rozepíšeme $x = A^{-1}b$, ze vzorce pro inversní matici plyne

$$x = \frac{1}{\det A}(\text{adj } A) \cdot b$$

takže pro x_i vychází

$$x_i = \frac{1}{\det A}((\text{adj } A)b)_i = \frac{1}{\det A} \cdot \sum_{j=1}^{n} (\text{adj } A)_{i,j} \cdot b_j = \frac{1}{\det A} \cdot \det A_i$$

Příklad

Úkolem je řešit soustavu rovnic

$$x + y = 3$$

$$x - 2y = 1$$

Determinant matice soustavy je

$$\det A = \begin{vmatrix} 1 & 1 \\ 1 & -2 \end{vmatrix} = -3$$

Poněvadž je $\det A \neq 0$, lze použít Cramerovo pravidlo.
Dále určíme

$$\det A_1 = \begin{vmatrix} 3 & 1 \\ 1 & -2 \end{vmatrix} = -7$$

$$\det A_2 = \begin{vmatrix} 1 & 3 \\ 1 & 1 \end{vmatrix} = -2$$

Řešení má tedy tvar

$$x = \frac{\det A_1}{\det A} = \frac{-7}{-3} = \frac{7}{3}$$

$$y = \frac{\det A_2}{\det A} = \frac{-2}{-3} = \frac{2}{3}$$

Zkouškou se přesvědčíme, že se skutečně jedná o řešení uvedené soustavy.

14 Vlastní čísla a vlastní hodnoty

Požadavky

- Vlastní čísla a vlastní hodnoty lineárního operátoru resp. čtvercové matice.
- Jejich výpočet.
- Základní vlastnosti.
- Uvedení matice na diagonální tvar.
- Informace o Jordanově tvaru v obecném případě.

Otázka vychází především ze skript pana Jiřího Tůmy a částečně i ze skript pana Jiřího Rohna.

14.1 Definice

Definice

Nechť **A** je čtvercová matice řádu n s reálnými (komplexními) prvky. Jestliže platí

$$Ax = \lambda x \tag{3}$$

pro jisté $\lambda \in \mathbb{C}$ a pro *nenulový vektor* $x \in \mathbb{R}^{n\times 1}$ $(\mathbb{C}^{n\times 1})$. Pak λ nazveme *vlastním číslem* matice **A** a vektor x *vlastním vektorem* příslušným k tomuto vlastnímu číslu.

Množinu všech vlastních čísel matice **A** nazýváme *spektrum* matice **A** a označujeme ji $\sigma(\mathbf{A})$.

Funkci $p(\lambda) = \det(\mathbf{A} - \lambda\mathbf{I}_n)$ nazveme *charakteristický polynom* matice **A**.

Pozorování

Z definice přímo plyne:

$$\lambda \in \sigma(\mathbf{A}) \Leftrightarrow \quad \textit{matice} \quad \mathbf{A} - \lambda\mathbf{I}_n \quad \textit{je} \quad \textit{singulární} \quad \Leftrightarrow \det(\mathbf{A} - \lambda\mathbf{I}_n) = 0$$

Poslední podmínka nám říká, jak najít vlastní čísla matice, pokud existují. Vlastní vektory vypočteme úpravou (3) na:

$$(\mathbf{A} - \lambda\mathbf{I}_n)x = 0$$

Definice

Je-li $F : \mathbf{V} \to \mathbf{V}$ lineární operátor na reálném (komplexním) vektorovém prostoru **V**, pak skalár λ nazýváme *vlastní číslo* lineárního operátoru **V**, pokud existuje nenulový vektor $x \in \mathbf{V}$, pro který platí $F(x) = \lambda x$. Je-li λ vlastní číslo operátoru F, pak každý vektor $x \in \mathbf{V}$, pro který platí $F(x) = \lambda x$, nazýváme *vlastní vektor* lineárního operátoru F příslušný vlastnímu číslu λ. Množinu všech vlastních čísel operátoru F označujeme $\sigma(F)$ a nazýváme *spektrum* operátoru F.

Definice *(podobné matice, diagonalizovatelnost)*

Řekneme, že matice $\mathbf{A}$ a $\mathbf{B}$ jsou *podobné*, pokud existuje nějaká regulární matice $\mathbf{P}$ taková, že platí $\mathbf{B} = \mathbf{P}^{-1}\mathbf{AP}$.

Reálná(komplexní) matice $\mathbf{A}$ řádu n se nazývá *diagonalizovatelná*, pokud existuje regulární reálná(komplexní) matice $\mathbf{P}$ řádu n, pro kterou platí, že součin $\mathbf{P}^{-1}\mathbf{AP}$ je diagonální matice, tj. pokud matice $\mathbf{A}$ je podobná nějaké diagonální matici.

Lineární operátor $F : \mathbf{V} \rightarrow \mathbf{V}$ na reálném(komplexním) vektorovém prostoru $\mathbf{V}$ se nazývá *diagonalizovatelný*, pokud existuje báze $\mathbb{B}$ prostoru $\mathbf{V}$, pro kterou platí, že matice $[F]_B$ operátoru F vzhledem k bázi $\mathbb{B}$ je diagonální.

14.2 Výpočet vlastních čísel a vlastních vektorů

Příklad

$$\mathbf{A} = \begin{pmatrix} 3 & 2 \\ 2 & 6 \end{pmatrix}, \text{ spočítáme tedy kdy se } \det \begin{pmatrix} 3-\lambda & 2 \\ 2 & 6-\lambda \end{pmatrix} = 0$$

$$\det \begin{pmatrix} 3-\lambda & 2 \\ 2 & 6-\lambda \end{pmatrix} = (3-\lambda)(6-\lambda) - 4 = \lambda^2 - 9\lambda + 14$$

$$\lambda^2 - 9\lambda + 14 = 0 \quad \text{dává dvě řešení:} \quad \lambda_1 = 2 \text{ a } \lambda_2 = 7$$

vlastní vektor příslušný vlastnímu číslu $\lambda_1 = 2$:

$$\begin{pmatrix} 3 & 2 \\ 2 & 6 \end{pmatrix} - \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} x = 0 \Rightarrow x = (-2, 1)$$

vlastní vektor příslušný vlastnímu číslu $\lambda_2 = 7$:

$$\begin{pmatrix} 3 & 2 \\ 2 & 6 \end{pmatrix} - \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} = \begin{pmatrix} -4 & 2 \\ 2 & -1 \end{pmatrix}$$

$$\begin{pmatrix} -4 & 2 \\ 2 & -1 \end{pmatrix} x = 0 \Rightarrow x = (1, 2)$$

14.3 Vlastnosti

Věta *(vlastnosti vlastních čísel)*

Pro komplexní čtvercovou matici $\mathbf{A}$ řádu n platí:

1. charakteristický polynom matice $\mathbf{A}$ řádu n je polynom stupně n s vedoucím koeficientem rovným $(-1)^n$
2. komplexní číslo λ je vlastním číslem matice $\mathbf{A}$ právě když je kořenem charakteristického polynomu $p(\lambda)$ matice $\mathbf{A}$

3. matice $\mathbf{A}$ má n vlastních komplexních čísel, počítáme-li každé tolikrát, kolik je jeho násobnost jako kořene charakteristického polynomu
4. pokud $\mathbf{A}$ je reálná matice, pak $\lambda \in \sigma(\mathbf{A})$ právě když komplexně sdružené $\overline{\lambda} \in \sigma(\mathbf{A})$

Důkaz

1. plyne z definice determinantu.
2. $\exists x \neq 0 : \mathbf{A}x = \lambda x \Leftrightarrow \mathbf{A}x - \lambda x = 0 \Leftrightarrow (\mathbf{A} - \lambda \mathbf{I}_n)x = 0$, tj. matice $(\mathbf{A} - \lambda \mathbf{I}_n)$ je singulární, takže musí mít nulový determinant.
3. plyne ze Základní věty algebry.
4. taktéž.

Věta
Determinant čtvercové matice je roven součinu jejích vlastních čísel.

Věta
Vlastními čísly horní(dolní) trojúhelníkové matice jsou právě všechny diagonální prvky.

Věta
Je-li $\mathbf{A}$ reálná symetrická matice, pak každé vlastní číslo matice $\mathbf{A}$ je reálné.

Věta
Je-li $\mathbf{A}$ čtvercová reálná(komplexní) matice řádu n, $\mathbf{P}$ reálná(komplexní) regulární matice stejného řádu a $\mathbf{B} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}$, pak obě matice $\mathbf{A}$ a $\mathbf{B}$ mají stejný charakterictický polynom a tedy i stejné spektrum.

Důkaz
$\det(\mathbf{P}^{-1}\mathbf{A}\mathbf{P} - t\mathbf{I}) = \det(\mathbf{P}^{-1}\mathbf{A}\mathbf{P} - t\mathbf{P}^{-1}\mathbf{I}\mathbf{P}) = \det(\mathbf{P}^{-1}) \cdot \det(\mathbf{A} - t\mathbf{I}) \cdot \det(\mathbf{P}) = \det(\mathbf{A} - t\mathbf{I})$.

Věta
Jsou-li $\mathbf{A}$, $\mathbf{B}$ čtvercové matice stejného typu, potom $\mathbf{AB}$ a $\mathbf{BA}$ mají stejná vlastní čísla.

14.4 Uvedení matice na diagonální tvar

Věta *(O diagonalizovatelnosti a bázi)*
Čtvercová reálná(komplexní) matice $\mathbf{A}$ řádu n je diagonalizovatelná, právě když existuje báze prostoru $\mathbb{R}^n$ ($\mathbb{C}^n$), která je složena z vlastních vektorů matice $\mathbf{A}$.

Lineární operátor $F : \mathbf{V} \to \mathbf{V}$ na reálném(komplexním) vektorovém prostoru $\mathbf{V}$ je diagonalizovatelný právě když existuje báze prostoru $\mathbf{V}$ složená z vlastních vektorů operátoru F.

Důkaz
Je-li $\mathbf{A}$ diagonalizovatelná, znamená to, že existuje regulární matice $\mathbf{R}$ taková, že $\mathbf{R}^{-1}\mathbf{A}\mathbf{R} = \mathbf{D}$ (a $\mathbf{D}$ je diagonální), což je to samé jako $\mathbf{A}\mathbf{R} = \mathbf{R}\mathbf{D}$. Sloupce matice R tvoří vlastní vektory příslušné vlastním číslům matice $\mathbf{A}$. $\mathbf{R}$ je regulární, takže vlastní vektory jsou lineárně nezávislé a tedy tvoří bázi.

Mám-li n lineárně nezávislých vlastních vektorů, mohu z nich sestavit matici $\mathbf{R}$ a pro ní už platí, že $\mathbf{R}^{-1}\mathbf{A}\mathbf{R} = \mathbf{D}$.

Důsledek
Je-li $\mathbf{A}$ čtvercová matice řádu n a $\mathbf{P}$ regulární matice taková, že $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$ pro nějakou diagonální matici $\mathbf{D}$, pak na hlavní diagonále matice $\mathbf{D}$ jsou všechna vlastní čísla matice $\mathbf{A}$.

Věta *(Vlastní čísla a diagonalizovatelnost)*
Platí:

1. Jsou-li $\lambda_1, ..., \lambda_m$ navzájem různá vlastní čísla matice $\mathbf{A}$ řádu n a $u_i \neq 0$ je vlastní vektor matice $\mathbf{A}$ příslušný vlastnímu číslu λ_i pro libovolné $i = 1, ..., m$, pak je posloupnost vektorů $u_1, \ldots, u_m$ lineárně nezávislá.
2. Má-li matice $\mathbf{A}$ řádu n celkem n navzájem různých vlastních čísel, pak je diagonalizovatelná.
3. Má-li lineární operátor $F : \mathbf{V} \to \mathbf{V}$ celkem n navzájem různých vlastních čísel, pak je diagonalizovatelný.

Důkaz

1. indukcí a sporem, $u_1, \ldots, u_k$ dávají nejmenší protipříklad, pak z rovnice $0 = \mathbf{A}0 = \sum_{i=1}^{k} a_i \lambda_i u_i$ a $0 = \lambda_k \cdot 0 = \lambda_k \cdot \sum_{i=1}^{k} a_i u_i$, pak dostávám spor (buď byly $u_1, \ldots, u_{k-1}$ závislé, nebo je u_k nulové)
2. z n lineárně nezávislých vlastních vektorů sestrojím matici $\mathbf{R}$ a platí $\mathbf{AR}$=$\mathbf{RD}$, kde $\mathbf{D}$ je diagonální matice s vlastními čísly na diagonále.

Věta *(O diagonalizovatelnosti a násobnostech)*
Čtvercová reálná(komplexní) matice $\mathbf{A}$ řádu n je diagonalizovatelná, právě když pro každé vlastní číslo λ matice $\mathbf{A}$ platí, že algebraická násobnost λ se rovná dimenzi nulového prostoru matice $\mathbf{A} - \lambda\mathbf{I}_n$, tj. číslu $\dim \mathcal{N}(\mathbf{A} - \lambda\mathbf{I}_n)$.

Neboli: čtvercová matice $\mathbf{A}$ řádu n je diagonalizovatelná, právě když pro každé její vlastní číslo λ_i s násobností r_i platí $\operatorname{rank}(\mathbf{A} - \lambda_i I) = n - r_i$.

Důkaz
Matice je diagonalizovatelná, právě když existuje báze prostoru $\mathbb{C}^n$ ($\mathbb{R}^n$), složená z vlastních vektorů, a tu lze rozložit na k bází $\operatorname{Ker}(\mathbf{A} - \lambda\mathbf{I})$, které mají dimenzi r_i.

Věta *(spektrální věta pro diagonalizovatelné matice)*
Čtvercová matice $\mathbf{A}$ řádu n se spektrem $\sigma(\mathbf{A}) = \{\lambda_1, ..., \lambda_t\}$ je diagonalizovatelná právě když existují matice $\mathbf{E}_1, ..., \mathbf{E}_t$ řádu n, pro které platí:

1. $\mathbf{A} = \lambda_1\mathbf{E}_1 + \lambda_2\mathbf{E}_2 + ... + \lambda_t\mathbf{E}_t$
2. ${\mathbf{E}_i}^2 = \mathbf{E}_i$ pro každé $i = 1, 2, ..., t$
3. $\mathbf{E}_i\mathbf{E}_j = 0$ pro libovolné dva různé indexy $i, j = 1, 2, ..., t$
4. $\mathbf{E}_1 + \mathbf{E}_2 + ... + \mathbf{E}_t = \mathbf{I}_n$

   Dále pro diagonalizovatelnou matici $\mathbf{A}$ platí, že
5. matice $\mathbf{E}_i$ jsou jednoznačně určené maticí $\mathbf{A}$ a vlastnostmi *1,2,3,4*
6. hodnost každé z matic $\mathbf{E}_i$ se rovná algebraické násobnosti vlastního čísla λ_i
7. je-li $f(x) = c_0 + c_1x + ... + c_kx^k$ libovolný polynom s komplexními koeficienty, pak platí $f(\mathbf{A}) = c_0\mathbf{I}_n + c_1\mathbf{A} + ... + c_k\mathbf{A}^k = f(\lambda_1)\mathbf{E}_1 + f(\lambda_2)\mathbf{E}_2 + ... + f(\lambda_k)\mathbf{E}_k$
8. nějaká matice $\mathbf{B}$ komutuje s maticí $\mathbf{A}$ (tj. $\mathbf{AB} = \mathbf{BA}$) právě tehdy, když komutuje s každou z matic $\mathbf{E}_i$ pro $i = 1, 2, ..., t$

14.5 Jordanův tvar v obecném případě

Definice *(Jordanův tvar)*
Diagonalizovatelné matice mají dobře pochopitelnou strukturu popsanou ve spektrální větě. Matice, které nelze diagonalizovat, nemají bázi složenou z vlastních vektorů, musí mít nějaké vícenásobné vlastní číslo λ, pro které je dimenze nulového prostoru $\mathcal{N}(\mathbf{J} - \lambda\mathbf{I}_n)$ menší než algebraická násobnost čísla λ. (viz věta o diagonalizovatelnosti a násobnostech)

Příklad takové matice řádu n, pro $n \geq 2$

$$\mathbf{J} = \begin{pmatrix} \lambda & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \lambda & \cdots & 0 & 0 \\ & & \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}$$

Všechny prvky na diagonále se rovnají stejnému číslu λ, všechny prvky bezprostředně nad hlavní diagonálou se rovnají 1, ostatní prvky jsou nulové.

Pozorování
Charakteristický polynom matice $\mathbf{J}$ se rovná:

$$p(t) = (\lambda - t)^n$$

Pozorování

Matice $\mathbf{J} - \lambda \mathbf{I}_n$ je v řádkově odsťupňovaném tvaru, její hodnost se rovná $n - 1$ a její nulový prostor $\mathcal{N}(\mathbf{J} - \lambda \mathbf{I}_n)$ má proto dimenzi rovnou 1, což se nerovná algebraické násobnosti vlastního čísla λ, matice $\mathbf{J}$ tedy není diagonalizovatelná.

Definice *(Jordanova buňka)*

Matice $\mathbf{J}$ se nazývá Jordanova buňka řádu n příslušná vlastnímu číslu λ.

Věta *(O Jordanově kanonickém tvaru)*

Pro každou čtvercovou matici $\mathbf{A}$ existuje regulární matice $\mathbf{P}$ taková, že

$$\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \begin{pmatrix} \mathbf{J}_1 & 0 & 0 & \cdots & 0 \\ 0 & \mathbf{J}_2 & 0 & \cdots & 0 \\ 0 & 0 & \mathbf{J}_3 & \cdots & 0 \\ & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \mathbf{J}_k \end{pmatrix}$$

kde každá z matic $\mathbf{J}_i$ pro $i = 1, ..., k$ je Jordanova buňka nějakého řádu n_i příslušná vlastnímu číslu λ_i. Čísla $\lambda_1, ..., \lambda_k$ jsou všechna, nikoliv nutně různá, vlastní čísla matice $\mathbf{A}$ a platí dále $n_1 + ... + n_k = n$. Dvojice n_i, λ_i pro $i = 1, ..., k$ jsou maticí $\mathbf{A}$ určené jednoznačně až na pořadí (tj. reprezentují třídu podobných matic).

Definice *(Hermitovskost)*

Nechť $\mathbf{A}$ je komplexní matice, potom matici $\mathbf{A}^H$, pro kterou platí, že $(\mathbf{A}^H)_{ij} = \overline{a_{ji}}$ nazýváme *hermitovskou transpozicí* matice $\mathbf{A}$ (někdy se používá název „konjugovaná matice“).

Komplexní čtvercová matice $\mathbf{A}$ se nazývá *unitární*, pokud platí, že $\mathbf{A}^H\mathbf{A} = \mathbf{I}$. Komplexní čtvercová matice $\mathbf{A}$ se nazývá *hermitovská*, pokud $\mathbf{A}^H = \mathbf{A}$.

Pozorování

Platí: $(\mathbf{AB})^H = \mathbf{B}^H\mathbf{A}^H$ (důkaz je stejný jako pro obyčejnou transpozici).

Věta *(O hermitovských maticích)*

Každá hermitovská matice A má všechna vlastní čísla reálná (i když je sama komplexní). Navíc existuje unitární matice R taková, že $R^{-1}AR$ je diagonální. (tzn. hermitovská matice je diagonalizovatelná).

Důsledek

Interpretace v $\mathbb{R}$: Pro každou symetrickou matici A platí, že všechna její vl. čísla jsou reálná a navíc existuje ortogonální matice R: $R^{-1}AR$ je diagonální. Příslušný vl. vektor x lze vzít reálný, protože $(A - \lambda I)x = 0$ – soustava lin. rovnic s reálnou singulární maticí – musí mít netriviální reálné řešení.

14.6 Spektrální věta - část důkazu

Tato část není v požadavcích ke zkouškám!

Důkaz
Důkaz spektrální věty je poměrně dlouhý - několik stránek, uvedu zde tedy jen část důkazu, doufám že tu lehčí :)

„A je diagonalizovatelná $\Rightarrow$ vlastnosti 1,2,3,4“

Nechť m_i je algebraická násobnost vlastního čísla λ_i pro $i = 1, ..., t$. Matice **A** je diagonalizovatelná, tedy dle **Definice 3** existuje regulární matice **P** řádu n taková, že součin $\mathbf{P}^{-1}\mathbf{AP}$ je diagonální matice, a tato diagonální matice má na diagonále vlastní čísla matice **A** dle **důsledku tvrzení 7 TODO**. Tedy

$$\mathbf{P}^{-1}\mathbf{AP} = \begin{pmatrix} \lambda_1\mathbf{I}_{m_1} & 0 & \cdots & 0 \\ 0 & \lambda_2\mathbf{I}_{m_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_t\mathbf{I}_{m_t} \end{pmatrix} \tag{4}$$

kde $\mathbf{I}_{m_i}$ jsou jednotkové matice řádu m_i. Označíme pro $i = 1, ..., t$ symbolem $\mathbf{D}_i$ matici, kterou dostaneme z blokové matice na pravé straně poslední rovnosti tak, že nahradíme všechny výskyty vlastního čísla λ_i číslem 1 a výskyty ostatních vlastních čísel λ_j pro $j \neq i$ číslem 0. Například

$$\mathbf{D}_2 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & \mathbf{I}_{m_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

Jedná se vlastně o "částečnou" jednotkovou matici, která má pouze na části diagonály čísla 1. Pak platí:

$$\begin{aligned} \mathbf{I}_n &= \mathbf{D}_1 + \mathbf{D}_2 + ... + \mathbf{D}_t \\ \mathbf{P}^{-1}\mathbf{AP} &= \lambda_1\mathbf{D}_1 + \lambda_2\mathbf{D}_2 + ... + \lambda_t\mathbf{D}_t \\ \mathbf{A} &= \lambda_1\mathbf{PD}_1\mathbf{P}^{-1} + \lambda_2\mathbf{PD}_2\mathbf{P}^{-1} + ... + \lambda_t\mathbf{PD}_t\mathbf{P}^{-1} \end{aligned}$$

V první rovnosti jsme vlastně jen sečetli "částečné jednotkové matice" $\mathbf{D}_i$ a výsledek je jednotková matice. Pokud všechny matice $\mathbf{D}_i$ vynásobíme vlastními čísly λ_i a sečteme je, dostaneme matici na pravé straně rovnice (4). A ve třetí rovnosti se jen zbavíme matic **P** a $\mathbf{P}^{-1}$ na levé straně.

Položíme $\mathbf{E}_i = \mathbf{PD}_i\mathbf{P}^{-1}$ pro $i = 1, ..., t$ a dostaneme tak z třetí rovnosti vlastnost 1.

Protože $\mathbf{D}_i{}^2 = \mathbf{D}_i$ a $\mathbf{D}_i\mathbf{D}_j = 0$ pro libovolné různé indexy $i, j, = 1, ..., t$, dostáváme

$$\begin{aligned} \mathbf{E}_i{}^2 &= \mathbf{PD}_i\mathbf{P}^{-1}\mathbf{PD}_i\mathbf{P}^{-1} = \mathbf{PD}_i{}^2\mathbf{P}^{-1} = \mathbf{PD}_i\mathbf{P}^{-1} = \mathbf{E}_i \\ \mathbf{E}_i\mathbf{E}_j &= \mathbf{PD}_i\mathbf{P}^{-1}\mathbf{PD}_j\mathbf{P}^{-1} = \mathbf{PD}_i\mathbf{D}_j\mathbf{P}^{-1} = \mathbf{P}0\mathbf{P}^{-1} = 0 \\ \mathbf{E}_1 + ... + \mathbf{E}_t &= \mathbf{PD}_1\mathbf{P}^{-1} + ... + \mathbf{PD}_t\mathbf{P}^{-1} = \mathbf{P}(\mathbf{D}_1 + ... + \mathbf{D}_t)\mathbf{P}^{-1} = \\ &= \mathbf{PI}_n\mathbf{P}^{-1} = \mathbf{I}_n \end{aligned}$$

což dokazuje vlastnosti 2,3,4. V první rovnosti jsme využili, že ${\mathbf{D}_i}^2 = \mathbf{D}_i$, ve druhé jsme využili $\mathbf{D}_i\mathbf{D}_j = 0$ a ve třetí $\mathbf{I}_n = \mathbf{D}_1 + \mathbf{D}_2 + ... + \mathbf{D}_t$.

Opačnou implikaci, tedy že z vlastností 1,2,3,4 plyne diagonalizovatelnost matice nebudu dokazovat. Ze zbývajících vlastností 5,6,7,8 dokážu vlastnosti 6 a 7.

Vlastnost 6

Matice $\mathbf{D}_i$ (z předchozího důkazu), má hodnost m_i, proto má tutéž hodnost i matice $\mathbf{E}_i = \mathbf{P}\mathbf{D}_i\mathbf{P}^{-1}$, což dokazuje 6.

Vlastnost 7

Tento důkaz vypadá na první pohled odporně ale nenechte se odradit :) je to pouze rozepisování sum.

Dle vlastnosti 1 :

$$\mathbf{A}^2 = (\lambda_1\mathbf{E}_1 + ... + \lambda_t\mathbf{E}_t)(\lambda_1\mathbf{E}_1 + ... + \lambda_t\mathbf{E}_t)$$

to se rovná (jen přepsaní na sumu, násobení každý s každým)

$$\sum_{i,j=1}^{t} \lambda_i\mathbf{E}_i\lambda_j\mathbf{E}_j$$

dáme li matice k sobě, vznikne nám $\mathbf{E}_i\mathbf{E}_j$ což je dle vlastnosti 3 rovno nule (pro různé indexy i a j), tyto násobení tedy můžeme ignorovat a přepsat sumu tak, aby se mezi sebou násobili pouze matice se stejným indexem. Dále víme z vlasnosti 2 že ${\mathbf{E}_i}^2 = \mathbf{E}_i$, tedy

$$\sum_{i=1}^{t} {\lambda_i}^2{\mathbf{E}_i}^2 = \sum_{i=1}^{t} {\lambda_i}^2\mathbf{E}_i$$

jestliže nyní předpokládáme

$$\mathbf{A}^l = \sum_{i=1}^{t} {\lambda_i}^l\mathbf{E}_i$$

pro nějaké $l \geq 2$, pak dostáváme (a upravujeme stejně jako v předchozím případě)

$$\mathbf{A}^{l+1} = (\lambda_1\mathbf{E}_1 + ... + \lambda_t\mathbf{E}_t)({\lambda_1}^l{\mathbf{E}_1}^l + ... + {\lambda_t}^l{\mathbf{E}_t}^l) =$$
$$= \sum_{i,j=1}^{t} \lambda_i\mathbf{E}_i{\lambda_j}^l{\mathbf{E}_j}^l = \sum_{i=1}^{t} {\lambda_i}^{l+1}{\mathbf{E}_i}^2 = \sum_{i=1}^{t} {\lambda_i}^{l+1}\mathbf{E}_i$$

Protože rovněž platí

$$\mathbf{A}^0 = \mathbf{I}_n = \mathbf{E}_1 + ... + \mathbf{E}_t = {\lambda_1}^0\mathbf{E}_1 + ... + {\lambda_t}^0\mathbf{E}_t$$

tedy jsme dokázali, že rovnost

$$\mathbf{A}^l = \sum_{i=1}^{t} {\lambda_i}^l\mathbf{E}_i$$

platí pro každé nezáporné celé číslo l. Pro každé číslo $j = 0, ...k$ dostáváme

$$c_j \mathbf{A}^j = c_j \sum_{i=1}^{t} \lambda_i{}^j \mathbf{E}_i$$

a tedy platí

$$f(\mathbf{A}) = \sum_{j=0}^{k} c_j \mathbf{A}_j = \sum_{j=0}^{k} c_j (\sum_{i=1}^{t} \lambda_i{}^j \mathbf{E}_i) = \sum_{i=1}^{t} (\sum_{j=0}^{k} c_j \lambda_i{}^j) \mathbf{E}_i = \sum_{i=1}^{t} f(\lambda_i) \mathbf{E}_i$$

15 Základy lineárního programování

Požadavky

- Simplexová metoda
- Věty o dualitě (bez důkazu)

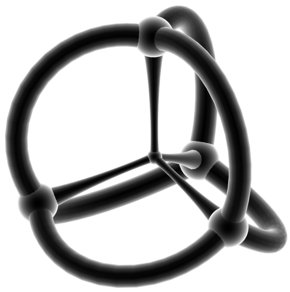
Lineární programování je označení pro úlohu maximalizovat jistou funkci n reálných proměnných na množině bodů polytopu v prostoru $\mathbb{R}^n$.

Nejprve si udělejme malý výlet do geometrie. *Polytop* je zobecněním polygonu (mnohoúhelníku) do vyšších dimenzích. Pro dimenzi 3 se ale používá ještě speciální název *polyhedron* a pro dimenzi 4 *polychoron*. My se v dalším textu omezíme na *konvexní polytopy*, což jsou konvexní obaly konečně mnoha bodů. Vzhledem k tomu, že tyto konvexní polytopy jsou průnikem jistého množství poloprostorů, můžeme je popsat maticovou rovnicí tvaru

$$Ax \leq b,$$

kde A je matice řádu $m \times n$ a m je počet poloprostorů, jejichž průnikem je daný polytop, a n je dimenze podprostoru, ve kterém polytop máme.

Simplex je „n–dimenzionální“ trojúhelník (průnik několika poloprostorů). Podle rostoucí dimenze je to tedy po řadě bod, úsečka, trojúhelník, čtyřstěn, pentachoron (viz obrázek 1) atd. Může být omezený i neomezený.



Obrázek 2: Pentachoron

Nyní přistupme k formální definici úlohy lineárního programování.

Úloha lineárního programování
Je dán konvexní polytop v prostoru $\mathbb{R}^n$ popsaný m nerovnostmi. Maticově to můžeme zapsat ve tvaru $Ax \leq b$, kde A je reálná matice řádu $m \times n$ a b je vektor m reálných čísel. Dále je dán vektor $c \in \mathbb{R}^n$. Funkce, kterou chceme maximalizovat, je $\sum_{i=1}^{n} c_i x_i$, neboli vektorově $c^T x$. Ještě navíc hledáme pouze mezi body se všemi souřadnicemi nezápornými (tj. $x_i \geq 0$ pro $i = 1, \ldots, n$).

Terminologie

1. Vektoru c říkáme *cenový vektor*, funkci $c^T x$ pak *účelová funkce*.
2. Nerovnosti $Ax \leq b$ a $x \geq 0$ jsou *omezující podmínky*, vektor b je *pravá strana úlohy*.
3. Konkrétní zadání úlohy lineárního programování (tj. matice A a vektory b, c) je *přípustné*, pokud existuje nějaký bod splňující $x \geq 0$ a $Ax \leq b$. Jinak je zadání *nepřípustné*.
4. Úloha je *neomezená*, pokud můžeme účelovou funkcí dosáhnout na přípustných bodech libovolně veliké hodnoty. Jinak je *omezená*.

Věta

Pro přípustnou a omezenou úlohu lineárního programování[1] existuje bod, ve kterém účelová funkce nabývá maxima. Těchto bodů obecně může být více a říkáme jim optimální řešení.

15.1 Simplexová metoda

Simplexová metoda je označení pro algoritmus řešící úlohu lineárního programování. Byla publikována v roce 1947 jedním ze zakladatelů lineárního programování američanem Georgem Dantzigem.

Idea

Zkonstruujeme přípustné řešení v některém vrcholu polytopu. Poté jdeme po hranách do vrcholů s vyšší hodnotou účelové funkce.

Omezující podmínku $Ax \leq b$ tedy změníme na $Ax = b$. Toho docílíme přidáním jedné nezáporné proměnné pro každou podmínku ($\sum x < b$ je totiž ekvivalentní $\sum x + y = b$ kde $y \in \mathbb{R}^+$). Tuto úpravu lze také zapsat jako $A := (A\ I)$. Dále předpokládáme, že matice A má lineárně nezávislé řádky. Pro podmnožinu indexů $I \subseteq \{1, 2, \ldots, n\}$ označme A_I matici A, ze které ponecháme pouze sloupce, které jsou v I. Analogicky pro libovolný vektor $w \in \mathbb{R}^n$ označme jako w_I vektor, z něhož ponecháme jenom souřadnice z I (má dimenzi $n - |I|$).

Báze (a to nemá nic společného s bází vektorového prostoru) je libovolná podmnožina indexů $B \subseteq \{1, 2, \ldots, n\}$ taková, že matice A_B je regulární. Navíc řekneme, že báze je *přípustná*, pokud rovnice $A_B x_B = b$ má nezáporné řešení. Vektor $x \in \mathbb{R}^n$ je tzv. *bazické řešení*[2], pokud existuje báze B taková, že $A_B x_B = b$ a $x_i = 0$ pro každé $i \in \{1, 2, \ldots, m\} \backslash B$.

Poznamenejme jen, že bazické řešení ještě nemusí být přípustné. Je-li navíc i přípustné, říkáme mu přirozeně *přípustné bazické řešení*. Proměnným x_j pro $j \in B$, kde B je báze, říkáme bazické.

Věta

Nechť $x \in \mathbb{R}^n$ je přípustné řešení. Pak x je bazické řešení, právě když sloupce matice A odpovídající kladným proměnným jsou lineárně nezávislé.

[1] Tedy existuje alespoň jedno řešení a účelová funkce je shora omezená.

Věta
Nechť B je m–prvková indexová množina $B \subseteq \{1, \ldots, n\}$ a A_B je regulární. Pak existuje nejvýše jedno přípustné bazické řešení x ($x_i \neq 0 \Leftrightarrow i \in B$).

Mezi první tvrzeními jsme uvedli, že má-li daná úloha lineárního programování nějaké přípustné řešení a je-li zároveň účelová funkce na množině přípustných řešení omezená, pak existuje optimální řešení (tj. nabývá se maxima). Dá se ale dokázat dokonce následující.

Věta
Má-li daná úloha optimální řešení, pak i některé bazické řešení je optimální.

Tato věta má obrovskou důležitost, neboť je jasné, že **bazických řešení je jen konečně mnoho**. Ukažme si fungování simplexové metody na konkrétním příkladu.
Příklad
Maximalizujte funkci $z(x_1, \ldots, x_5) = x_1 + x_2$ za omezujících podmínek $x_i \geq 0$ ($i = 1, \ldots, 5$) a

$$\begin{array}{cccccl} -x_1 & +x_2 & +x_3 & & & = 1 \\ +x_1 & & & +x_4 & & = 3 \\ & +x_2 & & & +x_5 & = 2 \end{array}$$

Řešení. Nejprve najdeme libovolné přípustné bazické řešení. Matice A a vektor b této úlohy jsou ze zadání

$$A = \begin{pmatrix} -1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix}$$

a $m = 3, n = 5$. Vidíme tedy, že jedním z bazických řešení je $R_1 = (0, 0, 1, 3, 2)^T$. Odpovídající báze indexů je $B = \{3, 4, 5\}$ (matice A_B je jednotková, a tedy regulární). Na základě tohoto vytvoříme tzv. *simplexovou tabulku* (počáteční přípustnou tabulku) tak, že vyjádříme bazické proměnné pomocí nebazických a přidáme jeden řádek s vyjádřenou účelovou funkcí pomocí nebazických proměnných.

$$\begin{array}{r|lll} x_3 = & 1 & +x_1 & -x_2 \\ x_4 = & 3 & -x_1 & \\ x_5 = & 2 & & -x_2 \\ \hline z = & & x_1 & +x_2 \end{array}, \quad R_1 = (0, 0, 1, 3, 2)^T, \quad z = 0$$

V bodě R_1 je $z(R_1) = 0$. Nyní budeme, jak bylo naznačeno, postupně zvyšovat hodnotu funkce z, dokud nezjistíme, že jsme nalezli optimální řešení. Hodnotu funkce z budeme zvětšovat zvětšením hodnoty některé nebazické (volné) proměnné.

Ponechejme $x_1 = 0$ a zvětšeme x_2 z 0 na 1 (jednička je nejlepší možná, viz první rovnici a $x_3 \geq 0$). Pak pomocí tabulky dostaneme nové přípustné řešení, konkrétně $R_2 = (0, 1, 0, 3, 1)^T$. Z první rovnice teď vyjádříme x_2:

$$x_2 = 1 + x_1 - x_3$$

a nahradíme touto rovnicí původní první rovnici $x_3 = 1 + x_1 - x_2$. Toto řešení odpovídá bázi $B = \{2, 4, 5\}$. Snadno zjistíme, že $z(R_2) = 0+1 = 1$. Nyní se stalo, že proměnná x_2 nahradila proměnnou x_3 v bázi. Tomuto procesu říkáme, že proměnná x_2 „vstoupila do báze“, x_3 z ní „vystoupila“.

Dostáváme tak novou simplexovou tabulku

$$\begin{array}{r|lll} x_2 = & 1 & +x_1 & -x_3 \\ x_4 = & 3 & -x_1 & \\ x_5 = & 1 & -x_1 & +x_3 \\ \hline z = & 1 & +2x_1 & -x_3 \end{array}, \quad R_2 = (0,1,0,3,1)^T, \quad z = 1$$

Nyní budeme zvyšovat x_1. První rovnice x_1 neomezuje, druhá říká $x_1 \leq 3$ a třetí nyní říká $x_1 \leq 1$ (jelikož $x_3 = 0$). Položme tedy $x_1 = 1$. Dostáváme nové řešení $R_3 = (1, 2, 0, 2, 0)^T, z(R_3) = 3$. Proměnná x_1 vstoupí do báze místo proměnná x_5. Nová báze je $B = \{1, 2, 4\}$.

Dostáváme další simplexovou tabulku

$$\begin{array}{r|lll} x_1 = & 1 & +x_3 & -x_5 \\ x_2 = & 2 & & -x_5 \\ x_4 = & 2 & -x_3 & +x_5 \\ \hline z = & 3 & +x_3 & -2x_5 \end{array}, \quad R_3 = (1,2,0,2,0)^T, \quad z = 3$$

Zvětšíme x_3 z 0 na 2 ($x_3 \leq 2$ plyne ze třetí rovnice tabulky) a tím obdržíme další řešení $R_4 = (3, 2, 2, 0, 0)^T$, báze je $B = \{1, 2, 3\}$, $z(R_4) = 5$. Odpovídající nová simplexová tabulka je

$$\begin{array}{r|lll} x_1 = & 3 & -x_4 & \\ x_2 = & 2 & & -x_5 \\ x_3 = & 2 & -x_4 & +x_5 \\ \hline z = & 5 & -x_4 & -x_5 \end{array}, \quad R_4 = (3,2,2,0,0)^T, \quad z = 5$$

Nyní je jasné, že libovolné zvýšení volné proměnné x_4 nebo x_5 sníží hodnotu účelové funkce. Z konstrukce simplexové metody plyne, že řešení R_4 je již optimální, neboť jsme prováděli pouze ekvivalentní rovnicové úpravy. Optimálním řešením dané úlohy je tedy bod $(3, 2, 2, 0, 0)$.

□

Časová složitost simplexové metody je $O(2^n)$. Jeden z nejhorších případů můžeme vzít n–dimenzionální krychli, která má přesně 2^n vrcholů. Na této krychli algoritmus může postupně navštívit všechny její vrcholy.

Simplexová metoda nachází uplatnění převážně při řešení optimalizačních úloh v inženýrství nebo ekonomii.

15.2 Duální úloha

Problém lineárního programování tak, jak byl popsán výše, označujeme jako *primární*. Ke každému primárnímu problému můžeme zkonstruovat *duální úlohu*. Připomeňme, že primární úloha byla najít

$$\max\{c^T x : x \in \mathbb{R}^n, Ax \leq b, x \geq 0\}.$$

Duální úloha k této pak je najít

$$\min\{b^T y : y \in \mathbb{R}^m, A^T y \geq c, y \geq 0\}.$$

Základem teorie duality lineárního programu jsou následující dvě věty – *(Slabá) věta o dualitě.*

Věta *(Slabá věta o dualitě)*

Pokud je x přípustné řešení primární úlohy a y přípustné řešení duální úlohy, pak hodnota duální účelové funkce v bodě y je alespoň tak veliká jako hodnota primární účelové funkce v bodě x.

Věta *(Věta o dualitě)*

Nechť x_* je optimální řešení primární úlohy. Pak existuje optimální řešení y_* duální úlohy takové, že

$$c^T x_* = b^T y_*.$$

Duální úloha ze života

...

16 Diskrétní matematika

Požadavky

- Uspořádané množiny
- Množinové systémy, párování, párování v bipartitních grafech (systémy různých reprezentantů)
- Kombinatorické počítání
- Princip inkluze a exkluze
- Latinské čtverce a projektivní roviny.

16.1 Uspořádané množiny

Definice *(Kartézský součin)*
Nechť X a Y jsou množiny. Symbolem $X \times Y$ označíme množinu všech uspořádaných dvojic tvaru (x, y), kde $x \in X$ a $y \in Y$. Formálně zapsáno: $X \times Y = \{(x,\ y); x \in X, y \in Y\}$ se nazývá *kartézský součin* množin X a Y.

Kartézský součin $X \times X$ někdy značíme jako X^2.

Definice *(relace)*
Relace R je množina uspořádaných dvojic. Jsou-li X a Y množiny, nazývá se libovolná podmnožina kartézského součinu $X \times Y$ *relací* mezi X a Y. Zdaleka nejdůležitější případ je $X = Y$. V takovém případě mluvíme o relaci na X, což je tedy libovolná podmnožina X^2.

Náleží-li (x, y) relaci R, tedy $(x, y) \in R$, říkáme, že x a y jsou v relaci R. Značíme xRy.

Definice *(druhy relací)*
Relace X může být:

- *reflexivní*, jestliže pro každné $x \in X$ platí xRx
- *ireflexivní*, jestliže platí $xRy \ \Rightarrow\ x \neq y$
- *symetrická*, jestliže $xRy \Rightarrow yRx$
- *tranzitivní*, jestliže $xRy \wedge yRz \Rightarrow xRz$
- *antisymetrická*, jestliže $xRy \wedge yRx \Rightarrow x = y$

Definice *(ekvivalence)*
Řekneme, že relace R na X je *ekvivalence* na X, jestliže je symetrická, reflexivní a tranzitivní.

Definice *(uspořádání, uspořádaná množina)*
Uspořádání na nějaké množině X je každá relace na X, která je reflexivní, tranzitivní a antisymetrická. *Uspořádaná množina* je dvojice (X, R), kde X je množina a R je uspořádání na X.

Pro uspořádání se používá značení $\leq$ nebo $\preceq$. Pro každé uspořádání lze odvodit „ostrou nerovnost“ $<$ nebo $\prec$, kde platí, že $x < y \Leftrightarrow x \leq y \wedge x \neq y$.

Příklady
Uspořádané množiny:

- $(\mathbb{N}, \leq)$
- $(\mathbb{N}, |)$, kde „|“ je relace „dělí“
- $(\mathcal{P}(X), \subseteq)$, kde $\mathcal{P}(X)$ označuje množinu všech podmnožin a $\subseteq$ normální množinovou inkluzi
- orientovaný acyklický graf (V, E) s relací $\rho : (a, b) \in \rho \equiv^{def}$ *existuje cesta z a do b*

Definice *(lineární uspořádání)*
Lineární uspořádání je takové uspořádání, kde pro každé dva prvky x a y platí buď $x \leq y$ nebo $y \leq x$. Někdy se také nazývá *úplné uspořádání.*

Uspořádání, které není úplné, nazýváme *částečným uspořádáním.*

Definice *(bezprostřední přechůdce)*
Bezprostřední předchůdce prvku y je takový prvek x, pro který platí $x < y$, a neexistuje žádné takové t, že $x < t < y$.

Poznámka *(Hasseův diagram)*
Při znázorňovaní se uspořádaná množina zakresluje pomocí bodů a šipek, jako kterákoliv jiná relace. Protože těchto šipek by bylo mnoho, vychází se z tranzitivity a znázorňují se šipky pouze mezi prvky a jejich bezprostředními předchůdci. Přijmeme-li navíc konvenci, že v obrázku povedou všechny šipky nahoru, není třeba zakreslovat směr šipek, pouze spojnice bodů. Takovéto znázornění se pak nazývá *Hasseův diagram.*

Poznámka *(uspořádání na kartézském součinu)*
Mám-li dvě množiny A a B a na nich uspořádání $\leq_A$ a $\leq_B$ můžu definovat „složené uspořádání“

- „po složkách“ – $(a_1, b_1) \leq (a_2, b_2) \equiv^{\text{def}} a_1 \leq_A a_2 \wedge b_1 \leq_B b_2$
- „lexikograficky“ – $(a_1, b_1) \leq (a_2, b_2) \equiv^{\text{def}} a_1 \leq_A a_2 \vee (a_1 = a_2 \wedge b_1 \leq_B b_2)$

Definice
Říkáme, že (X, R) a (Y, P) jsou *isomorfní uspořádané množiny,* pokud existuje nějaké vzájemně jednoznačné zobrazení $f : X \to Y$ takové, že pro každé $x, y \in X$ platí xRy právě když $f(x)Pf(y)$.

Definice *(Předuspořádání)*
Předuspořádání nazveme každou relaci, která je reflexivní a transitivní (nebudeme tedy požadovat antisymetrii – mohou vznikat „cykly“).

Poznámka
Mám-li množinu X s relací $\sim$, která je předuspořádání, potom relace $\sim$ je uspořádání na množině X/ρ (rozklad podle tříd ekvivalence ρ), kde $a\rho b \equiv (a \sim b \wedge b \sim a)$.

Definice
Nezávislý systém M podmnožin množiny X je podmnožina $P(X)$ taková, že každé dvě množiny $A, B \in M$ jsou neporovnatelné relací náležení.

Věta *(Spernerova)*
Libovolný nezávislý systém podmnožin n-prvkové množiny má nejvýš $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ množin.

TODO: Patří sem dobré uspořádání a Zernelova věta??? (to by znamenalo přidat sem i supremum, infimum, řetězec, nejmenší a největší prvek)

16.2 Množinové systémy, párování, párování v bipartitních grafech (systémy různých reprezentantů)

Definice
Nechť X a I jsou množiny. *Množinovým systémem nad X* nazveme $|I|$-tici $M = \{M_i; i \in I\}$, kde $M_i \subseteq X$

Je tedy možné, aby se tam táž množina objevila víckrát.

Definice *(systém různých reprezentantů)*
Systém různých reprezentantů (SRR) je funkce $f : I \to X$ taková, že $\forall i \in I : f(i) \in M_i$ a f je prostá.

Jinými slovy, SRR je výběr jednoho prvku z každé množiny M_i tak, že všechny vybrané prvky jsou navzájem různé. Obecně se tedy neuvažují nekonečné systémy.

Definice *(párování)*
Párování v grafu G je množina hran $F \subseteq E(G)$ taková, že každý vrchol grafu G patří nejvýše do jedné hrany z F.

Ekvivalentní definice jsou přes stupeň vrcholu (každý vrchol má stupeň nejvýše 1) nebo přes disjunktnost hran (každé dvě jsou disjunktní - žádné dvě nemají společný vrchol).

Definice *(bipartitní graf)*
Bipartitní graf je takový graf G, kde množinu vrcholů $V(G)$ můžeme rozdělit na dvě disjunktní podmnožiny V_1 a V_2 takové, že každá hrana z $E(G)$ spojuje vždy vrchol z V_1 s vrcholem z V_2.

Definice
Incidenčním grafem množinového systému M nad množinou X nazveme bipartitní graf

$$B_M = (I \cup X, \{\{i, x\}, x \in M_i\})$$

V podstatě si každý prvek z X i každý index I označíme vrcholem a spojíme každý index i s prvky x, které náleží do M_i. Z incidenčního grafu pak lze nahlédnout existenci SRR - ten existuje, právě když v incidenčním grafu existuje párování velikosti $|I|$.

Věta *(Hallova)*
Systém různých reprezentantů v M existuje, právě když pro každou $J \subseteq I$ je

$$\left|\bigcup_{j \in J} M_j\right| \geq |J|$$

Definice *(perfektní párování)*
Perfektním párováním nazveme párování M v grafu G, pro které platí

$$|M| = \frac{|V(G)|}{2}$$

Tedy perfektní párování je takové, kde je každý vrchol spárovaný s nějakým jiným vrcholem. Dalším důležitým pojmem je *maximální párování*, což je v podstatě nejlepší možné párování (pokrývá největší možný počet vrcholů), jakého jsme v daném grafu schopni dosáhnout.

Věta *(O párování v bipartitním grafu)*
Buď $G = (A \cup B, E)$ graf se dvěma partitami A a B a E neprázdná množina hran. Jestliže platí $\deg\, u \geq \deg\, v\ \forall u \in A, \forall v \in B$, potom existuje párování velikosti $|A|$. Díky tomu pokud má bipartitní graf všechny vrcholy stejného stupně, pak má perfektní párování.
Důkaz
Převede se na Hallovu větu s použitím „okolí“ vrcholů (tj. bodů přímo spojených s vrcholem hranou).

Věta *(Tutteova)*
Graf (V, E) má perfektní párování, právě když pro každou množinu vrcholů $A \subseteq V$ platí:

$$c_l(G \setminus A) \leq |A|$$

(tj. počet komponent souvislosti s lichých počtem vrcholů v indukovaném podgrafu je menší než velikost množiny vrcholů). Této vlastnosti se také někdy říká *Tutteova podmínka.*

Algoritmus *(Edmondsův algoritmus na perfektní párování)*
Vstupem algoritmu je graf $G = (V, E)$ a libovolné párování M (i prázdné). Výstupem je párování M', které alespoň o 1 větší než M, pokud je něčeho takového možné dosáhnout. Postup výpočtu:

1. Vybudujeme maximální možný „Edmondsův les“ párování M – do nulté hladiny umístíme volné vrcholy a prohledáváním do šířky sestrojíme max. strom takový, že se střídají párovací a nepárovací hrany (mezi sudou a lichou hladinou jen nepárovací, mezi lichou a sudou jen párovací).
   Některé vrcholy se v lese vůbec neobjeví – nazveme je „kompost“. Ty jsou už nějak spárovány mezi sebou a nebudeme je potřebovat.

2. Pokud existuje hrana mezi sudými hladinami různých stromů, máme „volnou střídavou cestu“ (tj. cestu liché délky mezi 2 volnými vrcholy, na které se střídají nepárovací a párovací hrany), na níž můžeme zalternovat hrany párování a to tak zvětšit o 1 a skončit.
3. Pokud existuje hrana mezi sudými hladinami téhož stromu, máme „květ“ (tj. kružnici liché délky, na které se střídají párovací a nepárovací hrany). Květ můžeme zkontrahovat a algoritmus rekurzivně pustit na takto získaný graf. Pokud dostaneme
   (a) staré párování beze změny, vrátíme $M' = M$
   (b) jiné (větší) párování $\hat{M}$, prohodíme párování na cestě v $\hat{M}$ od vrcholu květu v nejvyšší hladině (kam jsme květ zkontrahovali) k volnému vrcholu a přidáme květ zpátky (a párování sedí a je větší než M)
4. Není-li žádná hrana mezi sudými hladinami, vydej $M' = M$.

Hlavní algoritmus jen opakuje výše popsaný krok, dokud vrací větší párování než bylo předchozí. Celková složitost jednoho kroku je $O((m+n)n)$ a pro celý algoritmus $O((m+n)n^2)$.

16.3 Kombinatorické počítání

Věta

Nechť N je nějaká n-prvková množina a M je m-prvková množina ($m > 0$). Potom počet všech zobrazení $f : N \to M$ je m^n.

Věta

Libovolná n-prvková množina X má právě 2^n podmnožin.

Věta

Nechť $n > 0$. Každá n-prvková množina má právě 2^{n-1} podmnožin sudé velikosti a právě 2^{n-1} podmnožin liché velikosti.

Věta

Pro $m, n \geq 0$ existuje právě $m(m-1)(m-2)\dots(m-n+1)$ prostých zobrazení n-prvkové množiny do m-prvkové množiny.

Definice

Prostá zobrazení množiny X do sebe se nazývá *permutace množiny* X. Tato zobrazení jsou zároveň na.

Permutace si můžeme představit jako přerovnání množiny - např. $\{4213\}$ je permutací množiny $\{1234\}$. Jiný zápis permutací je pomocí jejich cyklů (*cyklus* v permutaci je pořadí prvků, kde začnu u nějakého prvku, pokračuji jeho obrazem v permutaci a toto opakuji, dokud nenarazím na první prvek). U cyklů znázorníme každý prvek množiny jako bod. Z každého bodu vychází a do každého vchází právě po jedné šipce. Šipka vycházející z prvního prvku množiny ukazuje na první prvek permutace, šipka z druhého prvku množiny na druhý prvek permutace atd. Zápis se pak provádí tak, že každou kružnici zapíšeme po řadě zvlášť (např. $p = ((1,4,5,2,8)(3)(6,9,7))$ je zápis permutace (483529617).

Věta *(Faktoriál)*
Počet permutací na n-prvkové množině je $n \cdot (n-1) \cdot \dots \cdot 1$. Toto číslo pojmenujeme *faktoriál* n a značíme $n!$.

Definice *(Binomické koeficienty)*
Nechť $n \geq k$ jsou nezáporná celá čísla. *Binomický koeficient* neboli kombinační číslo $\binom{n}{k}$ (čteme n nad k) je funkce proměnných n, k, daná jako

$$\binom{n}{k} = \frac{n(n-1)(n-2)\dots(n-k+1)}{1 \cdot 2 \cdot \dots \cdot k} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}$$

nebo

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Definice
Nechť X je množina a k je nezáporné celé číslo. Pak $\binom{X}{k}$ budeme značit *množinu všech k-prvkových podmnožin* množiny X.

Věta
Pro každou konečnou množinu X je počet všech jejích k-prvkových podmnožin roven $\binom{|X|}{k}$.

Věta *(Vlastnosti kombinačních čísel)*
Platí:

$$\binom{n}{k} = \binom{n}{n-k}$$

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$$

Důkaz
První je zřejmé ze vzorce pro kombinační čísla, druhé se ukaže jednoduše pro použití komb. čísel – mějme množinu X a v ní prvek a. Kolik je podmnožin X obsahujících, resp. neobsahujících a?

Důsledek
Z druhé vlastnosti plyne vzhled *Pascalova trojúhelníku*, tedy že v $n+1$. řádku jsou vždy právě binomické koeficienty $\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{n}$.

Věta *(O počtu způsobů zápisu)*
Nezáporné celé číslo m lze zapsat jako součet r nezáporných sčítanců právě $\binom{m+r-1}{r-1}$ způsoby.

Důkaz
Důkazem je onen pokus s rozdělováním m kuliček mezi r přihrádek (nebo spíš vkládání přihrádek mezi kuličky v řadě).

Věta *(Binomická věta)*
Pro nezáporné celé číslo n a libovolná $x, y \in \mathbb{R}$ platí:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Věta *(Multinomická věta)*
Pro libovolná čísla $x_1, \ldots, x_m \in \mathbb{R}$ a $n \in \mathbb{N}_0$ platí:

$$(x_1 + \cdots + x_m)^n = \sum_{\substack{k_1+\cdots+k_m=n \\ k_1,\ldots,k_m \geq 0}} \binom{n}{k_1, \ldots, k_n} x_1^{k_1} x_2^{k_2} \cdot \cdots \cdot x_m^{k_m}$$

kde ta věc uprostřed v tom vzorci je *multinomický koeficient*, definovaný:

$$\binom{n}{k_1, \ldots, k_n} = \frac{n!}{k_1! k_2! \ldots k_n!}$$

16.4 Princip inkluze a exkluze

Věta *(Princip inkluze a exkluze)*
Pro každý soubor $A_1, A_2, \ldots, A_n$ konečných množin platí

$$\left| \bigcup_{i=1}^{m} A_i \right| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n\}}{k}} \left| \bigcap_{i \in I} A_i \right|$$

Důkaz
Nechť x je libovolný prvek $A_1 \cup A_2 \cup \cdots \cup A_n$. Kolikrát přispívá x vlevo a kolikrát vpravo?

Vlevo: jednou - triviální *Vpravo*: Nechť j ($1 \leq j \leq n$) označuje počet množin A_i, do kterých patří x. Můžeme množiny přejmenovat aby platilo $x \in A_1, A_2, \ldots, A_j$ a $x \notin A_{j+1}, \ldots, A_n$. Prvek se tedy objevuje v průniku každé k-tice množin $A_1, A_2, \ldots, A_j$ (a v žádných jiných). Protože existuje právě $\binom{j}{k}$ k-prvkových podmnožin j-prvkové množiny, bude se x objevovat v $\binom{j}{k}$ průnicích k-tic vybraných ze všech n prvků. Velikosti k-tic jsou přitom započteny se znaménkem $(-1)^{k-1}$, tudíž x na pravé straně přispívá veličinou

$$\begin{aligned} j - \binom{j}{2} + \binom{j}{3} - \cdots + (-1)^{j-1}\binom{j}{j} = \\ = 1 - \binom{j}{0} + \binom{j}{1} - \binom{j}{2} \cdots + (-1)^{j-1}\binom{j}{j} = \\ = 1 - \sum_{i=0}^{j} \binom{j}{i} (-1)^i = 1 - (1-1)^j = 1 \end{aligned}$$

□

16.5 Latinské čtverce a projektivní roviny

Definice *(Projektivní rovina)*

Konečná projektivní rovina je množinový systém (B, P), kde B je konečná množina a P je systém podmnožin množiny B, splňující:

1. $\forall p \neq p' \in P : |p \cap p'| = 1$
2. $\forall x \neq y \in B \; \exists p \in P : x, y \in p$
3. $\exists$ *4 body* $a, b, c, d \in B : \forall p \in P : |\{a, b, c, d\} \cap p| \leq 2$

Projektivní rovinu si lze představit jako množinu bodů B a množinu *přímek* P (jak se ostatně prvky těchto množin nazývají). Pak si lze podmínky představit takto:

1. Každé dvě přímky se protínají právě v jednom bodě.
2. Pro každé dva různé body x a y existuje přímka, která jimi prochází.
3. Existují čtyři body tak, že žádné 3 z nich neleží na jedné přímce (body v obecné poloze).

Věta

Buď (B, P) projektivní rovina. Potom všechny její přímky mají stejný počet bodů, tedy $\forall p, q \in P : |p| = |q|$

Definice

Řád projektivní roviny (B, P) je číslo $|p| - 1$, kde p je libovolná přímka z P $(p \in P)$.

Věta

Nechť (B, P) je projektivní rovina řádu n. Potom platí, že každým bodem prochází právě $n + 1$ přímek a $|B| = |P| = n^2 + n + 1$

Věta

Jestliže $n = p^2$, kde p je prvočíslo, pak existuje konečná projektivní rovina řádu n.

Definice *(Latinský čtverec)*

Latinský čtverec řádu n je matice $A \in \{1, \ldots, n\}^{n \times n}$, $\forall i, j \neq j' : A_{ij} \neq A_{ij'}$ a $A_{ji} \neq A_{j'i}$.

V podstatě se jedná o čtverec n krát n, kde v každém řádku i sloupci jsou vepsaná všechna čísla od 1 do n.

Definice

Mějme dva latinské čtverce A, B stejných rozměrů $n \times n$. Pak řekneme, že je *ortogonální* (značíme $A \bot B$), jestliže platí:

$$\forall a, b \in \{1, \ldots, n\} \; \exists i, j : A_{ij} = a, B_{ij} = b$$

Pokud tedy ty dva latinské čtverce „položíme přes sebe“, vznikne nám na každé pozici dvojice čísel od 1 do n s tím, že každá dvojice je unikátní.

Věta

Nechť M je množina latinských čtverců řádu n, z nichž každé dva jsou navzájem ortogonální. Potom $|M| \leq n-1$

Věta

Pro $n \geq 2$, projektivní rovina řádu n existuje právě tehdy, když existuje soubor $n-1$ vzájemně ortogonálních latinských čtverců řádu n.

Důkaz

1. *Implikace $\Leftarrow$:* Vezmu jednu – „vnější" – přímku projektivní roviny. Na ní leží $n+1$ bodů, které nazvu $A_0, \ldots, A_n$. Přímky jdoucí z krajních bodů A_0 a A_n tvoří mřížku (nazvu ji T) – protínají se v n^2 bodech.

   Potom každý z vnitřních bodů A_i ($1?i?n-1$) definuje lat. čtverec: každá přímka jdoucí z nějakého z vnitřních bodů A_i se s přímkami z A_0 a z A_n protne právě jednou a každé 2 přímky z A_i prochází mimo vnější přímku různými body. Každá přímka proch. každým řádkem i sloupcem mřížky T právě jednou $\Rightarrow$ dostávám latinský čtverec:

   $$(L^k)_{ij} = l \Leftrightarrow T_{ij} \in p_l^k$$

   kde L^k značí k-tý lat. čtverec, T_{ij} bod mřížky T na souřadnicích (i,j) a p_l^k l-tou přímku jdoucí z bodu A_k.

   Čtverce jsou ortogonální - sporem nechť pro mají dva čtverce (k-tý a k'-tý) na souřadnicích stejnou uspořádanou dvojici hodnot (a,b) na dvou různých místech. Pak by se přímky p_a^k a $p_b^{k'}$ protínaly ve 2 bodech.

2. *Implikace $\Rightarrow$:* Vytvořím přímku q s body $A_0, \ldots, A_n$ a mřížku T o $n \times n$ bodech. Do ní přidám přímky $p_{1,1}, \ldots, p_{n-1,n}$:

   $$p_l^k = \{A_k\} \cup \{T_{ij} | L_{ij}^k = l\}$$

   Pak je třeba ověřit axiomy projektivní roviny.

17 Teorie grafů

Požiadavky

- Základní pojmy teorie grafů, reprezentace grafu.
- Stromy a jejich základní vlastnosti, kostra grafu.
- Eulerovské a hamiltonovské grafy.
- Rovinné grafy, barvení grafů.

17.1 Základní pojmy teorie grafů, reprezentace grafu

Definice *(Graf)*
Graf G je uspořádaná dvojice (V, E), kde V je nějaká množina a E je množina dvouprvkových podmnožin množiny V (takže neuspořádaných dvojic). Prvky množiny V se jmenují **vrcholy grafu** G a prvky množiny E **hrany grafu** G.

Definice *(Orientovaný graf)*
G je dvojice (V, E), kde E je podmnožina kartézského součinu $V \times V$. Prvky E (tj. uspořádané dvojice prvků z V) nazýváme orientované hrany grafu.

Definice *(Symetrizace grafu)*
Orientovanému grafu $G = (V, E)$ přiřadíme neorientovaný graf $\mathrm{sym}(G) = (V, \bar{E})$ kde $\bar{E} = \{\{x, y\}; (x, y) \in E \vee (y, x) \in E\}$. Graf $\mathrm{sym}(G)$ se nazývá **symetrizace** grafu G. *(Z orientovaného grafu se odstraní údaje o směru hran.)*

Definice *(Důležité typy grafů)*

- **úplný graf** K_n: $V = \{1, \ldots, n\}, E = \binom{V}{2}$ *(Každý vrchol je spojen hranou s každým např. K_5 — „pentagram“.)*
- **kružnice** C_n: $V = \{1, \ldots, n\}, E = \{\{i, i+1\}; i = 1, \ldots, n-1\} \cup \{\{1, n\}\}$ *(V kružnici se nesmí opakovat vrcholy.)*
- **cesta** P_n: $V = \{0, 1, \ldots, n\}, E = \{\{i-1, i\}; i = 1, \ldots, n\}$ *(Jako kružnice, ale bez poslední hrany.)*
- **bipartitní graf:** $V = \{u_1, \ldots, u_n\} \cup \{v_1, \ldots, v_m\}$, $E \subseteq \{\{u_i, v_j\}; i = 1, \ldots, n, j = 1, \ldots, m\}$; v **úplném bipartitním grafu** je $E = \{\{u_i, v_j\}; i = 1, \ldots, n, j = 1, \ldots, m\}$ *(Každý vrchol z jedné partity je spojen hranou pouze s některými (v úplném z každým) vrcholem druhé partity. Např. $K_{3,3}$, úplný bipartitní graf na 3 a 3 vrcholech.)*

Definice *(Sled, tah)*
Pro graf $G = (V, E)$ definujeme **sled** jako posloupnost $(v_0, e_1, v_1, \ldots, e_n, v_n)$, kde $e_i = \{v_{i-1}, v_i\} \in E$ pro $i = 1, \ldots, n$. **Tah** je sled, ve kterém se žádná hrana neopakuje.

Definice *(Isomorfismus grafů)*

Dva grafy G, G' považujeme za **isomorfní** (značíme $G \simeq G'$), pokud se liší jen v označení vrcholů a hran, tj. pokud existuje vzájemně jednoznačné zobrazení $f : G \to G'$ tak, že platí $\{x, y\} \in E \Leftrightarrow \{f(x), f(y)\} \in E'$.

Definice *(Podgraf, indukovaný podgraf)*

Graf G je **podgrafem** grafu G', jestliže $V(G) \subseteq V(G')$ a $E(G) \subseteq E(G') \cap \binom{V(G)}{2}$. Pro **indukovaný podgraf** G grafu G' platí, že $V(G) \subseteq V(G')$ a $E(G) = E(G') \cap \binom{V(G)}{2}$. *(Indukovaný podgraf dostaneme vymazáním některých vrcholů původního grafu a všech hran tyto vrcholy obsahujících.)*

Definice *(Souvislost)*

Neorientovaný graf je **souvislý**, jestliže mezi každými jeho dvěma vrcholy v něm existuje cesta. Pro orientované grafy definujeme **slabou souvislost** — po symetrizaci se z něj stane souvislý neorientovaný graf — a **silnou souvislost** — každé dva vrcholy lze spojit orientovanou cestou v obou směrech.

Poznámka

Pro orientované grafy není samotný pojem „souvislost“ definován.

Definice *(n-souvislost)*

Graf je vrcholově **n-souvislý**, pokud má alespoň $n + 1$ vrcholů a po odebrání libovolných $n - 1$ vrcholů dostaneme vždy souvislý graf. Podobně (přes odebírání hran) definujeme **hranovou n-souvislost.**

Poznámka

Vrcholová n-souvislost je silnější podmínka než hranová n-souvislost, protože při odebírání $n-1$ vrcholů můžeme (a většinou musíme) odebrat více než $n-1$ hran.

Definice *(Komponenta souvislosti)*

Komponenta souvislosti grafu je jeho maximální souvislý podgraf. (Sjednocením všech komponent grafu dostaneme původní graf).

Definice *(Most)*

Most je hrana, která neleží ve 2-souvislém podgrafu (po jejím odstranění se zvětší počet komponent).

Definice *(Blok)*

Blok je maximální vrcholově 2-souvislý podgraf grafu. Samotný graf o 2 vrcholech spojených jednou hranou je také blok. *(2-souvislý podgraf, ke kterému se nedá přidat žádný vrchol, protože by přestal být 2-souvislý.)*

Definice *(Artikulace)*

Artikulace je vrchol v souvislého grafu G takový, že $G - v$ není souvislý.

Definice *(Blokový graf)*

je graf incidence (sousednosti) bloků a artikulací — artikulacím a blokům odpovídají vrcholy, hrany značí incidenci bloků a artikulací.

Věta

Blokový graf souvislého grafu je strom.

Definice *(Hranové pokrytí)*

Množinu $C \subseteq E$ v grafu $G = (V, E)$ nazveme **hranovým pokrytím,** pokud každý vrchol $v \in V$ je obsažen alespoň v jedné hraně $e \in C$.

Definice *(Stupeň vrcholu)*

Stupeň vrcholu, $\deg_G(v)$, je počet hran grafu G obsahujících vrchol v. V případě orientovaného grafu rozlišujeme **vstupní stupeň vrcholu,** $\deg^+_G(v)$, což je počet vstupních hran, podobně **výstupní stupeň vrcholu.**

Definice *(Párování)*

Každá množina vzájemně disjunktních hran v grafu se nazývá **párování**.

Definice *(k-faktor grafu)*

k-faktor je podgraf $G' = (V, E')$ grafu $G = (V, E)$ takový, že $(\forall v \in V) \deg_{G'}(v) = k$.

Poznámka *(1-faktor grafu)*

1-faktor je vlastně párování na všech vrcholech (úplné párování).

Věta *(Princip sudosti)*

$\sum_{v \in V} \deg_G(v) = 2|E(G)|$

Definice *(Skóre grafu)*

Skóre grafu je posloupnost stupňů vrcholů grafu, přičemž nezáleží na pořadí, v jakém jsou uváděny.

Věta *(Věta o skóre)*

Nechť $D = (d_1, \dots, d_n)$ je posloupnost přirozených čísel. Předpokládejme, že $d_1 \leq d_2 \leq \cdots \leq d_n$ a označme symbolem D' posloupnost $(d'_1, \dots, d'_{n-1})$, kde

$$d'_i = \begin{cases} d_i & \text{pro } i < n - d_n \\ d_i - 1 & \text{pro } i \geq n - d_n \end{cases}$$

Potom D je skóre grafu, právě když je D' skóre grafu. *(Jakoby odebereme poslední vrchol (V_n) a myslíme si, že byl propojen s předchozími d_n vrcholy.)*

Důkaz

Jedna implikace je triviální, druhá (máme D skóre grafu – a tedy k němu nějaký graf G a dokazujeme, že D' je taky skóre grafu G') není o moc těžší – „přepojíme“ hrany tak, aby z vrcholu v_n šly právě do $v_{n-d_n}, \dots v_{n-1}$ a v_n odebereme.

Definice *(Metrika grafu)*
Pro souvislý graf G definujeme **metriku** jako funkci $d_G : V \times V \to \mathbf{R}$, kde číslo $d_G(v, v')$ představuje délku nejkratší cesty z v do v'. Funkce d_G má následující vlastnosti (tj. splňuje axiomy metriky, jak ji známe z metrickýcj prostorů):

1. $d_G(v, v') \geq 0$, a $d_G(v, v') = 0 \Leftrightarrow v = v'$;
2. $(\forall v, v' \in V)(d_G(v, v') = d_G(v', v))$ *(symetrie)*
3. $(\forall v, v', v'' \in V)(d_G(v, v'') \leq d_G(v, v') + d_G(v', v''))$ *(trojúhelníková nerovnost)*

Definice *(Některé grafové operace)*
Nechť $G = (V, E)$ je graf. Definujeme

- **odebrání hrany:** $G - e = (V, E \setminus \{e\})$, kde $e \in E$ je hrana grafu G
- **přidání nové hrany:** $G + \bar{e} = (V, E \cup \{\bar{e}\})$, kde $\bar{e}$ je dvojice vrcholů, která není hranou v G
- **odebrání vrcholu:** $G - v = (V \setminus \{v\}, \{e \in E; v \notin e\})$, kde $v \in V$ (odebereme vrchol v a všechny hrany do něj zasahující)
- **dělení hrany:** $G\%e = (V \cup \{z\}, ((E \setminus \{\{x, y\}\}) \cup \{\{x, z\}, \{z, y\}\})$, kde $\{x, y\} \in E$ je hrana a $z \notin V$ je nový vrchol (na hranu $\{x, y\}$ „přikreslíme“ nový vrchol z).

Řekneme, že graf G' je **dělení** grafu G, pokud G' je isomorfní grafu vytvořenému z grafu G postupným opakováním operace dělení hrany.

17.2 Reprezentace grafu

Definice *(Nakreslení)*
Graf lze reprezentovat např. jeho nakreslením – lze si pod tím představit i grafické znázornění na papír. Formální definici nakreslení provedeme v sekci o rovinných grafech.

Definice *(Matice sousednosti)*
Mějme graf $G = (V, E)$ s n vrcholy $v_1, \ldots, v_n$. **Matice sousednosti** grafu G je čtvercová matice $A_G = (a_{ij})_{i,j=1}^n$ řádu n definovaná předpisem

$$a_{ij} = \begin{cases} 1 & \text{pro } \{v_i, v_j\} \in E \\ 0 & \text{jinak} \end{cases}$$

(Po umocnění matice sousednosti A^k představuje číslo $a_{ij}^{(k)}$ počet sledů délky k z vrcholu v_i do vrcholu v_j v grafu G.)

Definice *(Matice vzdáleností)*
Pro grafy s ohodnocenými hranami lze zkonstruovat **matici vzdáleností** — je to matice sousednosti, do které se v případě, že hrana existuje, ukládá místo jedničky její ohodnocení.

Definice *(Laplaceova matice)*

$$(L_G)_{uv} = \begin{cases} \deg u & u = v \\ -1 & \{u,v\} \in E \\ 0 & u \neq v \wedge \{u,v\} \notin E \end{cases}$$

(Na hlavní diagonále je stupeň vrcholu, kde vede hrana, tam je -1, jinde 0.)

Poznámka

Laplaceovu matici lze použít mj. k výpočtu počtu koster grafu, jak uvidíme v následující sekci.

Definice *(Matice incidence)*

Řádky matice odpovídají vrcholům, sloupce odpovídají hranám. Prvek matice se rovná -1, pokud v tomto vrcholu začíná daná hrana, $+1$ pokud tam tato hrana končí, 0 jinak. Neorientované grafy mají u obou vrcholů hrany hodnotu $+1$.

Definice *(Seznam sousedů)*

Pomocí dvou polí; v jednom čísla všech následníků, v druhém poli indexy určující, kde začíná sekvence sousedů daného vrcholu.

Definice *(Seznam hran)*

Pole s prvky o dvou složkách, zaznamenávají se do něj hrany ve formě obou jejich vrcholů; pro orientované grafy lze stanovit, že první složka bude reprezentovat počáteční a druhá koncový vrchol hrany.

17.3 Stromy a jejich základní vlastnosti

Definice *(Strom, list)*

Strom je souvislý graf neobsahující kružnici. **List** (koncový vrchol) je vrchol stupně 1.

Věta

Počet stromů na n-vrcholové množině je n^{n-2}.

Věta *(Charakterizace stromů)*

Pro graf $G = (V, E)$ jsou následující podmínky ekvivalentní:

1. G je strom.
2. Pro každé dva vrcholy $x, y \in V$ existuje právě jedna cesta z x do y. *(jednoznačnost cesty)*
3. Graf G je souvislý a vynecháním libovolné hrany vznikne nesouvislý graf. *(minimální souvislost)*
4. Graf G neobsahuje kružnici a každý graf vzniklý z G přidáním hrany již kružnici obsahuje. *(maximální graf bez kružnic)*
5. G je souvislý a $|V| = |E| + 1$.
6. G je acyklický a $|V| = |E| + 1$.

Definice *(Kostra grafu)*

Kostra grafu G je strom, který je podgrafem G a obsahuje všechny vrcholy grafu G.

Věta *(Počet koster)*

Počet koster grafu G je $\det(L'_G)$, kde L'_G je matice, která vznikne odstraněním i-tého řádku a i-tého sloupce z Laplaceovy matice charakterizující graf.

??? Dukaz

17.4 Eulerovské a hamiltonovské grafy

Definice *(Eulerovský graf)*

Graf $G = (V, E)$ se nazývá **eulerovský**, jestliže existuje takové pořadí všech hran $e_1, \ldots, e_n$, že $e_i \cap e_{i+1} \neq 0 \wedge e_1 \cap e_n \neq 0$, tedy každé dvě po sobě jdoucí hrany mají společný vrchol a rovněž první a poslední hrana se protínají, žádná hrana se neopakuje. Jinými slovy: graf je eulerovský, pokud v něm existuje uzavřený sled $(v_0, e_1, v_1, \ldots, e_{m-1}, v_{m-1}, e_m, v_0)$, v němž se každá hrana vyskytuje právě jednou. Takový tah nazýváme **uzavřeným eulerovským tahem.**

Věta *(Charakteristika eulerovského grafu)*

Graf $G = (V, E)$ je eulerovský právě tehdy, když je souvislý a každý vrchol G má sudý stupeň.

Důkaz

„$\Rightarrow$“: tato implikace je triviální — eulerovský graf musí být souvislý, do každého vrcholu musím vstoupit i z něj vystoupit, což zvýší stupeň vždy o 2.

„$\Leftarrow$“: Mějme tah maximální délky $v_0, e_1, \ldots, e_m, v_m$. První a poslední vrchol tahu jsou totožné, jinak by do prvního vrcholu vedl lichý počet hran, a jelikož graf má všechny stupně sudé, dal by se tah prodoužit. Vidíme, že každou hranou v grafu vede nějaký uzavřený tah (nejdelší tah hranou je uzavřený, protože jinak by šel z vrcholu ze sudým stupněm prodlužovat).

Náš maximální tah obsahuje všechny hrany a vrcholy, protože pokud ne, ze souvislosti jistě existuje vrchol, který je v max. tahu, z něhož vede hrana, která v max. tahu není. Tou vede uzavřený tah a pokud ho spojíme s naším maximálním tahem, dostaneme delší, což je spor.

Definice *(k-hamiltonovský graf)*

Graf je **k-hamiltonovský**, pokud existuje posloupnost všech vrcholů $v_1, \ldots, v_n$ taková, že $d_G(v_i, v_{i+1}) \leq k \wedge d_G(v_n, v_1) \leq k$. *(Do každého vrcholu smíme jen jednou.)* O grafu říkáme jednoduše, že je **hamiltonovský**, pokud je 1-hamiltonovský.

Definice *(Hamiltonovská kružnice)*

Hamiltonovská kružnice je kružnice procházející každým vrcholem grafu právě jednou. Graf má takovou kružnici, právě když je hamiltonovský. Její nalezení je NP-úplný problém.

Poznámka
Problém nalezení hamiltonovské kružnice se dá upřesnit na problém nalezení hamiltonovské kružnice s nejmenší vahou v ohodnoceném grafu, což je známý problém obchodního cestujícího. Je tedy také NP-úplný, ale existují algoritmy, jejichž řešení jsou blízká optimálnímu.

Věta *(Diracova)*
Graf $G = (V, E)$ je hamiltonovský, pokud platí:

$$\forall v \in V : \deg v \geq \frac{|V|}{2}$$

Důkaz
Dokážeme o něco silnější lemma pro jeden vrchol, z kterého Diracova věta plyne: pro dva vrcholy u, v v grafu G nespojené hranou platí, že pokud $\deg u + \deg v \geq |V|$, potom je graf G hamiltonovský, právě když G s přidanou hranou je hamiltonovský.

Jedna implikace je triviální, takže vezmeme tu druhou. Máme v grafu $G + \{u, v\}$ hamiltonovskou kružnici C. Pokud ta neobsahuje $\{u, v\}$ tak je i v grafu G a končíme, pokud tuto hranu obsahuje, označíme pro vrcholy grafu v pořadí, v jakém je prochází hamiltonovská kružnice $u = v_1, v_2, \ldots, v_n = v$:

$$A := \{i, \{u, v_i\} \in E\}$$
$$B := \{i + 1, \{v, v_i\} \in E\}$$

Pokud mají tyto množiny neprázdný průnik, nalezneme vrcholy v_k a v_{k+1}, přes které můžeme kružnici „přepojit“. A ani B neobsahují „1“, takže $|A \cup B| \leq n - 1$. Potom

$$|A \cap B| = |A| + |B| - |A \cup B| \geq |V| - |A \cup B| \geq 1$$

takže takový bod v_k existuje.

Věta
Každý souvislý graf je 3-hamiltonovský.

Důkaz
$G = (V, E)$ je souvislý, existuje v něm tedy kostra $T = (V, E')$, která je souvislá. Kostra vznikla ubráním některých hran, takže $d_T(x, y) \geq d_G(x, y) (\forall x, y \in V)$. Stačí tedy dokázat, že kostra T je 3-hamiltonovská.

Lemma
Každý strom je 3-hamiltonovský.

Důkaz
Indukcí:

1. pro $n \leq 4$ triviální
2. Máme dvě komponenty T_1, T_2, každá je 3-hamiltonovská. Graf je souvislý $\rightarrow$ existuje most z T_1 do T_2. Most vede přes vrcholy x', x, y, y', kde $x, x' \in T_1, y, y' \in T_2$. Potom existuje 3-hamiltonovské propojení komponent T_1, T_2 : $x, (T_1), x', y', (T_2), y$.

Věta
Graf je vrcholově 2-souvislý, právě když v něm mezi každými dvěma různými vrcholy existují dvě vrcholově disjunktní cesty.

Důkaz
Implikace $\Leftarrow$ je zřejmá, opačná se dá ukázat sporem – nechť ve dvousouvislém grafu mezi nějakými dvěma vrcholy neexistují dvě vrcholově disjunktní cesty. Pak vezmu vrchol, který je na každé cestě mezi těmito dvěma a odeberu ho – a tím se graf stane nesouvislým, což je spor.

Věta
Graf je vrcholově 2-souvislý, právě když jej lze vytvořit z trojúhelníku (t.j. z K_3) posloupností dělení a přidávání hran (definice těchto operací jsou na začátku kapitoly).

Věta
Každý 2-souvislý graf je 2-hamiltonovský.

Důkaz
??? Do každého vrcholu vedou 2 vrcholově i hranově disjunktní cesty — při zpáteční cestě použiju druhou. Důkaz podobně jako u věty o 3-hamiltonovských grafech.

17.5 Rovinné grafy

Definice *(Oblouk)*
Oblouk je podmnožina roviny tvaru $o = \gamma(\langle 0, 1\rangle) = \{\gamma(x); x \in \langle 0, 1\rangle\}$, kde $\gamma : \langle 0, 1\rangle \rightarrow \mathbb{R}^2$ je nějaké prosté spojité zobrazení intervalu $\langle 0, 1\rangle$ do roviny. Přitom body $\gamma(0)$ a $\gamma(1)$ nazýváme **koncové body** oblouku o.

Definice *(Nakreslení grafu)*
Nakreslením grafu $G = (V, E)$ rozumíme přiřazení, které každému vrcholu v grafu G přiřazuje bod $b(v)$ roviny a každé hraně $e = \{v, v'\}$ přiřazuje oblouk $o(e)$ v rovině s koncovými body $b(v)$ a $b(v')$. Zobrazení $b(v)$ je prosté (různým vrcholům odpovídají různé body) a žádný z bodů tvaru $b(v)$ není nekoncovým bodem žádného z oblouků $o(e)$. Graf spolu s nakreslením nazýváme **topologický graf.**

Definice *(Rovinný graf)*
Nakreslení grafu G, v němž oblouky odpovídající různým hranám mají společné nanejvýš koncové body, se nazývá **rovinné nakreslení**. Graf G je **rovinný,** má-li alespoň jedno rovinné nakreslení.

Definice *(Stěna grafu)*
Mějme G rovinný topologický graf. Množinu $A \subseteq \mathbb{R}^2 \setminus X$ bodů roviny (kde X je množina všech bodů všech oblouků nakreslení grafu G) nazveme **souvislou,** pokud pro libovolné dva body $x, y \in A$ existuje oblouk $o \subseteq A$ s koncovými body x, y. Relace souvislosti rozdělí množinu všech bodů roviny, které neleží v žádném z oblouků nakreslení, na třídy ekvivalence. Ty nazýváme **stěnami** topologického rovinného nakreslení grafu G.

Definice *(Topologická kružnice)*
Uzavřená křivka v rovině neprotínající sebe sama; formálně se definuje jako oblouk, jehož koncové body splývají.

Věta *(Jordanova, o kružnici)*
Každá topologická kružnice k rozděluje rovinu na právě dvě souvislé části („vnitřek“ a „vnějšek“), přičemž k je jejich společnou hranicí.

Věta *(Kuratowského)*
Graf G je rovinný, právě když žádný jeho podgraf není isomorfní dělení grafu $K_{3,3}$ ani K_5.

Věta *(Eulerův vzorec)*
Nechť $G = (V, E)$ je souvislý rovinný graf, a nechť s je počet stěn nějakého rovinného nakreslení G. Potom platí $|V| - |E| + s = 2$.

Důkaz
Indukcí podle počtu hran. Pro graf sestávající pouze z jednoho vrcholu vzorec platí.

1. Pokud přidaná hrana nevytvoří kružnici, nezměnil se počet stěn, ale o jednu se zvětšil počet vrcholů a hran (graf musí být vždy souvislý, takže jediná možnost jak tohoto dosáhnout, je připojit další vrchol).
2. Pokud přidaná hrana vytvoří kružnici, zvětší se počet stěn o jednu (přidaná hrana sousedí se dvěma různými stěnami — podle Jordanovy věty o kružnici — které před přidáním byly stěnou jedinou), počet hran také o jednu, a počet vrcholů se nezmění.

Vzorec tedy v obou případech platí.

Věta *(2-souvislý rovinný graf)*
Dvousouvislý rovinný graf má hranice libovolné stěny libovolného nakreslení jako kružnice.

Věta *(Maximální počet hran rovinného grafu)*
Nechť G je rovinný graf s alespoň 3 vrcholy. Potom $|E| \leq 3|V|-6$. Rovnost nastává pro každý maximální rovinný graf, t.j. rovinný graf, ke kterému nelze již přidat žádnou hranu (při zachování množiny vrcholů) tak, aby zůstal rovinný. Pokud graf G navíc neobsahuje trojúhelník (t.j. K_3 jako podgraf) a má-li alespoň 3 vrcholy, potom $|E| \leq 2|V| - 4$.

Důkaz
Obě tvrzení můžeme dokázat pro maximální rovinný graf. V prvním případě je určitě dvousouvislý, protože jinak můžu ještě nějaké dva body spojit. Navíc každá stěna musí být trojúhelník (je-li čtverec nebo něco většího, také jdou ještě nějaké dva body spojit). Tím dostanu, že $3s = 2|E|$ a zbytek vyjde z Eulerova vzorce.

Druhý případ má jednu zvláštnost – takový graf může být hvězda. Pro tu je ale tvrzení splněno. Pokud není hvězda, už musí být dvousouvislý a všechny stěny musí být čtverce, takže dostanu $4s = 2|E|$ a z Eulerova vzorce i celý výsledek.

Důsledek
Rovinný graf má alespoň jeden vrchol stupně nejvýše 5.

17.6 Barvení grafu

Definice *(Neorientovaný graf s násobnými hranami (multigraf))*
je trojice (V, E, ε), kde V a E jsou disjunktní množiny a $\varepsilon : E \to \binom{V}{2} \cup V$ je zobrazení *(hrany prohlásíme za „abstraktní“ objekty a ε určuje pro každou hranu dvojici vrcholů, které jsou jejími „konci“).*

Poznámka
Pro orientovaný graf je pojem definován obdobně, pouze hrany jsou přiřazeny uspořádané dvojici vrcholů, tedy: $\varepsilon : E \to \langle v_1, v_2 \rangle \cup V$.

Definice *(Geometrický duál grafu)*
Nechť G je topologický rovinný graf. Označme S množinu stěn G. Jako **(geometrický) duál grafu** definujeme multigraf tvaru (S, E, ε), kde ε se definuje předpisem $\varepsilon(e) = \{S_i, S_j\}$, jestliže hrana e je společnou hranicí stěn S_i a S_j (přičemž může být $S_i = S_j$, jestliže z obou stran hrany e je tatáž stěna). Značíme jej G^*. *(Sice opravdu platí $G^{**} = G$, ale pak již pro spočítání druhého duálu potřebujeme znát duál i pro multigrafy!)*

Úloha ***(barvení mapy)***
Uvažme politickou mapu, na níž jsou vyznačeny hranice států. Předpokládejme, že každý stát tvoří souvislou oblast ohraničenou nějakou topologickou kružnicí. Dvě oblasti pokládáme za sousední, jesliže mají společný aspoň kousek hranice. Každý stát na takové mapě chceme vybarvit nějakou barvou tak, že sousední státy nikdy nebudou mít stejnou barvu. Jaký minimální počet barev je potřeba?

Definice *(Barevnost grafu)*
Buď $G = (V, E)$ graf, k přirozené číslo. Zobrazení $b : V \to \{1, \ldots, k\}$ nazveme **obarvením grafu** G pomocí k barev, pokud pro každou hranu $\{x, y\} \in E$ platí $b(x) \neq b(y)$. **Barevnost (chromatické číslo) grafu** G, označovaná $\chi(G)$, je minimální počet barev potřebný k obarvení G.

Lemma
Duální graf rovinného grafu je rovinný graf.

Převod úlohy barvení mapy na úlohu hledání barevnosti grafu
Máme-li mapu, kterou chápeme jako nakreslení nějakého grafu G, potom otázka obarvitelnosti mapy pomocí k barev je ekvivalentní s obarvitelností duálního grafu G^* pomocí k barev. Na druhé straně platí, že každý rovinný graf se vyskytne jako podgraf duálního grafu nějakého vhodného grafu. Takto lze převést problém barvení map na problémy barevnosti rovinných grafů.

Věta *(Věta o pěti barvách)*
Pro každý rovinný graf G platí $\chi(G) \leq 5$.

Důkaz
Indukcí dle počtu vrcholů grafu. Pro $|V| \leq 5$ je tvrzení triviální. Podle důsledku věty o počtu hran v rovinném grafu existuje vrchol stupně ≤ 5. Pokud má vrchol v stupeň < 5, použijeme indukční předpoklad: obarvíme graf $G - v$ 5 barvami a v přiřadíme barvu, která není mezi barvami jeho (nejvýše čtyř) sousedů. Zbývá tedy případ, kdy má v stupeň 5 a jeho sousedi jsou obarveni různými barvami. Graf G má pevně zvolené rovinné nakreslení a v tomto nakreslení budou t, u, x, z, y sousedé vrcholu v v takovém pořadí, v jakém příslušné hrany vycházejí z vrcholu v (např. po směru hodinových ručiček). Uvažme vrcholy x a y a nechť $V_{x,y}$ je množina všech vrcholů grafu $G' = G - v$ obarvených barvami $b(x)$ nebo $b(y)$. Zřejmě $x, y \in V_{x,y}$.

Nastávají dva případy:

1. Neexistuje cesta z x do y používající pouze vrcholů z $V_{x,y}$. Mějme $V'_{x,y}$ množinu vrcholů, které jsou v G' spojeny s x cestou používající jen vrcholy z $V_{x,y}$. Definujeme nové obarvení b' takto: $b'(s) = b(s)$, pokud $s \notin V'_{x,y}$; a pokud $s \in V'_{x,y}$, změníme barvu s z $b(y)$ na $b(x)$ nebo z $b(x)$ na $b(y)$ (tzn. na množině $V_{x,y}$ zaměníme barvy). Zřejmě b' je obarvení, a protože $b'(x) = b'(y) = b(y)$, můžeme položit $b'(v) = b(x)$. Tedy b' je obarvení grafu G 5 barvami.
2. Pokud taková cesta existuje (označme ji P), uvažme vrcholy t a z. Zřejmě $V_{x,y}$ a $V_{t,z}$ jsou disjunktní množiny. Cesta P spolu s hranami $\{v, x\}$ a $\{v, y\}$ tvoří kružnici, která odděluje t a z, a proto by každá cesta z t do z musela použít některý vrchol této kružnice. Neexistuje tedy cesta z t do z používající pouze vrcholů z $V_{t,z}$ a obarvení grafu G 5 barvami lze zkonstruovat stejně jako v předchozím případě, pouze musíme začít s vrcholy z a t.

Věta *(Problém čtyř barev)*
Je možné každou mapu obarvit 4 barvami?

Důkaz
Věta platí, ale je velmi těžké ji dokázat (probírání mnoha případů počítačem).

Poznámka
NP-úplné problémy: je dán neorientovaný graf G a číslo k.

1. Je možné G obarvit k barvami?
2. Totéž, ale předem víme, že k=3.
3. Totéž, ale graf je rovinný.
4. Totéž, ale stupeň libovolného vrcholu je nejvýše 4.
5. Je dáno obarvení třemi barvami, dotaz na netriviálně jiné.

17.7 Základní grafové algoritmy

Tato sekce není požadovaná ke zkoušce!

(Nebo teda je požadovaná, ale v informatice, kde je vypracovaná zvlášť)

V tomto oddíle zavedeme pro odhady časových složitostí algoritmů značení $n = |V(G)|$ a $m = |E(G)|$.

Algoritmus *(Dijkstrův algoritmus pro hledání nejkratší cesty)*
Máme graf G, jehož hrany jsou ohodnoceny kladnými čísly, tzn. že je dáno zobrazení $w : E(G) \to (0, \infty)$. (Ohodnocení $w(e)$ hrany e si představujeme jako její délku. Délka cesty je rovna součtu délek jejích hran a vzdálenost $d_{G,w}(u, v)$ vrcholů u, v je rovna nejmenší z délek všech cest spojujících u, v. „Obyčejná“ grafová vzdálenost je speciální případ, totiž je-li $w(e) = 1$ pro každou hranu e.) Hledáme nejkratší cestu z vrcholu s do všech ostatních vrcholů.

1. (Inicializace)
   „Odhad“ vzdálenosti $d(\cdot)$ u počátečního vrcholu s nastavíme na 0, odhady u všech ostatních vrcholů na ∞ (známe cestu délky 0 z s do s, délky ostatních cest neznáme). Do množiny A vrcholů, u nichž ještě není odhad definitivní, dáme všechny vrcholy kromě s.
2. (Volba množiny N)
   Do množiny N právě zpracovávaných vrcholů uložíme všechny vrcholy z A, které mají ze všech vrcholů z A minimální odhad vzdálenosti; tyto vrcholy z A vyřadíme.
3. (Aktualizace odhadů)
   Pro každou hranu $e = \{v, y\} \in E$, kde $v \in N, y \in A$, porovnáme hodnoty $d(y)$ a $d(v) + w(v, y)$. Pokud $d(v) + w(v, y) < d(y)$ (přes vrchol v vede do y kratší cesta, než jsme zatím znali), nastavíme $d(y)$ na tuto hodnotu. Po vyčerpání všech takových hran pokračujeme dalším krokem.

4. (Test ukončení)
   Jestliže odhady vzdáleností všech vrcholů v množině A jsou ∞, algoritmus končí, jinak pokračuje krokem 2.

Po skončení algoritmu je buď $A = 0$ (je-li G souvislý) nebo A obsahuje pouze vrcholy nedosažitelné cestou z vrcholu s.

??? Algoritmus jsem opravil, i když je to vcelku zbytečné … kdyžtak to někdo zkontrolujte.

Věta *(Složitost Dijkstrova algoritmu)*
Lze ho implementovat v čase $O(n \log n + m)$ — např. pomocí Fibonacciho hald.

Poznámka
Pokud hledáme nejkratší cestu pouze do jednoho zadaného vrcholu c, můžeme ukončit Dijkstrův algoritmus hned poté, co tento vrchol opustí množinu A (jeho vzdálenost se stane definitivní). Výpočet také můžeme urychlit následující heuristikou: máme funkci $h : V(G) \to \langle 0, \infty)$ splňující $h(c) = 0$ a pro každou hranu $e = \{u, v\} \in E$ platí $|h(u) - h(v)| \leq w(e)$ (v problémech dopravního spojení to může být např. vzdálenost vzdušnou čarou od cíle). Potom při volbě množiny N vybíráme prvky s minimálním součtem dosavadního odhadu a heuristické funkce — $d(v) + h(v)$. Je-li h kvalitní, dá se čekat, že algoritmus najde definitivní vzdálenost do c rychleji.

Algoritmus *(Prohledávání do šířky)*
Máme graf $G = (V, E)$ a počáteční vrchol s. Na začátku položíme $V_0 = \{s\}$, v dalších krocích položíme $V_{i+1} = \{v \in V \setminus (V_0 \cup \dots \cup V_i) : \exists u \in V_i, \{u, v\} \in E\}$. Složitost algoritmu je $O(n + m)$.

Algoritmus *(Prohledávání do hloubky)*
??? Poměrně jasné, často vede k exponenciální složitosti. Nutno rozlišovat metodu zpracování prvků — **preorder, inorder** nebo **postorder.**

Algoritmus *(Hladový (Kruskalův) algoritmus na hledání minimální kostry)*
Mějme souvislý graf $G = (V, E)$ s ohodnocením hran w. Hrany máme uspořádány vzestupně podle váhy, $w(e_1) \leq \dots \leq w(e_n)$.

1. Položme $E_0 = 0$
2. Z množiny E_{i-1} spočítáme množinu E_i následovně:

$$E_i = \begin{cases} E_{i-1} \cup \{e_i\} & \text{neobsahuje-li graf } (V, E_{i-1} \cup \{e_i\}) \text{ kružnici} \\ E_{i-1} & \text{jinak} \end{cases}$$

Algoritmus se zastaví, pokud E_i má $n - 1$ hran. Poslední množina E_i jsou hrany minimální kostry grafu G.

Věta *(Složitost Kruskalova algoritmu)*

Při implementaci potřebujeme v podstatě vyřešit úlohu udržování ekvivalence (UNION-FIND): máme množinu vrcholů, na počátku je rozdělena do jednoprvkových tříd ekvivalence. Navrhněte datové struktury a algoritmus, který efektivně vykonává dvě operace:

1. Sjednocení tříd (UNION): učinit dva vrcholy ekvivalentními t.j. nahradit třídy je obsahující jejich sjednocením.
2. Testování ekvivalence (FIND): Pro dané dva vrcholy rozhodnout, zda jsou momentálně ekvivalentní.

V průběhu algoritmu hledání minimální kostry vykonáme $n-1$ operací UNION — jednu při každém přidání hrany, a m operací FIND — při každém testování, zda přidávaná hrana nevytvoří kružnici. *(pozn.: Vrcholy této hrany musí ležet v různých komponentách.)*

Řešení: vrcholy mají přiřazenu značku určující třídu ekvivalence, do které patří; a pro každou třídu ekvivalence existuje seznam jejích vrcholů. Testování ekvivalence je pak porovnání dvou značek o složitosti $O(1)$ a při sjednocení tříd musím přeznačit a přemístit vrcholy jedné ze tříd, což zabere $O(n)$ času. Pokud přeznačujeme vždy menší třídu, vyjde odhad potřebného času $O(n \log n + m)$.

Algoritmus *(Jarníkův (Primův) algoritmus na hledání minimální kostry grafu)*

Je dán souvislý graf $G = (V, E)$. Budeme postupně vytvářet množiny $V_0, V_1, \dots \subseteq V$ vrcholů a $E_0, E_1, \dots \subseteq$ hran, přičemž $E_0 = 0$ a $V_0 = \{v\}$, kde v je libovolně zvolený vrchol. V i-tém kroku algoritmu vybereme z množiny hran $\{\{x, y\} \in E(G); x \in V_{i-1} \wedge y \in V \setminus V_{i-1}\}$ tu s minimálním ohodnocením (bude to $e_i = \{x_i, y_i\}$) a položíme $V_i = V_{i-1} \cup \{y_i\}$ a $E_i = E_{i-1} \cup \{e_i\}$. Pokud žádná taková hrana neexistuje, algoritmus končí, to nastane v $(n-1)$-ním kroku a E_{n-1} je množina hran minimální kostry grafu. *(Kostru tedy začínám budovat od jediného vrcholu a v každém kroku k ní přidám nejkratší z hran mezi vrcholy kostry a zbytkem vrcholů.)*

Poznámka

Jarníkův algoritmus lze implementovat v čase $O((n + m) \log n)$.

Algoritmus *(Topologické třídění)*

Problém: V orientovaném grafu $G = (V, E)$ sestrojte prosté zobrazení $f : V \to \{1 \dots |V(G)|\}$ tak, aby $\forall (v_1, v_2) \in E; f(v_1) < f(v_2)$. *(Tedy máme očíslovat vrcholy prvními přirozenými čísly tak, aby hrany vedly jen z vrcholu s nižším číslem do vrcholu s vyšším číslem.)*

Algoritmus: Nejprve nastavíme čítač na 1. Nalezneme vrchol, do kterého nevede žádná hrana; tento vrchol očíslujeme čítačem a odtrhneme ho od grafu (sestrojíme indukovaný podrgraf) a zvýšíme čítač. Tento krok opakujeme, dokud množina vrcholů grafu není prázdná. Pokud nemůžeme v nějakém kroku nalézt bod, do kterého nevede žádná hrana, nelze graf topologicky setřídit.

Využití: Odpovídají-li vrcholy grafu jednotlivým krokům nějakého postupu a hrany časovým závislostem, které je třeba zachovat, odpovídá topologické setřídění tohoto grafu (jednomu z) pořadí, ve kterém je nutné kroky vykonávat.